University of Groningen Press

Edited by Jonida Milaj

Legal challenges in Data Driven Innovation



Legal challenges in Data Driven Innovation

LEGAL CHALLENGES IN DATA DRIVEN INNOVATION

EDITED BY JONIDA MILAJ

University of Groningen Press
Groningen



Legal challenges in Data Driven Innovation Copyright © 2026 by The Authors is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License, except where otherwise noted.

CONTENTS

Introduction 1

Part I. Data and Innovation

Chapter 1: The Reality of the GDPR's Deterrent Effect 7
Carmen Pennanen

Chapter 2: GDPR: Innovating the Right to Be Forgotten with Blockchain 22
Cristian Costin

Chapter 3: Schrödinger's Data: Rethinking the Binary Distinction Between Personal and Non- Personal Data in the Age of Synthetic Information. 40
Vilma Margarit

Chapter 4: Data Ownership, Consent, and User Privacy in the World of Video Games 56
Willem Drapers

Chapter 5: Automated Vehicles and the lawfulness of data processing under Art. 6 GDPR 86
Maximilian Kloth

Chapter 6: Sailing into Monopoly: How Data Accumulation by Autonomous Ships Violates Competition Law 104
Inés López Abad

Part II. AI and Data

Chapter 7: Porter's Hypothesis: Reframing the Effects of the GDPR on AI Innovation 123
Karabo Lerato Mokoena
Chapter 8: Anonymisation as a Tool for Data Protection for AI Model Training 145
Marina El Moufti
Chapter 9: The Use of Automated Deception Detection for Law Enforcement in the EU: Regulatory and Technical Assessment under the AI Act 160
Natálie Binderová
Chapter 10: The Legal and Ethical Challenges Posed by AI-Assisted Police Reports in the Criminal Procedure 179
Konstantina Kelesidi

Part III. Data Spaces and Global Challenges

Chapter 11: Consent as a Catalyst? The GDPR, the DGA, and the Role of Data Altruism Organizations in Fostering European Innovation 199
Paulina Anna Ryszkowska
Chapter 12: The European Health Data Space and Medical AI Devices 216
Mariam Ibraham
Chapter 13: Patents, Data Privacy, and Innovation within the European Health Data Space 231
Darina Pitkevica
Chapter 14: AI, Competition, and Geopolitics: Europe's Need for Digital Independence 250
Luke Crofton Arbuthnot
Chapter 15: Tracing Flight Lines Between Times: A Minimal Insight Into the Contemporary Reality of Data Colonialism in Latin America 280
Eduardo Aguirre Mercado

The world in which we live, is experiencing an unparalleled increase in digital technologies. Data is at the core of the current digital innovation. It is estimated that global data generation will triple between 2025 and 2029. The reasons behind this worldwide growth in data are varied, but undeniably they include the increased use of digital technologies in all areas of life.

While the volume of available data is important, in terms of innovation, availability coped with the knowledge on how to use the data is the key to success. Data analysts, information technology engineers and the likes focus on gathering, linking, interpreting, using data, creating algorithms and code in order to address specific problems and create new digital solutions. The role of lawyers in this framework is not of less importance. Lawyers need to ensure that all of these data driven activities comply with the applicable legal framework and that all the safeguards are in place for the protection of fundamental rights.

The 2nd Data Driven Innovation workshop, organized in March 2025 at the University of Groningen by the Security, Technology and e-Privacy research group (STeP) together with the students of the LLM program in Technology Law and Innovation, focused on the current legal challenges in Data Driven Innovation.

This edited volume takes stock of current legal debates and presents a number of selected chapters that reflect upon core legal problems of Data Driven Innovation. The chapters are presented in three main parts.

Part one focuses on general legal challenges created by Data Driven Innovation.

In her chapter, Carmen Pennanen, discusses shortcomings and deterrence challenges in the enforcement of The General Data Protection Regulation (GDPR). She provides clear suggestions to overcome enforcement deficiencies for the law to fulfil its purpose and function.

Cristian Costin focuses on the challenges that the use of blockchain technology creates for the right to be forgotten. For the author, the solution is not to reject technology, but rather to innovate – both legally and technically – so that the imperatives of data protection can coexist with the benefits of decentralization.

For Vilma Margarit, synthetic data challenges the binary distinction between personal and non-personal data. She efficiently uses the thought provoking Schrödinger's experiment for illustrating her concerns.

Willem Drappers focuses in his chapter on issues related to personal data and privacy in the world of videogames, especially when service providers are engaged in more than one line of business. In his analysis, he argues that the principle of purpose limitation should be relied upon for creating clearly defined borders and not allow for repurposing of data for targeted advertising outside of the industry.

Both Maximilian Kloth and Inés López Abad focus their attention on autonomous transportation means and the data that those modes of transport collect and use. While Maximilian analyses the legal bases for collecting and processing data in autonomous cars, Inés analyses the effects that data accumulation in autonomous ships has for the proper application and effectiveness of Competition law.

Part two focuses on the use of data for the development of AI technology.

Karabo Lerato Mokoena engages in the 'Regulation v. Innovation' debate. She discusses thought provoking questions and calls for a critical reflection on: 'What kind of innovation do we want?'

In her chapter, Marina El Moufti focuses on the anonymization of personal data for training AI models. She acknowledges current limitations of anonymization and offers recommendations to manage re-identification risks.

Natálie Binderová discusses AI technology used for law enforcement purposes. She assesses from a regulatory and technical perspective the use of automated deception detection tools and their legal qualification under the AI act. Current shortcomings with regards to the accuracy, robustness and cybersecurity of these tools are identified.

The legal and ethical challenges posed by AI-assisted law enforcement reports are discussed in the chapter of Konstantina Kelesidi. She argues that the use of AI tools by law enforcement creates challenges for the protection of the rights to fair trial and the presumption of innocence.

Data spaces and global challenges created by data driven innovation are at the core of the chapters included in the third part of the book.

In her chapter, Paulina Anna Ryszkowska analyses the role of data altruism organizations in fostering innovation. She concludes that these organizations have little to no added value to fostering scientific research and innovation in the EU due to significant legal and administrative burdens that outweigh any potential benefits.

Mariam Ibrahim discusses the European Health Data Space (EHDS). While she recognizes the merits of the new regulation, she argues that it falls short of comprehensively addressing all critical risks associated with AI in healthcare, as for example: algorithmic bias, data shifts, the misuse of AI tools in clinical workflows, as well as the lack of transparency and explainability in medical AI tools.

The European Health Data Space is also analyzed by Darina Pitkevica. Her focus is both on data and innovation as well as on Intellectual property issues. She argues that the EHDS cannot succeed by technology or legislation alone. Its legitimacy depends on how it distributes access, how it shares benefits, and

how it respects the autonomy of the individuals whose data it seeks to mobilize.

Focusing on global challenges, Luke Crofton Arbuthnot analyses Europe's need for digital independence. He argues that for achieving digital sovereignty a cohesive EU-wide strategy, ensuring alignment between regulatory frameworks, industrial policy, and digital infrastructure development, is essential.

The last chapter of this edited volume turns the attention to sustainability issues of AI data centers and especially on the creation of some forms of data colonialism in the Global South. In his chapter, Eduardo Aguirre Mercado argues that any Data Driven Innovation debate must combine the protection of data subjects' rights with the current issues that historically press the Global South.

Putting together this volume was encouraged by the students of the LLM program in Technology Law and Innovation. The volume has a dual aim. On one side it recognizes that the students' dedication, enthusiasm, debates, critical thinking and hard work were not only a source of energy and inspiration during class but has resulted in good quality work that is worth to be shared with the world. On the other side, it aims to share current debates and challenges in Data Driven Innovation and to inspire other researchers and students in the Technology law domain to research legal challenges of Data Driven Innovation and to contribute for the protection of fundamental rights and legally compliant Innovation.

Jonida Milaj*

Groningen, March 2026

* Jonida Milaj is Associate Professor in Technology Law and Human Rights at the University of Groningen, The Netherlands.

PART I. DATA AND INNOVATION

CHAPTER 1: THE REALITY OF THE GDPR'S DETERRENT EFFECT

Carmen Pennanen

1. Introduction

European Union (EU) data protection standards are only as effective as their enforcement. Without proper compliance and strong oversight, they risk becoming empty promises. With the introduction of the General Data Protection Regulation (GDPR), Europeans were given the ability to report privacy violations to national data protection authorities, which are empowered to investigate breaches and issue fines to prevent future violations. Coming into effect in May 2018,[1] the GDPR was designed to strengthen data protection across the EU by enforcing stricter regulations and imposing substantial fines for non-compliance.

Aiming to safeguard individuals' fundamental rights, particularly their right to data protection,[2] while ensuring the free movement of personal data within the EU,[3] the GDPR addresses the challenges posed by rapidly advancing digital technologies. Recognising that private companies leverage personal data on an unprecedented scale,[4] the regulation sought to enhance corporate responsibility and strengthen regulatory enforcement to build public trust in the

1. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, art 99(2).

2. Ibid, art 1(2).

3. Ibid, art 1(1), 1(3).

4. Ibid, rec 6.

digital economy.[5] However, despite its ambitious goals, the practical implementation of the GDPR has often fallen short, with enforcement lagging behind the regulation's political commitments.

Central to effective enforcement is the role of sanctions. The GDPR enforcement system is built around administrative sanctions, with data protection authorities (DPAs) in each EU member state having the primary responsibility to investigate violations and impose penalties.[6] For serious breaches, Article 83(4) of the GDPR provides that fines can be as high as €20 million or 4% of a company's global annual turnover from the previous year, whichever is higher. For less severe violations, the maximum fine is €10 million or 2% of the turnover.[7] At the EU level, the European Data Protection Board (EDPB) helps ensure uniform application of the GDPR by resolving disputes between national DPAs, issuing guidance, and interpreting key GDPR provisions.[8]

One of the many objectives of sanctions is to deter future infringements.[9] Rather than solely punishing a party for a violation, the sanctions serve as a warning, discouraging potential lawbreakers by threatening consequences.[10] Moreover, a sanction imposed on an offender may have a preventive effect, discouraging both repeat offences by the violator and similar offences by others.[11] By making the consequences of non-compliance clear, sanctions can

5. Ibid, rec 7.

6. Heli Korkka-Knuts, Eelis Paukku, Jaakko Markus, 'Reassessing Deterrence: The Effectiveness of Administrative Sanctions across three EU Regulatory Frameworks' (2025) Helsinki Legal Studies Research Paper No. 90 <https://dx.doi.org/10.2139/ssrn.5169603> accessed 20 March 2025.

7. GDPR (n 1), art 83(4).

8. Korkka-Knuts, Paukku, Markus (n 6).

9. W. Gregory Voss, Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2021) 37/1 Santa Clara High Tech, p. 23 <https://ssrn.com/abstract=3695473> accessed 20 March 2025.

10. Ibid.

11. Ibid.

serve as a strong deterrent, encouraging individuals to follow the law rather than risk punishment.[12] However, despite these mechanisms, there remains a significant gap between the GDPR's intended deterrent effect and its actual impact on compliance—a gap this essay aims to explore by analysing the key factors behind the inconsistency.

This essay proceeds in three main steps. First, it outlines the economic theory of sanctions and deterrence to provide a conceptual framework for assessing whether the GDPR can achieve its intended deterrent effect. Second, it examines empirical evidence on compliance behaviour, drawing primarily on survey data collected by the European Center for Digital Rights (noyb). Third, it compares these theoretical expectations with the reality of enforcement practices across EU member states, drawing on official GDPR enforcement statistics to evaluate whether GDPR sanctions have functioned as an effective deterrent.

Methodologically, the essay adopts a Law and Economics approach, combining doctrinal analysis of rational choice and deterrence theory with empirical evidence from surveys and GDPR enforcement databases. This approach enables a critical assessment of the extent to which the GDPR's sanctioning regime translates into real-world compliance.

2. Economic Theory of Sanctions and Deterrence

To better understand how sanctions achieve deterrence, it is useful to turn to economic theory, which offers a structured framework for evaluating how individuals respond to incentives and risks.

The economic theory of crime, originating from Gary Becker's work and building on the earlier insights of Jeremy Bentham, outlines the conditions under which a sanction can effectively deter misconduct.[13] This theory is grounded in rational choice theory, which assumes that individuals are rational actors who weigh the potential costs and benefits of their actions.[14] Applied to

12. Ibid.

13. Gary S Becker, 'Crime and punishment: An economic approach' (1968) 76/2 Journal of Political Economy <https://www.jstor.org/stable/1830482> accessed 20 March 2025.

14. Thomas S Ulen, '0710 Rational Choice Theory in Law and Economics' (2000) 790.

crime, the rational choice theory suggests that a potential offender evaluates the expected benefits of committing an offence against the expected costs,[15] such as the risk of detection and punishment. A crime is committed only if the perceived benefits outweigh the expected costs. Therefore, a sanction will serve as a deterrent if the anticipated penalty, considering the likelihood of enforcement, is greater than the potential gain from the offence.[16]

The deterrent effect depends not only on the severity of the sanction but also on the probability of detection and enforcement.[17] The higher the expected cost of non-compliance (calculated as the sanction multiplied by the probability of enforcement), the less attractive the violation becomes.[18] Consequently, sanctions must be both severe and consistently enforced to maintain their deterrent effect. Without credible and consistent enforcement, even the harshest penalties lose their deterrent power, as offenders may perceive the risk of punishment as negligible.

Ideally, the mere threat of a sanction should be sufficient to prevent misconduct, but if violations go unpunished or are lightly sanctioned, the credibility of the threat weakens.[19] The deterrent effect diminishes when actors observe that non-compliance, even serious violations, has no consequences. Furthermore, individuals often underestimate the likelihood of enforcement,[20] a cognitive bias that undermines deterrence unless sanctions are imposed consistently and visibly. To ensure long-term deterrence, enforcement must be not only possible but visibly executed, reaffirming the real risk of punishment and reinforcing compliance.[21]

---

15. Becker (n 13) 176.

16. Voss, Bouthinon-Dumas (n 9) 40-41.

17. Becker (n 13) 176.

18. Ibid 177.

19. Voss, Bouthinon-Dumas (n 9) 42.

20. Ibid.

21. Daniel S Nagin, 'Deterrence in the Twenty-First Century' (2013) 42/1 Crime and Justice

3. Factors Influencing Organisational Compliance Decisions

In order to link compliance behaviour with deterrence theory, this essay draws on data from a questionnaire conducted by the noyb. The survey, which targeted over 1,000 data protection professionals, including data protection officers (DPOs) and members of internal compliance departments at large companies, aimed to uncover the most significant internal and external factors influencing compliance.[22] These professionals are deeply involved in the decision-making processes of data controllers and processors, making their insights crucial for understanding the dynamics at play.

One key finding from the survey is that 74.4% of respondents believe that if a DPA 'would walk through the door of an average company tomorrow, it would surely find relevant GDPR violations'.[23] This statistic reveals a significant gap between organisations' awareness of GDPR requirements and their actual compliance. It suggests that many businesses either fail to fully implement necessary data protection measures or operate within a culture of partial compliance, where privacy obligations are not given sufficient priority.[24] From the standpoint of deterrence theory, this data indicates that the threat of enforcement actions and fines may not be acting as an effective deterrent. It appears that organisations either underestimate the likelihood of inspection or accept the risk of minor violations, weakening the deterrent effect that the GDPR enforcement mechanism is designed to have.

Further complicating the issue, DPOs face significant challenges in convincing decision-makers to implement necessary changes for GDPR compliance.

---

in America 1975–2025 199, 201 <https://doi.org/10.1086/670398> accessed 22 March 2025.

22. noyb, 'GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts' <https://noyb.eu/sites/default/files/2024-01/GDPR_a culture of non-compliance.pdf> accessed 20 March 2025.

23. Ibid 2.

24. Ibid.

The survey highlights that 56% of respondents reported difficulties in achieving higher compliance in departments such as sales and marketing, where short-term business goals often take precedence over long-term regulatory compliance.[25] The data also shows that 38.5% of DPOs struggle to convince senior management of the importance of compliance, and 32.3% report pressure from senior management to reduce compliance efforts.[26] This resistance weakens the deterrent effect of potential enforcement actions, as it suggests that the threat of fines and penalties is not being taken seriously at higher organisational levels. From a deterrence perspective, this indicates that the risk of penalties may not be perceived as immediate or severe enough to drive full organisational compliance.

The data shows the critical role that financial penalties, and particularly high fines, play in motivating organisations to align with data protection standards. 63.5% of respondents identified fear of fines as the primary driver of compliance,[27] suggesting that the threat of substantial financial repercussions exerts a strong deterrent effect. This is further supported by the fact that 61.5% agree high fines have a powerful impact on organisational behaviour,[28] reinforcing the argument that meaningful enforcement, through significant penalties, is essential to shaping compliance decisions. Moreover, the deterrent effect is not limited to organisations that have been fined themselves, as 51.6% of DPOs reported that observing fines imposed on other companies influences their own organisation's compliance efforts as well.[29] This spillover effect indicates that enforcement actions create industry-wide caution, extending the impact of deterrence beyond just the organisations directly involved. Additionally, reputational harm emerged as a complementary motivator, with respondents

25. noyb (n 22) 11.

26. Ibid 2.

27. Ibid 3.

28. Ibid.

29. Ibid.

acknowledging that public exposure of GDPR violations also drives compliance.[30]

However, the data also reveals a critical limitation to this spillover effect, as deterrence seems to remain largely national, even many years after the GDPR's adoption.[31] Despite its goal of creating a harmonised data protection framework across the EU, privacy professionals reported that significant differences persist in how the regulation is interpreted, applied, and enforced among EU member states.[32] This fragmentation undermines the GDPR's broader deterrent effect, as organisations tend to focus on and be influenced by enforcement actions within their own jurisdictions. Indeed, only 23.0% and 22.8% of respondents consider decisions from foreign DPAs or courts influential, compared to 48.5% and 45.7% for national decisions.[33] While the Court of Justice of the European Union (CJEU) exerts some influence (43.4%),[34] it still falls short of national enforcement bodies in shaping compliance behaviour.

From a deterrence theory perspective, these findings suggest that the lack of consistent enforcement and interpretation weakens the GDPR's effectiveness in ensuring compliance across the EU. If organisations view the regulation as fragmented or unevenly applied, they may be less likely to be deterred by penalties in other jurisdictions, potentially undermining the broader goals of GDPR to create a harmonised data protection framework across Europe. To enhance the deterrence effect, there may need to be better alignment in enforcement practices across the EU and a more unified approach to GDPR interpretation.

The fragmentation in GDPR enforcement and the predominance of national deterrence effects have led to a crucial development in organisational behaviour: rather than aiming for full compliance, many companies have shifted to

30. Ibid.

31. Ibid.

32. Ibid.

33. Ibid.

34. noyb (n 22) 3.

a 'risk-based approach'.[35] This method of compliance, shaped by strategic cost-benefit analyses, reflects a calculated response to perceived enforcement gaps and highlights the limits of GDPR's deterrent power.

4. The Risk-Based Approach to GDPR Compliance

Privacy professionals' written responses to the noyb questionnaire provide insight into the organisations' shift in strategy. Instead of full compliance, they tend to adopt a 'risk-based approach', whereby compliance efforts are adjusted in proportion to the perceived likelihood of enforcement and the severity of potential sanctions.[36] In cases where the probability of enforcement appears unlikely, and where the anticipated possible consequences, such as fines or reputational damage, are considered to be minimal, some businesses may deliberately choose not to fully comply with all of their legal obligations under the Regulation.

Such conduct aligns with the rational choice theory, as actors seek to maximise benefits and minimise costs through strategic decision-making.[37] When applied to GDPR compliance, this theory explains why, in the face of low perceived enforcement risk, organisations might prioritise short-term economic gains over regulatory compliance. Without a credible threat of detection or punishment, the incentive to invest and allocate resources to comprehensive data protection measures is minimised.

From a deterrence theory perspective, these findings highlight the essential role of effective enforcement in influencing organisational behaviour in terms of regulatory compliance. To disrupt the current trend of cost-benefit calculation, which is driving risk-based compliance, both the perceived probability of enforcement and the severity of penalties must be significantly increased. This

35. Ibid 21.

36. Ibid 21-22.

37. Jan Trzaskowski, 'Persuasion, manipulation, choice architecture and 'dark patterns'' in Andrej Savin and Jan Trzaskowski (eds) *Research Handbook on EU Internet Law* (Edward Elgar Publishing, 2023) 309 <https://doi.org/10.4337/9781803920887> accessed 4 May 2025.

aligns with Article 83(1) of the GDPR, under which the imposition of fines must be effective, proportionate, and dissuasive.[38] If enforcement bodies can raise the anticipated cost of non-compliance, organisations will have a greater incentive to allocate resources toward full compliance.

Ultimately, strengthening enforcement is not only about punishment. It is necessary to uphold the rule of law, guarantee legal certainty, and ensure that data subjects' rights are effectively protected across the EU. Without such measures, the GDPR risks becoming a framework that is more aspirational than operational, with compliance being driven by perceived risk rather than a legal obligation.

5. The Reality of GDPR Enforcement

Given that the effectiveness of GDPR sanctions in deterring non-compliance largely depends on consistent and strong enforcement, it is essential to examine whether supervisory authorities across the EU are actively engaged in carrying out their responsibility. This involves evaluating the authorities' practical enforcement actions, including their frequency and severity. As highlighted in the noyb questionnaire, many organisations adopt a risk-based approach to GDPR compliance, strategically weighing the likelihood of enforcement against the costs of compliance.[39] This approach is predicated on a perception that enforcement is inconsistent and that the probability of detection is low. To evaluate whether this perception accurately reflects reality, it is necessary to examine concrete data on fines, complaints, and breach notifications within the EU. A closer analysis of actual enforcement patterns can reveal whether the current enforcement landscape supports or undermines GDPR's intended deterrent effect and whether the observed gap between theoretical compliance incentives and real-world organisational behaviour can be explained by shortcomings in practical enforcement.

While GDPR fines have steadily increased in both number and monetary

38. GDPR (n 1), art 83(1).

39. noyb (n 22) 21-22.

value since the regulation entered into force in 2018,[40] this upward trend in financial penalties can give a misleading impression of strong enforcement. At face value, the sharp rise in fines, which reached particularly high totals of 2,295 fines and an overall sum of €5,643,223,783 by the start of 2025,[41] may suggest that the GDPR is being strictly enforced. However, a closer look at the enforcement patterns reveals a concentration of fines in a small number of high-profile cases, rather than a broad and consistent application of the law across the board.

Ireland and Luxembourg, in particular, distinguish themselves by the exceptionally high monetary value of the fines they have imposed under the GDPR. As of early 2025, Ireland has issued fines totalling approximately €3.5 billion, while Luxembourg follows with over €746 million.[42] However, these headline figures hide the reality that most enforcement in these jurisdictions is largely concentrated on a few tech giants, including Apple, Google, Meta, Microsoft, and Amazon, due to the location of their European headquarters. For example, in Luxembourg, virtually the entire total fine amount stems from a single €746 million fine against Amazon.[43] Similarly, in Ireland, five fines alone account for over €2.65 billion,[44] which amounts to more than 75% of all fines issued by the Irish Data Protection Commission (DPC). This pattern of isolated, high-value fines against well-known companies creates an illusion of strong enforcement, while the vast majority of violations seem to receive little attention or minimal penalties.

This uneven enforcement points to a broader systemic issue. While large fines imposed on a limited number of major companies often attract public

40. 'Fines Statistics: Chronological Statistics' (*GDPR Enforcement Tracker*, February 2025) <https://www.enforcementtracker.com/?insights> accessed 20 March 2025.

41. Ibid.

42. 'Fines Statistics: Highest Fines by Country' (*GDPR Enforcement Tracker*, February 2025) <https://www.enforcementtracker.com/?insights> accessed 20 March 2025.

43. 'Fines Statistics: Highest individual fines (Top 10)' (*GDPR Enforcement Tracker*, February 2025) <https://www.enforcementtracker.com/?insights> accessed 20 March 2025.

44. Ibid.

attention and suggest that the GDPR's deterrent effect is functioning, they do not indicate a healthy, comprehensive enforcement regime. Instead, these symbolic fines seem to hide certain underlying challenges, such as potential resource constraints within supervisory authorities, regulatory delays, and a general lack of enforcement. Regardless, effective deterrence requires more than occasional large fines. It demands consistent oversight, timely regulatory action, and equal accountability for all data controllers and processors, not just the most visible entities.

The case of the Netherlands illustrates the concerning gap between the number of data protection complaints and breach notifications, and the limited enforcement actions taken in response. Between 2021 and 2024, the Dutch DPA received tens of thousands of complaints and data breach notifications each year, yet issued relatively few fines. In 2021, it received 18,914 complaints and 24,866 data breach reports but issued only 11 fines.[45] In 2022, there were over 13,000 complaints and more than 21,000 breaches, resulting in 13 fines.[46] In 2023, reported breaches rose to over 25,000, but just 8 fines were imposed.[47] In 2024, despite 37,839 reported breaches, the DPA issued only 6 fines.[48] This clear contrast between the high volume of potential GDPR violations and the relatively low number of fines imposed highlights significant shortcomings in enforcement capacity and effectiveness. It raises broader concerns about whether DPAs can adequately uphold data protection standards, despite widespread non-compliance.

It must be emphasised that enforcement plays a critical role because, as revealed by the noyb questionnaire, fines have been identified as the most

45. AP Annual Report 2023 (*Autoriteit Persoonsgegevens*, 1 July 2024) p. 29 <https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2023> accessed 20 March 2025.

46. Ibid.

47. Ibid.

48. AP Annual Report 2024 (*Autoriteit Persoonsgegevens*, 20 March 2025) p. 27, 29 <https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2024> accessed 21 March 2025.

influential factor in driving compliance.[49] If fines are seen as rare or symbolic rather than routine and inevitable, their deterrent effect is weakened. A system that depends mostly on occasional, high-profile penalties without widespread and consistent enforcement risks undermining public trust and reducing the overall effectiveness of data protection law.

This disparity between the volume of violations and the limited enforcement highlights a critical flaw in the GDPR's implementation. While the regulation has a strong framework in theory, its effectiveness depends on consistent and visible enforcement in practice. The evidence from various member states reveals a pattern where only a small fraction of breaches and complaints result in tangible consequences, thereby diminishing the regulation's deterrent power. In this context, the perception among organisations that the probability of being caught or penalised is low makes perfect sense, as it reflects the reality of enforcement as it currently stands. These systemic enforcement gaps allow many organisations to weigh the low risk of sanctions against the cost of compliance and choose the former.

6. Conclusion

The GDPR was established to safeguard personal data across the EU by threatening substantial fines, with the aim of creating a credible deterrent against non-compliance. However, the regulation's practical enforcement has revealed significant shortcomings that undermine its theoretical strength. Despite its potential to impose severe financial penalties, enforcement across member states has been inconsistent, fragmented, and disproportionately focused on a small number of high-profile cases involving large tech companies.

This uneven enforcement landscape has led many organisations to adopt a calculated, risk-based approach to GDPR compliance.[50] Instead of striving for full compliance with data protection obligations, businesses often weigh the perceived low risk of detection and penalties against the cost of imple-

49. noyb (n 22) 3.

50. Ibid 21-22.

menting comprehensive compliance measures.[51] As shown through both economic deterrence theory and empirical data, the effectiveness of any sanction depends not only on its severity but also on the perceived likelihood of enforcement. In the case of GDPR, a lack of widespread, consistent enforcement reduces the expected cost of non-compliance, thereby weakening its deterrent power.

Moreover, the fragmentation in enforcement across EU member states diminishes GDPR's intended harmonising effect.[52] Organisations tend to focus on the actions of their national data protection authorities rather than EU-wide enforcement trends,[53] further weakening the regulation's ability to influence organisational behaviour across borders. This national focus, combined with visible enforcement gaps, contributes to a credibility gap between GDPR's legal obligations and its practical impact.

For the GDPR to fulfil its purpose and function as more than a symbolic framework, the EU must address these enforcement deficiencies. This requires investing in the capacity of data protection authorities, harmonising enforcement practices, and ensuring that sanctions are applied visibly and consistently across all member states. Without such improvements, GDPR enforcement risks continue to be inconsistent, enabling organisations to view compliance as a strategic risk instead of a legal obligation. Ultimately, strong and uniform enforcement is not only essential for deterring non-compliance but also for upholding the fundamental rights the GDPR was designed to protect.

Bibliography

AP Annual Report 2023 (*Autoriteit Persoonsgegevens*, 1 July 2024) <https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2023> accessed 20 March 2025

AP Annual Report 2024 (*Autoriteit Persoonsgegevens*, 20 March 2025)

51. Trzaskowski (n 37), 309.

52. noyb (n 22) 3.

53. Ibid.

<https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2024> accessed 21 March 2025

Becker, 'Crime and punishment: An economic approach' (1968) 76/2 Journal of Political Economy <https://www.jstor.org/stable/1830482> accessed 20 March 2025

'Fines Statistics' (*GDPR Enforcement Tracker*, February 2025) <https://www.enforcementtracker.com/?insights> accessed 20 March 2025

Korkka-Knuts, Paukku, Markus, 'Reassessing Deterrence: The Effectiveness of Administrative Sanctions across three EU Regulatory Frameworks' (2025) *Helsinki Legal Studies Research Paper* No. 90 <https://dx.doi.org/10.2139/ssrn.5169603> accessed 20 March 2025

Nagin, 'Deterrence in the Twenty-First Century' (2013) 42/1 Crime and Justice in America 1975–2025 199 <https://doi.org/10.1086/670398> accessed 22 March 2025

noyb, 'GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts' <https://noyb.eu/sites/default/files/2024-01/GDPR_a culture of non-compliance.pdf> accessed 20 March 2025

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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

Trzaskowski, 'Persuasion, manipulation, choice architecture and 'dark patterns'' in Andrej Savin and Jan Trzaskowski (eds) *Research Handbook on EU Internet Law* (Edward Elgar Publishing, 2023) <https://doi.org/10.4337/9781803920887> accessed 4 May 2025.

Ulen, '0710 Rational Choice Theory in Law and Economics' (2000)

Voss, Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2021) 37/1 Santa Clara High Tech <https://ssrn.com/abstract=3695473> accessed 20 March 2025

About the author

Carmen Pennanen

Carmen Pennanen completed the LLM in Technology Law and Innovation at the

University of Groningen. She is currently undertaking an Associate Traineeship at Geradin Partners, a pan-European law firm specialising in competition law, litigation, and digital regulation.

CHAPTER 2: GDPR: INNOVATING THE RIGHT TO BE FORGOTTEN WITH BLOCKCHAIN

Cristian Costin

1. Introduction

Blockchain technology has rapidly emerged as a disruptive force in many sectors, offering an immutable, decentralised ledger that promises enhanced security, transparency, and trust. Yet this very immutability—which is the technology's greatest strength—poses a fundamental challenge when considered against one of the European Union's cornerstone data protection rights: the Right to Be Forgotten under the General Data Protection Regulation (GDPR).[1]

At the heart of this regulatory framework lies Article 17 of the GDPR, which enshrines the right of individuals to obtain the erasure of their personal data in certain circumstances.[2] However, blockchain's design—as an append-only, tamper-resistant ledger—means that once data is recorded, it is practically impossible to remove it.[3] This inherent conflict between the technology's immutability and the right to erasure presents a vexing question: how can we innovate to reconcile these two imperatives?

1. Jure Globocnik, 'The Right to Be Forgotten Is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' (2020) 69 GRUR International 380.

2. 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) [2016] OJ L119/1, art 17

3. Rahime Belen-Saglam and others, 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems' (2023) 4 Blockchain: Research and Applications 2,4

This article critically examines the tension between blockchain's immutable design and the GDPR's Right to Be Forgotten. It begins by outlining the legal framework underpinning the right to erasure under the GDPR and its interpretative guidance. Next, it discusses seminal EU case law – notably *Google Spain* and *GC and Others v CNIL* – that has shaped the contours of this right.[4];[5] The analysis then turns to the legal and technical challenges that blockchain presents, including issues of data replication, the identification of data controllers, and the feasibility of actual erasure in a decentralised network. Finally, the article proposes a series of innovative solutions—ranging from off-chain storage and encryption techniques to the use of chameleon hash functions and regulatory adaptations—that could enable blockchain to comply with the GDPR without undermining its core features.

2. Article 17 of the GDPR

Article 17 of the GDPR codifies the right of individuals to request the deletion of their personal data under specified conditions.[6] This right applies when the personal data are no longer necessary for the purposes for which they were collected or processed, when consent is withdrawn and no other legal basis for processing exists, and when the data were processed unlawfully.[7] Additionally,

4. Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317 (13 May 2014)

5. Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773 (24 September 2019)

6. 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) [2016] OJ L119/1, art 17

7. 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) [2016] OJ L119/1, art 17

the article provides exceptions, notably where the retention of data is required for exercising the right of freedom of expression and information, for compliance with a legal obligation, or for the establishment, exercise or defence of legal claims.[8]

The GDPR does not impose an absolute obligation to delete personal data. Rather, it requires data controllers to weigh the interests of the data subject against public interest and other competing rights. This balancing act is central to the operation of the right to erasure, reflecting a nuanced understanding that data protection must be balanced against freedoms such as expression and information.

2.1. The Tension with Blockchain's Immutability

While Article 17 envisions a world where data can be actively managed and erased when necessary, blockchain technology challenges this vision by its very nature.[9] The design of blockchain is such that data, once recorded, is distributed among numerous nodes and cryptographically sealed in an immutable ledger.[10] This creates an apparent irreconcilable tension: on one hand, the GDPR requires data to be erasable upon a valid request; on the other, blockchain's architecture does not allow for deletion or modification of recorded data.

This inherent conflict has led some commentators to describe the relation-

8. 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) [2016] OJ L119/1, art 17(3)

9. 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) [2016] OJ L119/1, art 17

10. Rahime Belen-Saglam and others, 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems' (2023) 4 Blockchain: Research and Applications 2,4

ship between blockchain and the GDPR as one of 'unstoppable force versus immovable object.'[11] For regulators and legal practitioners alike, the question then becomes: can the rigid, decentralised nature of blockchain be reconciled with a right that demands flexibility and reversibility? The answer, as this article argues, lies in innovative interpretations of the law and in technical adaptations that seek to render personal data effectively 'forgotten' without altering the immutable nature of the ledger itself.

3. EU Case Law on the Right to Be Forgotten

3.1. Google Spain (C-131/12)

In the landmark case of *Google Spain* (C-131/12), the CJEU recognised for the first time that search engine operators, as data controllers, have responsibilities under data protection law.[12] The case arose from a Spanish national's request to have certain search results linking to an old newspaper article about his financial difficulties removed from Google's search results.[13] The decision set forth that individuals could request the removal of links to personal data that were 'inadequate, irrelevant or no longer relevant,' thus establishing the basis for the Right to Be Forgotten in EU law.[14]

11. B Shoaib, 'The Immutable Blockchain Confronts the Unstoppable GDPR' (2023) 14(1) *Seattle Journal of Technology, Environmental & Innovation Law* art 5 https://digitalcommons.law.seattleu.edu/sjteil/vol14/iss1/5/

12. **Case C-131/12** *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317 (13 May 2014) para 83.

13. **Case C-131/12** *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317 (13 May 2014) para 20.

14. **Case C-131/12** *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317 (13 May 2014) para 92-94.

3.2. GC and Others v CNIL (C-136/17)

In this case, the CJEU dealt with de-referencing requests concerning sensitive personal data, such as criminal records and health information.[15] The Court underscored that search engines must carry out a careful balancing test when assessing de-referencing requests, weighing the data subject's right to privacy against the public's right to access information. [16] The ruling reinforced the view that, even in the case of sensitive data, the right to erasure is not absolute and must be considered alongside other fundamental rights, notably freedom of expression and information.[17]

This decision is significant because it illustrates the CJEU's commitment to protecting individual privacy while also safeguarding public interest. By insisting on a case-by-case analysis, the Court recognised the complexity of data protection in the digital age, where the same piece of information can have divergent implications depending on context.

3.3. Implications for Blockchain

The jurisprudence established by *Google Spain* and *GC and Others v CNIL* serves as a foundation for the debate on blockchain and the Right to Be Forgotten. The decisions confirm that data controllers must, where feasible, respect data subjects' rights by removing or de-referencing personal data that is no longer justified by public interest.[18] However, the cases were decided in contexts where controllers have clear decision-making power – such as search engines that can be compelled to adjust their algorithms. In blockchain, the absence of

15. **Case C-136/17** *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773 (24 September 2019)

16. **Case C-136/17** *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773 (24 September 2019) para 22-31.

17. **Case C-136/17** *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773 (24 September 2019) para 62.

18. See previous paragraphs.

a centralised controller complicates matters significantly.[19] The decentralised, immutable nature of blockchain means that the typical mechanisms of deletion or de-referencing do not easily apply.[20] Thus, while EU case law supports the principle of the right to erasure, its application to blockchain technology remains a novel and challenging frontier that requires innovative legal and technical solutions.

4. Legal and Technical Challenges

4.1. Immutability and the Inability to Delete

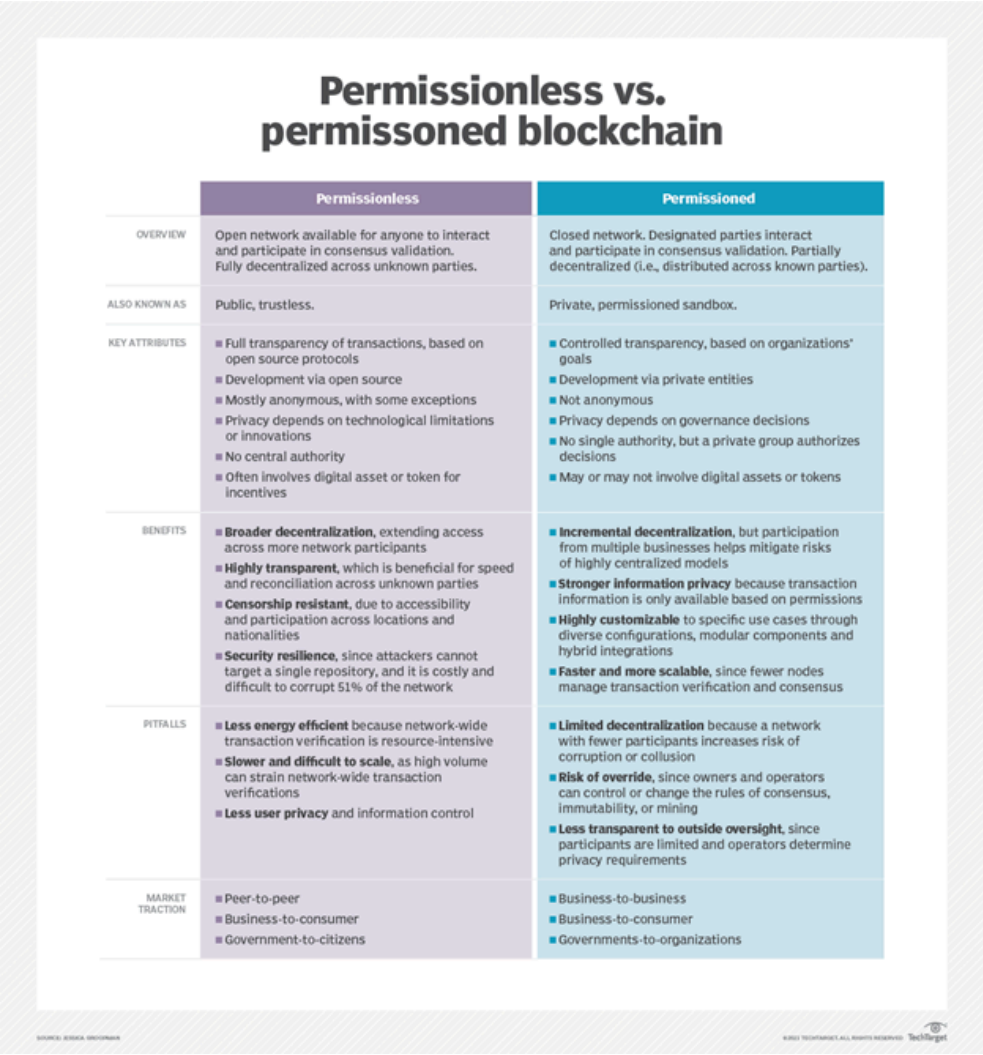
As previously discussed, the inherent immutability of data on the blockchain poses significant challenges in the absence of a centralised controller. In public blockchains, every participating node holds a complete copy of the ledger, and no central authority exists to enforce deletion.[21] Even in permissioned blockchains, where governance may be more centralised, altering historical records can undermine the trust model upon which the technology is built.[22] Consequently, a data subject's request for deletion becomes technically unachievable if personal data is stored on a public blockchain.

19. Rahime Belen-Saglam and others, 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems' (2023) 4 Blockchain: Research and Applications

20. Ammar Zafar, 'Reconciling Blockchain Technology and Data Protection Laws: Regulatory Challenges, Technical Solutions, and Practical Pathways' (2025) 11

21. Gautami Tripathi, Mohd Abdul Ahad and Gabriella Casalino, 'A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges' (2023) 9.

22. This comes as a consequence of not decentralizing. The whole concept of blockchain is to remain fully independent and transparent to the public and to the authorities.



Permissionless vs. permissoned blockchain

	Permissionless	Permissioned
OVERVIEW	Open network available for anyone to interact and participate in consensus validation. Fully decentralized across unknown parties.	Closed network. Designated parties interact and participate in consensus validation. Partially decentralized (i.e., distributed across known parties).
ALSO KNOWN AS	Public, trustless.	Private, permissioned sandbox.
KEY ATTRIBUTES	▪ Full transparency of transactions, based on open source protocols ▪ Development via open source ▪ Mostly anonymous, with some exceptions ▪ Privacy depends on technological limitations or innovations ▪ No central authority ▪ Often involves digital asset or token for incentives	▪ Controlled transparency, based on organizations' goals ▪ Development via private entities ▪ Not anonymous ▪ Privacy depends on governance decisions ▪ No single authority, but a private group authorizes decisions ▪ May or may not involve digital assets or tokens
BENEFITS	▪ **Broader decentralization**, extending access across more network participants ▪ **Highly transparent**, which is beneficial for speed and reconciliation across unknown parties ▪ **Censorship resistant**, due to accessibility and participation across locations and nationalities ▪ **Security resilience**, since attackers cannot target a single repository, and it is costly and difficult to corrupt 51% of the network	▪ **Incremental decentralization**, but participation from multiple businesses helps mitigate risks of highly centralized models ▪ **Stronger information privacy** because transaction information is only available based on permissions ▪ **Highly customizable** to specific use cases through diverse configurations, modular components and hybrid integrations ▪ **Faster and more scalable**, since fewer nodes manage transaction verification and consensus
PITFALLS	▪ **Less energy efficient** because network-wide transaction verification is resource-intensive ▪ **Slower and difficult to scale**, as high volume can strain network-wide transaction verifications ▪ **Less user privacy** and information control	▪ **Limited decentralization** because a network with fewer participants increases risk of corruption or collusion ▪ **Risk of override**, since owners and operators can control or change the rules of consensus, immutability, or mining ▪ **Less transparent to outside oversight**, since participants are limited and operators determine privacy requirements
MARKET TRACTION	▪ Peer-to-peer ▪ Business-to-consumer ▪ Government-to-citizens	▪ Business-to-business ▪ Business-to-consumer ▪ Governments-to-organizations

Figure 1.0[23]

23. 'Permissioned vs. Permissionless Blockchains: Key Differences | TechTarget' (*Search CIO*) <https://www.techtarget.com/searchcio/tip/Permissioned-vs-permissionless-blockchains-Key-differences> accessed 28 March 2025.

4.2. Determining What Constitutes Personal Data

Another challenge is determining what data in a blockchain setup actually counts as 'personal data' under the GDPR. In many blockchain applications, there are two types of data: (1) **transactional data**, which might include details of a transaction or record (and could be personal, depending on context), and (2) **public keys (addresses)** used to pseudonymously represent participants.[24] At first glance, one might assume that if only hashes or encrypted data are on-chain, perhaps that avoids GDPR issues. However, EU regulators have taken a cautious view: hashed data can still be personal data if it can be linked back to an individual with additional information, and public keys are often considered personal data if they correspond to a single user.[25]

4.3. Identifying the Data Controller

Blockchains often involve the replication of data across nodes in multiple jurisdictions.[26] An erasure request under GDPR typically obliges a controller to not only delete data in its possession but also to inform any third parties with whom the data was shared to also erase it.[27] In a blockchain, every node that has a full copy of the ledger is effectively a recipient of the personal data. As

---

24. Rahime Belen-Saglam and others, 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems' (2023) 4 Blockchain: Research and Applications 6

25. 'Anonymising Personal Data "Not Enough to Protect Privacy", Shows New Study | Imperial News | Imperial College London' (*Imperial News*, 23 July 2019) <https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/> accessed 28 March 2025.

26. See Figure 1.1 below.

27. 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) [2016] OJ L119/1, art 17(2)

noted, informing them to 'erase' the data is futile if the system doesn't support deletion.[28]

Moreover, many nodes may reside outside the EU, raising questions of jurisdiction and enforcement.[29] EU law can reach controllers and processors abroad if processing is related to offering goods/services to EU individuals or monitoring their behaviour which could apply to some blockchain activities, but enforcement in a decentralised network is uncharted territory.[30] The result is a *de facto* irreversibility of personal data on public blockchains: once it enters, it propagates beyond easy reach of EU regulators.

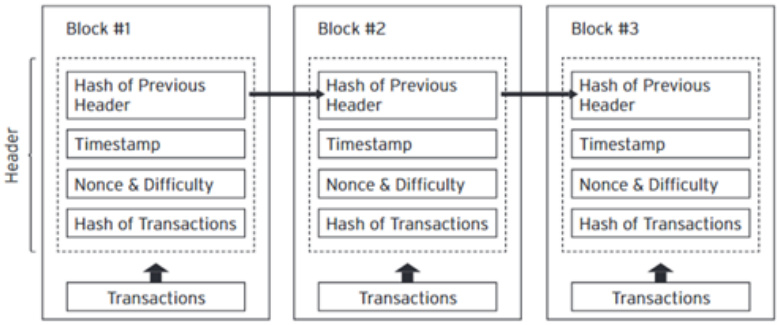


FIGURE 1.1 Simplified Bitcoin blockchain

Figure 1.1[31]

28. It is increasingly evident, that a public blockchain is unfeasible for the right to be forgotten.

29. See Figure 1.1 below.

30. 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) [2016] OJ L119/1, art 3(2)

31. Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 23 <https://www.jstor.org/stable/j.ctv2867sp> accessed 28 March 2025.

4.4. Technical Limitations and Workarounds

Beyond the legal issues, technical challenges also abound. For instance, even if data controllers attempted to 'delete' data by rendering it inaccessible (for example, by deleting decryption keys), the original encrypted or hashed data remains on the blockchain. While such measures might satisfy the spirit of the GDPR by making the data non-processable, they do not constitute literal deletion.[32] Moreover, these techniques are subject to the risk that future advances in cryptanalysis or changes in key management protocols could render the data accessible once more. Therefore, any technical workaround must be robust, verifiable, and designed to offer long-term protection against re-identification.

In summary, the immutable nature of blockchain, the difficulty of isolating personal data from non-personal data, the challenges in pinpointing data controllers, and the global replication of data all combine to create a landscape in which the practical application of the Right to Be Forgotten is severely constrained.

5. Proposals and Solutions for Reconciling Blockchain with the Right to Be Forgotten

5.1. Off-Chain Storage and Hash Pointers

One of the most promising approaches is to ensure that personal data is not stored on the blockchain itself but rather maintained off-chain in traditional databases, with the blockchain storing only cryptographic hashes or pointers to that data.[33] By doing so, the blockchain serves as an audit trail or proof of integrity, while the actual personal data – which is subject to deletion under Article 17 – can be modified or erased from the off-chain storage when

32. Since the hashed data remains on the blockchain, with enough outside parameters, there is a risk of getting reidenfitied, even if the data is encrypted or anonymised.

33. Mongetro Goint, Cyrille Bertelle and Claude Duvallet, 'Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems' (2023) 11 Mathematics 1592.

required. This method not only reduces the risk of irreversible data retention but also aligns with the GDPR's principles of data minimisation and storage limitation.[34]

This solution has already found favour with several regulatory bodies, including the French data regulator CNIL, which has recommended that personal data be stored in a modifiable environment off-chain and linked to immutable on-chain records only through non-identifying references.[35] In effect, this design ensures that the blockchain does not process personal data in a manner that would trigger the GDPR, while still reaping the benefits of an immutable ledger for verification purposes.

5.2. Encryption and Crypto-Erasure

Another innovative solution is the use of strong encryption combined with a strategy known as crypto-erasure. In this model, personal data is stored on-chain only in an encrypted format, and the decryption keys are held by either the data controller or the data subject.[36] Should an erasure request be made, the key can be destroyed, rendering the encrypted data completely inaccessible. Although the encrypted data remains on the blockchain, its inaccessibility would, in practical terms, satisfy the objective of erasure by ensuring that no personal data is available for processing.[37]

The argument comes from the fact that the GDPR does not mandate the physical deletion of data but rather requires that the data no longer be attrib-

34. This also comes as a feasibility/cost advantage. Upkeeping such a large data base is not cost efficient.

35. 'Distributed Ledger Technologies and GDPR's Right to Be Forgotten: Can They Get along? – CiTiP Blog' <https://www.law.kuleuven.be/citip/blog/distributed-ledger-technologies-and-gdprs-right-to-be-forgotten/> accessed 28 March 2025.

36. M Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17.

37. Ibid.

utable to a natural person.[38] As long as the encryption is sufficiently robust and the keys are securely destroyed, the residual data on the blockchain cannot be used to identify an individual, and thus falls outside the scope of the GDPR.[39] However, encryption does not guarantee permanent inaccessibility—advances in cryptography or key recovery techniques could potentially expose the data in the future.

5.3. Chameleon Hashes and Editable Blockchains

A more radical technical innovation involves the use of chameleon hash functions, which allow for controlled modifications to the blockchain. Chameleon hashes are cryptographic hash functions that include a trapdoor mechanism; knowledge of the trapdoor key permits authorised parties to alter the input data while still producing the same hash value.[40] In a blockchain context, this means that if personal data needs to be 'erased', an authorised party could modify the block's contents (or at least the portion containing the personal data) without disrupting the overall integrity of the chain.[41]

This approach, however, raises significant concerns. The introduction of a trapdoor key necessitates the existence of a trusted authority or a consortium of parties who control the key, thereby compromising the decentralised ethos that is fundamental to blockchain technology.[42] Moreover, even if such a sys-

38. 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) [2016] OJ L119/1, Recital 26

39. However, the issue here is that the right to erasure would be influenced by the state of the art cryptographic measures. If somehow those cryptographic keys are brute forced (making a computer 'guess' the code).

40. Giuseppe Ateniese and others, 'Redactable Blockchain — or — Rewriting History in Bitcoin and Friends' (2016) <https://eprint.iacr.org/2016/757> accessed 28 March 2025.

41. Ibid.

42. Ibid.

tem were implemented in a permissioned blockchain, it would likely be unacceptable for public blockchains, where the value lies in decentralisation and resistance to censorship.[43] Nonetheless, chameleon hash-based solutions offer an intriguing possibility for scenarios where a controlled, editable ledger is acceptable—such as in private blockchains operated by regulated institutions.

5.4. Legal Adaptations and Regulatory Guidance

From a legal perspective, there is also room for innovative interpretations of the GDPR that could accommodate blockchain's technical realities. The GDPR's provisions are intentionally flexible, and the obligation to erase should be interpreted in light of what is technically feasible. In circumstances where literal deletion of data is impossible due to the decentralised nature of the technology, regulators might accept alternative measures—such as rendering data inaccessible through encryption or key destruction—as fulfilling the purpose of the right to be forgotten.

Such an interpretation would require clear regulatory guidance, likely issued by the European Data Protection Board (EDPB) or national supervisory authorities. In fact, several data protection authorities have already begun to engage with the issue.[44] The Spanish Data Protection Agency (AEPD), for example, has explored the possibility of 'hard forks' in blockchain systems that would create a new version of the ledger omitting the requested data.[45] Although such measures may be technically drastic and limited to permissioned environments, they illustrate the willingness of EU regulators to consider innovative solutions that balance the GDPR's objectives with technological constraints.

Another potential legal adaptation is the development of codes of conduct or

43. This just creates an already overcomplicated system.

44. 'EDPB | European Data Protection Board' <https://www.edpb.europa.eu/edpb_en> accessed 28 March 2025.

45. Ceyhun Pehlivan Valín Elena, 'Spanish AEPD: Harmonising Blockchain with the GDPR's Right to Be Forgotten' (*Passle*, 13 November 2024) <https://techinsights.linklaters.com//post/102jo4a/spanish-aepd-harmonising-blockchain-with-the-gdprs-right-to-be-forgotten> accessed 28 March 2025.

certification mechanisms specific to blockchain technology. Under GDPR Articles 40–42, self-regulatory measures and industry standards can play an important role in demonstrating compliance. A well-designed code of conduct for blockchain operators might, for example, specify acceptable methods for handling personal data—such as the use of off-chain storage, encryption protocols, and data expiry rules—and provide a framework for accountability and redress in the event of a data subject's erasure request.[46] Such voluntary measures, once approved by data protection authorities, could offer much-needed legal certainty in an area where traditional legal mechanisms struggle to keep pace with rapid technological change.

5.5. Data Protection by Design

Ultimately, the most promising solution may be to embed privacy into the very architecture of blockchain systems from the outset. GDPR mandates that data protection be incorporated into the design of systems and processes—a concept known as 'data protection by design and by default'.[47] For blockchain developers, this means critically evaluating whether personal data should be stored on-chain at all and, if it must be, employing techniques such as pseudonymisation, encryption, and off-chain storage to minimise the risk of non-compliance.[48] By designing blockchain systems with privacy in mind from the beginning, developers can create environments where personal data is only ever processed in ways that are reversible, controllable, or effectively anonymised.

---

46. While far away (or maybe impossible), a European blockchain would streamline an immense amount of information and processes.

47. 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) [2016] OJ L119/1, Art 25.

48. This must be done on a case by case basis; processors that need personal data for providing accurate services or in the fulfilment of obligations could have a blockchain design that stores both the Hashed values and the personal data on chain.

In conclusion of this section, no single silver-bullet solution exists yet. The likely path forward is a **multi-pronged approach:** (1) *Architectural choices* (like permissioned networks or off-chain data storage) to reduce GDPR friction, (2) *Cryptographic tools* (encryption, hashing, possibly chameleon functions in private networks) to enable post-hoc privacy, and (3) *Legal interpretations* that acknowledge technical limits and allow alternative compliance methods. By combining these, one can envision a scenario in which a blockchain-based system can **honour a Right to Be Forgotten request** to a satisfactory degree: for example, the personal data is encrypted and stored off-chain, the on-chain link is anonymised or pruned, and an audit trail on the chain can even prove that deletion was requested and fulfilled (ensuring accountability). Such innovative alignment would uphold data subject rights without wholly sacrificing the benefits of blockchain innovation.

6. Conclusion

Blockchain's immutable architecture with the GDPR's Right to Be Forgotten presents a formidable challenge. Yet as this article has shown, the solution is not to reject blockchain technology outright but rather to innovate—both legally and technically—so that the imperatives of data protection can coexist with the benefits of decentralisation. The evolution of EU case law, particularly the seminal decisions in *Google Spain* and *GC and Others v CNIL*, underscores the importance of balancing individual privacy rights with freedom of expression and public interest. However, these rulings were rendered in contexts where data controllers had clear authority and means to modify data. In the decentralised world of blockchain, new solutions must be found.

A multi-pronged approach is required. Off-chain storage and the use of hash pointers allow for the separation of personal data from the immutable ledger, ensuring that personal data can be deleted or modified without compromising the blockchain's integrity. Encryption combined with crypto-erasure offers another promising avenue, as does the development of chameleon hash functions for permissioned networks. Finally, embedding privacy by design into blockchain architectures offers the most sustainable solution, ensuring that personal data is never unnecessarily exposed.

The task for policymakers, regulators, and technologists is to work collaboratively in developing standards, codes of conduct, and technical frameworks that harmonize the GDPR's lofty ideals with the realities of blockchain technol-

ogy. In doing so, Europe can maintain its high data protection standards while fostering an environment of innovation. Such a balanced approach is not only desirable but essential in an era where the digital footprint of individuals is indelible and the promise of blockchain is ever-expanding.

In sum, blockchain can indeed innovate the Right to Be Forgotten by challenging legal and technical paradigms to evolve. The GDPR was not designed with blockchain in mind, but its technology-neutral language provides a platform for reinterpretation and adaptation. With careful design and proactive regulatory engagement, blockchain systems can be re-engineered to protect individual privacy while maintaining the trust and transparency that are their hallmark. This evolution is vital for ensuring that in the digital age, the right to privacy remains robust and effective—even on a ledger that is, by its very nature, immutable.

Bibliography

Cases

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12) [2014] ECLI:EU:C:2014:317 (13 May 2014).

GC and Others v Commission nationale de l'informatique et des libertés (CNIL) (Case C-136/17) [2019] ECLI:EU:C:2019:773 (24 September 2019).

Legislation

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) [2016] OJ L119/1.

Books

De Filippi P and Wright A, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) https://www.jstor.org/stable/j.ctv2867sp accessed 28 March 2025.

Journal Articles and Academic Papers

Ateniese G et al, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2016) https://eprint.iacr.org/2016/757 accessed 28 March 2025.

Belen-Saglam R et al, 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems' (2023) 4Blockchain: Research and Applications .

Finck M, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17.

Globocnik J, 'The Right to Be Forgotten Is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' (2020) 69 GRUR International 380.

Mongetro Goint, Bertelle C and Duvallet C, 'Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems' (2023) 11 Mathematics 1592.

Shoaib B, 'The Immutable Blockchain Confronts the Unstoppable GDPR' (2023) 14(1) *Seattle Journal of Technology, Environmental & Innovation Law* 5 https://digitalcommons.law.seattleu.edu/sjteil/vol14/iss1/5/.

Tripathi G, Abdul Ahad M and Casalino G, 'A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges' (2023) 9.

Zafar A, 'Reconciling Blockchain Technology and Data Protection Laws: Regulatory Challenges, Technical Solutions, and Practical Pathways' (2025) 11.

Websites

'Anonymising Personal Data "Not Enough to Protect Privacy", Shows New Study | Imperial News | Imperial College London' (*Imperial News*, 23 July 2019) https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/ accessed 28 March 2025.

'Distributed Ledger Technologies and GDPR's Right to Be Forgotten: Can They Get along? – CiTiP Blog' https://www.law.kuleuven.be/citip/blog/distributed-ledger-technologies-and-gdprs-right-to-be-forgotten/ accessed 28 March 2025.

'EDPB | European Data Protection Board' https://www.edpb.europa.eu/edpb_en accessed 28 March 2025.

'Permissioned vs Permissionless Blockchains: Key Differences | TechTarget' (*Search CIO*) https://www.techtarget.com/searchcio/tip/Permissioned-vs-permissionless-blockchains-Key-differences accessed 28 March 2025.

Pehlivan Valín Elena C, 'Spanish AEPD: Harmonising Blockchain with the GDPR's Right to Be Forgotten' (*Passle*, 13 November 2024) https://techinsights.linklaters.com//post/102jo4a/spanish-aepd-harmonising-blockchain-with-the-gdprs-right-to-be-forgotten accessed 28 March 2025.

About the author

Cristian Costin

Cristian Costin completed the LLM in Technology Law and Innovation at the University of Groningen. He currently works as an expert for the Ministry of Labour in Moldova and contributes for the standardisation of national legislation with the standards of the European Union.

CHAPTER 3: SCHRÖDINGER'S DATA: RETHINKING THE BINARY DISTINCTION BETWEEN PERSONAL AND NON- PERSONAL DATA IN THE AGE OF SYNTHETIC INFORMATION.

Vilma Margarit

I. Introduction

One might wonder what the Austrian physicist's famous thought experiment and data classification have in common. In fact, the paradoxical dual state of simultaneous aliveness and death of Schrödinger's cat, could be used as a practical foundation to exemplify a similar behaviour when distinguishing between personal and non-personal data in the context of synthetic information. The European data protection framework has at its core the binary distinction between personal and non-personal data. However, the current increase in the implementation of synthetic data, meaning algorithmically generated information, poses a challenge to this rigid classification. This is mainly because while synthetic data is often seen as a privacy-enhancing technology, not all synthetic information is the same and the risk of reidentification makes its classification legally ambiguous. Hence, as it will be further illustrated, and much like Schrödinger's hypothetical cat sealed inside a box – which results both death and alive until the box is opened, data's categorisation may require a more fluid approach. This opinion paper examines whether the binary model under the GDPR is sufficient to mitigate the adverse impacts of synthetic data. The first chapter exemplifies the nature of this kind of data, as well as the methodologies utilised to generate it, and possible legal challenges related to its use. Next, the limitations of the current EU data protection law framework are highlighted, particularly focusing on its applicability on synthetic data and dynamic data flows. Finally, the paper introduces alternative perspectives to the risk-based approach and binary divide between personal and non-personal data, drawing also from quantum mechanics notions. By critiquing the inade-

quacy of the current framework considering synthetic data through a critical, and interdisciplinary technology-focused legal lens, this paper argues data protection law must evolve beyond static classification, focusing instead on the ever-evolving status of data. At the same time, it recognises further discussion is still needed within a field that is relatively novel.

II. Understanding Synthetic Data

A. What is Synthetic Data?

The Alan Turing Institute defines synthetic data as: "data that has been generated using a purpose-built mathematical model or algorithm, with the aim of solving a (set of) data science task(s)".[1] In simple terms, it is artificially generated data which replicates the structure, properties, and characteristics of real-world data.[2] In 2021 the Wall Street Journal published a prediction estimating that by 2024, 60% of the data utilised for AI development and analytics would be synthetically generated.[3] An Europol report further warns against the fact that almost 90% of the content online will be synthetically generated by 2026, as well as the fact that synthetic data's volume will reach a peak of 60% in 2030.[4] The widest use of synthetic data can be observed in fields like machine learning, data analysis, and software testing, where access to real data results

1. James Jordon and others, 'Synthetic Data – What, Why and How?'

2. Preeti Patel, 'Synthetic Data' (2024) 41 Business Information Review 48 <https://doi.org/10.1177/02663821241231101> accessed 23 March 2026.

3. 'Fake It to Make It: Companies Beef Up AI Models With Synthetic Data – WSJ' <https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601> accessed 23 March 2026.

4. 'StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia' <https://stratcomcoe.org/publications/trends-in-ai-from-red-and-blue-team-perspectives-synthetic-data-in-a-data-drivensociety-vs- sentiment-analysis/256> accessed 23 March 2026.

limited due to privacy concerns or lack of data availability.[5] This kind of data is often considered to be a "privacy-enhancing technology" (PET), as it *seemingly* offers a privacy-preserving alternative to real world information,[6] an issue that will be discussed further in-depth in the following sections.

B. Types of Synthetic Data

7

	training_data	deidentified_data	synthetic_data
	0	0	0
CustomerID	11000	fb178a0f	0178b12f
Title	nan	nan	nan
FirstName	Jon	Tammy	Cathy
MiddleName	V	Christopher	Ashley
LastName	Yang	Harding	Gordon
Suffix	nan	nan	nan
AddressLine1	3761 N. 14th St	3432 Michelle Drives Suite 828	0521 Tammy Ramp Suite 678
AddressLine2	nan	nan	8935 Burke Streets
City	Rockhampton	Rockhampton	Bobigny
StateProvinceName	Queensland	b48517a3	55caead9
CountryRegionName	Australia	d7df265f	ff5390c8
PostalCode	4700	4700	94070
PhoneNumber	1 (11) 500 555-0162	623.419.5397x53019	+1-795-579-1785x881
BirthDate	1966-04-08	1966-04-28	1977-07-09
Education	Bachelors	Bachelors	High School
Occupation	Professional	Professional	Manual
Gender	M	M	M
MaritalStatus	M	M	M
HomeOwnerFlag	1	1	0
NumberCarsOwned	0	0	2
NumberChildrenAtHome	0	0	0

***Figure 1**: Example of the Process of Data Synthetisation from Real-World Training Data (Generated with Gretel.AI by Moez Ali).*

The generation of synthetic data can take many forms, including through popular deep learning architectures like Generative Adversarial Networks (GANs).[8]

---

5. ibid.

6. iIbid.

7. Table courtesy of Moez Ali, 'Synthetic Data Is the Future of Artificial Intelligence' (*Medium*, 18 January 2023) <https://moez-62905.medium.com/synthetic-data-is-the-future-of-artificial-intelligence-6fcfd2ce1a14> accessed 23 March 2026.

8. Jordon and others (n 1).

It is important however to highlight that these AI models must be trained on real data, meaning the synthetic information will not result to be inherently private – standard GANs are incapable of generating private or unbiased data and require additional computation behind basic sample generation.[9] At the same time, when the GANs are employed to generate fully private synthetic data without access to the authentic one, no statistical inferences about the real world will be drawn.[10] Within this context, two categories of synthetic data are identifiable: information generated based on real- world data and information generated without real-world training data. While the former results more accurate, it is not inherently private. The latter on the other hand, might fully preserve privacy but results useless for analytical predictions. However, a last category complicates this division: *partially* or "hybrid" synthetic data.[11] This kind of data is generated based on the identification of attributes within the original data, dividing them between "quasi-identifiers" and "sensitive attributes" – the first ones can be disclosed, while the second must be protected.[12] Because quasi-identifiers may be sensitive in some cases, this third kind of synthetic data does not generally satisfy privacy guarantees.[13]

C. Benefits, Drawbacks and Legal Challenges

At first glance, data synthesis may seem like a promising solution to many issues in training datasets and big data analytics. However, these perspectives are often rooted in misconceptions. A first popular assumption is the fact that synthetic data can help with debiasing, by producing samples that do not con-

9. 'StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia' (n 4).

10. ibid.

11. Ana Beduschi, 'Synthetic Data Protection: Towards a Paradigm Change in Data Regulation?' (2024) 11 Big Data & Society 20539517241231277 <https://doi.org/10.1177/20539517241231277> accessed 23 March 2026.

12. Jordon and others (n 1).

13. ibid.

tain historical biases.[14] Firstly, synthetic data resides in the same space as real data, taking value from it and mimicking its characteristics including bias.[15] Because of this, the generation of synthetic datasets usually lacks a sufficient level of diversity, leading to an unbalanced data distribution in relation to attributes like gender, age, and race.[16] If a synthetic dataset is primarily based on real-world data prioritising individuals from a certain racial group, it will inevitably fail at mitigating the very bias it aims to address.[17] A second widely adopted use of synthetic data is for the development of OpenAI and Microsoft's generative models, circumventing IP abuse issues, privacy and data access.[18] While a viable alternative, synthetic data is often generated from web-scrapped publicly available data,[19] which is not always in line with data protection principles such as data minimisation and accuracy.[20] Since AI models may "hallucinate" (generate outputs with inaccurate information) even when trained on representative high-quality data,[21] assessing synthetic data's source reliability becomes crucial. This eventually leads to a data "ouroboros"[22] – how can the accuracy of synthesised data be assessed when generated without real-world

14. ibid.

15. ibid.

16. 'Synthetic Data in AI: Challenges, Applications, and Ethical Implications' <https://arxiv.org/html/2401.01629v1> accessed 23 March 2026.

17. ibid.

18. Patel (n 2).

19. 'Synthetic Data in AI: Challenges, Applications, and Ethical Implications' (n 16).

20. European Data Protection Supervisor, *Generative AI and the EUDPR: First EDPS Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems* (3 Junehttps://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf accessed 23 March 2026.

21. ibid.

22. A circular symbol depicting a snake or dragon devouring its own tail. Generally used to represent a never-ending, perpetually repeating cycle.

training data or it consists of information that is only partially synthetic? As previously discussed, the most prominent application of synthetic data is its use as a privacy-enhancing alternative to traditional data.[23] At the same time, Beduschi warns about a crucial concern: depending on *how* it has been generated, synthetic data still presents a risk of re-identification, which plays a key role in determining the applicability of the GDPR.[24] While fully synthetic data may fall outside the scope of the Regulation, establishing a clear re-identification threshold to distinguish between personal and non-personal data remains challenging within a binary framework.[25] This is especially true for hybrid and partially synthetic datasets, where traces of real-world data complicate this dichotomous classification.[26]

III. The Binary Paradigm: Personal vs Non-Personal Data

The GDPR adopts a "binary approach", differentiating between two kinds of data: personal and non-personal.[27] Only the former is captured by the Regulation, defined in Art. 4(1) GDPR as data directly or indirectly relating to an "identified or identifiable natural person", a definition which has been generally interpreted in a very broad way.[28] This is a paramount principle of EU data

23. Giulia Finocchiaro and others, 'The Regulatory Future of Synthetic Data – Data Synthesis as a Resource for Scientific Research, Innovation, and Public Policy in the European Legal Landscape' <https://doi.org/10.5281/ZENODO.13342141> accessed 23 March 2026.

24. Beduschi (n 11).

25. ibid.

26. ibid.

27. Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11 <https://doi.org/10.1093/idpl/ipz026> accessed 23 March 2026.

28. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

protection law: data is strictly classified within a binary paradigm. This legal perspective however, does not reflect the reality of data, which would be better represented by collocating it as part of a dynamic spectrum – oscillating between personal, non-personal and "anything in between".[29] Synthetic data perfectly exemplifies this grey area, as its classification within the GDPR is not always straightforward.[30] However, let us first examine the regulatory framework in place.

A. Recital 26 GDPR: A Risk-Based Approach

Recital 26 of the GDPR contains the legal test to differentiate between personal and nonpersonal data, embracing a risk-based approach to qualify data: when there is a "reasonable risk" of identification, data will be treated as personal.[31] The Recital further explains that this is connected to the "means reasonably likely to be used" for re-identification, as well as looking at factors such as costs, time, and available technology.[32] The applicability of this test has however led to complications, specifically considering that data collection and information flows are complex processes.[33] The landmark case of *Breyer v. Germany* concerning whether IP addresses are personal data laid down the grounds for two further criteria: a subjective and an objective one. The former translates in the

---

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1, art 4(1).

29. Alessandro El Khoury, 'Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics' (Social Science Research Network, 1 December 2018) <https://papers.ssrn.com/abstract=3356767> accessed 23 March 2026.

30. Beduschi (n 11).

31. GDPR, recital 26.

32. ibid.

33. El Khoury (n 29).

capacity of a provider to use their resources to identify the data subject, while the latter focuses on the possibility of identification regardless of the provider's capabilities.[34] In *Breyer* the Court makes clear that any data might potentially be personal, if the data controller has the *lawful means* to obtain additional information that would allow the identification of a data subject.[35]

B. Article 29 Working Party: Towards Legal Uncertainty

In sharp contrast to the risk-based approach of identification in the GDPR, Article 29 Working Party proposes a strict parallel test within its Opinion 05/2014 on anonymisation techniques.[36] The Working Party takes anonymisation to a rather extreme length, defining it as a process of "permanent erasure, i.e. making it impossible to process personal data".[37] This is also reinforced by the way controllers' handling of data is interpreted: "when a data controller [...] hands over part of the datasets (after removal or masking of identifiable data), the resulting dataset is still personal data".[38] As the following sections will illustrate, achieving perfect anonymisation is impossible. The Working Party's emphasis on irreversibility and permanence greatly diverges from the legislative text of the Regulation, as Recital 26 recognises technology as constantly evolving and absolute anonymisation as unattainable.[39] These two conflicting interpretations have created lack of clarity over which test should be applied in practice, ultimately undermining legal certainty.[40]

---

34. ibid.

35. *Breyer v Germany* [2020] ECtHR 50001/12.

36. Article 29 Data Protection Working Party, '*Guidelines on Consent under Regulation 2016/679*' < https://ec.europa.eu/newsroom/article29/items/623051/en> accessed 23 March 2026

37. ibid.

38. ibid.

39. ibid.

40. Finck and Pallas (n 27).

IV. Re-Identification Issues & Synthetic Data

A. The Tension Between Utility, Fidelity & Privacy in Synthetic Data

Utility, fidelity and privacy are three fundamental attributes of synthetic data.[41] Utility refers to the capability of the synthetic data to generate results that are similar to those of the original data, revealing its usefulness for a given task. Fidelity is about the statistically match between the synthetic and real-world data, while the degree of privacy within synthetic data is determined by how much information it reveals about the original data utilised to produce it.[42] These three attributes result intrinsically linked as for example when fidelity increases, privacy of the synthetic data set will decrease – it is thus impossible to generate synthetic data that will be useful for *all* cases.[43]

B. Pseudonymisation, Anonymisation and the "In-Between"

There is no clear-cut answer as to whether synthetic data is anonymous or pseudonymous.[44] For a synthetic dataset to be truly anonymous, any inferences about individuals' characteristics and attribute values must be prevented.[45] Furthermore, in the case of synthetic data one must also think about the risk of inferring attributes. An example of this would be to have a synthetic

41. Jordon and others (n 1).

42. ibid.

43. ibid.

44. Gernot Fritz Lyon Markus Kattnig, Christine Chong, Christine, 'Synthetic Data: A Privacy Panacea?' (*Passle*, 6 November 2024) <https://technologyquotient.freshfields.com//post/102jnj9/synthetic-data-a-privacy-panacea> accessed 23 March 2026.

45. Marina Anagnostaki, 'Synthetic data: Anonymized data or Pseudonymized data?' (*datenschutz notizen | News-Blog der DSN GROUP*, 27 March 2023) <https://www.datenschutz-notizen.de/synthetic-data-anonymized-data-or-pseudonymized-data-3541386/> accessed 23 March 2026.

salary database, based on original salary values. While original names, addresses and other identifiable attributes might be changed, the relationship between variables is preserved. In this scenario, the synthetic data cannot be considered truly anonymous – a link to the original data remains. At the same time, a certain degree of privacy protection is present, as no sensitive information is revealed. In this context, identification risks should be assessed contextually, carefully determining whether re- identification is a real concern, whether it poses actual harm to individuals or if there is a feasible effort for re-identification. Re-identification is thus a crucial factor in determining the applicability of the GDPR to the processing of synthetic data. However, the specific threshold for a risk of re-identification in this context remains unclear.[46] Some have argued that there will always be a residual risk of re-identification, even in *fully* synthetic datasets and those generated through differential private methods.[47]At the same time, this risk may not materialise at all, meaning the synthetic dataset could be considered effectively anonymous. These ambiguities ultimately create significant legal uncertainty for those processing synthetic datasets. If the synthetic data is generated through one-to-one mapping, meaning that each synthetic data is equal to the original one, the source feature and patterns will be maintained. This generation method implies the synthetic data should be defined as pseudonymous – in this case reidentifiction would be possible as per art. 4(5) GDPR through additional information with data matching or a similar technique.[48] Pseudonymised or "de-identified" data remains thus personal data, greatly differing from completely anonymised information.[49]

According to the EDPS (European Data Protection Supervisor), as synthetic data is the product of an artificial process and unrelated to a real individual, it falls

46. Beduschi (n 11).

47. ibid.

48. Finocchiaro and others (n 23).

49. ibid.

outside the scope of the GDPR.[50] A further argument supporting this is the fact that if the synthetic data is properly generated without allowing direct association of records and individuals' data, the result would be entirely new "original data".[51] Unfortunately, the practical reality does not reflect this line of reasoning. In a landmark study, researchers have estimated that 99.98% of Americans could be re-identified in any dataset by utilising just 15 demographic attributes.[52] Data that has been initially identified as anonymous, could potentially become personally identifiable in the future.[53] In this sense, data seems to be subject to what El Khoury calls "double relativity", i.e. non-personal data "located at time 0 could become personal data in another moment of the timeline".[54] Thus, if synthetic data is deemed to be both personal and non-personal simultaneously due to the persistent risk of re-identification and complex information flows, the EU legislative data protection framework's binary classification might be insufficient in addressing the challenges related to synthetic data.

V. Challenging the Paradigm: Borrowing from Quantum Mechanics

Multiple scholars have already expressed the need to revolutionise the risk-based approach contained within the GDPR, and with it the binary categorisation of personal and nonpersonal data – specifically considering novel uses

50. ibid.

51. Anagnostaki (n 45).

52. Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069 <https://doi.org/10.1038/s41467-019-10933-3> accessed 23 March 2026.

53. Lyon (n 44).

54. El Khoury (n 29).

of data such as synthetic information and data-driven AI models.[55] Beduschi proposes starting points of discussion for the transformation of the binary approach to data, especially how that would look like for hybrid and partially synthetic datasets but ultimately provides no concrete solutions.[56] Finck and Pallas advocate for a "system change" rooted in the acceptance that a residual identification risk will always be present, while at the same time recognising that completely shaking the foundations of the binary approach would remove incentives for data controllers to behave in a manner that aligns with data protection principles (at the detriment of data subjects' rights).[57] Perhaps the most interesting alternative is presented by El Khoury, who readily criticises the limitations of applying a binary approach in practice within an environment where the degree of identifiability changes depending on the circumstances and capabilities of data controllers.[58] He further explains that the fragility of the present "virtual border" between personal and non- personal data can be easily disregarded, and calls for a notion of personal data that borrows from the field of quantum mechanics. At the core of his paper is the application of the concepts of "entanglement" and "superposition" to data protection. In physics, entanglement means that two particles always remain connected, allowing for an instant correlation of their state, regardless of the distance between them. Similarly, within the data protection context entanglement occurs when previously non-personal data becomes personal due to its linkage with ulterior information across multiple datasets. This would imply data exists in a "quantum superposition": it is not inherently personal or non-personal until processed, analysed, or linked to other datasets.[59] The binary classification of the GDPR does not reflect this reality and it is suggested instead to accept data as having a "fluid" status, with the ability to shift at any time between per-

55. ibid; Finck and Pallas (n 27).

56. Beduschi (n 11).

57. Finck and Pallas (n 27).

58. El Khoury (n 29).

59. ibid.

sonal and non-personal, depending on the way it is processed, linked or reinterpreted over time.

By focusing on the processing operations that trigger the transition from one "state" to the other, El Khoury proposes a dynamic alternative to an otherwise static legal test and identifies a three-tier classification list for data: personal, non-personal and *potentially personal*, i.e. a grey area for potential identification. The legal assessment in this case would be focused on how processing may or may not trigger entanglement and re- identification risks, rather than assessing whether data is personal at a fixed point in time. Based on this line of reasoning, several queries may follow, for example: if data's status is always considered "fluid", would not *all* data ultimately be classified as "potentially personal" data, especially synthetic data generated from real-world information? And if so, does a three-tier structure classification of EU data protection law still make sense in this context? While there are certain positive aspects to this proactive compliance model, as opposed to a reactionary approach to re-identification risks, it also opens the door to future research and discussion.

VI. Conclusion

Considering new algorithmic advancements within data protection, such as the ability to generate synthetic information from real-world data, the traditional binary classification of data under EU law appears to be increasingly inadequate in addressing the complexities of these new kinds of data. While the GDPR distinguishes between personal and non-personal data, synthetic information occupies what can be defined as a "grey area", where there always remains a risk of re-identification and linkability to other datasets and information. A key issue has been identified in this persistent risk, particularly in synthetic datasets as traces of real- world data complicate their classification under the existing binary paradigm. While the GDPR defines pseudonymisation and anonymisation, synthetic data does not neatly fit in these categories. An increasing number of scholars have thus been advocating for a reform of the binary paradigm and the risk-based approach to re-identification, with few however proposing viable alternatives. An interesting approach has been the one of scholar El Khoury, who suggests treating data in the era of Big Data and AI analytics like physical quantum particles capable of fluidity and constant change. Opposed to a static classification, this proactive perspective offers a third data categorisation: "potentially personal data" – data that does not cur-

rently identify an individual but could in the future. While the model seems a feasible alternative, it also raises questions to be taken as a starting point for broader discussion within the nascent and rapidly evolving realm of synthetic data.

VII. Bibliography

Primary Sources:

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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* (WP216, 10 April 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf accessed 23 March 2026

European Data Protection Supervisor, *Generative AI and the EUDPR: First EDPS Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems* (3 June 2024) https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf accessed 23 March 2026

Secondary Sources:

Ali M, 'Synthetic Data Is the Future of Artificial Intelligence' (Medium, 18 January 2023) https://moez-62905.medium.com/synthetic-data-is-the-future-of-artificial-intelligence-6fcfd2ce1a14 accessed 23 March 2026

Anagnostaki M, 'Synthetic Data: Anonymized Data or Pseudonymized Data?' (Datenschutz-Notizen, 27 March 2023) https://www.datenschutz-notizen.de/synthetic-data-anonymized-data-or-pseudonymized-data-3541386/ accessed 23 March 2026

Beduschi A, 'Synthetic Data Protection: Towards a Paradigm Change in Data Regulation?' (2024) *Big Data & Society* https://journals.sagepub.com/doi/10.1177/20539517241231277 accessed 23 March 2026

Bergmanis-Korāts G and others, *Trends in AI from Red and Blue Team Perspectives: Synthetic Data in a Data-Driven Society vs Sentiment Analysis* (NATO Strategic Communications Centre of Excellence, 21 December 2022) https://stratcomcoe.org/publications/trends-in-ai-from-red-and-blue- teamperspectives-synthetic-data-in-a-data-driven-society-vs-sentiment-analysis/256 accessed 23 March 2026.

Castellanos S, 'Fake It to Make It: Companies Beef Up AI Models With Synthetic Data' *The Wall Street Journal* (New York, 23 July 2021) https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601 accessed 23 March 2026

El Khoury A, 'Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics' (2018) 11(3) *Erasmus Law Review* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356767 accessed 23 March 2026

Finck M and Pallas F, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10(1) *International Data Privacy Law* 11 https://academic.oup.com/idpl/article/10/1/11/5802594 accessed 23 March 2026

Finocchiaro G and others, *The Regulatory Future of Synthetic Data: Data Synthesis as a Resource for Scientific Research, Innovation, and Public Policy in the European Legal Landscape* (Italian Institute for Privacy and Data Protection & Data Intermediaries Alliance, 19 August 2024) https://zenodo.org/records/13342141 accessed 23 March 2026

Freshfields Bruckhaus Deringer, 'Synthetic Data: A Privacy Panacea?' (Technology Quotient, 6 March 2024) https://technologyquotient.freshfields.com/post/102jnj9/synthetic-data-a-privacy-panacea accessed 23 March 2026

Hao S and others, 'Synthetic Data in AI: Challenges, Applications, and Ethical Implications' (arXiv, 3 January 2024) https://arxiv.org/html/2401.01629v1 accessed 23 March 2026

Patel P, 'Synthetic Data' (2024) 41(2) *Social Science Information https://doi.org/10.1177/02663821241231101 accessed 23 March 2026*

Rocher L, Hendrickx JM and de Montjoye Y-A, 'Estimating the Success of ReIdentifications in Incomplete Datasets Using Generative Models' (2019) 10 *Nature Communications* 3069 https://pubmed.ncbi.nlm.nih.gov/31337762/ accessed 23 March 2026

The Royal Society, *Synthetic Data: An Overview and Key Considerations* (The Royal Society, 2023) https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Synthetic_Data_Survey-24.pdf accessed 23 March 2026

About the author

Vilma Margarit

Vilma Margarit completed the LLM in Technology Law and Innovation (cum laude) at the University of Groningen in 2025. She is currently pursuing a PhD at the Institute for Information Law (IViR), University of Amsterdam. Her main area of research is the tension between confidentiality claims of private actors and the need for transparency for public interest research in the context of AI and other digital technologies.

CHAPTER 4: DATA OWNERSHIP, CONSENT, AND USER PRIVACY IN THE WORLD OF VIDEO GAMES

Willem Drapers

1. Introduction

In the last decade, multinational technology corporations such as Microsoft, Sony, and Tencent have acquired and invested significant sums in the world of video games, a rapidly growing sector in the media industry.[1] The global revenue in the games market has steadily increased from 135.4 billion in 2019 to 186.1 billion in 2025 with expected continued growth.[2] For example, Microsoft publisher labels now consist of Xbox Game Studios, Bethesda Softworks, and King media and in 2023 they announced plans to purchase Activision Blizzard for 68.7 billion.[3][4] In China, Tencent acquired Riot Games in 2015 with a 99.7%

1. 'Game Changer: Accelerating the Media Industry's Most Dynamic Sector' (*BCG Global*, 7 June 2023) <https://www.bcg.com/publications/2023/drivers-of-global-gaming-industry-growth> accessed 24 March 2025.

2. 'Global Games Market Outlook: Key Growth Drivers and Challenges for 2025-2027' (*Newzoo*, 6 March 2025) <https://newzoo.com/resources/blog/global-games-market-update-q1-2025> accessed 24 March 2025.

3. 'How Microsoft's Activision Blizzard Deal Is Transformative' (*Knowledge at Wharton*) <https://knowledge.wharton.upenn.edu/article/how-microsofts-buy-of-activision-blizzard-is-transformative/> accessed 24 March 2025.

4. Microsoft News Center, 'Microsoft to Acquire Activision Blizzard to Bring the Joy and Community of Gaming to Everyone, across Every Device' (*Stories*, 18 January 2022) <https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-

equity stake, furthermore, Tencent holds significant ownership stakes in Epic Games, a large store front for games such as Fortnite and the Roblox Corporation.[5] While it runs its own social media platforms, Tencent has also made investments in other notable platforms like Snapchat, Discord, and Reddit.[6]

Gaming, with millions of users across all age groups and income levels, is the world's leading entertainment industry. However, what remains largely unnoticed is that modern devices pose a serious threat to consumer privacy. The potential uses of user data from gaming platforms are numerous and the ways that big technology corporations leverage this data for competitive advantages may be detrimental to how we as consumers are targeted. Video gaming already involves processing[7] a large volume of personal data from users, which will likely only increase as the industry progresses. Personal data is often collected through user interactions with digital platforms, including social media and online gaming applications. Furthermore, the kernel level anti-cheat systems some games employ, for example, are granted more access to your device than the data subjects (users) have.[8] Riot Games (under Tencent) introduced Vanguard's kernel level anti-cheat[9], which is like *'Riot installing a camera*

---

bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/> accessed 24 March 2025.

5. 'Britannica Money' (23 March 2025) <https://www.britannica.com/money/Tencent> accessed 24 March 2025.

6. Ibid.

7. 'Art. 4(2) GDPR – Definitions – General Data Protection Regulation (GDPR)', *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*.

8. Nisha Ellis, 'What Is Anti-Cheat? Online Gaming and Security Risks | Schellman' (*Schellman Compliance*) <https://www.schellman.com/blog/cybersecurity/what-is-anti-cheat> accessed 24 March 2025.

9. '/Dev/Null: Anti-Cheat Kernel Driver' (3 February 2020) <https://www.leagueofle-

in every room of your house and getting a copy of every key inside'.[10] This is viewed largely as intrusive and excessive by users, especially considering that it permanently runs on every startup and can do things you can't do without your knowledge.[11] This paper does not assume abuse, but envisions adequate duty of care by design in preserving privacy while stopping threat actors.

Additionally, the recent designation of Riot Games' parent company, tech conglomerate Tencent, as a Chinese military company highlights other risks.[12] On January 7 2025, the Pentagon dropped a list (formally known as the Section 1260H list) which identified 126 Chinese military companies, with consequences such as a ban on purchases and investments in designated companies and their subsidiaries.[13] Specifically, the implications for U.S. big tech firms and Chinese state-owned enterprises are especially troubling, as these entities operate within an increasingly interconnected global market where technology, data, and geopolitical interests converge.[14]

---

gends.com/en-us/news/dev/dev-null-anti-cheat-kernel-driver/> accessed 24 March 2025.

10. 'Why You Should Reconsider Playing League of Legends: The Risks of Kernel-Level Anti-Cheat Software.Md' (*Gist*) <https://gist.github.com/stdNullPtr/2998eacb71ae925515360410af6f0a32> accessed 25 March 2025.

11. Ted Litchfield published, 'According to Experts on Kernel Level Anticheat, Two Things Are Abundantly Clear: 1) It's Not Perfect and 2) It's Not Going Anywhere' (*PC Gamer,* 27 February 2024) <https://www.pcgamer.com/according-to-experts-on-kernel-level-anticheat-two-things-are-abundantly-clear-1-its-not-perfect-and-2-its-not-going-anywhere/> accessed 25 March 2025.

12. Pam K Ferdinand, 'Tencent Branded a Chinese Military Company by US Government' (*Game Rant*, 8 January 2025) <https://gamerant.com/tencent-chinese-military-company-list-us-government/> accessed 24 March 2025.

13. 'Tencent: US Designates the Firm a Chinese Military Company' (*BBC,* 7 January 2025) <https://www.bbc.com/news/articles/c9q78wn9g8zo> accessed 24 March 2025.

14. Cathy Gaphty, 'The Impact of U.S. Designation of Tencent as a Chinese Military Company on Local and State Governments' (*Critical Path Security*, 13 January 2025)

The geopolitical risks associated with data-driven innovation cannot be overstated, as the potential implications of harvesting user game data are profound and far-reaching. As the story of Cambridge Analytica (CA) has shown, the use of personal data of millions of people in this case was used to influence elections and public perceptions across the world.[15] Brittany Kaiser, a former employee of CA explained how very simply, '*It's like a boomerang. You send your data out. It gets analyzed. And it comes back at you as targeted messaging to change your behavior.*'[16] Additionally, she stated publicly that the CA methodology was classified as a weapon by the British government emphasizing its use of weapons-grade communications tactics.[17] Considering that CA was a subsidiary of the SCL group, a firm entrenched in the military industrial complex, it becomes even more evident that the methods employed were at the level of a psy-op.[18] Although CA ceases to exist now, many other companies doing the same sort of work still exist.[19] Naturally, the technology still exists, therefore it becomes vital to understand how data and its uses may affect our lives.

Data-driven innovations now play a crucial role in shaping content creation, distribution, and monetization across various industries. Streaming services use data to determine which shows and movies to produce, while gaming companies leverage user data to enhance gameplay, introduce new features, and

---

<https://www.criticalpathsecurity.com/the-impact-of-u-s-designation-of-tencent-as-a-chinese-military-company-on-local-and-state-governments/> accessed 25 March 2025.

15. nanda, 'Weapons-Grade Communication' (*Living my truth – A seeker's blog*, 25 July 2019) <https://livingmytruth.se/weapons-grade-communication/> accessed 24 March 2025.

16. Ibid.

17. Ibid.

18. Adam D Hernandez, 'Cambridge Analytica: Military Psy-Ops Privatized' 6.

19. Poppy Noor, 'There Are Plenty More like Cambridge Analytica. I Know – I've Used the Data' The Guardian (23 March 2018) <https://www.theguardian.com/commentisfree/2018/mar/23/plenty-more-like-cambridge-analytica-data-facebook> accessed 24 March 2025.

improve user interfaces.[20] The process of data collection and analysis ensures that entertainment continuously evolves to meet the demands of consumers. However, are the various data points across these platforms and mediums are combined? What if the data was used to profile users cognitive or physical ability? What are the consequences of a profile so dense with information that a user's entire future could be mapped out? To understand why these data points matter, first it must be understood what data games produce and what the obligations are of companies that collect such data.

This opinion paper explores the depth of data collection and the implications of acquisition by big tech for consumers. First, the extent of user data and privacy risks of individuals are highlighted through the invasiveness of Riot anticheat, the lacklustre privacy policy from Blizzard and the extent of biometric data collection in video games. The overarching geopolitical and cybersecurity implications are mentioned throughout to exemplify the broader potential risk factors. Lastly, the European data protection and competition law rules are considered, considering the scope. The scope for data ownership, transparency and user privacy is explored in the age of surveillance capitalism. This paper seeks to uncover the compliance of the gaming industry with the GDPR (in tandem with the categorization of high-risk under the AI act). Uncovers competition law elements that have been neglected in the collection of data from the gaming industry and how that puts consumers at risk.

2. Data Protection Challenges and Enforcement Trends

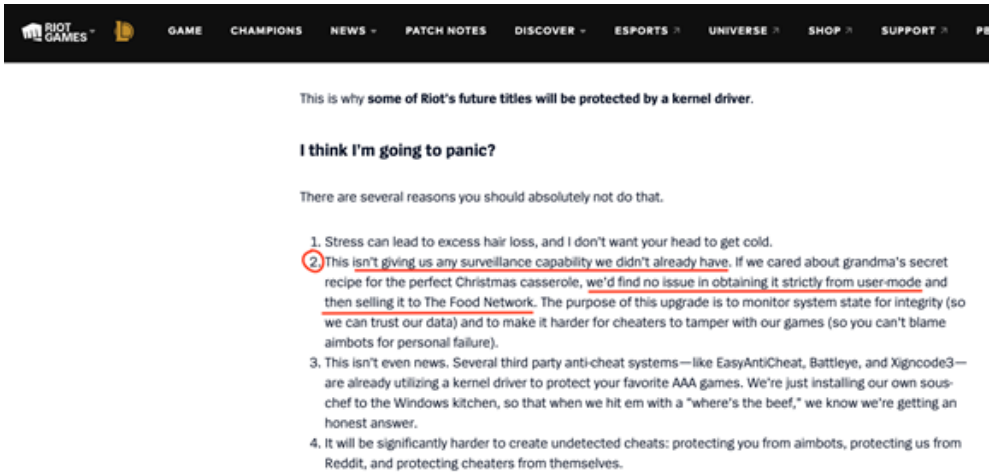
2.1. Kernel Level Access

Why does cyber security and kernel level access matter? Although esoteric to the uninitiated, in the game industry, there exist several large competing tech conglomerates with ties to government and state that have kernel level access

20. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013) 6.

to our household digital devices.[21] Aside from the nature of geopolitics, this is a recipe for vulnerabilities and data harvesting. In fact, developers don't even need kernel level access to acquire user data, as was openly mentioned on a dev press release on Vanguard anti-cheat.

Figure 1: Riot games developer "mirageofpenguins" on the anti-cheat kernel driver[22]



Both user and kernel modes can access the unencrypted files and pictures on your hard drive, but kernel access gives a degree of control of the entire device, hardware and software included, that user-mode does not.[23] Several other companies use kernel-level anti-cheating software (think of Easy Anti-Cheat and BattlEye). However, there is a significant distinction in their operational modes compared to Riot's approach.[24]

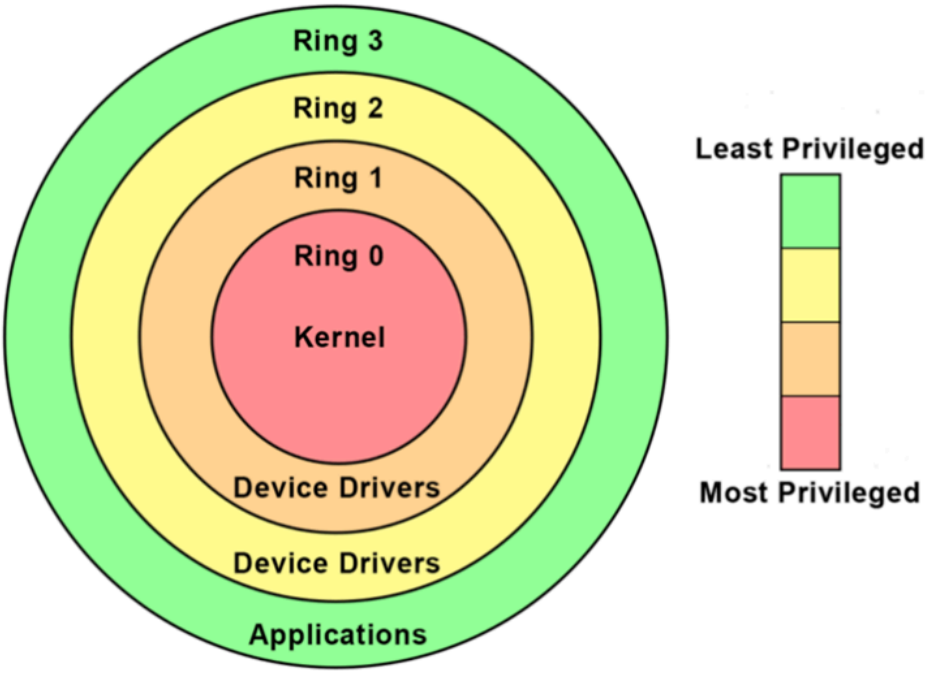
21. Ellis (n 8).

22. '/Dev/Null: Anti-Cheat Kernel Driver' (n 9).

23. 'Riot Requires Kernel Level Anti-Cheat Software' (*Tuta*) <https://tuta.com/blog/riot-requires-kernel-level-anticheat> accessed 24 March 2025.

24. Ibid.

Figure 2: What is user mode?[25]



User mode is the least privileged environment in an operating system where applications like browsers, WinRAR, and games run.[26] In user mode, apps can't access system resources directly and must use the OS's APIs to interact with other processes or memory. Kernel mode, however, is even deeper than that.

Unlike Riot's continuous, 'always-on' anti-cheat mechanism, Epic's Easy Anti-Cheat and BattlEye only activate while the user is actively engaged in the game.[27] This design choice offers several advantages. First, it alleviates users' concerns about constant surveillance and the potential privacy implications of persistent kernel-level access. Second, it introduces an additional layer of security. If Vanguard were to be compromised, all machines running the software, regardless of whether they are in use, could be vulnerable to exploits.

---

25. '/Dev/Null: Anti-Cheat Kernel Driver' (n 9).

26. Ibid.

27. 'Riot Requires Kernel Level Anti-Cheat Software' (n 23).

To illustrate the dangers further, online gaming applications, companies, and websites are inherently targeted for cyber-attacks, resulting in theft of personal and financial information. Examples include the Easy Anti-Cheat hack, an obvious disaster when Apex Legends user accounts were hijacked live during a grand-final tournament;[28] the Extended Copy Protection (XCP) from Sony, where bad actors compromised affected systems;[29] the backdoor vulnerability introduced by Street Fighter 5's kernel level anti-cheat.[30] In 2022, a ransomware developer also took advantage of Genshin Impact's kernel level anti-cheat to disable antivirus processes.[31];[32] However, the additional threat of companies performing unethical practices still exists. Take the ESEA case for

28. Andy Chalk published, 'Easy Anti-Cheat Washes Its Hands of the Apex Legends Hacking Disaster That Saw Streamer Accounts Hijacked Live: "There Is No RCE Vulnerability within EAC"' (*PC Gamer,* 18 March 2024) <https://www.pcgamer.com/games/battle-royale/easy-anti-cheat-washes-its-hands-of-the-apex-legends-hacking-disaster-that-saw-streamer-accounts-hijacked-live-there-is-no-rce-vulnerability-within-eac/> accessed 25 March 2025.

29. 'When Sony BMG Exposed Millions To Malware Attacks and Why' <https://www.onsecurity.io/blog/when-sony-bmg-exposed-millions-to-malware-attacks/> accessed 25 March 2025.

30. Chris Williams, 'Double KO! Capcom's Street Fighter V Installs Hidden Rootkit on PCs' (*The Register,* 23 September 2016) <https://www.theregister.com/2016/09/23/capcom_street_fighter_v/> accessed 25 March 2025.

31. Published (n 11).

32. 'Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus' (*Trend Micro*, 24 August 2022) <https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html> accessed 25 March 2025.

example and their hidden Bitcoin mining enslaver.[33];[34] Albeit the need for cybersecurity measures in gaming industry,[35] the high value of personal data and the fact that they are prime targets for malicious actors seeking to acquire and exploit it for financial gain or other nefarious purposes renders them a risk.

2.2. Personal Data at the Centre of Monetization

Personal data[36] is 'information relating to an identified or identifiable natural person' which includes, but is not limited to, pseudonyms, location, contact information, payment details, and any personal data shared within chat systems.[37] They can also be classified as sensitive data in accordance with recital 51 of the General Data Protection Regulation (GDPR) as they refer to information that reveals patterns of behaviour, biometric information, religious beliefs, and health conditions of individuals. Regarding the context of video

33. Jack Clark in San Francisco, 'Gaming Co ESEA Hit by m Fine for Hidden Bitcoin Mining Enslaver' (*The Register,* 20 November 2013) <https://www.theregister.com/2013/11/20/esea_gaming_bitcoin_fine/> accessed 25 March 2025.

34. Robert McMillan, 'Gaming Company Fined M for Turning Customers Into Secret Bitcoin Army' (*Wired)* <https://www.wired.com/2013/11/e-sports/> accessed 25 March 2025.

35. Amir Raz, 'Gaming Industry: The Need For Cyber Security' (*Coralogix*, 13 December 2022) <https://coralogix.com/blog/gaming-need-cyber-security/> accessed 25 March 2025.

36. 'Art. 4(1) GDPR – Definitions – General Data Protection Regulation (GDPR)' –*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

37. Wardyński & Partners – Karolina Romanowska, 'What Does Your Video Game Know about You? Data Processed by the Gaming Industry' (*Lexology*, 6 August 2021) <https://www.lexology.com/library/detail.aspx?g=9170c73a-7104-4212-9e63-13c181e95d78> accessed 24 March 2025.

games, such information can consist of, but not limited to, avatar names, chat logs, and telemetry data. Of particular significance, in game data is telemetry data and metrics derived thereof. While telemetry captures raw data on users actions, such as every button press and mouse movements, behavioural telemetry focuses on the real-time collection and analysis of users actions and decision-making during gameplay.[38] Behavioural telemetry and gameplay metrics can be considered biometric under the GDPR.[39] The science behind game data incorporates big data and AI analysis, but also psychology, sociology, and design.[40] Accordingly, derogations on the general prohibition for processing special categories must be explicitly provided unless 'explicit consent' is given.[41] The privacy policy of Microsoft's Blizzard below provides an illustrative example. Notably, Riot Games maintains similar provisions in its own privacy framework. Specifically, point 5 of the information-sharing section within Blizzard Entertainment's privacy policy is depicted highlighting the vagueness and confusion in the figures provided below.

Figure 3: Blizzard privacy Policy[42]

38. Fatih Talha Boyraz, 'It Is Not Just a Click: Protection of in-Game Behaviour Data as Biometric Data under the GDPR' (2024) 7 Interactive Entertainment Law Review 12.

39. Ibid 12.

40. Ibid.

41. 'Recital 51 – Protecting Sensitive Personal Data' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/recitals/no-51/> accessed 26 March 2025.

42. 'Blizzard Entertainment Privacy Policy – Legal – Blizzard Entertainment' <https://www.blizzard.com/en-sg/legal/8c41e7e6-0b61-42c4-a674-c91d8e8d68d3/blizzard-entertainment-privacy-policy> accessed 26 March 2025.

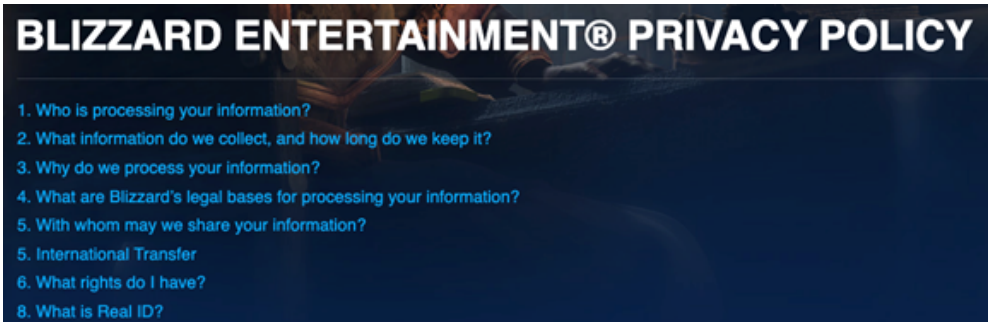


Figure 4: Point 5. With whom may we share your information?[43]

1. With partners and service providers. Blizzard may provide information to its vendors, consultants, marketing partners, research firms and other service providers or business partners. For example, we may provide information to such parties to help facilitate event ticket sales, conduct surveys on our behalf and process payments for our products and/or games. We share some of our players' game data with our community of developers, who create applications and websites that benefit our player community. You may opt out of having your game data included in this program by opting out of game-data sharing in the Privacy section of your Battle.net account.

The processing of this personal data serves various purposes, such as managing relationships with the user base through updates, facilitating in-game communication via chat systems, implementing anti-cheat mechanisms, and, notably, enabling game monetization through advertisements and in-app purchases. The privacy policy stipulates an ex-post opt out mechanism for sharing of game-data with other firms. However, fails to mention data that has already been shared. Additionally, there exists a lack of transparency and explicit consent granted for the processing of personal data for other purposes such as profile building.[44] A data collection assessment in section 3 reveals the extent of data collection.

Game companies face the challenge of balancing the interests of the user base, such as implementing anti-cheat mechanisms with the processing of personal data. As video games evolve and process more data points, the incentives to improve game mechanics to maintain user interest and improve monetizing schemes increases. Mobile games for example do not require a dedicated

43. Ibid.

44. *'Art. 4(4) GDPR – Definitions – General Data Protection Regulation (GDPR)', 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

device to allow for play and most of us carry one with us daily. Such games cater to a larger portion of the population and usually follow the 'freemium' economic models where the game itself is free of charge, but users can pay for additional features within the game.[45] Mainly regulated by app-stores, users have access to replicas of puzzles, board games, simulations (such as farming, building, dating), and strategy games.[46] These games rely on in-game advertisements and the purchasing of in-game features or items. Such monetization mechanisms rely on processing of personal data to remain profitable, whether it's a targeted advertisement or marketing features user's desire. For mobile games, the GDPR applies to operations of data processing when sold within the European Union (EU). However, much of the observation EU data protection authorities apply are targeted at the processing of data for advertising purposes. Thus far, the collection of data to sell to third parties continues, and there is an evident lack of scrutiny on the data that is used for other purposes.[47]

There are benefits to research and data collection in gaming. It prevents hacking or cheating in games, improving experience. It can enhance health education such as Fooya, a mobile game that implements implicit learning into

45. Magalie Dansac Le Clerc Preux Marlyse Lissan, Antoine, 'Key Tech Law Trends in Video Gaming | Part 1: Awareness of Data Privacy Challenges and the Importance of Cybersecurity Strategy' (*Connect On Tech*, 22 May 2023) <https://connectontech.bakermckenzie.com/
key-tech-law-trends-in-video-gaming-part-1-awareness-of-data-privacy-challenges-and-the-importance-of-cybersecurity-strategy/> accessed 24 March 2025.

46. Ibid.

47. Dragana Martinovic and others, 'You Are What You Play: Breaching Privacy and Identifying Users in Online Gaming', *2014 Twelfth Annual International Conference on Privacy, Security and Trust* (IEEE 2014) 37 <http://ieeexplore.ieee.org/document/6890921/> accessed 24 March 2025.

its gameplay mechanic.[48] It can be a facilitator of cognitive development[49], social and community building, and mental health.[50] In light of our lives increasingly becoming digital, the fabric of contemporary culture is undergoing a transformation. This shift is characterised by the pervasive integration of digital technologies into nearly every aspect of human existence, from communication and commerce to entertainment and education.

The advent of the internet, social media, and mobile devices has redefined how we interact, spend time, and express ourselves. In today's media and entertainment landscape, our daily routines are increasingly structured around screen time and the information economy.[51] After a day of work, many return home to immerse themselves in television shows, streaming services like Netflix, or video games. The current consumption landscape is dominated by algorithms tailoring content to individual preferences, creating personalised experiences that keep viewers and users engaged.

Consequently, the entertainment industry is not confined to traditional broadcast models any longer; instead, they leverage biometric data analytics to understand consumer behaviour and optimize content and its delivery. This data-driven approach allows for the creation of personalized recommendations, and targeted content updates.[52] As a result, consumers are presented with a continuous stream of new and engaging material, reinforcing the cycle of consumption and driving further investment in digital entertainment.

Modern technologies allow these sorts of data to reveal personal infor-

48. Raphael Jeong Hin Chin and Rahul Ladhania, 'Enhancing Health Education Through AI-Enabled Game'.

49. CS Green and D Bavelier, 'Learning, Attentional Control, and Action Video Games' (2012) 22 Current Biology R197.

50. Andrew K Przybylski, C Scott Rigby and Richard M Ryan, 'A Motivational Model of Video Game Engagement' (2010) 14 Review of General Psychology 154.

51. Mayer-Schönberger and Cukier (n 20) 16.

52. Albérico Travassos Rosário and Joana Carmo Dias, 'How Has Data-Driven Marketing Evolved: Challenges and Opportunities with Emerging Technologies' (2023) 3 International Journal of Information Management Data Insights 100203.

mation.[53] As such, data points are collected, sold, and transferred to other entities through corporate mergers and acquisitions; in addition, they are concentrated in different ways that may create opportunities for abuse and deanonymization (e.g., to target potential customers).[54]

3. Type of Data Collected and Behavioural Telemetry as Biometric Information

3.1. Scope and Definitions

Biometric data is personal data resulting from technical processing of physical, physiological, or behavioural characteristics that uniquely identifies an individual.[55] This allows the processor to confirm the unique identification of a natural person.

Behavioural telemetry as biometric information is real-time collection and analysis of user actions and decisions during gameplay. This includes inferences about a user's biometric identity, age, gender, personality traits, interests, skills, emotions, consumption habits, and other behavioural characteristics.[56] In fact, it may qualify as data concerning health under the definition of article 4(15) GDPR.[57] An example is Google's patent for game ads

53. Boyraz (n 38).

54. Martinovic and others (n 47) 37.

55. 'Art. 4(14) GDPR – Definitions – General Data Protection Regulation (GDPR)', *'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*.

56. Jacob Leon Kröger and others, 'Surveilling the Gamers: Privacy Impacts of the Video Game Industry' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3881279> accessed 24 March 2025.

57. 'Art. 4(15) GDPR – Definitions – General Data Protection Regulation (GDPR)', *'data concerning health' means personal data related to the physical or mental health of a natural*

which evaluate user actions.[58] As a consequence, identification of users psychographic profiles and behavioural traits can reveal information such as kindness, leadership, defeatism, infidelity, and punctuality.[59]

Furthermore, the integration of social media accounts into gaming platforms increases the risk, as users often grant access to their personal profiles without fully understanding the extent of the data being shared.[60] Cybercriminals can exploit even minimal stolen information, such as login credentials, to significantly effect to one's personal life. Many popular games permit users to log in or integrate their social network accounts, however, these platforms frequently obscure the scope of data collected during such integrations.[61] Legal frameworks governing privacy are often written in opaque jargon, which effectively masks the data processing activities of gaming companies.[62] Therefore, in the current geopolitical climate, it is important to understand how game data can be utilised.

3.2. Extent of Data Collected

Modern gaming systems record all user interactions in timestamped logs, capturing a history of actions and player events, including details like duration,

---

person, including the provision of health care services, which reveal information about his or her health status.

58. Nate Anderson, 'Google Patent for Game Ads Evaluates User Actions, Psychology' (*Ars Technica*, 15 May 2007) <https://arstechnica.com/uncategorized/2007/05/google-patent-for-game-ads-evaluates-user-actions-psychology/> accessed 26 March 2025.

59. Boyraz (n 38) 16.

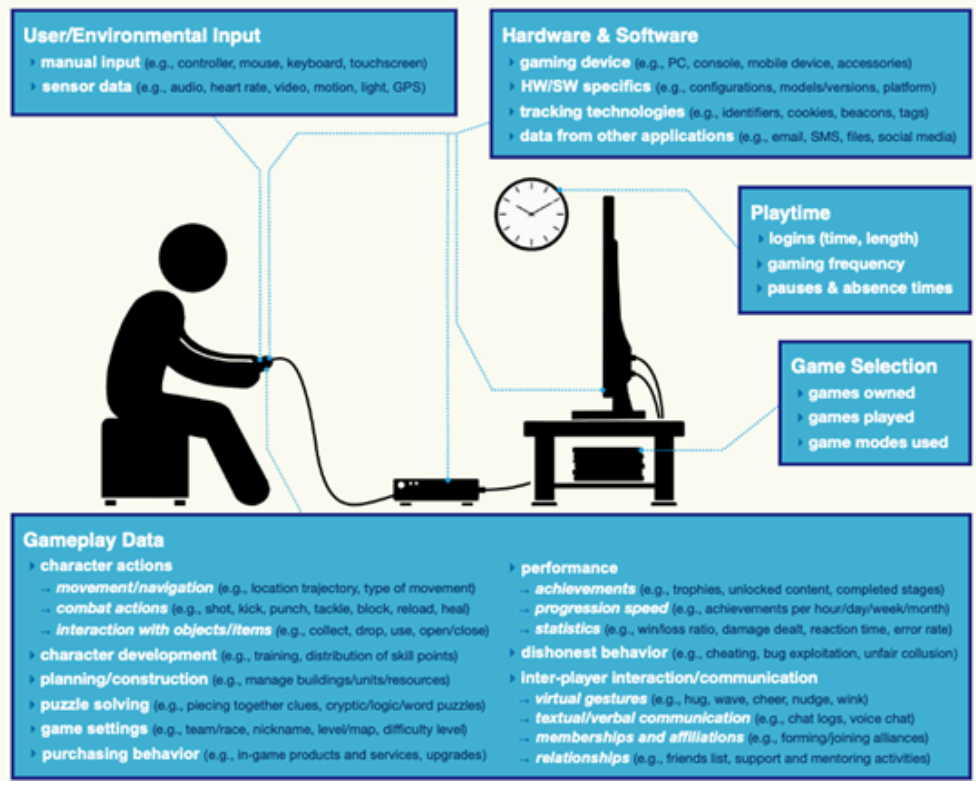
60. amlegals, 'Data Privacy Laws: Implications for the Online Gaming Industry' (*Law Firm in Ahmedabad*, 19 June 2024) <https://amlegals.com/data-privacy-laws-implications-for-the-online-gaming-industry/> accessed 24 March 2025.

61. Ibid.

62. Kröger and others (n 56) 14.

frequency, and accuracy of in-game actions.[63] These systems use a variety of sensors to track additional data, such as voice, gestures, heart rate, facial expressions, and location.[64] Furthermore, gaming systems often collect information about a user's hardware and software setup, as well as access data from other applications and social media profiles, using tracking technologies like identifiers and cookies.[65] Hence, inference of personal information from gameplay data, evident in the figure below on the classification of data types.

Figure 5: A classification of data types commonly collected by video games[66]



63. ibid 3.

64. ibid.

65. Ibid.

66. Ibid 4.

The metrics captured depend on the game type and its business model, but there is a growing trend toward more sophisticated video games, leading to a greater variety of data collected.[67] The tracking and profiling of anonymous users can be exploited. Thus, a company's ability to link gameplay behaviour to a user's real identity significantly increases the potential for data misuse.[68]

Behavioural patterns in interacting with a game can provide insights into a user's degree of engagement[69] and level of motivation[70], as well as emotional states, including emotional arousal and the valence of emotions (positive, negative, and neutral).[71] These patterns also reveal more specific affective states such as fun, frustration, and feelings of challenge[72], as well as complex emotions like distress, pride, shame, admiration, and reproach.[73] Additionally, they

67. Ibid 4.

68. D. Martinovic, V. Ralevich, J. McDougall, M. Perklin, "You Are What You Play": Breaching Privacy and Identifying Users in Online Gaming, in: 2014 Twelfth Annual International Conference on Privacy, Security and Trust, IEEE, Toronto, 2014, Pp. 31–39. URL: Https://Doi.Org/10.1109/PST. 2014.6890921.

69. I. Ghergulescu, C. H. Muntean, Measurement and Analysis of Learner's Motivation in Game-Based E-Learning, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives, Springer, New York, NY, 2012, Pp. 355–378. URL: Https://Doi.Org/10.1007/978-1-4614-3546-4_18.

70. E. E. Mattheiss, M. D. Kickmeier-Rust, C. M. Steiner, D. Albert, Approaches to Detect Discouraged Learners: Assessment of Motivation in Educational Computer Games, in: Proceedings of eLearning Baltics (eLBa), Rostock, 2010, Pp. 1–10.

71. Kröger and others (n 56).

72. N. Shaker, G. Yannakakis, J. Togelius, Towards Automatic Personalized Content Generation for Platform Games, in: 6th AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, AIIDE, Stanford, CA, 2010, Pp. 63–68.

73. J. Sabourin, B. Mott, J. C. Lester, Modeling Learner Affect with Theoretically Grounded Dynamic Bayesian Networks, in: S. D'Mello, A. Graesser, B. Schuller, J.-C. Martin (Eds.), Affective Computing and Intelligent Interaction, Volume 6974, Springer, Berlin, 2011,

can indicate anticipatory emotions such as joy, hope, anxiety, and anticipatory relief, along with hopelessness.[74] Cognitive states such as focus, curiosity, and confusion[75], as well as broader experiences like disappointment, boredom, interest, confidence, and satisfaction[76], are also reflected in such patterns.

Gameplay data can then be leveraged to assess a variety of skills, including teamwork, language proficiency, financial acumen, math fluency, information and communication technology (ICT) skills, creative problem-solving, spatial navigation, fine motor skills, metacognition, systems thinking, memory retention, cultural knowledge, and comprehension of specific scientific concepts.[77] Additionally, game-based assessment approaches facilitate the tracking of cognitive development and learning trajectories over time, allowing for the identification of knowledge gaps and learning difficulties, such as reading problems.[78] These methods evaluate a broad spectrum of abilities and monitoring, thereby providing insights into both individual skill sets. To exemplify the privacy implications, a paper by Jacob Leon Kröger focused on three sensor types that are increasingly found in modern gaming devices, showcasing an overview of sensitive inferences.

Pp. 286–295. URL: Https: //Doi.Org/10.1007/978-3-642-24600-5_32, Series Title: Lecture Notes in Computer Science.'

74. 'K. Mun˜oz, P. M. Kevitt, T. Lunney, J. Noguez, L. Neri, An Emotional Student Model for Game-Play Adaptation, Entertainment Computing 2 (2011) 133–141. URL: Https://Doi.Org/10.1016/j.Entcom.2010.12.006.

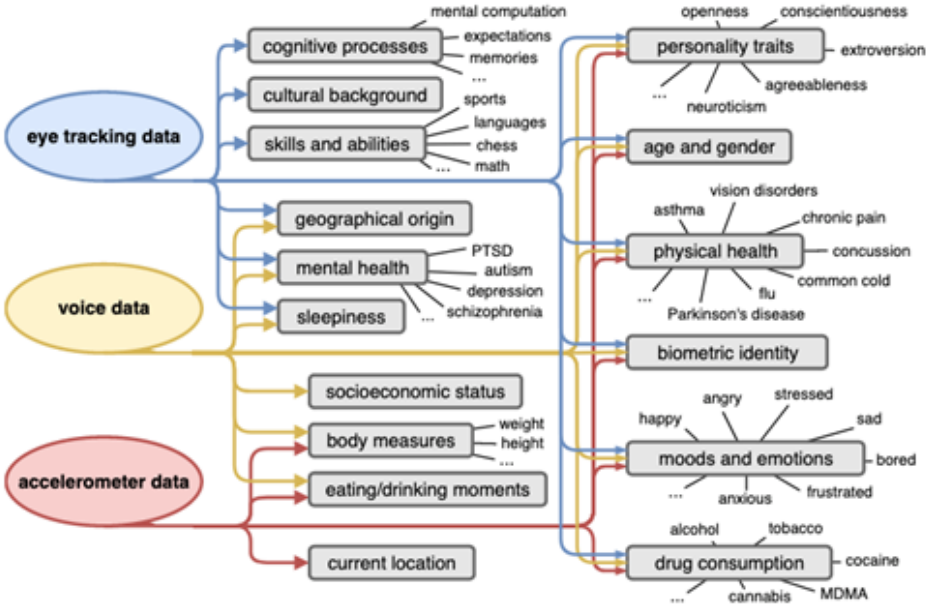
75. J. Sabourin, B. Mott, J. C. Lester, Modeling Learner Affect with Theoretically Grounded Dynamic Bayesian Networks, in: S. D'Mello, A. Graesser, B. Schuller, J.-C. Martin (Eds.), Affective Computing and Intelligent Interaction, Volume 6974, Springer, Berlin, 2011, Pp. 286–295. URL: Https: //Doi.Org/10.1007/978-3-642-24600-5_32, Series Title: Lecture Notes in Computer Science. (n 73).

76. E. E. Mattheiss, M. D. Kickmeier-Rust, C. M. Steiner, D. Albert, Approaches to Detect Discouraged Learners: Assessment of Motivation in Educational Computer Games, in: Proceedings of eLearning Baltics (eLBa), Rostock, 2010, Pp. 1–10. (n 70).

77. Kröger and others (n 56) 7.

78. Ibid.

Figure 6. Overview of sensitive inferences that can be drawn from eye-tracking data, voice recordings, and accelerometer data.[79]



Another example is a patented profiling method analyses play traces to assess whether a user is frugal (e.g., saving in-game money despite attractive spending options), fiscally responsible (e.g., making careful investments and prioritizing strategic purchases), or wasteful (e.g., taking financial risks and spending money impulsively on irrelevant items).[80] This method evaluates the 'trading-consciousness', of users thereby indicating their suitability for financial trading products, and detects an eagerness to explore new products or services based on how they develop their in-game characters.

An example of two primary goals of mining gaming data is the ability to iden-

79. Ibid 11.

80. E. J. Landers, B. G. Chun, S. B. Martin, M. H. Chang, A. Rao, T. H. Nguyen, D. S. Pelton, Utilizing Gaming Behavior to Evaluate Player Traits, 2019. URL: Https://Patents.Google.Com/Patent/US10357713B1/En.

tify groups of users with shared traits and to analyze specific users.[81] Through gameplay data or user equipment specifications, several personality traits can be inferred, including:

1. Financial status, based on the type of hardware owned.
2. Age, estimated from the timing of hardware purchases.
3. Leadership inclination, determined by whether the user leads or follows.
4. Geographical location, deduced from IP addresses and time zones.
5. Offensive or defensive tendencies, indicated by where the user dies—within their own sector (defensive) or in the opponent's (offensive).
6. Addictive behaviour, evidenced by playing more than 10 hours daily.
7. Defeatist attitude, gauged by the frequency of resignation attempts.

These insights help understand user behaviour and preferences. The breadth of data collected through gaming extends to a diverse set of personal and behavioural information, which can be utilised for various purposes, such as surveillance.

> *'Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.'*
>
> — Shoshana Zuboff, The Age of Surveillance Capitalism[82]

3.3. Legal Implications

Gaming platforms are controllers of personal data, which are stored, and processed as part of the platform's operational framework.[83] Thus, under article 32 GDPR, they need to implement appropriate technical and organizational measures to ensure an appropriate level of security that corresponds to the

81. Martinovic and others (n 47) 35.

82. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power – Zuboff, Shoshana* (2018) <http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019> accessed 26 March 2025.

83. 'Art. 24 GDPR – Responsibility of the Controller' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-24-gdpr/> accessed 26 March 2025.

risk.[84] Especially since users usually ignore the sale of data to third parties and write it off as insignificant, however, the nature of gaming data is to profile users.[85] Therefore, there is a need to adequately apply data protection laws to gaming to protect users is needed. The scope of application on that front, entails the application of Article 9(1) of the GDPR applies exclusively to biometric data when such data is used for the purpose of identification, rather than for verification or authentication.[86] Additionally, under the AI Act, AI systems designed for biometric categorization based on sensitive attributes or characteristics refer to Article 9(1) of the GDPR. As such, using biometric data shall be categorized as high-risk.[87] The classification implies heightened legal responsibilities for gaming companies, triggering risk-based provisions within the GDPR.

Users have gained more rights through the GDPR, such as the right to delete, update, access, and control personal data. As we have concluded, gaming data are classified as (high risk) biometric and health data. Therefore, an analysis of the GDPR principles is warranted, namely the principles of processing (article 5 GDPR) and the lawfulness of processing (under Article 6 GDPR) in line with the necessary impact assessments.

The AI Act introduces new impact assessment methods, such as the Fundamental Rights Impact Assessment (FRIA), which complements the Data Protection Impact Assessment (DPIA) under the GDPR. While DPIAs are mandatory for high-risk data processing involving health data, FRIAs focus on AI systems

84. 'Art. 32 GDPR – Security of Processing' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-32-gdpr/> accessed 26 March 2025.

85. AXEL, 'How Concerned Are Consumers Really When It Comes to Data Privacy?' (*Medium*, 28 August 2018) <https://medium.com/@AxelUnlimited/how-concerned-are-consumers-really-when-it-comes-to-data-privacy-21c4587ddc5c> accessed 26 March 2025.

86. 'Art. 9 GDPR – Processing of Special Categories of Personal Data' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-9-gdpr/> accessed 26 March 2025.

87. 'Recital 54 | EU Artificial Intelligence Act' <https://artificialintelligenceact.eu/recital/54/> accessed 26 March 2025.

classified as high-risk.[88] Gaming data processing relies on machine learning or AI based systems.[89] If a FRIA includes a DPIA[90], organizations do not need to conduct both assessments separately.[91] The AI Act also mandates additional safeguards, such as transparency obligations, human oversight, and risk management frameworks, to address AI-driven technologies. Enforcement presents challenges; however, ensuring that game data is retained only for a limited time before deletion can be a solution. Automatic ex-ante opt-out requirements and synthetic data generation are proposed solutions to address these issues. Considering the definition of default under the guidance of the European Data Protection guidelines 'refers to the preselected value of a configurable setting that is assigned to a software application'.[92]

The AI Act introduces a regulatory challenge in biometric identification. Article 2(7) of the AI Act references the GDPR with two exceptions: Article 10 (sensitive data) and Article 59 (explicit request for DPIA during sandbox experimentation). The AI Act may dilute GDPR protections. Recital 26 emphasizes a risk-based approach, prioritising harm prevention over individual privacy. Under the GDPR, the use of biometric identification must comply with strict legal requirements, including obtaining explicit consent for sensitive data processing. Potential biometric identification poses additional concerns about privacy, necessitating transparent safeguards.

---

88. 'Article 6: Classification Rules for High-Risk AI Systems | EU Artificial Intelligence Act' <https://artificialintelligenceact.eu/article/6/> accessed 26 March 2025.

89. Boyraz (n 38) 20.

90. 'Art. 35 GDPR – Data Protection Impact Assessment' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-35-gdpr/> accessed 26 March 2025.

91. 'Article 27: Fundamental Rights Impact Assessment for High-Risk AI Systems | EU Artificial Intelligence Act' 27 <https://artificialintelligenceact.eu/article/27/> accessed 26 March 2025.

92. 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020' <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 26 March 2025.

In terms of competition, digital companies operate on data collection and monetization, therefore it would be remiss to exclude the potential for anti-competitive effects and reduction in consumer welfare if data pooling and was not considered. Transparency serves as a safeguard and allows users to know how data is being processed.[93] However, the information asymmetry thereof is so large that it remains difficult for consumers to make informed decisions.[94] Network effects exist in the world of gaming, as on an individual level gamers are incentivised to stay with a game or service through ecosystems, game addictiveness and incentivization's, or targeted recommendations. Users therefore face a form of locking in where sister services have preferential treatment over competitors. Such data ecosystems are where data-driven companies gain their market power.[95] The result is a strong network effects of data allowing for more analysis on individuals and generate user retention. It is beyond the scope of this paper to delve into analysis of market power. However, evidence shows that merger oversight in the past has not always accounted for data driven market power. As a result, data pooling has driven technology corporations to absorb gaming companies in part to pool more data points.[96] Thus, effective competition can be held back by disguised sources of market power.

4. Conclusions

In this papers view, as companies increasingly invest in multiple platforms and sectors simultaneously, the need for clear boundaries between these data domains becomes necessary. For instance, a company that operates in gaming, social media, and advertising must ensure that data collected for one purpose,

93. Peter van de Waerdt, *Data Is Power: On the Fundamental Connections between Data Protection Law and Competition Law as Applied to the Digital Market* (University of Groningen 2024) 19.

94. Ibid 73.

95. Ibid 119.

96. Ibid 120.

such as gaming, is not repurposed for another, such as targeted advertising outside the industry and profiling.

This reflects a broader concern about maintaining the integrity of data usage across different businesses, which aligns with principles of 'data protection by design and default.'[97] This mandates that data protection considerations must be integrated into the design and development phases of any system or process that processes personal data. This principle is needed to ensure compliance with GDPR requirements from the outset, rather than addressing privacy concerns as an afterthought. The possibility for an ex-post opt-out mechanism risks diluting the protections intended by the GDPR, shifting from a rights-based approach to a more risk-based one, particularly in the development of AI systems. Such a shift can undermine the compliance required by design and default, potentially weakening user privacy safeguards.

Additionally, by focusing on the importance of building walls between gaming platforms and other sectors, gaming companies can avoid risks associated with data misuse, leaks, and improve user trust. This approach is particularly relevant considering privacy policy's such as Blizzard's. Digital companies in the gaming industry rely heavily on data collection and monetization, which raises issues on anti-competitive effects and potential harm to consumer welfare. While transparency is essential for safeguarding user rights by informing them about how their data is processed, the vast information asymmetry makes it challenging for consumers to make fully informed decisions. Network effects further exacerbate this issue as data ecosystems play a central role in enabling them. This permits companies to gain significant market power through extensive data analysis and user retention strategies. Although this paper does not analyse market power in depth, evidence suggests that past merger oversight has often failed to account for the dynamics of data-driven market power. As a result, large technology corporations have increasingly acquired gaming companies to pool more data points, potentially stifling competition by leveraging disguised sources of market power.

97. 'Art. 25 GDPR – Data Protection by Design and by Default' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-25-gdpr/> accessed 26 March 2025.

Bibliography:

amlegals, 'Data Privacy Laws: Implications for the Online Gaming Industry' (*Law Firm in Ahmedabad*, 19 June 2024) <https://amlegals.com/data-privacy-laws-implications-for-the-online-gaming-industry/> accessed 24 March 2025

Anderson N, 'Google Patent for Game Ads Evaluates User Actions, Psychology' (*Ars Technica*, 15 May 2007) <https://arstechnica.com/uncategorized/2007/05/google-patent-for-game-ads-evaluates-user-actions-psychology/> accessed 26 March 2025

'Art. 4 GDPR – Definitions – General Data Protection Regulation (GDPR)' <https://gdpr-info.eu/art-4-gdpr/> accessed 26 March 2025

'Art. 9 GDPR – Processing of Special Categories of Personal Data' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-9-gdpr/> accessed 26 March 2025

'Art. 24 GDPR – Responsibility of the Controller' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-24-gdpr/> accessed 26 March 2025

'Art. 25 GDPR – Data Protection by Design and by Default' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-25-gdpr/> accessed 26 March 2025

'Art. 32 GDPR – Security of Processing' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-32-gdpr/> accessed 26 March 2025

'Art. 35 GDPR – Data Protection Impact Assessment' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-35-gdpr/> accessed 26 March 2025

'Article 6: Classification Rules for High-Risk AI Systems | EU Artificial Intelligence Act' <https://artificialintelligenceact.eu/article/6/> accessed 26 March 2025

'Article 27: Fundamental Rights Impact Assessment for High-Risk AI Systems | EU Artificial Intelligence Act' <https://artificialintelligenceact.eu/article/27/> accessed 26 March 2025

AXEL, 'How Concerned Are Consumers Really When It Comes to Data Privacy?' (*Medium*, 28 August 2018) <https://medium.com/@AxelUnlimited/how-concerned-are-consumers-really-when-it-comes-to-data-privacy-21c4587ddc5c> accessed 26 March 2025

'Blizzard Entertainment Privacy Policy – Legal – Blizzard Entertainment' <https://www.blizzard.com/en-sg/legal/8c41e7e6-0b61-42c4-a674-c91d8e8d68d3/blizzard-entertainment-privacy-policy> accessed 26 March 2025

Boyraz FT, 'It Is Not Just a Click: Protection of in-Game Behaviour Data as Biometric Data under the GDPR' (2024) 7 Interactive Entertainment Law Review 12

'Britannica Money' (23 March 2025) <https://www.britannica.com/money/Tencent> accessed 24 March 2025

Center MN, 'Microsoft to Acquire Activision Blizzard to Bring the Joy and Community of Gaming to Everyone, across Every Device' (*Stories*, 18 January 2022) <https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/> accessed 24 March 2025

Chin RJH and Ladhania R, 'Enhancing Health Education Through AI-Enabled Game'

'D. Martinovic, V. Ralevich, J. McDougall, M. Perklin, "You Are What You Play": Breaching Privacy and Identifying Users in Online Gaming, in: 2014 Twelfth Annual International Conference on Privacy, Security and Trust, IEEE, Toronto, 2014, Pp. 31–39. URL: Https://Doi.Org/10.1109/PST.2014.6890921'

'/Dev/Null: Anti-Cheat Kernel Driver' (3 February 2020) <https://www.leagueoflegends.com/en-us/news/dev/dev-null-anti-cheat-kernel-driver/> accessed 24 March 2025

'E. E. Mattheiss, M. D. Kickmeier-Rust, C. M. Steiner, D. Albert, Approaches to Detect Discouraged Learners: Assessment of Motivation in Educational Computer Games, in: Proceedings of eLearning Baltics (eLBa), Rostock, 2010, Pp. 1–10.'

'E. J. Landers, B. G. Chun, S. B. Martin, M. H. Chang, A. Rao, T. H. Nguyen, D. S. Pelton, Utilizing Gaming Behavior to Evaluate Player Traits, 2019. URL: https://Patents.Google.Com/Patent/US10357713B1/En.'

Ellis N, 'What Is Anti-Cheat? Online Gaming and Security Risks | Schellman' (*Schellman Compliance*) <https://www.schellman.com/blog/cybersecurity/what-is-anti-cheat> accessed 24 March 2025

Ferdinand PK, 'Tencent Branded a Chinese Military Company by US Government' (*Game Rant*, 8 January 2025) <https://gamerant.com/tencent-chinese-military-company-list-us-government/> accessed 24 March 2025

Francisco JC in S, 'Gaming Co ESEA Hit by $1m Fine for Hidden Bitcoin Mining Enslaver' <https://www.theregister.com/2013/11/20/esea_gaming_bitcoin_fine/> accessed 25 March 2025

'Game Changer: Accelerating the Media Industry's Most Dynamic Sector' (*BCG Global*, 7 June 2023) <https://www.bcg.com/publications/2023/drivers-of-global-gaming-industry-growth> accessed 24 March 2025

Gaphty C, 'The Impact of U.S. Designation of Tencent as a Chinese Military Company on Local and State Governments' (*Critical Path Security*, 13 January 2025) <https://www.criticalpathsecurity.com/the-impact-of-u-s-designation-of-tencent-as-a-chinese-military-company-on-local-and-state-governments/> accessed 25 March 2025

'Global Games Market Outlook: Key Growth Drivers and Challenges for 2025-2027' (*Newzoo*, 6 March 2025) <https://newzoo.com/resources/blog/global-games-market-update-q1-2025> accessed 24 March 2025

Green CS and Bavelier D, 'Learning, Attentional Control, and Action Video Games' (2012) 22 Current Biology R197

'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020' <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> accessed 26 March 2025

Hernandez AD, 'Cambridge Analytica: Military Psy-Ops Privatized'

'How Microsoft's Activision Blizzard Deal Is Transformative' (*Knowledge at Wharton*) <https://knowledge.wharton.upenn.edu/article/how-microsofts-buy-of-activision-blizzard-is-transformative/> accessed 24 March 2025

'I. Ghergulescu, C. H. Muntean, Measurement and Analysis of Learner's Motivation in Game-Based E-Learning, in: D. Ifenthaler, D. Eseryel, X. Ge (Eds.), Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives, Springer, New York, NY, 2012, Pp. 355–378. URL: Https://Doi.Org/10.1007/978-1-4614-3546-4_18.'

'J. Sabourin, B. Mott, J. C. Lester, Modeling Learner Affect with Theoretically Grounded Dynamic Bayesian Networks, in: S. D'Mello, A. Graesser, B. Schuller, J.-C. Martin (Eds.), Affective Computing and Intelligent Interaction, Volume 6974, Springer, Berlin, 2011, Pp. 286–295. URL: Https://Doi.Org/10.1007/978-3-642-24600-5_32, Series Title: Lecture Notes in Computer Science.'

'K. Muñoz, P. M. Kevitt, T. Lunney, J. Noguez, L. Neri, An Emotional Student Model for Game-Play Adaptation, Entertainment Computing 2 (2011) 133–141. URL: Https://Doi.Org/10.1016/j.Entcom.2010.12.006.'

Kröger JL and others, 'Surveilling the Gamers: Privacy Impacts of the Video Game Industry' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3881279> accessed 24 March 2025

Martinovic D and others, 'You Are What You Play: Breaching Privacy and Identifying Users in Online Gaming', *2014 Twelfth Annual International Conference*

on Privacy, Security and Trust (IEEE 2014) <http://ieeexplore.ieee.org/document/6890921/> accessed 24 March 2025

Mayer-Schönberger V and Cukier K, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013)

McMillan R, 'Gaming Company Fined $1M for Turning Customers Into Secret Bitcoin Army' *Wired* <https://www.wired.com/2013/11/e-sports/> accessed 25 March 2025

'N. Shaker, G. Yannakakis, J. Togelius, Towards Automatic Personalized Content Generation for Platform Games, in: 6th AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, AIIDE, Stanford, CA, 2010, Pp. 63–68.'

nanda, 'Weapons-Grade Communication' (*Living my truth – A seeker's blog*, 25 July 2019) <https://livingmytruth.se/weapons-grade-communication/> accessed 24 March 2025

Noor P, 'There Are Plenty More like Cambridge Analytica. I Know – I've Used the Data' *The Guardian* (23 March 2018) <https://www.theguardian.com/commentisfree/2018/mar/23/plenty-more-like-cambridge-analytica-data-facebook> accessed 24 March 2025

Preux MDLC Marlyse Lissan, Antoine, 'Key Tech Law Trends in Video Gaming | Part 1: Awareness of Data Privacy Challenges and the Importance of Cybersecurity Strategy' (*Connect On Tech*, 22 May 2023) <https://connectontech.bakermckenzie.com/key-tech-law-trends-in-video-gaming-part-1-awareness-of-data-privacy-challenges-and-the-importance-of-cybersecurity-strategy/> accessed 24 March 2025

Przybylski AK, Rigby CS and Ryan RM, 'A Motivational Model of Video Game Engagement' (2010) 14 Review of General Psychology 154

published AC, 'Easy Anti-Cheat Washes Its Hands of the Apex Legends Hacking Disaster That Saw Streamer Accounts Hijacked Live: "There Is No RCE Vulnerability within EAC"' *PC Gamer* (18 March 2024) <https://www.pcgamer.com/games/battle-royale/easy-anti-cheat-washes-its-hands-of-the-apex-legends-hacking-disaster-that-saw-streamer-accounts-hijacked-live-there-is-no-rce-vulnerability-within-eac/> accessed 25 March 2025

published TL, 'According to Experts on Kernel Level Anticheat, Two Things Are Abundantly Clear: 1) It's Not Perfect and 2) It's Not Going Anywhere' *PC Gamer* (27 February 2024) <https://www.pcgamer.com/according-to-experts-

on-kernel-level-anticheat-two-things-are-abundantly-clear-1-its-not-perfect-and-2-its-not-going-anywhere/> accessed 25 March 2025

'Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus' (*Trend Micro*, 24 August 2022) <https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html> accessed 25 March 2025

Raz A, 'Gaming Industry: The Need For Cyber Security' (*Coralogix*, 13 December 2022) <https://coralogix.com/blog/gaming-need-cyber-security/> accessed 25 March 2025

'Recital 51 – Protecting Sensitive Personal Data' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/recitals/no-51/> accessed 26 March 2025

'Recital 54 | EU Artificial Intelligence Act' <https://artificialintelligenceact.eu/recital/54/> accessed 26 March 2025

'Riot Requires Kernel Level Anti-Cheat Software' (*Tuta*) <https://tuta.com/blog/riot-requires-kernel-level-anticheat> accessed 24 March 2025

Rosário AT and Dias JC, 'How Has Data-Driven Marketing Evolved: Challenges and Opportunities with Emerging Technologies' (2023) 3 International Journal of Information Management Data Insights 100203

Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power – Zuboff, Shoshana* (2018) <http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019> accessed 26 March 2025

'Tencent: US Designates the Firm a Chinese Military Company' (7 January 2025) <https://www.bbc.com/news/articles/c9q78wn9g8zo> accessed 24 March 2025

van de Waerdt P, *Data Is Power: On the Fundamental Connections between Data Protection Law and Competition Law as Applied to the Digital Market* (University of Groningen 2024)

Wardyński & Partners – Karolina Romanowska, 'What Does Your Video Game Know about You? Data Processed by the Gaming Industry' (*Lexology*, 6 August 2021) <https://www.lexology.com/library/detail.aspx?g=9170c73a-7104-4212-9e63-13c181e95d78> accessed 24 March 2025

'When Sony BMG Exposed Millions To Malware Attacks and Why' <https://www.onsecurity.io/blog/when-sony-bmg-exposed-millions-to-malware-attacks/> accessed 25 March 2025

'Why You Should Reconsider Playing League of Legends: The Risks of Kernel-

Level Anti-Cheat Software.Md' (*Gist*) <https://gist.github.com/stdNullPtr/2998eacb71ae925515360410af6f0a32> accessed 25 March 2025

Williams C, 'Double KO! Capcom's Street Fighter V Installs Hidden Rootkit on PCs' <https://www.theregister.com/2016/09/23/capcom_street_fighter_v/> accessed 25 March 2025

About the author

Willem Drapers

Willem Drapers completed the LLM in Technology Law and Innovation at the University of Groningen. He is currently working as in-house legal counsel for Momentum AI.

CHAPTER 5: AUTOMATED VEHICLES AND THE LAWFULNESS OF DATA PROCESSING UNDER ART. 6 GDPR

Maximilian Kloth

1. Introduction

Innovation brings new opportunities and challenges. In the past, inventions like light bulbs, ovens or, most impactful, cars were transformative; now, data-driven products are reshaping industries. Analogue products have been infused with data, enabling them to interconnect, interact and become 'livelier'. Especially in the case of road traffic, the term automated vehicle (AV) has become a symbol of data-driven innovation. This development has garnered attention from both the industry and European and national legislators. As of right now, the use of AV that keeps both the human in and out of control over the vehicle has been legalised at the European and national levels. The latter form, examined here, uses Artificial Intelligence (AI) to drive independently without any human intervention. AVs, as data-driven products, rely on vast amounts of data for their functioning, which is being collected by sensors, radars and GPS trackers. From a data protection perspective, this raises the question of how such excessive data reaping complies with the provisions of the GDPR.[1] Data is not only essential but also decisive for the functioning of a fully automated AV. To this end, GDPR conformity plays a significant role in the success of this innovation, considering the potential economic impact of potential liability for fines and penalties.[2] Considering also that the protection of per-

1. 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, and repealing Directive 95/46/EC.

2. Art. 83, 84 GDPR.

sonal data is only an extension of the guaranteed fundamental right of privacy, it is also important to scrutinise how to find a balance between the protection of fundamental rights and beneficial innovation.

Against this background, this paper scrutinises the GDPR conformity of AVs regarding data processing. Drawing from the GDPR's structure, it assesses first which type of personal data and from what data subject it's being collected (B.). Secondly, the question of processing shall be addressed (C.). Lastly, it analyses Article 6 GDPR (D.) Section E concludes the paper.

2. Categorisation of the Collected Data

The GDPR only applies to the processing of personal data, which is the first hinge of the door leading to the GDPR's application.[3] Such data is defined as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'.[4] The determining factor of the qualification of data as personal data is the possibility of identification, which leads to the reverse conclusion that de-personalised data does not fall under the GDPR's scope. The term identification refers to the data's origin from a natural person (data subject).

Therefore, in the case of AV, two questions must be distinguished: Does the AV de-personalise the collected data? (I.) And who is the data subject? (II.)

2.1. The Collected Data

Typically, AVs are equipped with different types of sensors (e.g. cameras, GPS, ranging sensors) for functioning.[5] Their specific purpose differs from creating

3. Ibid. Art. 2 (1).

4. Ibid. Art. 4 (1).

5. Ioannis Krontiris and others, 'Autonomous Vehicles: Data Protection and Ethical Consid-

a 3D real-life road map model, the categorisation of external objects into humans or obstacles, communication with other vehicles or the assessment of the driver's vital functions.[6] Such data can be roughly categorised into data about the vehicle and its passengers (internal data) and about vehicle-external entities (external data). Examples of internal data include data on the drivers and passengers like name, address, but also in-vehicle video and biometric data for the authentication of the driver (e.g., voice, fingerprint authentication) or his monitoring (e.g., image processing for fatigue detection), data on personal devices like MAC addresses, trip information, vehicle location data, vehicle identification number and vehicle-related data (model code, registration date).[7] On the other hand, external data contains data on license plates of surrounding vehicles, video recordings including identifying information like faces of pedestrians, bikers, sensor data from LIDAR, RADAR, etc. Such information involves other persons and data received from other vehicles (location, etc.).[8]

2.2. De-Personalising Data

Considering the vast amount of collected data, de-personalisation of such data plays a crucial role in ensuring the lawful and practical use of AVs.[9] This process can be achieved through various means. A common tool is anonymising or pseudonymising[10] data by altering it in such a way that re-identification becomes unlikely because the identifying data parts have been either removed

---

erations', *Proceedings of the 4th ACM Computer Science in Cars Symposium* (Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3385958.3430481> accessed 10 March 2025, 2. Data and actors defined.

6. Ibid.

7. Ibid.

8. Ibid.

9. Yao Xu and others, 'Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics' (2025) 16 World Electric Vehicle Journal 6, 9, 20.

10. This term is defined in Art. 4 (5) GDPR.

or covered by layering more information on it.[11] However, such processes are susceptible to the pitfalls of possible re-identification by re-using remotely saved personal data or combining external personal datasets.[12] A similar issue relates to the way so-called synthetic data is used. Such data is artificially created and solely copies the non-personal parameters of the data collected prior.[13] Also, in this case, the remains of personal data or the combination of different data sources may lead to the data's corruption. Therefore, the method of encrypted data processing tools (EDPS) seems promising, because in this case, the original data remains in its original form but is then encrypted for further use.[14] By doing so, the AV can compute and analyse the data without exposing personal information. This is especially of importance for data that contains information about human characteristics, such as the driver's monitoring data or pedestrian faces, because such factors allow easier re-identification. Additionally, external data is crucial for the AV's functioning, as the AV needs to distinguish between moving human pedestrians and an obstacle, for instance.

Although the use of EDPS can help achieve indirect conformity with the GDPR by avoiding applicability, it comes with high computational costs and the mandatory requirements of pre-processing the data, which can be overall translated into higher costs.[15] This is exacerbated by the fact that external data is constantly collected by the AV, and therefore, continuous encryption is mandatory. Economically, the cost of implementing EDPS in a fully automated vehicle is higher than the compliance cost with the GDPR. Therefore, EDPS is currently not a feasible way to ensure full de-personalisation of all collected data.

11. Yao Xu and others (n 9) 20.

12. Ibid.

13. Ibid.

14. Ibid (n 9) 21.

15. Ibid.

In the end, a total de-personalisation is unrealistic.[16] This leads to the follow-up question of: who is the data subject that's being protected by the GDPR, specifically under Article 6 GDPR?

2.3. Data Subjects

The AV scenario does not only provide a number of involved parties on the processing side,[17] but also on the data subject side. Clarity can be gained by differentiating between vehicle-internal and external subjects reflecting the differentiation of the collected personal data. On the internal side, the driver and possible passengers will be considered as data subjects.[18] Outside the vehicle, all other traffic participants such as pedestrians and cyclists can also be considered data subjects because the AV records its environment, which includes recording of faces.[19] Whether drivers of other vehicles can also be considered as data subjects depends on the question of the Vehicle Identification Number (VIN) and if it can be considered as personal data as well. In a recent judgment, the ECJ stressed that for the assessment of personal data '*account should be taken of all the means likely reasonably to be used either by the controller, within the meaning of Article 4(7) of the GDPR, or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity'.*[20] Therefore, it has been

16. Agreeing Meriem Benyahya and others, 'The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis' (2022) 12 Applied Sciences 4413, 1, 16.

17. Cf. fn. 3.; in detail Ibid. (n 16) 9-11.

18. In this context it is important to refer to Art. 2 (2) (c) GDPR which excludes the processing of personal data by a natural person during a purely personal or household activity from the GDPR's scope. But this exception depends heavily on the question of whether the driver is the controller/processor or not.

19. This not questioning at all Benyahya and others (n 16) 11; agreeing Maria Cristina Gaeta, 'Data Protection and Self-Driving Cars: The Consent to the Processing of Personal Data in Compliance with GDPR' (2019) 24, 1, 4.

20. C-319/22 *Gesamtverband Autoteile-Handel eV v Scania CV AB* [2023] para 45.

ruled that VINs also qualify as personal data as both the VIN, in the form of an alphanumeric code, and the name and address of vehicle certificate holder must be present on the certificate itself.[21] Considering the fact that being the certificate holder and a driver are not mutually exclusive, the driver of another vehicle can also be a data subject.

3. Processing of the Collected Data

The second hinge that opens the door to the GDPR is the processing of the collected data by the AV. Processing refers to *'any operation [...] which is performed on personal data [...], whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.*[22] Prima facie, this definition may lead to the conclusion that every collected data is processed by the AV. Since AVs rely heavily on sensors, they continuously record their surroundings which fulfils this definition. Such recorded data is also stored in the working memory which enables the AV to stop if the recorded object is recognised as a road crossing pedestrian. Lastly, data may also be altered if the AV contains AI with a machine learning function. In this case, the data is consumed by the AI's algorithm to adapt itself based on the traffic experience.

However, it has been argued that a differentiation needs to be made in the case that the data, collected in the volatile memory, is being overridden by the AV's AI in a matter of a second.[23] This view is primarily based on the assumption that the fundamental rights of the data subject are only impaired if the

21. Ibid. para 46-48.

22. Art. 4 (2) GDPR.

23. Judith Klink-Straub and Tobias Straub, 'Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen Beim Automatisierten Fahren' [2018] Neue Juristische Wochenschrift 3201, 3202.

analysed data can potentially be perceived by the natural person concerned.[24] Only in such cases, the GDPR protects the data subject.

Nevertheless, such argumentation is not convincing, considering the legal text and the overall system of data protection. First, Article 4 (2) GDPR does not contain a time limitation regarding data processing. The duration of the processing is therefore irrelevant to the question of data subject status from the GDPR's perspective. This is also supported by the fact that the exception stated in Article 9 (2) GDPR regarding sensitive personal data does not contain a de minimis processing provision. In summary, the mere wording prohibits such a perspective. Systematically, the assumption that the GDPR's protection is solely focused on human actors is not convincing. The GDPR addresses both the controller and the processor with obligations. Not only natural persons but also legal persons, authorities and agencies can be an addressee.[25] Therefore, data protection concerns also arise if processing and use of personal data by non-natural persons happens. Additionally, such a view is supported by Article 22 GDPR, which provides the data subject with individual claims in the case of fully automated processing where the human is out of the loop.[26] Finally, the former view overlooks the fact that the GDPR aims to ensure a high level of data protection,[27] which is not achieved if the scope of application is already narrowly defined by such a differentiation. Rather, the balancing of interests in the question of lawful processing and relevant exceptions should be discussed. This is supported above all by the extensive catalogue of Article 6 (1) and 9 (2) GDPR, which, in contrast to the concept of processing, is far more graduated.

In summary, differentiation is not appropriate. All personal data collected by the AV can also be processed, which leads to the subsequent question of the processing's lawfulness.

---

24. Ibid.

25. Art. 4 (7, 8) GDPR.

26. In such a case, the data processing would become unlawful, which enables the data subject to activate claims provided by Art. 77, 79, 82 GDPR.

27. Ibid. Rec. 7, 10.

4. Lawfulness of Processing (Art. 6 GDPR)

Under the GDPR, the processing of personal data is lawful in six exhaustively listed cases.[28] In the case of AVs four of them could apply: these are consent, compliance with a legal obligation, protection of vital interests of the data subject and the overweighing legitimate interests pursued by the controller.

4.1. Consent

The possibility of giving consent underlines the fact that data privacy is not an absolute right[29] and the importance of the self-determined individual who can dispose his fundamental rights in an independent manner. Such understanding of the rule of law is pinpointed in the requirements of legally binding consent stated in the GDPR's provision. First, consent must be '*given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement*'.[30] Second, the data subjects' consent must cover one or more specific purposes of processing and, in the case of multiple purposes, must address all purposes.[31]

As addressed earlier, it is important to distinguish between internal and external data subjects, because the circumstances of collection and processing differ significantly.

4.1.1 Internal Data Subjects

For both the driver and passenger, the requirement of consent seems to be satisfiable without any hurdles. As Recital 32 GDPR elaborates, an act of the data subject is mandatory which is considered to be satisfied in case of written con-

28. Ibid. Art. 6 (1).

29. Ibid. Rec. 4.

30. Ibid. Rec. 32.

31. Ibid.; Art. 6 (1).

sent '*by [actively] ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his [...] personal data*'.[32] Therefore, it is possible that a voice assistant is installed in the AV that asks all users before the start to give consent. Also, the installation of a ticking box which appears on the AV's control screen after activating the electronics seems feasible. In such a case, the first requirement would be satisfied because the data subjects are deciding without any external pressure. Also, Article 7 (4) GDPR does not apply. The provision demands the processing of data that is not essential for the provision of the service. The aim is to prevent the controller from processing more data than is necessary for the fulfilment of the contract or provision of the service. However, as described above, the processing of all collected data is necessary for the performance of the AV. The second requirement seems to be more critical. Considering the ambiguity of the collected data and the multitude of purposes, giving informed consent to all of the possible uses is difficult. The AV does not process the collected data for the sole purpose of functioning, but also for safety, maintenance and development. Therefore, it would be necessary that either the control screen box would list off all purposes set up by the manufacturer or that the voice assistant would report all those purposes. Such an amount of information could hinder an informed agreement. This leads to questions about whether the GDPR sets up any benchmark for informed consent.

Neither the wording of Recital 32 nor of Article 6, 7 GDPR provides any information on what circumstances the consent is informed. Therefore, the wording is open to the solution above. Systematically, Article 12 (1) GDPR sets up a transparency threshold for information given by the controller. They must be presented in a '*concise, transparent, intelligible and easily accessible form, using clear and plain language*'.[33] Nevertheless, it should be noted that Article 12 GDPR is part of chapter three, which addresses the rights of the data subject. The question of consent is located under the heading of the second chapter, which means that there is a clear separation. This is also underpinned by the fact that Article 12 (1) GDPR explicitly refers to the provisions of Articles 13, 14, 15-22 and 34, but not Article 6 GDPR. In conclusion, the systematic argument does not convince. Lastly, the GDPR's telos, which is the protection of the data subject's fundamental rights, is not infringed if the subject faces the described amount of information. Considering the technical possibility that the box can only be ticked after scrolling down the whole text, in combination with the permanent accessibility of the information, it provides enough freedom for the data sub-

32. Ibid. Rec. 32.

33. Ibid. Art. 12 (1).

ject to inform themselves without any pressure. This also applies in the case of a voice assistant, which may ask the user if the text should be repeated and at what speed. In the end, the second requirement can also be fulfilled.

To conclude this paragraph, the provision of Article 7 (1) GDPR must be finally addressed, which shifts the burden of proof regarding consent to the controller. This can be realised by simply logging time and location when the box is clicked and by storing the verbal agreement. In summary, GDPR compliance in the case of internal subjects is possible.

4.1.2 External Data Subjects

The processing of external data by the AV does happen without actual knowledge of the external data subjects. Although some subjects may be aware that AVs are data-driven products and rely on continuous data farming, such subconsciousness is not sufficient under the GDPR's framework. One part of consent is a clear and affirmative act of the subject. Drawing a reverse conclusion from this leads to the realisation that implied or tacit behaviour is not sufficient for consent.[34] Therefore, there is no consent if the AV processes the personal data of external subjects.[35]

4.1.3 Pitfalls

Although lawful processing of internal data is possible under the provision of Art. 6 (1) (a) GDPR, there is a pitfall when it comes to GDPR conformity of AV.[36] This is because recognising the existence of a self-determined and free person not only means that they can consent to the impairment of their fundamental rights, but also that they can revoke this consent. Withdrawal is the other side of the coin. The GDPR stipulates that the data subject shall have the right

34. Ibid. Rec. 32.

35. Simone Scagliarini, 'Smart Roads and Autonomous Driving vs. Data Protection: The Problem of the Lawfulness of the Processing' <https://iris.unimore.it/handle/11380/1257141> accessed 11 March 2025, 189, 194.

36. Without any deeper analysis Marjory S. Blumenthal and Karlyn D. Stanley, *Data Drive Legal Regimes for Automated Vehicles*, in: Gereon Meyer and Sven Beiker (eds), *Road Vehicle Automation 11* (Springer Nature Switzerland 2024), p. 76, <https://link.springer.com/10.1007/978-3-031-67466-2> accessed 10 March 2025.

to withdraw at any time.[37] Withdrawing shall be possible under the means of giving consent,[38] which emphasises the close relationship between both. This leads to legal uncertainty for the controller as the GDPR conformity is built on sand. Since the data subject is not obliged to give any reasoning, the controller is exposed to the arbitrariness of the user. Both the driver and the passenger may withdraw their consent during the use of the AV. After this moment, every processing of data becomes unlawful.[39]

In conclusion, solely relying on consent is not a convincing approach to secure GDPR conformity.

4.2. Compliance with Legal Obligations

The focus now shifts to the second possibility of lawful processing. This is compliance with legal obligations. Such obligations can stem from EU legislation and domestic frameworks. For instance, in Germany, § 63a Road Traffic Act enshrines the controller's obligation to save and store the data which indicates the switch from non-automated to automated driving and vice versa. In this case, the personal data about the location and time of the switch[40] is processed lawfully, as it falls under this specific legal obligation. However, such a provision only captures a small amount of the processed data.

4.3. Protection of Internal and External Data Subject's Vital Interests

Contrary to the prior option, the provision of Article 6 (1) (d) GDPR could serve as a broader option for the lawful processing.[41] If the processing is necessary

37. Ibid. Art. 7 (3) GDPR.

38. Ibid.

39. Ibid.

40. Such data is personal because from both criteria third parties can relocate the data subjects' route and determine ex-post the location.

41. Without further analysis Eva Fialová, 'AUTONOMOUS VEHICLES AND EUROPEAN DATA

to protect the vital interests of the data subject or another natural person, it should be considered lawful.[42] As AVs are considered to be safer compared to human-driven vehicles[43] and are expected to significantly lower crash rates, it seems that the data processing aims also to protect the vital interests of the internal and external data subjects. For instance, when the automated driving mode is activated, the AV checks the driver's physical condition to ensure that they are still attentive and able to retake control. Currently, Volkswagen has developed an emergency assistant which checks if a driver is losing consciousness due to a heart attack, fainting, or other causes of total incapacity.[44] The system uses sensors to detect when the driver has not performed typical actions, for example steering, braking, or accelerating, for a certain period. Supported by other systems, the emergency assistant intervenes immediately and brings the vehicle to a safe stop. Focussing on external data subjects, it can be said that the processing of data with the overarching purpose of ensuring a safe drive also serves, at least indirectly, the purpose of protecting the vital interests of pedestrians.

However, to prove the correctness of this perspective it needs to be assessed what vital interests are in the GDPR's understanding and what the scope of Article 6 (1) (d) GDPR is.

Vital interests are not defined in the GDPR. Recital 112 only stipulates that physical integrity, or life, is part of vital interests. From this, it can be concluded that the term refers to the physical condition of the data subject from a medical perspective. Regarding the provision's scope, the mere wording only refers to the protection of vital interests ensured by the data processing. Therefore, the wording leaves space for a broad application, which would include every data

---

PROTECTION LAW' (2020) 17 MECCA Journal of Middle European Construction and Design of Cars 6, 1, 2.

42. Art. 6 (1) (d) GDPR.

43. Mohamed Abdel-Aty and Shengxuan Ding, 'A Matched Case-Control Analysis of Autonomous vs Human-Driven Vehicle Accidents' (2024) 15 Nature Communications 4931, 1, 3, 4.

44. 'Emergency Assist' (*Volkswagen Newsroom*) <https://www.volkswagen-newsroom.com/de/emergency-assist-3680> accessed 14 March 2025.

processing directly or indirectly linked to the data subject's vital interests. However, this assumption is shaken by a glance at the Recitals. First, the provision's exceptional character is being stated by emphasising that it shall, in principle, only take place where the processing cannot be manifestly based on another legal basis.[45] Second, vital interests are closely linked to scenarios such as epidemics, man-made disasters,[46] or if the data subject is unable to give consent but the transfer of personal data is necessary to protect their vital interests.[47] These cases underline the provision's aim, which envisions a concrete medical scenario in the form of a direct crisis.[48] It can be derived that the provision is intended to address the healthcare sector. Systematically, such data would also very likely fall under the provision of Article 9 GDPR as it can be defined as data concerning health. This provision prohibits, in principle, every processing of such data, if not an exemption applies, which is highly doubtful as already researched.[49] Also, this underlines the exceptional character of Article 6 (1) (d) GDPR. This leads to the conclusion that the provision needs to be interpreted strictly, respecting the narrow scope. Therefore, the processing of external data by AVs in principle does not fall under this provision, as there is only an indirect link to healthcare and the physical condition. With regards to the internal data, it depends on the concrete case. If an emergency assistant will bring the AV to a safe stop and reach out to an ambulance, a clear link to healthcare and a personal medical crisis is given.

45. Rec. 46 GDPR.

46. Ibid.

47. Ibid. Rec. 112.

48. Scagliarini (n 35) 195; Kotschy, Waltraut, ' Article 6 Lawfulness of processing', in Christopher Kuner, and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), https://doi-org.proxy-ub.rug.nl/10.1093/oso/9780198826491.003.0035, accessed 26 Mar. 2025.

49. Trix Mulder and Nynke E Vellinga, 'Exploring Data Protection Challenges of Automated Driving' (2021) 40 Computer Law & Security Review 105530, 1, 7.

4.4 Controller's Legitimate Interest

Article 6 (1) (f) GDPR demands a balance between the controller's legitimate interests and the fundamental rights and freedoms of the data subjects. A general balancing of interests without criteria is always exposed to the risk of being too vague and thus has the opposite effect on a legal balance. Therefore, the European Data Protection Board (EDPB) has established guidelines for applying Article 6 (1) (f) GDPR, which includes a 3-step test. This test creates a robust framework for the balancing of interests and is used as a basis below.

Firstly, there must be a legitimate interest. In the absence of a definition, the concept of legitimate interest must be understood broadly.[50] It can therefore generally include legal, economic or even idealistic interests. However, given the primacy of Union law, the effet-utile principle and the specific defence concept of the GDPR, it is convincing to establish three cumulative criteria for such an interest. These are the lawfulness of the interest, a clear and precise articulation and the actual existence of the interest, i.e. the factual necessity.[51] In the case of AV, many possible interests come into consideration. These include ensuring road safety, theft prevention, product development, vehicle monitoring and insurance and liability interests. Ensuring road safety is required by the existing road traffic law of the member states and therefore represents a de facto legal interest. This interest is also specific enough, as the road traffic law standards form a benchmark for the purpose for which the data processing takes place. For example, processing for route planning is aimed at complying with the speed limit and not causing injury to other road users. Finally, there is a risk of liability if road safety is impaired. It follows from this that such an interest also exists in fact, as the controller wants to avoid liability from an economic point of view. In conclusion, the first step is matched in the case of AV.

The second requirement is that the data processing must be necessary. This means that it must be the mildest but equally effective measure regarding

50. CJEU, judgment of 7 December 2023, Joined Cases C-26/22 and C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958), para. 76.

51. 'Edpb_guidelines_202401_legitimateinterest_en.Pdf' <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> accessed 26 March 2025 p. 8.

the fundamental rights of the data subject to fulfil the legitimate interest.[52] In other words, there must be no less data protection-intensive measures available. As stated at the beginning, data processing is the basic prerequisite for the functioning of an AV.[53] Without the processing of location and behavioural data collected from traffic participants, as well as monitoring data from the driver, the vehicle is not able to make decisions and move in traffic in real time. Therefore, there is a prima facie need for data processing. About less intensive alternative measures, the technical possibility of using de-personalised data should again be considered.[54] In this context, the principle of data minimisation[55] should also be emphasised. For example, if it is not necessary to fully identify the data subjects, which is the case, for example, if the vehicle categorises whether objects can move or not for route planning. In summary, the second step will be fulfilled in the utmost cases.

The third step of the test consists of the actual balancing of interests. Here, the EDPB guidelines set out many criteria that need to be considered.[56] To summarise, a general overall assessment is required, which includes the type and manner of data processing, the consequences of processing and subjective expectations of the processing. For the context of AV, it is helpful to draw up a specific, but not exhaustive, catalogue of criteria.

The more sensitive the data, i.e. the greater the comparability to the catalogue of Article 9 (1) GDPR, the more likely it is that the interests of the data subject will prevail. This is likely to apply to all data from which specific habits and behaviours can be inferred, such as time and location data.[57] Secondly, the type and manner of processing must play a role. Given the intensity of the interference, a differentiation must be made for data stored in the AV's work-

52. Ibid. p. 12.

53. Cf. B. I.

54. Cf. B. II.

55. Art. 5 (1) (c) GDPR.

56. 'Edpb_guidelines_202401_legitimateinterest_en.Pdf' (n 50) p. 12-17.

57. Klink-Straub and Straub (n 23) 3204.

ing memory for a very short time and is processed, altered and deleted there directly, and for data that is stored permanently and unchanged.[58] Thirdly, it must also be considered whether the data subject has consciously consented to data processing or not. The model of the free and self-determined person makes a difference in the assessment of whether the data subject, like the driver, has consciously placed himself in the situation of data processing or whether, as in the case of pedestrians, the processing takes place without any objective awareness. In the latter case, covert and secret processing is comparable, so the principle of transparency (Article 5 (1) (a) GDPR) may not be upheld.

Considering this, the mere nature of the balancing prohibits a final and rigid conclusion. However, it can be said that most data related to the safe and secure performance of the AV will fall under the provision. Such processing is in the interest of all parties. Additionally, this type of data is only used for the exact moment, which fulfils the second criterion. Although external data subjects may still not know about the processing, this factor would be outbalanced if the AV only senses the existence of obstacles and movements and not the faces of pedestrians. If the opposite were to apply, the result could shift, considering that there is neither a relationship between third-party traffic participants nor the AV, as well as no specific awareness about the exact data processing of the AV. Contrary to external parties, internal data subjects may be more aware of the extent to which the AV processes the collected personal data. But also, this would reach a limit if such data were used for non-essential commercial purposes, as such processing does not have a direct link with the AV's functioning and is therefore unexpected and intrusive. An example of such a case would be the sharing of trip data with third parties for marketing purposes.

In the end, it needs to be stressed that these results may change from case to case as Article 6 (1) (f) GDPR demands a case-to-case assessment. The decisive factor here is, above all, the specific technical and legal organisation of the use of the AV.

58. Ibid.

5. Conclusion

The legal issues of the lawfulness of data processing in AVs under Article 6 GDPR have been addressed in the above article. It was shown that AVs are currently using technical methods to de-personalise data. However, these have not yet proven to be completely successful, as either re-identification is possible, or the implementation costs are not economically viable. As a result, a large proportion of the data collected falls within the scope of the GDPR as personal data. These are also processed in their entirety. A differentiation about the storage period is not appropriate, as such factors can be considered later as part of the lawfulness of the processing. This is the only way to achieve the desired high level of protection of the GDPR. The grounds for consent in Article 6 (1) (a) GDPR, do apply to processing. Such processing based on consent is at least possible for internal data subjects, whereby the possibility of withdrawal proves to be a high uncertainty factor. Article 6 (1) (c) GDPR applies but only covers a small part of the data. Due to the narrow scope of application and exceptional nature, data processing cannot be based on Article 6 (1) (e) GDPR. Ultimately, the regulation on the balancing of interests proves to be the correct basis for lawful data processing. Here, a case-by-case assessment must be made based on the criteria established, whereby it can be determined that processing that serves the interests of all parties involved is lawful. Consequently, it can be concluded that the use of AV is possible in accordance with the GDPR. Data protection and innovation are not mutually exclusive, but rather mutually beneficial, so that law and technology merge to form a structure that guarantees a technologised future for free and self-determined people.

Bibliography

Abdel-Aty M and Ding S, 'A Matched Case-Control Analysis of Autonomous vs Human-Driven Vehicle Accidents' (2024) 15 Nature Communications 4931

Benyahya M and others, 'The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis' (2022) 12 Applied Sciences 4413

'Edpb_guidelines_202401_legitimateinterest_en.Pdf' <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en> accessed 26 March 2025

'Emergency Assist' (*Volkswagen Newsroom*) <https://www.volkswagen-newsroom.com/de/emergency-assist-3680> accessed 14 March 2025

Fialová E, 'AUTONOMOUS VEHICLES AND EUROPEAN DATA PROTECTION LAW' (2020) 17 MECCA Journal of Middle European Construction and Design of Cars 6

Gaeta MC, 'Data Protection and Self-Driving Cars: The Consent to the Processing of Personal Data in Compliance with GDPR' (2019) 24

Klink-Straub R am AJ and Straub T, 'Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen Beim Automatisierten Fahren' [2018] Neue Juristische Wochenschrift 3201

Krontiris I and others, 'Autonomous Vehicles: Data Protection and Ethical Considerations', *Proceedings of the 4th ACM Computer Science in Cars Symposium* (Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3385958.3430481> accessed 10 March 2025

Meyer G and Beiker S (eds), *Road Vehicle Automation 11* (Springer Nature Switzerland 2024) <https://link.springer.com/10.1007/978-3-031-67466-2> accessed 10 March 2025

Mulder T and Vellinga NE, 'Exploring Data Protection Challenges of Automated Driving' (2021) 40 Computer Law & Security Review 105530

Scagliarini S, 'Smart Roads and Autonomous Driving vs. Data Protection: The Problem of the Lawfulness of the Processing' <https://iris.unimore.it/handle/11380/1257141> accessed 11 March 2025

Xu Y and others, 'Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics' (2025) 16 World Electric Vehicle Journal 6

About the author

Maximilian Kloth

Maximilian Kloth completed the LLM Technology Law and Innovation at the University of Groningen. He is currently undertaking his law clerkship at the Court of Appeal (Kammergericht) in Berlin.

CHAPTER 6: SAILING INTO MONOPOLY: HOW DATA ACCUMULATION BY AUTONOMOUS SHIPS VIOLATES COMPETITION LAW

Inés López Abad

1. Introduction

In just under three hours, one of history's major maritime tragedies occurred, sealing the fate of the RMS Titanic, and forever reshaping the future of naval design.[1] The loss of 1,501 lives left behind a historical lesson of maritime protocol, which in 1914 triggered the first version of the International Convention for Safety of Life at Sea (SOLAS), and created enduring agreements that continue to govern maritime operations today.[2] More than a century later, the maritime industry is entering another era of revolutionary change.[3] The development of Maritime Autonomous Surface Ships (MASS), defined by the International Maritime Organization (IMO) as vessels that operate without human interaction, promises a reduction in the human factors that have led to past maritime dis-

1. Bruno S. Frey and others, 'Behavior under Extreme Conditions: The Titanic Disaster' (2011) 25 Journal of Economic Perspectives 209.

2. Irena Jurdana and others, 'Shipboard Data Compression Method for Sustainable Real-Time Maritime Communication in Remote Voyage Monitoring of Autonomous Ships' (2021) 13 Sustainability 8264.

3. Mingyu Kim and others, 'Autonomous Shipping and its Impact on Regulations, Technologies, and Industries' (2020) 4 Journal of International Maritime Safety, Environmental Affairs, and Shipping 17.

asters.[4] This technological evolution has attracted substantial industry interest and investment, catalysed by the combination of lower operational costs and higher safety.[5] Industry leaders have embraced this transformation with considerable optimism. For example, Mikael Makinen, former president of Rolls-Royce Marine, asserts that autonomous shipping represents the inevitable future of this industry.[6]

Harnessing data plays a fundamental role in providing the benefits of MASS.[7] In our current society firms are known for achieving high turnovers based on business models that involve the use of data.[8] The impact of data and technology reaches far beyond digital markets and can extend to traditional industries such as the maritime one.[9] As the vessels navigate the world's oceans, they generate vast volumes of data, including real-time weather patterns, detailed cargo information, and optimal routing algorithms.[10] Not only is this data collection a byproduct of technological advancements, but it is also becoming

4. Sarang Thombre and others, 'Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review' (2022) 23 IEEE *Transactions on Intelligent Transportation Systems 64.*

5. Ziaul Haque Munim and others, 'Autonomous Ships for Container Shipping in the Arctic Routes' (2022) 27 Journal of Marine Science and Technology 320.

6. Esa Jokioinen and others, 'Remote and Autonomous Ships: The Next Steps' (*Rolls-Royce*, AAWA Position Paper) < https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf > accessed 14 March 2025.

7. Ibid.

8. Bruno Lasserre and others, 'Competition Law and Big Data: The Enforcers' View' (2017) 1 Italian Antitrust Review 87.

9. Ibid.

10. 'Big Data in the Maritime Industry: Use Cases and Challenges', (*Sedna*) <https://sedna.com/resources/big-data-in-the-maritime-industry-use-cases-and-challenges#:~:text=derive from it.-,Top sources of big data in maritime,, berthing schedules, and more < accessed 20 August 2025.

the most valuable asset in maritime commerce.[11] Maritime data provides companies with significant competitive advantages in route optimisation, predictive maintenance and market forecasting.[12] The progression from the safety reforms of 1914 to today's autonomous shipping initiatives illustrates the industry's capacity for transformative change.[13] Nevertheless, as MASS technology advances from experimental trials to commercial deployment, new complexities are introduced, including competitive market dynamics.

As part of the European Union's competition law framework, Article 102 TFEU prohibits dominant undertakings from abusing their market position through anti-competitive behaviors.[14] While this framework was developed for traditional markets, recent enforcement actions against technology giants, such as Google or META, show its evolving application to data driven digital environments.[15] The maritime sector faces similar competitive dynamics, given that shipping companies and technology providers leverage MASS data to create competitive advantages.[16] This transformation raises concerns about market concentration and competitive fairness, particularly as early MASS developers

11. Divya Tejwani, 'Navigating the Future: How AI, Big Data, and Autonomous Systems are Reshaping Maritime Transport', (*UNCTAD*, 17 October 2024) < https://unctad.org/news/navigating-future-how-ai-big-data-and-autonomous-systems-are-reshaping-maritime-transport#:~:text=Currently, the maritime industry is,their way into shipping operations > accessed 2 September 2025.

12. Ibid.

13. David Appleton, 'What's going on with Autonomous Ships?' (*YouTube*, 15 October 2024) < https://www.youtube.com/watch?v=ZRtS5v9EmLU > accessed 13 March 2025.

14. Article 102 TFEU.

15. European Commission, 'Antitrust: Commission opens investigation into possible anti-competitive conduct by Google and Meta, in online display advertising' (Press Release, 11 March 2022).

16. 'Remote and Autonomous Ship Operations Driving the Future of Marine Data Management' (*American Journal of Transportation*, 15 January 2024) < https://www.ajot.com/news/remote-and-autonomous-ship-operations-driving-the-future-of-marine-data-management > accessed 20 March 2025.

accumulate vast amounts of data that create significant barriers to entry the market for potential competitors.[17] Inevitably, companies with superior data access, risk engaging in exclusionary practices that could foreclose competition entirely.

This paper aims to investigate to what extent data accumulation by dominant MASS operators may constitute abuse under Article 102 TFEU. Through an interdisciplinary literature review of competition law and MASS technology, this paper develops a theoretical framework examining relevant legal concepts and their application to maritime data markets. The central argument of this paper is that the concentration of maritime data, in the hands of dominant MASS operators, presents substantial risks of anti-competitive behavior. As a result, competition law principles need to address the unique characteristics of these emerging markets before entrenched monopolistic structures become irreversible.[18] For this, it is important to first understand the way MASS collects data and its value in the market.

2. Data Generation as the Compass for Autonomous Ships

While the term 'data' lacks a universally accepted definition, the Data Governance Act provides useful guidance, defining it as 'any digital representation of acts, facts or information, including in the form of sound, visual or audiovisual recording'.[19] Regarding MASS, this encompasses a broad spectrum of information generated through vessel operations, ranging from basic navigational

17. Lasserre and others (n. 8).

18. A. Komianos, 'The Autonomous Shipping Era. Operational, Regulatory, and Quality Challenges' (2018) 12 The International Journal on Marine Navigation and Safety of Sea Transportation 335.

19. Regulation (EU) No 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1, art. 2 (11).

coordinates to complex environmental assessment.[20] The volume and value of data collected in the maritime industry is following the general trend of exponential growth.[21] Therefore, to illustrate this point, this section examines the importance of data in this industry.

2.1. Understanding the Volume of Maritime Data

Digital data is collected by various devices which are installed on-board. For instance, in order to avoid collision, autonomous ships are equipped with sensors that detect objects and trigger self-steering actions.[22] MASS vessels primarily collect navigational data, including GPS, environmental conditions, and comprehensive engine diagnostics, such as temperature and pressure readings across various mechanical components.[23] This data collection relies on sophisticated sensor systems that can be categorized into two primary families: visual sensors (cameras) and remote sensing technologies (RADAR and LiDAR).[24] These sensors function as perception elements, by scanning the environment, gathering the data about the surroundings, and using it to make informed decisions.[25]

On top of that, sensor fusion is one of the key technologies for any reliable autonomous vehicle navigation.[26] This guarantees accuracy at all times, as the input data from multiple sensors is combined and analysed. The way this

20. Jurdana and others (n. 2).

21. Kim and others (n. 3).

22. Komianos (n. 18).

23. Peide Wang, 'Research on Comparison of LiDAR and Camera in Autonomous Driving' [2021] Journal of Physics: Conference Series 1.

24. Cadence System Analysis, 'The Use of RADAR Technology in Autonomous Vehicles' < https://resources.system-analysis.cadence.com/blog/msa2022-the-use-of-radar-technology-in-autonomous-vehicles> accessed 10 April.

25. Ibid.

26. Jokioinen and others (n. 6).

works is that the sensor data is seamlessly integrated to have an up-to-date map of the ship's environment.[27] The constructed blueprint can be augmented with data from static map databases such as electronic nautical charts (ECDIS), which present static objects of the surrounding area.[28] When at sea and harbor areas, there are nautical and terrain charts to obtain data about shipping lanes and coastal terrain.[29] Sometimes, relating to image and sound processing, AI techniques can also facilitate the detection and identification of objects embedded in data shots generated by different sensors.[30] All these techniques of sensor fusion show that massive amounts of data and the combination of data sets are needed for the smooth operation and success rate of autonomous ships.

Diagram 1: Fusion of Visual Light and Thermal Imaging at Night.[31]



Additionally, the technological infrastructure supporting MASS operations extends beyond individual vessel systems through the adoption of Intelligent Information Technology (IIT).[32] Central to this development is the Internet of Ships (IoS), which interconnects various shipboard systems and devices, enabling the collection, sharing, and exchange of data both internally and

27. ibid.

28. Thombre and others (n. 4).

29. Jokioinen and others (n. 6).

30. Thombre and others (n. 4).

31. Jokioinen and others (n. 6).

32. Tejwani (n. 11).

externally.[33] Through these integrated systems, MASS vessels generate unprecedented volumes of operational data that form the foundation for autonomous navigation and broader maritime intelligence. When MASS are equipped with a greater number of sensors and extensive data storage capabilities, they can operate more efficiently, providing a competitive advantage over ships from smaller companies with limited technological resources.[34]

2.2. Understanding the Strategic Value of Maritime Data

The collection and use of data creates efficiencies and can have pro-competitive effects.[35] For example, the data collected by the sensors in MASS can be made available to insurers to investigate the causes of accidents or damages to the vessels and cargo.[36] The exchange of data enhances risk management in maritime transportation and may lead to lower ship and cargo insurance costs, compared to vessels that lack the capability to integrate a similar number of sensors. The possession or access to data can constitute a barrier for market entry if new entrants are unable to either collect similar data or to buy access to sources of such data as the incumbents. Overall, data can be a synonym of market power, depending on case-by-case basis scenarios.[37]

The importance of maritime data can also be seen in the use of Big Data Platforms (BDP) and Big Data Analytics (BDA) for operations.[38] This is because these technologies process the vast amounts of data to predict the optimal

33. Ibid.

34. C Kooij and others, 'When will Autonomous Ships Arrive? A Technological Forecasting Perspective' (2018) International Naval Engineering Conference & Exhibition 1.

35. Lasserre and others (n. 8).

36. Anastasia Tsvetkova and others, 'Creating Value through Autonomous Shipping: An Ecosystem Perspective' (2022) 24 Maritime Economics & Logistics 255.

37. Lasserre and others (n. 8).

38. Nick Lambert, Jonathan Turner and Andy Hamflett, *Technology and the Blue Economy: From Autonomous Shipping to Big Data* (Kogan Page Publishers 2019)

ship routes.[39] BDA can even reveal hidden patterns, correlations, and trends, supporting decisions about operational efficiency.[40] Another example are the pricing models which given the availability of real-time AIS data and advanced analytics are enabling a shift towards dynamic pricing strategies.[41] By leveraging, BDA shipping companies can adjust their pricing in real time to maximise profitability, based on port congestion levels or real-time fuel prices.[42] Inevitably, this advantage may facilitate tacit collusion or enable pricing strategies that maintain higher prices without explicit communication between firms.[43] In order to understand the application of competition law to the data accumulation in MASS, we will now look at the competitive landscape.

3. Market Structure and Dominance Concerns

To understand the application of competition law to MASS data accumulation, careful analysis of how traditional competition concepts adapt to data-driven markets and the unique characteristics of maritime operations needs to be made. Article 102 TFEU requires two fundamental elements: market dominance and abuse of that dominant position.[44] In the *Hoffmann-La Roche* case, dominance is described as 'a position of economic strength which enables it to prevent effective competition'.[45] Nevertheless, establishing dominance requires first defining the relevant market.

39. Ibid.

40. Tejwani (n. 11).

41. Ibid.

42. Lambert and others (n. 38).

43. Ibid.

44. Article 102 TFEU.

45. *Hoffmann-La Roche & Co AG v Commission* Case 85/76 [1979] ECR 461.

3.1. Market Definition and Dominance

The global MASS market size is projected to expand from USD 5.6 billion in 2023 to USD 12.3 billion by 2032, representing a 9.1% annual growth rate.[46] The primary factors driving this market growth, are the potential cost savings and enhanced safety measures.[47] As a result, there is robust competition starring leading companies that are aggressively competing for the same customers.[48] More specifically, the established maritime players are Kongsberg Maritime, Hyundai Heavy Industries and Samsung Heavy Industries, accounting for a share of 45% in the market.[49] It is important to note that this consolidation around few dominant platforms, mirrors patterns observed in other technology-driven industries. For instance, the digital market is dominated by the Big Tech companies.[50]

Diagram 2: Overview of the Growing Trend in the Autonomous Ship Market.[51]

---

46. Satchit Desai, 'Autonomous Ships Market Size, Share & Growth' (*Markets and Markets*, September 2022) < https://www.marketsandmarkets.com/Market-Reports/autonomous-ships-market-267183224.html?gad_source=1&gad_campaignid=272040196&gbraid=0AAAADxY7SwUwjO-gyCV_nl3vG4nGJop3A&gclid=Cj0KCQjw267GBhCSARIsAOjVJ4ECkyW0eZyloVHmFMJgx7r5xbAX1Ez_bQKiVUsRZopTRhg_I4zNpJIaAhmzEALw_wcB > accessed 10 September 2025.

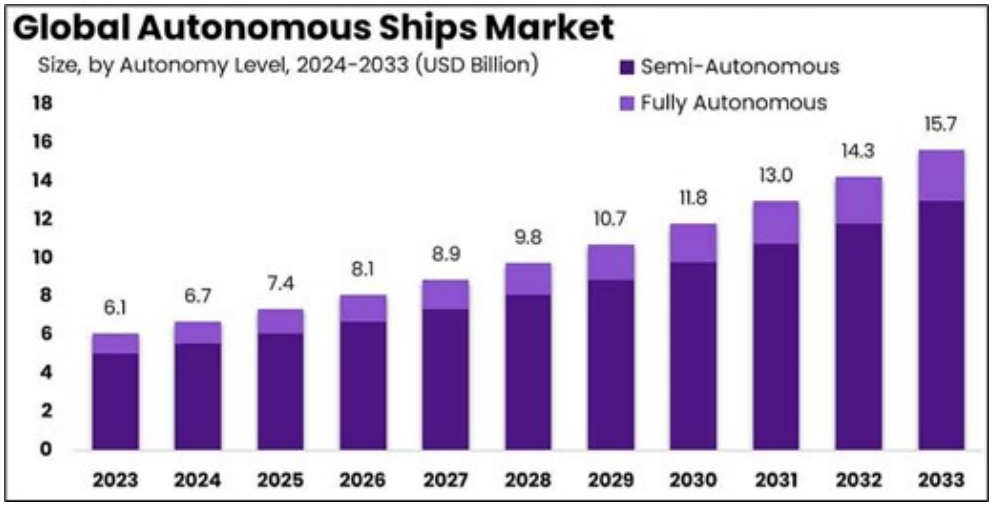
47. Tsvetkova and others (n. 36).

48. Sejal Akre, 'Autonomous Ships Market Segmentation' (*Market Research Future*, September 2025) < https://www.marketresearchfuture.com/reports/autonomous-ships-market-8103#:~:text=Autonomous Ships Market Regional Insights,investment shaping the industry's landscape > accessed 15 September 2025.

49. Suraj Gujar and Partha Paul, 'Autonomous Ships Market Size' (*GMI*, February 2025) < https://www.gminsights.com/industry-analysis/autonomous-ships-market > accessed 10 September 2025.

50. Anna Gerbrandy, 'Conceptualizing Big Tech as Modern Bigness and its implications for European Competition Law' (Universiteit Utrecht) < https://www.uu.nl/sites/default/files/anna_gerbrandy modern bigness EC.pdf > accessed 5 September 2025.

51. Yogesh Shinde, 'Autonomous Ships Market to Hit USD 15.7 Billion by 2033' (*Scoop*, 29 July



The market definition for MASS encompasses a range of vessels, from partially automated to fully autonomous. The reason for this is that actual autonomous ships are not yet a reality in large scale commercial shipping. In fact, the closest humanity has gotten to fully ship automation, is the YARA Birkeland project, a zero-emission vessel which, since spring of 2022, has been operating in Norway to transport mineral fertilizers.[52] This project has been on a two-year test trial and is expected to gain its certificate for autonomous operations by 2026.[53]

To no one's surprise, maritime markets have unique characteristics that complicate traditional dominance analysis. A company may hold dominant positions on specific trade routes while facing competition globally, requiring nuanced market definition approaches. It is important to note that, dominance may manifest through control of essential datasets rather than conventional market metrics. For example, a MASS operator with exclusive access to critical

---

2024) < https://scoop.market.us/autonomous-ships-market-news/ > accessed 18 September 2025.

52. YARA, 'Yara Birkeland, Two Years on' (*YARA*, 28 April 2024) < https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/ > accessed 15 March 2024.

53. Komianos (n.18).

shipping route data, port operational information, or comprehensive weather patterns may possess dominant positions even with relatively modest vessel market share. In the *META v. Bundeskartellamt* case, the court found the excessive collection of personal data as an abuse of dominance.[54] This reflects the Courts' recognition that dominance can arise from control of essential facilities or indispensable inputs to market participation. In fact, autonomous ship systems are protected by proprietary interfaces, which makes the legal accessibility of the data very expensive.[55] Usually, to avoid unauthorized access, ship systems are kept isolated from the Internet.[56] Even when the proprietary interface can be accessed, the data transfer is usually serial-data and unidirectional.[57]

3.2. Abuse

MASS technology introduces significant lock-in effects through accumulated operational data that becomes increasingly valuable over time.[58] The abuse element encompasses both exploitative practices, such as excessive pricing, and exclusionary conduct that forecloses competition. In MASS contexts, exclusionary abuses present particular concerns given the cumulative nature of data and the potential for dominant operators to prevent competitors from accessing datasets necessary for effective market participation. Companies with early access to datasets can optimise routes more effectively, predict maintenance needs more accurately, and develop superior autonomous navigation algorithms. Weather data, port congestion information, and navigational hazard updates may constitute essential inputs for safe and efficient maritime opera-

54. *Meta Platforms Inc v Bundeskartellamt* Case C-252/21 [2023] ECLI:EU:C:2023:537.

55. Thombre and others (n. 4).

56. Ibid.

57. Ibid.

58. Ki-Young Lee, 'Effects of Maritime Autonomous Surface Ships and Important Problems of Maritime Autonomous Surface Ships to Strengthen Port Competitiveness' (2024) 40 Journal of Korea Port Economic Association 79.

tions. Wireless communication and data acquisition are also essential to MASS and have been qualified as technical barriers to entry.[59] This is because companies that establish dominance in key shipping routes or port relationships can leverage these positions to exclude competitors from critical data sources.[60] Companies controlling access to such data may face obligations to provide access on reasonable and non-discriminatory terms.

In the *Google Shopping* judgement, the court established that algorithmic manipulation favoring proprietary services constitutes abuse.[61] By analogy, this precedent could suggest that MASS operators using superior datasets to disadvantage competitors in related markets, such as cargo booking platforms or port services, may face similar scrutiny. In addition, the European Commission is investigating Amazon because it is both a market participant and infrastructure provider, and it is suspected to be abusing its dual roles.[62] Similarly, MASS operators that both provide autonomous shipping services and control the data platforms enabling maritime operations face conflicts of interest that may constitute abuse under Article 102 TFEU.

59. Rino Sriwijaya, 'Autonomous Ships and Entry Barriers in the Merchant Shipping Market' (Dissertation, Newcastle University 2016) < https://www.researchgate.net/profile/Rino-Sriwijaya/publication/325089301_Autonomous_Ships_and_Entry_Barriers_in_the_Merchant_Shipping_Market/links/5af58ee94585157136caf7ab/Autonomous-Ships-and-Entry-Barriers-in-the-Merchant-Shipping-Market.pdf?__cf_chl_tk=DeC_SeL5QJV89t3.M2kKQq9IP66cP8hqas0XyWf2GPU-1757946840-1.0.1.1-SPmL050tWNQNOuoJ7kceGS1mtgVIC3e87_eaz6ZWpv0> accessed 10 September 2025.

60. Imdad Ali Shah, *Cybersecurity in the Transportation Industry* (Scrivener Publishing LLC 2024) ch 9.

61. General Court: *Google and Alphabet v Commission* (*Google Shopping*) Case T-612/17.

62. European Commission, 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices' (Press Release, 10 November 2020).

4. Conclusion

In an alternate universe where the Titanic was an autonomous ship and the collision with the iceberg was successfully avoided, our seas would be fully transited by unmanned ships. Maybe in search of a similar reality, today, data-driven technologies are penetrating the maritime industry.[63] The autonomous ship market is characterised by strategic partnerships and increasing government support.[64] That is why, the competitive landscape showcases a range of companies investing in research and development for the maritime sector.[65] As of this moment, MASS is already proving to be the perfect solution to have more cost-efficient voyages, safer ships, and even environmentally friendly transportation alternatives. In fact, countries such as the Netherlands are already in testing phases for the deployment of autonomous water taxis and ferries.[66] Despite the popularity and raise in market size for autonomous ships, the competitive market dynamics are at stake. Through the blueprint created of how autonomous ships collect data, using camera, LiDAR and RADAR sensors, as well as the process of sensor fusion, we can clearly understand the importance that data holds for their effective functioning. As a result, the marginalisation of smaller competitors due to differentiated data access creates a snowball effect, which might cause smaller companies to attract fewer customers and less data.[67]

The importance of data in MASS cannot be disregarded and the accumulation of maritime data by dominant companies can constitute an abuse of dominance. As demonstrated throughout this analysis, the stakes are particularly high in the MASS industry, where data dominance translates into

63. Gerasimos Theotokatos and others, 'Autonomous Shipping – An Analysis of the Maritime Stakeholder Perspective' (2023) 22 WMU Journal of Maritime Affairs 5.

64. Tsvetkova and others (n. 36).

65. ibid.

66. David Appleton, 'What's going on with Autonomous Ships?' (*YouTube*, 15 October 2024) < https://www.youtube.com/watch?v=ZRtS5v9EmLU > accessed 13 March 2025.

67. Ibid.

operational advantage and market control. Competition authorities are therefore advised to apply existing competition principles specifically tailored to data-driven maritime markets. Just as in the Golden Age of Piracy treasures in *ships* were fiercely protected, the data gathered by MASS must be safeguarded and regulated. Only through such protection can a level playing field in this rapidly advancing industry be ensured.

5. Bibliography

Primary Sources

General Court: *Google and Alphabet v Commission* (*Google Shopping*) Case T-612/17

Hoffmann-La Roche & Co AG v Commission Case 85/76 [1979] ECR 461

Regulation (EU) No 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1, art. 2 (11)

Treaty of the Functioning of the European Union (Consolidated Version) [2012] OJ C326/47.

Meta Platforms Inc v Bundeskartellamt Case C-252/21 [2023] ECLI:EU:C:2023:537

Secondary Sources

Books:

Ali Shah I, *Cybersecurity in the Transportation Industry* (Scrivener Publishing LLC 2024)

Lambert N, Turner J and Hamflett A, *Technology and the Blue Economy: From Autonomous Shipping to Big Data* (Kogan Page Publishers 2019)

Journal Articles:

European Commission, 'Antitrust: Commission opens investigation into possible anticompetitive conduct by Google and Meta, in online display advertising' (Press Release, 11 March 2022)

European Commission, 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices' (Press Release 2020)

Haque Munim Z and others, 'Autonomous Ships for Container Shipping in the Arctic Routes' (2022) 27 Journal of Marine Science and Technology 320

Jurdana I and others, 'Shipboard Data Compression Method for Sustainable

Real-Time Maritime Communication in Remote Voyage Monitoring of Autonomous Ships' (2021) 13 Sustainability 8264

Kim M and others, 'Autonomous Shipping and its Impact on Regulations, Technologies, and Industries' (2020) 4 Journal of International Maritime Safety, Environmental Affairs, and Shipping 17

Kooij C and others, 'When will Autonomous Ships arrive? A Technological Forecasting Perspective' (2018) International Naval Engineering Conference & Exhibition 1

Komianos A, 'The Autonomous Shipping Era. Operational, Regulatory, and Quality Challenges' (2018) 12 The International Journal on Marine Navigation and Safety of Sea Transportation 335

Lasserre B and others, 'Competition Law and Big Data: The Enforcers' View' (2017) 1 Italian Antitrust Review 87

Lee K, 'Effects of Maritime Autonomous Surface Ships and Important Problems of Maritime Autonomous Surface Ships to Strengthen Port Competitiveness' (2024) 40 Journal of Korea Port Economic Association 79

Frey B and others, 'Behavior under Extreme Conditions: The Titanic Disaster' (2011) 25 Journal of Economic Perspectives 209

Theotokatos G and others, 'Autonomous Shipping – An Analysis of the Maritime Stakeholder Perspective' (2023) 22 WMU Journal of Maritime Affairs 5

Thombre S and others, 'Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review' (2022) 23 IEEE *Transactions on Intelligent Transportation Systems 64*

Tsvetkova A and others and Magnus Hellström, 'Creating Value through Autonomous Shipping: An Ecosystem Perspective' (2022) 24 Maritime Economics & Logistics 255

Wang P, 'Research on Comparison of LiDAR and Camera in Autonomous Driving' [2021] Journal of Physics: Conference Series 1

Websites & Blogs:

Akre S, 'Autonomous Ships Market Segmentation' (*Market Research Future*, September 2025) < https://www.marketresearchfuture.com/reports/autonomous-ships-market-8103#:~:text=Autonomous Ships Market Regional Insights,investment shaping the industry's landscape > accessed 15 September 2025

'Big Data in the Maritime Industry: Use Cases and Challenges', (*Sedna*) <https://sedna.com/resources/big-data-in-the-maritime-industry-use-cases-

and-challenges#:~:text=derive from it.-,Top sources of big data in maritime,, berthing schedules, and more < accessed 20 August 2025

Cadence System Analysis, 'The Use of RADAR Technology in Autonomous Vehicles' < https://resources.system-analysis.cadence.com/blog/msa2022-the-use-of-radar-technology-in-autonomous-vehicles> accessed 10 April

Desai S, 'Autonomous Ships Market Size, Share & Growth' (*Markets and Markets*, September 2022) < https://www.marketsandmarkets.com/Market-Reports/
autonomous-ships-market-267183224.html?gad_source=1&gad_campaignid=272040196&gbraid=0AAAADxY7SwUwjO-gyCV_nl3vG4nGJop3A&gclid=Cj0KCQjw267GBhCSARIsAOjVJ4ECkyW0eZyloVHmFMJgx7r5xbAX1Ez_bQKiVUsRZopTRhg_I4zNpJIaAhmzEALw_wcB > accessed 10 September 2025

Gerbrandy A, 'Conceptualizing Big Tech as Modern Bigness and its implications for European Competition Law' (Universiteit Utrecht) < https://www.uu.nl/sites/default/files/anna_gerbrandy_modern_bigness_EC.pdf > accessed 5 September 2025

Gujar S and Paul P, 'Autonomous Ships Market Size' (*GMI*, February 2025) < https://www.gminsights.com/industry-analysis/autonomous-ships-market > accessed 10 September 2025

Jokioinen E and others, 'Remote and Autonomous Ships: The Next Steps' (*Rolls-Royce*, AAWA Position Paper) < https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf > accessed 14 March 2025

'Navigating the Future: How AI, Big Data, and Autonomous Systems are Reshaping Maritime Transport', (*UNCTAD*, 17 October 2024) < https://unctad.org/news/navigating-future-how-ai-big-data-and-autonomous-systems-are-reshaping-maritime-transport#:~:text=Currently, the maritime industry is,their way into shipping operations > accessed 2 September 2025

Rostek D. and Baldauf M., 'Technologies for Situational Awareness in Autonomous Shipping' (*IATED Digital Library,* 2024) < https://library.iated.org/view/ROSTEK2024TEC > accessed 24 March 2025

'Remote and Autonomous Ship Operations Driving the Future of Marine Data Management' (*American Journal of Transportation*, 15 January 2024) < https://www.ajot.com/news/remote-and-autonomous-ship-operations-driving-the-future-of-marine-data-management > accessed 20 March 2025

Shinde Y, 'Autonomous Ships Market to Hit USD 15.7 Billion by 2033' (*Scoop*,

29 July 2024) < https://scoop.market.us/autonomous-ships-market-news/ > accessed 18 September 2025

Sriwijaya R, 'Autonomous Ships and Entry Barriers in the Merchant Shipping Market' (Disseration, Newcastle University 2016) < https://www.researchgate.net/profile/Rino-Sriwijaya/publication/325089301_Autonomous_Ships_and_Entry_Barriers_in_the_Merchant_Shipping_Market/links/5af58ee94585157136caf7ab/Autonomous-Ships-and-Entry-Barriers-in-the-Merchant-Shipping-Market.pdf?__cf_chl_tk=DeC_SeL5QJV89t3.M2kKQq9IP66cP8hqas0XyWf2GPU-1757946840-1.0.1.1-SPmL050tWNQNOuoJ7kceGS1mtgVIC3e87_eaz6ZWpv0> accessed 10 September 2025

Tejwani D, 'Navigating the Future: How AI, Big Data, and Autonomous Systems are Reshaping Maritime Transport', (*UNCTAD*, 17 October 2024) < https://unctad.org/news/navigating-future-how-ai-big-data-and-autonomous-systems-are-reshaping-maritime-transport#:~:text=Currently,%20the%20maritime%20industry%20is,their%20way%20into%20shipping%20operations > accessed 2 September 2025

YARA, 'Yara Birkeland, Two Years on' (*YARA*, 28 April 2024) < https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/ > accessed 15 March 2024

Videos:

Appleton D, 'What's going on with Autonomous Ships?' (*YouTube*, 15 October 2024) < https://www.youtube.com/watch?v=ZRtS5v9EmLU > accessed 13 March 2025

About the author

Inés López Abad

Inés López Abad completed the LLM Technology Law and Innovation programme at the University of Groningen during the academic year 2025-2026. She is currently attending a Master's exchange programme at the University of Newcastle Australia.

PART II. AI AND DATA

CHAPTER 7: PORTER'S HYPOTHESIS: REFRAMING THE EFFECTS OF THE GDPR ON AI INNOVATION

Karabo Lerato Mokoena

1. Introduction

James DeMonaco's movie *The Purge* explores a society in which all crimes are legalised for one night, allowing individuals and companies to profit from the breakdown of social order and widespread violence without consequences.[1] In the movie, those with power steal, stalk, and physically and psychologically torture the vulnerable. However, once regulations are reintroduced to abolish the purge, everyone must adapt to the structured environment. Similarly, big tech companies once operated in a regulatory void,[2] racing to harvest and monetise user data with little oversight or ethical considerations.[3] For example, in 2021, a Facebook whistleblower revealed that Meta's internal research showed that their algorithm amplifies harmful content and polarises political views on the platform.[4] Despite this, Meta continued to push the algorithm because it

1. James DeMonaco, *The Purge* (Universal Pictures, 2013).

2. Kean Birch & Kelly Bronson, 'Big Tech' (2022) 31(1), 1–14 Science as Culture, 3 <https://doi.org/10.1080/09505431.2022.2036118> accessed 25 March 2025.

3. Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization" (2022) 3: 1 Organization Theory 3 <https://doi.org/10.1177/26317877221129290> accessed 25 March 2025.

4. Haugen Frances, 'Facebook's Whistleblower Testimony to the U.S Senate' (2021) <https://www.youtube.com/watch?v=KCy4V2iMP6w> accessed 23 March 2025.

increased ad revenue from high content engagement.[5] Meta is not the only one; the favoured business model for data-driven companies, such as Google, Amazon and Microsoft, is *collect first, profit next, then think later*.[6] These companies take advantage of regulators' hesitancy to regulate, the reduced computing costs and the sophistication of analytical tools to profit from vast amounts of data, some of which is personal data.[7]

Specifically, advancements in artificial intelligence (AI) systems allow organisations to enhance their purging capabilities and process vast amounts of personal and personally identifiable data.[8] This indiscriminate collection and processing, along with the various AI training techniques used to develop

5. In July 2024, Meta announced a .07 billion total revenue, 98% of which comes from ad sales; See Meta Reports Third Quarter 2024 Results (investor.atmeta.com, July 2024) <https://investor.atmeta.com/investor-news/press-release-details/2024/Meta-Reports-Third-Quarter-2024-Results/default.aspx> accessed 25 March 2025.

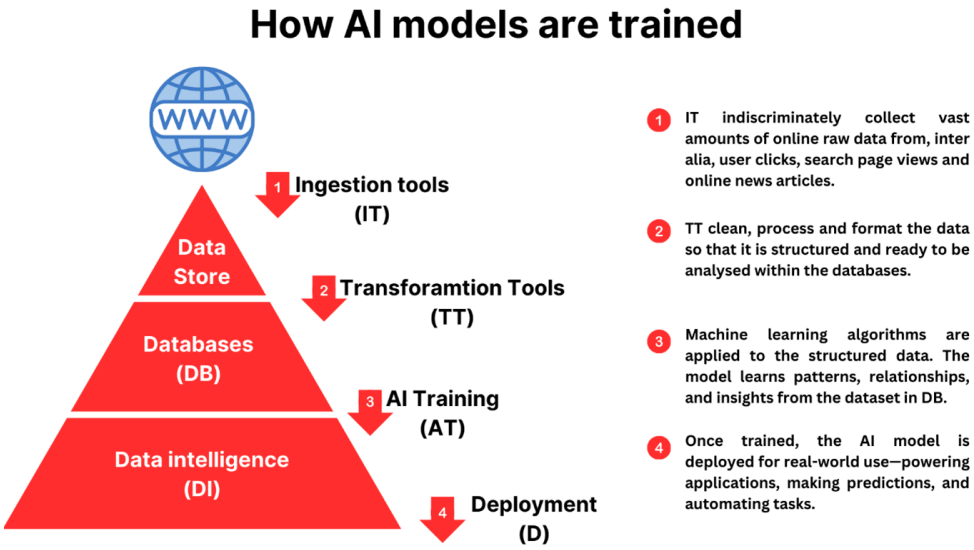
6. Shoshana Zuboff (n3) 3.

7. European Data Protection Board, Opinion 04/2024 on the use of personal data for the training of AI models (EDPB 2024) 12 <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> accessed 12 March 2025;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, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR)Article 4(1) GDPR defines **personal data** as 'any information relating to an identified or identifiable natural person (data subject)'. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

8. EDPB 2024 (n7) 12 An AI model must be distinguished from an AI system. An **AI system** is 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment'.' **AI models**, on the other hand, encompass the product resulting from the training mechanisms applied to a set of training data in the context of AI, machine learning or other related processes.

underlying AI models, introduce both identified and unforeseen risks to the safeguarding of personal data.[9]

Figure 1: How data is used to train AI models. [10]



Source: Author.

Figure 1 illustrates that AI models are designed to be 'blind', as data protection principles are overlooked at the outset. Instead, these models focus on ensuring reliable signals rather than prioritising the accuracy, transparency or fairness of the information they transmit.[11] This is inconsistent with the EU's human-centric, trustworthy, and responsible AI vision.[12] So, just as the end of

---

9. EDPB 2024 (n7) 3.

10. OECD "The value of data in digital- based business models: Measurement and economic policy implications" (*www.oecd.org*, 30 August 2022) 11 < https://dx.doi.org/10.1787/d960a10c-en> accessed 2 March 2025.

11. Shoshana Zuboff (n3) 5.

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

The Purge restores legal order, the General Data Protection Regulation (GDPR)[13] and related digital regulatory frameworks[14] aim to limit exploitative data practices. While critics say that the GDPR hinders AI innovation by increasing compliance burdens,[15] this paper argues that it may foster long-term innovation by meeting the criteria of Porter's hypothesis for effective and innovation-inducing regulation.[16]

2. Porter's Hypothesis

Porter's hypothesis states that ***'Well-crafted environmental regulations can result in innovation and innovation offsets***.'[17] This is because companies do not have all the insight into all possible profitable, innovative avenues.[18] Accordingly, regulation can assist companies in overcoming organisational inertia by mitigating complacency and exposing firms to new issues, possibilities and technologies.[19] For example, environmental laws such as the CO2 emissions standards for cars created new markets for electric vehicles (EVs).[20] Car manufacturers

13. GDPR (n7) art. 2(1).

14. The EU Digital Ecosystem Framework consists of several initiatives, regulations, and strategies aimed at fostering the digital transformation of the EU's economy and society while ensuring digital security, privacy, and ethical use of technology.

15. Knut Blind, Crispin Niebel and Christian Rammer (2024) The impact of the EU General data protection regulation on product innovation, Industry and Innovation, 31:3, 311-351, 334 <https://DOI: 10.1080/13662716.2023.2271858> accessed 5 March 2025.

16. Micheal Porter and Class van der Linde "Toward a New Conception of the Environment Competitiveness Relationship." The Journal of Economic Perspectives, 9 4 (1995) 97–118. JSTOR 100 <http://www.jstor.org/stable/2138392> accessed 11 March 2025.

17. Ibid (n16) 101.

18. Ibid (n16) 103.

19. Ibid (n16) 102.

20. Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019

such as Volkswagen and BMW have expanded their EV production, thereby lowering emissions, increasing mobility and leading innovations in battery efficiencies.[21] In the case of environmental regulations, emissions standards created profitable avenues for companies in EV technologies.

Within the context above, innovation is the generation, acceptance and implementation of new ideas, processes, products or services, and regulation is the implementation of rules by public authorities to influence the market activity of private actors.[22] In this paradigm, regulation balances private interests with societal values and public interests.[23]

2.1. Regulation vs Innovation Debate

Porter's hypothesis emerged amid rising awareness of environmental issues and debates about whether environmental regulations harm economic growth.[24] This narrative mirrors the current backdrop against which AI innova-

---

setting CO2 emission performance standards for new passenger cars and for new light commercial vehicles, and repealing Regulations (EC) No 443/2009 and (EU) No 510/2011 (recast) (Text with EEA relevance).

21. Monolith "Balancing sustainability and innovation: Investments in EV battery testing and AI integration" (*www.monolith.com*, June 2024) <https://www.monolithai.com/blog/ev-sustainability-oems> accessed 20 March 2025.

22. Omar Alghamdi and Gomaa Agag, 'Competitive Advantage: A Longitudinal Analysis of the Roles of Data-Driven Innovation Capabilities, Marketing Agility, and Market Turbulence' (2024) 76 *Journal of Retailing and Consumer Services* 103547 7 < https://doi.org/10.1016/j.jretconser.2023.103547> accessed 5 March 2025.ECD/Eurostat, 'Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation' 1 – 226(4th edn, OECD Publishing 2018) 156 <https://doi.org/10.1787/9789264304604-> accessed 12 March 2025.

23. These interests need to be balanced as private entities seek to maximise their profits, sometimes as the cost of public interest such as safety and privacy.

24. Crispin Niebel, 'The Impact of the General Data Protection Regulation on Innovation and

tion is debated in the EU today. At the Paris AI summit in February 2025, US Vice President JD Vance argued that regulation deters innovators from taking the risks necessary to advance the ball.[25] Similarly, scholars and industry stakeholders also state that the GDPR restricts innovation by increasing costs and complicating business activities.[26]

However, these debates overlook the proven detrimental effects of ignoring data protection principles in AI innovation. An example of this is the Anthropic study,[27] which highlights the *importance of data governance in training AI models. The researchers found that as few as 250 malicious documents* can embed backdoors into AI models, making them vulnerable to poisoning attacks.[28] This risk highlights how data protection principles, such as data minimisation, can be useful, as indiscriminate collection and processing of training data pose a threat to the privacy, security, and performance of AI models.

Since the GDPR debate on AI innovation is framed similarly to how environmental regulations were first viewed, this warrants applying Porter's hypothesis by analogy.

---

the Global Political Economy' (2021) 40 Computer Law & Security Review 105523 6 < https://doi.org/10.1016/j.clsr.2020.105523> accessed 7 March 2025.

25. JD Vance, 'Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France' (11 February 2025) The American Presidency Project <https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france> accessed 25 March 2025.

26. Knut Blind, Crispin Niebel & Christian Rammer (n15) 313.

27. Alexandra Souly, Javier Rando, Ed Chapman, Xander Davies, Burak Hasircioglu, Ezzeldin Shereen, Carlos Mougan, Vasilios Mavroudis, Erik Jones, Chris Hicks, Nicholas Carlini, Yarin Gal, Robert Kirk, Poisoning Attacks on LLMs Require a Near-constant Number of Poison Samples (2025) https://arxiv.org/abs/2510.07192 accessed 13 January 2026.

28. Ibid (n27) 1. A **poisoning attack**, especially in AI and Machine Learning, is a cyberattack where attackers corrupt an AI model's training data by injecting malicious, biased, or incorrect information to degrade performance, introduce vulnerabilities, or cause harmful, inaccurate outputs.

2.2. The Application of Porter's Hypothesis

As predicted by Porter, environmental regulation has so far had a positive impact on green innovations.[29] For example, renewable energy technologies (RET) have created new markets and addressed imminent threats to society. In 2024, RET accounted for 46.9% of energy generation in Europe, reducing energy-related costs for companies and reducing dependence on depleting natural resources.[30] This current state of affairs further reinforces the conclusion that the application of Porter's hypothesis is appropriate and relevant to the discussion in this paper, as the hypothesis has been proven in real-world conditions.

According to PH, a well-crafted regulation clearly states its objectives and focuses on the outcomes rather than a specific technology.[31] It also encourages ongoing innovation by providing some market incentives.[32] It fosters cooperation and coordination between regulators at different government levels, including third countries, while minimising confusion about a regulation's features.[33] Jeff & Palmer (1997) further developed PH.[34]

Figure 2: Jeff & Palmer's (1997) expansion on Porter's hypothesis.[35]

---

29. Alessio Tartaro and Adam Smith et al, 'Assessing the impact of regulations and standards on innovation in the field of AI', (2023) Papers 2302.04110, arXiv.org. 4 <DOI:10.48550/arXiv.2302.04110> accessed 7 March 2025.

30. European Commission, 'EU Trade in Goods: Import and Export Statistics' (*EUROSTAT*, 19 March 2025) <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250319-1> accessed 20 March 2025.

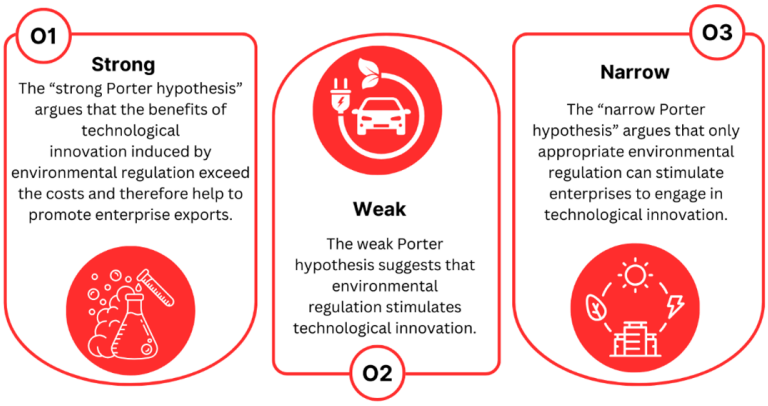
31. Micheal Porter and Class van der Linde (n31) 101.

32. Micheal Porter and Class van der Linde (n31) 101.

33. Micheal Porter and Class van der Linde (n31) 101.

34. Adam B Jaffe and Karen Palmer, 'Environmental Regulation and Innovation: A Panel Data Study' (1997) 79(4) Review of Economics and Statistics 610, 610–619 <https://doi.org/10.1162/003465397557196> accessed 17 March 2025.

35. Yujuan Wu and Jacquline Tham, 'The Impact of Environmental Regulation, Environment,



Source: Author

The authors expanded PH into three categories: the strong version, exemplified by renewable energy sectors, in which companies like Siemens increase their exports of clean energy technologies that outweigh the costs associated with compliance.[36]

The weak version is demonstrated by the investment in electric vehicles, which creates new technologies and markets. Lastly, the narrow version, exemplified by regulations such as REACH,[37] which led French companies (Lafarge

---

Social and Government Performance, and Technological Innovation on Enterprise Resilience under a Green Recovery' (2023) 9(10) Heliyon 20278 3 <https://doi.org/10.1016/j.heliyon.2023.e20278> accessed 18 March 2025.

36. Siemens Energy, 'Expanding Renewables' (*Siemens Energy*, 2025) <https://www.siemens-energy.com/global/en/home/energy-transition/strategies/expand-renewables.html> accessed 25 March 2025; Siemens, *Sustainability Report 2024* (2024) 31 <https://assets.new.siemens.com/siemens/assets/api/uuid:32a7154d-edba-47bc-8e9b-9761617ba774/sustainability-report.pdf> accessed 20 March 2025.

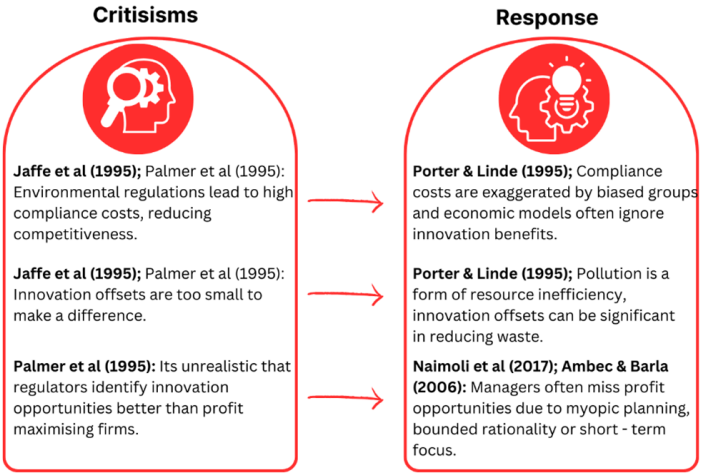
37. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (Text with EEA relevance)Text with EEA relevance.

and Ciment Calcia) to develop a chemical composition that is as durable as cement but reduces environmental footprint by 65%.[38]

2.3. Critics of Porter's Hypothesis

While a detailed discussion of PH's critiques falls outside the scope of this paper, the figure below outlines some key criticisms that are also raised against the GDPR. These serve to highlight the debate surrounding its validity and practical applicability.

Figure 3: Critiques of Porter's hypothesis and Porter's response to critiques.



Source: Author.

In response to similar criticisms in the sphere of AI and Data, it's important to note that studies show that compliance costs do negatively affect small and medium-sized enterprises (SMEs) and AI start-ups.[39] However, these costs can be mitigated by the body of packages introduced by the Commission that seek to simplify compliance and inject financial resources for SMEs and startups,

38. Energy Industry Review, 'Is Green Concrete Truly Environmentally Friendly?' (*Energy Industry Review*, 2023) <https://energyindustryreview.com/analysis/is-green-concrete-truly-environmentally-friendly/> accessed 22 March 2025.

39. Nicholas Martin and Crispin Niebel et al (n34) 1310.

such as the EU Horizon programme.[40] Additionally, the collection and processing of vast amounts of data that may be inaccurate or useless is a sign of inefficiency, as it increases computing costs and may result in poor-performing AI models.[41] So, by implementing data protection principles in AI training, companies can maximise innovation offsets by reducing inefficiency in their processing mechanisms.

Lastly, due to the current business models of data-driven companies, managers overlook opportunities for profit, such as leveraging privacy as a selling point and using data accuracy to develop higher-performing AI models.[42] This is because companies have a myopic view of the many opportunities for profit in the data-driven sphere, focusing on short-term profit maximisation rather than innovative ways to address the needs and demands of individuals and businesses alike.

3. Porter's Hypothesis and the GDPR

The GDPR has led to more investment in compliance innovation and regulatory-exploiting innovations.[43] Meaning that the weak hypothesis best describes the trajectory of GDPR in AI innovation at present. However, once learning has occurred, the compliance costs will be outweighed by technological innovation in AI and Data, leading to the application of the strong version of PH. This is

40. European Commission, 'Funding Programmes and Open Calls: Horizon Europe' (*Research and Innovation*) https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls_en accessed 14 March 2025.

41. Max Ebers and Karsten Sein (eds), *Privacy, Data Protection and Data-driven Technologies* (1st edn, Routledge 2024) 143 <https://doi-org.proxy-ub.rug.nl/10.4324/9781003502791> accessed 2 March 2025.

42. Ibid (n41) 144.

43. Nicholas Martin and Crispin Niebel et al "How Data Protection Regulation Affects Startup Innovation" (2019) 21, 1307–1324 Inf Syst Front 1318 <https://doi.org/10.1007/s10796-019-09974-2> accessed 5 March 2025.

because the GDPR satisfies the criteria of a well-crafted regulation in terms of PH.

3.1. The GDPR is Technologically Neutral and sets Clear Goals.

Generally, the GDPR's objectives are transparent: the regulation aims for '*... the protection of personal data*' and the promotion of '*the free movement of personal data within the Union...*'.[44] Thus, Articles 24 and 34(1) require controllers and processors to achieve these objectives by implementing appropriate technical and organisational measures, without mandating the use of a particular technology.[45] The aims outlined above have recently been reinforced in the Schrems judgment, in which the court, when deciding on the lawfulness of data transfers to third countries,[46] reiterated that the purpose of GDPR is to provide a high level of data protection while allowing for the free movement of data.[47] It is clear from the law's wording that the GDPR focuses on the outcome of the AI model's training processes, giving controllers the freedom to choose the most appropriate measure for their business model to provide the protections guaranteed by the GDPR.

3.2. The GDPR Induces Innovation, and Market Incentives are Present.

How the GDPR stimulates innovation can be discussed under the principle of

44. GDPR (n7) art. 2(1).

45. GDPR (n7) Recital 15.

46. The question before the court was whether the European Commission's 'Safe Harbor' decision (Decision 2000/520/EC), which allowed the transfer of personal data from the EU to the United States, provides an adequate level of protection as required under EU data protection law.

47. Case C-446/21 *Maximilian Schrems v Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)*, Judgment of the Court (Fourth Chamber) of 4 October 2024 para 43.

data minimisation, as this is a point of tension in AI and data. Article 5 (1)(c) requires the controller to process personal data '*in a manner that is … limited to what is necessary for processing*'.[48] Recital 78 requires the '*minimisation of personal data*' as an organisational measure for data protection by design and default.[49] Additionally, the courts have previously held that the principle of data minimisation must be interpreted in light of the principle of proportionality under Article 5(4) of the Treaty on the European Union.[50] This means that processing personal data for training purposes must not be excessive in relation to the desired training goals.[51]

In essence, data minimisation does not exclude the use of personal data in training AI models; instead, training must be conducted in accordance with data protection principles. Data may be minimised using various technical measures. Such as privacy-by-design techniques like k-anonymity, which replaces an exact data point with a range, data masking that replaces personal data with randomised values, or synthetic data that is artificially generated and does not relate to real individuals.[52] For example, DeepMind, a UK-based AI company, developed a privacy-preserving machine learning tool that employed federated learning[53] and differential privacy[54] methods to train AI models with-

48. GDPR (n7) art. 5(1)(e).

49. GDPR (n7) rec. 78.

50. C-439/19 – Latvijas Republikas Saeima (Points de pénalité) EU:C:2021:504, para 98.

51. Treaty on European Union [2016] OJ C202/13, Article 5(4).

52. It must be noted that the use of synthetic data is only a workaround, as the underlying model also needs to be trained on personal data.

53. A machine learning technique where AI models are trained locally on decentralised devices or servers instead of collecting data in a central location. Only model updates (not raw data) are shared.

54. A privacy-enhancing technique that adds mathematical noise to data before analysis, ensuring AI models learn from general patterns without identifying individual users.

out accessing raw data.[55] This approach has enabled Google's Gboard keyboard (powered by DeepMind) to improve text prediction without storing users' typing history. This is evidence that AI innovation can occur without violating the principle of data minimisation. Furthermore, companies may exploit regulatory innovation to create new markets. This is already happening with privacy-enhancing technologies (PETs). The PET market, spurred by the GDPR, is constantly growing, and Europe holds the second-largest share of the global market.[56]

Admittedly, compliance costs under the GDPR may predominate over innovation in the short term, since regulations disrupt existing ways of doing things. However, a study by Blind & Neibel (2024) found that the GDPR promoted incremental innovation in the surveyed German companies.[57] These companies were forced to reorganise their data management, leading to improvements in existing products.[58] However, radical innovation saw a slight decline since resources needed for GDPR compliance limited the capacity to develop entirely new products.[59]

According to PH, this is an expected consequence of regulation in the short term since innovation cannot always completely offset the cost of compliance. Only once learning reduces the cost of innovation-based solutions will radical innovation thrive. In the meantime, the more immediate barriers to DDI should

55. Balancing data protection with business innovation: A guide for UK start – ups (*jpplaw.co.uk*) <https://www.jpplaw.co.uk/news/data-protection/balancing-datrotection-with-business-innovation-a-guide-for-uk-startups/> accessed 12 March 2025.

56. Fortune Business Insights 'Privacy Enhancing Technologies Market Size, Share, Trend 2032' (*www.fortunebusinessinsights.com*, 2024) <https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241> accessed 16 March 2025.

57. Knut Blind, Crispin Niebel and Christian Rammer, (n15) 313.

58. Knut Blind, Crispin Niebel and Christian Rammer, (n15) 313.

59. Knut Blind, Crispin Niebel and Christian Rammer, (n15) 313.

be addressed, such as a lack of digital infrastructure, capital investment and a shortage of skills.[60]

3.2.1. GDPR Market Incentive

Regarding the market incentives provided by the GDPR, a study conducted by Martin (2019) found that compliance with the GDPR was a prerequisite to participating in business-to-business (B2B) markets in the EU.[61] This means that companies are incentivised to demonstrate GDPR compliance to do business with other businesses. However, unlike the tag '*eco–friendly*' in environmental sectors, *'data protection-friendly'* has limited potential as a competitive differentiator in business-to-consumer (B2C).[62] This is because most users choose products based on functionality and price, but as consumer awareness rises, this will change. Moreover, it should be noted that GDPR compliance does not exclude firms' liability in data breaches. However, the possession of data protection certifications and adherence to codes of conduct may be considered mitigating factors, decreasing the amount of the fine imposed.[63]This further incentivises companies to comply, given the €20 million or 4% of global turnover (whichever is higher) penalty for non-compliance.

3.3. Multi-level Governmental and International Cooperation and Guidance are Promoted under the GDPR.

The GDPR allows cooperation among different actors and guides the implementation of cooperation mechanisms.

Figure 4: Co-operation mechanisms for the enforcement of the GDPR.[64]

60. Knut Blind, Crispin Niebel and Christian Rammer, (n15) 314.

61. Nicholas Martin and Crispin Niebel et al (n43) 1318; GDPR (n7) Recital 15.

62. Nicholas Martin and Crispin Niebel et al (n43) 1318;

63. European Data Protection Board, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR' (Version 2.1, 24 May 2023) 26 < https://www.edpb.europa.eu/system/files/2023 06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf> accessed 10 March 2025.

64. GDPR (n7).

Authority	Role in GDPR enforcement	Cooperation Mechanism
Court of Justice of the European Union. **(EU Level)**	Interprets GDPR and ensures uniform application across the EU.	Provides authoritative interpretations of GDPR for NC under Article 267 TFEU. Such as in *Facebook v Ireland case*, where it held that DPAs must give effect to effective judicial remedies under Art. 78 GDPR by investigating complaints.
National Courts. **(Member state level)**	Hears and decides on GDPR related cases within their jurisdiction. (Art. 79 and Rec. 143 GDPR).	Works with DPAs to ensure the enforcement of their decisions and can refer questions on GDPR interpretation to the CJEU under Art. 267 TFEU.
European Commission. **(EU level)**	Oversees GDPR mechanisms, negotiates international agreements, and ensures GDPR compliance. (Art. 45 - 50 GDPR).	Works with DPAs and the EDPB to ensure GDPR's uniform application in terms of Article 50 GDPR and facilitates and enters into international cooperation on transfer of data under Art. 45 GDPR.
European Data Protection Board (EDPB). Estbalished under Art. 68(1) GDPR. **(EU level)**	Made up of representatives from DPAs of Member States and can enter into international agreements such as the EU - Us *Data Privacy Framework* (Art. 45 GDPR).	Provides binding decisions in cross-border cases under At. 65 GDPR and promotes consistent application through guidelines and recommendations under Art. 70 GDPR.
National Data Protection Authorities (DPAs). Established under Art. 51(1) **(Member State level)**	Enforce GDPR at the national level, handle complaints, conduct investigations, give warnings and impose fines (Art. 58(2) GDPR).	Cooperates with other DPAs for cross-border processing cases under Art. 60 GDPR and participate in information for mutual assistance and joint operations with other DPAs under Art. 61 & 62 GDPR.

Source: Author

In a scenario where a company (for example DDI Inc) wants to train its AI model on the data originating from the EU, this cooperation mechanism would operate in the following way:

1. DDI Inc. would conduct a Data Protection Impact Assessment, since data processing would involve using new technology – AI.[65]
2. Where this DPIA shows a high risk to data protection, the controller can consult the supervisory authority (SA) on how to proceed.[66]
3. This advice is further informed by the opinions of the European Data Protection Board (EDPB) and by the interpretation of the Courts.
4. If DDI Inc. disagrees with the decision issued by DDI Inc., it can start proceedings in the national court to resolve the dispute.[67]
5. The NC may also refer preliminary questions to the Court of Justice of the European Union (CJEU) for further clarification.[68]

65. GDPR (n7) art. 35(1).

66. GDPR (n7) art. 36.

67. GDPR (n7) art. 78.

The co-operation mechanisms create an open communication channel and enables multi-governmental cooperation and guidance to minimise confusion regarding GDPR principles and their application. As the French Commission Nationale de l'Informatique et des Libertés (CNIL) stated, SAs would take the time to explain to companies how they must do things rather than just issuing fines.[69] However, if DDI Inc. does not heed the SA's advice and subsequently infringes the GDPR, the SA can exercise its broad discretionary powers to issue warnings, reprimand controllers, ban processing, or even issue an administrative fine.[70] This is exactly what happened with ChatGPT in Italy, where it was temporarily banned pending an investigation into its GDPR compliance. It was unbanned once compliance was demonstrated.[71]

3.3.1. The GDPR needs Stronger Enforcement

Rules are only as effective as their enforcement mechanisms, and the GDPR cannot achieve its stated objectives or foster innovation unless its provisions are enforced consistently and effectively across the board, including in respect of both local and international organisations. Admittedly, the European Commission (EC) has acknowledged some areas that must be addressed in the enforcement of the GDPR:[72]

---

68. *Treaty on the Functioning of the European Union* [2012] OJ C 326/47 art. 267.

69. JosePorters hypothesisJerome " The GDPR's impact on innovation should not be overstated" (*cdt.org*, April 1 2019) European Policy, Privacy and Data, < https://cdt.org/insights/the-gdprs-impact-on-innovation-should-not-be-overstated/> accessed 8 March 2025.

70. GDPR (n7) art. 58(2).

71. Econotimes, 'ChatGPT: Lessons Learned from Italy's Temporary Ban of the AI Chatbot' (*Econotimes*, 9 May 2023) https://www.econotimes.com/ChatGPT-lessons-learned-from-Italys-temporary-ban-of-the-AI-chatbot-1654725?utm_source=chatgpt.com accessed 20 March 2025.

72. European Commission, *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*

- Harmonisation of complaint procedures and guidelines by regulators across different member states.
- DPAs must develop more practical tools for executing obligations under GDPR (especially for SMEs).
- The EDPB and the DPA should continue to clarify central aspects of the GDPR and provide guidance.
- MS should not go beyond the scope of the GDPR by adding requirements that were not initially stipulated.

Since enforcement is the primary driver of regulatory compliance, these areas should be prioritised to ensure legal certainty, consistency, and the effective realisation of the GDPR's policy objectives.

4. Conclusion

It is worth noting that the GDPR is still in its infancy, and companies will continue to learn to innovate under the GDPR with guidance from SA's. However, for this to happen, company compliance is crucial, as learning cannot occur without the effective implementation of the GDPR, even though the GDPR does not distinguish between intentional and unintentional violations of its principles. Stronger enforcement measures, such as market bans, must be taken against blatant disregard for GDPR principles for it to achieve the EU's data protection objectives.[73]

The case of Clearview AI provides a good example.[74] Not only is the business model blind by design, but Clearview has also ignored numerous orders requiring it to implement technical and organisational safeguards to comply with

---

COM(2020) 264 final 6 <https://ec.europa.eu/info/sites/info/files/2nd_report_on_gdpr_implementation_en.pdf> accessed 25 March 2025.

73. Banning should be the last resort, as SAs have extensive corrective powers under Article 58(2) GDPR, giving DDI companies ample opportunity to conform to GDPR.

74. CNIL, Decision No. SAN-2021-012, 16 December 2021, Clearview AI Inc. – Unlawful Processing of Biometric Data; Garante per la protezione dei dati personali, Decision No. 9751436, 10 February 2022, Clearview AI Inc. – Violation of GDPR Provisions; Autoriteit Persoonsgegevens, 17 January 2022, Decision on Clearview AI Inc., Processing of Biometric Data without a Lawful Basis.

GDPR. Such situations can be addressed under the current legal framework by applying the GDPR in conjunction with the EU AI Act.[75] Firstly, the Member States' DPAs should serve as the Market Surveillance Authority for the adequate supervision of AI, as advocated by the Dutch DPA.[76] This will allow authorities to handle matters under the same roof, leading to effective enforcement of the GDPR and AI Act. Secondly, in the event of repeated non-compliance with the AI Act, which encompasses data protection principles, the Market Surveillance Authority has the power to take corrective action and even restrict or prohibit AI systems from the EU market.[77] This power should be exercised without fear or favour, as barring repeat offenders is justified because the EU has the authority to exclude products that fail to meet safety standards and the responsibility to protect citizens' data rights. For those who worry that EU citizens will miss out on new technologies, a critical reflection is needed. **'What kind of innovation do we want?'**

Bibliography

Treaties and Legal Documents

Treaty on the Functioning of the European Union [2012] OJ C 326/47

Treaty on European Union [2016] OJ C202/13

75. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

76. Dutch Authority for Digital Infrastructure, Dutch Data Protection Authority, '2nd (Interim) Advice on the Dutch Supervisory Structure for the AI Act' (16 May 2024) The Minister of Economic Affairs and Climate Policy, The Minister for Digitalisation, The Minister for Legal Protection.

77. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance.) art. 14(h).

Legislation

Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019 setting CO2 Emission Performance Standards for New Passenger Cars and for New Light Commercial Vehicles, and Repealing Regulations (EC) No 443/2009 and (EU) No 510/2011 (Recast) (Text with EEA Relevance)

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on Market Surveillance and Compliance of Products and Amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA Relevance)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance)

Case Law

Case C-446/21 Maximilian Schrems v Meta Platforms Ireland Limited (formerly Facebook Ireland Limited), Judgment of the Court (Fourth Chamber) of 4 October 2024

Case C-439/19 – Latvijas Republikas Saeima (Points de pénalité) EU: C:2021:504

Decisions and opinions

Autoriteit Persoonsgegevens, 17 January 2022, Decision on Clearview AI Inc., Processing of Biometric Data without a Lawful Basis

CNIL, Decision No. SAN-2021-012, 16 December 2021, Clearview AI Inc. – Unlawful Processing of Biometric Data

European Data Protection Board, Opinion 04/2024 on the Use of Personal Data for the Training of AI Models (EDPB 2024)

Garante per la protezione dei dati personali, Decision No. 9751436, 10 February 2022, Clearview AI Inc. – Violation of GDPR Provisions

Commission documents

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

European Commission, Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation COM(2020) 264 final 6

Guidelines and reports

European Data Protection Board, 'Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR' (2023)

OECD, 'The Value of Data in Digital-Based Business Models: Measurement and Economic Policy Implications' (2022)

European Data Protection Board, Opinion 04/2024 on the use of personal data for the training of AI models (EDPB 2024)

Books

Ebers M and Sein K, "Privacy, Data protection and Data – driven Technologies" (1st edn, Routledge 2024)

ECD/Eurostat, 'Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation' (4th edn, OECD Publishing 2018)

Journal Articles

Alghamdi O and Agag G, 'Competitive Advantage: A Longitudinal Analysis of the Roles of Data-Driven Innovation Capabilities, Marketing Agility, and Market Turbulence' (2024) 76 Journal of Retailing and Consumer Services 103547

Ambec S and Barla P "Can environmental regulations be good for business? An assessment of the Porter hypothesis" (2006) Energy Stud Rev, 14

Birch K and Kelly Bronson K, 'Big Tech' (2022) 31(1) Science as Culture 1–14

Blind K, Niebel C and Rammer C, 'The Impact of the EU General Data Protection Regulation on Product Innovation' (2024) 31:3 Industry and Innovation 311–351

Jaffe AB and Palmer K, 'Environmental Regulation and Innovation: A Panel Data Study' (1997) 79(4) Review of Economics and Statistics 610–619

Martin N and Niebel C, " How data protection affairs affect startup innovation" (2019) 21, 1307 – 1324 Inf Syst Font

Naimoli S and Kodjak D, German J and Schultz J "International competitiveness and the auto industry: what's the role of motor vehicle emission standards?" (2017) The Int Council Clean Transp, 13

Niebel C, 'The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy' (2021) 40 Computer Law & Security Review 105523 6

Porter M and van der Linde C, 'Toward a New Conception of the Environment-Competitiveness Relationship' (1995) 9:4 The Journal of Economic Perspectives 97–118

Tartaro A and Smith A et al, "Assessing the impact of regulations and standards on innovation in the field of AI, (2023) Papers 2302.04110

Wu Y and Tham J, 'The Impact of Environmental Regulation, Environment, Social and Government Performance, and Technological Innovation on Enterprise Resilience Under a Green Recovery' (2023) 9(10) Heliyon 20278 3

Zuboff S, 'Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilisation' (2022) 3:1 Organisation Theory 3

Online Resources:

Balancing Data Protection with Business Innovation: A Guide for UK Start-ups (jpplaw.co.uk, 2024)

D Vance, 'Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France' (www.precidency.ucsb.edu, 11 February 2025). The American Presidency Project

Econotimes, 'ChatGPT: Lessons Learned from Italy's Temporary Ban of the AI Chatbot' (www.econotimes.com, 9 May 2023)

Energy Industry Review, 'Is Green Concrete Truly Environmentally Friendly?' (www.energyindustryreview.com, 2023)

European Commission, 'EU Trade in Goods: Import and Export Statistics' (EUROSTAT, 19 March 2025)

Fortune Business Insights, 'Privacy Enhancing Technologies Market Size, Share, Trend 2032' (www.fortunebusinessinsights.com, 2024)

Garante per la protezione dei dati personali, 'The Data Protection Authority's Investigative Procedure' (www.garanteprivacy.it, 10 January 2025)

Jerome J, 'The GDPR's Impact on Innovation Should Not Be Overstated' (www.cdt.org, 2019)

Meta, ‘Meta Reports Third Quarter 2024 Results’ (www.investor.atmeta.com, July 2024)

Marques I, ‘Will Loss of AI Specific Liability Rules Leave Victims Without Recourse?’ (Euronews.com, 4 March 2025)

Monolith, ‘Balancing Sustainability and Innovation: Investments in EV Battery Testing and AI Integration’ (www.monolithai.com, June 2024)

Siemens Energy, ‘Expanding Renewables’ (www.siemens-energy.com, 2025)

Siemens, Sustainability Report 2024 (assets.new.siemens.com, 2024)

Other

Haugen Frances, Facebook’s Whistleblower Testimony to the U.S Senate (2021)

About the author

Karabo Lerato Mokoena

Karabo Lerato Mokoena obtained an LLM in Technology Law and Innovation from the University of Groningen, after completing her undergraduate studies (LLB, BA Hons in Psychology and BA Law) at the University of Johannesburg. She practises digital technology law in Cape Town, South Africa. Karabo helps data-driven, AI-enabled businesses across all sectors use data and AI lawfully by embedding compliance by design and default into how they operate. She is also a member of AI Safety South Africa where she is upskilling in technical AI governance.

CHAPTER 8: ANONYMISATION AS A TOOL FOR DATA PROTECTION FOR AI MODEL TRAINING

Marina El Moufti

Abstract

This paper assesses whether anonymisation is an effective tool for AI model training taking into account personal data protection obligations. The paper explores the potential incompatibility between data controllers complying with the obligations of the GDPR, namely upholding the accountability, lawfulness, data minimisation, purpose and storage limitation data processing principles, and using pre-obtained personal data for AI model training. Anonymisation of personal data used for AI model training is proposed as a tool to overcome this incompatibility by transforming personal data into data which is no longer linked to data subjects, rendering the GDPR inapplicable to pre-collected anonymised personal data. Various anonymisation techniques are explored to assess their effectiveness at anonymising data while maintaining the utility of AI models and preventing re-identification risks. The paper concludes by acknowledging the limitations of anonymisation in rendering personal data 'truly anonymous', while offering various recommendations based on the EDPB guidelines and the *Breyer* case to manage re-identification risks.

1. Problem Definition and Relevance

The General Data Protection Regulation (GDPR) has altered the way personal data is processed in the European Union (EU) and beyond by setting a framework for how personal data of individuals in the EU is processed and how entities established within the EU can process personal data. With the increased development and use of artificial intelligence (AI) systems globally, new challenges to personal data protection arise. This is because the established EU

framework of personal data protection becomes challenged with this technology pursuant to the 'Collingridge Dilemma'.

There is misalignment between the speed of regulation and the speed of technological innovation as regulating technology ex-ante does not allow for fully understanding its implications, however, regulating ex-post may lead to regulation which is insufficiently effective to address the technological innovation.[1] The GDPR was published in the Official Journal of the European Union in 2016, before significant advancements in the field of AI had been realised. AI systems' reliance on vast amounts of personal and non-personal data, autonomous nature, widespread use, and ability to make inferences and predications from various data points may lead to a loss of control and oversight over personal data, leading to an incompatibility with the GDPR.[2]

This incompatibility may make complying with the GDPR's data protection principles challenging for data controllers who intend on using pre-obtained personal data for the purpose of AI model training. In those instances, anonymisation could be used as a tool to circumvent the applicability of the GDPR. The GDPR's subject matter is the protection of individuals' personal data.[3] This is data linked to an identified or identifiable natural person ('data subject').[4] According to Recital 26 GDPR, the GDPR does not apply to data that cannot be linked to identified or identifiable individuals or personal data that has undergone anonymisation leading to personal data no longer being

1. Daniel Tigard, 'Chapter 1: Embedded ethics as preparatory regulation of technology: a new solution to the Collingridge Dilemma?' (2022) Novel Beings Edward Elgar Publishing <https://doi.org/10.4337/9781800889262.00008>accessed Sep 18, 2025, 13.

2. Giovanni Sartor, Francesca Lagioia, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' PE 641.530 (Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA), June 2022), 2.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L119 (GDPR), art. 1(1).

4. GDPR, art. 4(1).

linked to that data ('anonymized data').[5] Although not all data used for training AI models is personal data, personal data can be part of the training data, in which case the GDPR will apply. Once pre-obtained personal data is anonymised, it is no longer data belonging to an identified or identifiable individual, hence, obligations of data controllers under the GDPR will cease to apply. Therefore, anonymisation can be used as a tool for processing pre-obtained personal data for AI model training, free from GDPR obligations over the anonymised data.

This paper explores the relationship between anonymisation and the applicability of the GDPR to pre-obtained personal data intended for AI model training. Section 2 expands on the conflict between AI model training and data protection principles under the GDPR, namely the accountability, lawfulness, data minimisation, and purpose and storage limitation principles. Section 3 clarifies what anonymisation entails by introducing various anonymisation techniques and their limitations. Section 4 examines the potential drawbacks of using anonymisation for AI model training including decreased utility of AI systems and re-identification risks. Section 5 concludes the paper by reflecting on whether anonymisation is the optimal tool for circumventing GDPR obligations in the context of AI model training while also offering recommendations to mitigate risks of re-identification and demonstrating regulatory compliance.

2. The Conflict Between AI Model Training and Data Protection Principles

Conflicts may arise between using personal data for AI model training and data protection principles under the GDPR, insofar as training techniques may impede compliance with the Regulation's requirements. AI model training is reliant on a variety of techniques, this includes supervised learning, unsupervised learning, and reinforcement learning.[6] Supervised learning matches an

5. GDPR, Recital 26.

6. Philipp Hacker, 'A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act' (2021) Law, Innovation and Technology 13 (2) 257–301 < https://doi.org/10.1080/17579961.2021.1977219> accessed 26 March 2025.

algorithm's predictions with data based on the training dataset to find the most accurate output,[7] while reinforcement learning optimally uses data in a learning environment to return a response to the system on which output would be the best.[8] In many cases, reinforcement learning is built upon supervised learning models.[9] Reinforcement learning can be compared to 'trial-and-error' learning, aiming at improving the accuracy of outputs.[10] AI models based on supervised, unsupervised, and reinforcement learning techniques rely on data of personal and non-personal nature for training datasets. When personal data is used to train AI systems, this data falls under the scope of the GDPR.

Article 5(2) GDPR holds controllers, who determine the purposes and means of the processing of personal data, responsible for complying with the data protection principles, however, the nature of AI undermines accountability.[11] Training datasets tend to be extremely large and may include both personal and non-personal data, causing difficulty in separating personal data from non-personal data, especially when the data is collected through web scraping.[12] This creates uncertainty regarding the GDPR's applicability over the training dataset. Even when the applicability of the GDPR can be established, implementing data protection principles such as lawfulness, data minimisation, and purpose and storage limitation remains challenging.

Training AI models does not consist of merely processing data in a fixed and pre-defined manner, instead inferences and predictions based on the train-

7. Ibid.

8. Ibid.

9. Ibid.

10. Michael Chen, 'What Is Reinforcement Learning?' (*Oracle.com*, 3 April 2024) < https://www.oracle.com/nl/artificial-intelligence/machine-learning/reinforcement-learning/ > accessed 26 March 2025.

11. GDPR, art. 5(2); GDPR, art. 4(7).

12. Rainer Mühlhoff, Hannah Ruschemeier, 'Regulating AI with Purpose Limitation for Models' (2024) Journal of AI Law and Regulation 1 1 <https://doi.org/10.21552/aire/2024/1/5> accessed 18 September 2025, 24-39, II (1).

ing data and training techniques are made, resulting in continuous repurposing and unforeseen usage of training data.[13] Thus, AI systems do not merely process personal data based on instructions given by a controller, they can generate outputs for widespread and undefined purposes, conflicting with the data minimisation and purpose and storage limitation principles.[14] Furthermore, using personal data for AI model training may cause friction with the principle of lawfulness when personal data processing is based on consent. Given that AI systems continuously generate new data during training, each distinct purpose of processing would require renewed consent from the data subject, resulting in a need for continuous consent requests. Such a requirement would impose a disproportionate burden on both controllers and data subjects, thereby rendering consent an impractical lawful basis for personal data processing in this context.[15] Consequently, using pre-obtained personal data for AI model training may undermine the accountability principle by creating obstacles for controllers to implement the principles of lawfulness, data minimisation, and purpose and storage limitation.

3. Anonymisation

Data anonymisation techniques must be applied to render personal data anonymous. There are various anonymisation techniques, including suppression, character replacement, shuffling, noise addition, and generalisation. They vary in efficacy levels depending on the corresponding purpose of anonymis-

13. Rania El-Gazzar, Karen Stendal, 'Examining How GDPR Challenges Emerging Technologies' (2020) Journal of Information Policy 1 10 237–275 <https://doi.org/10.5325/jinfopoli.10.2020.0237> accessed 27 March 2025.

14. Ibid.

15. Eirini Mougiakou, Spyros Papadimitriou, Konstantina Chrysafiadi, Maria Virvou, 'Artificial intelligence in educational games and consent under general data protection regulation' (2025) Intelligent Decision Technologies 2025 0(0) < https://doi.org/10.1177/187249812513228> accessed 27 March 2025.

ing personal data.[16] Nevertheless, these techniques are not foolproof, and re-identification is possible in most anonymisation methods.[17]

Suppression entails removing attributes which are unnecessary for analysis from a dataset.[18] Suppression can also be used when no other technique can successfully anonymise data.[19] Notably, this technique removes risks of re-identification once attributes have been permanently deleted as their linked data is irretrievable.[20] Character replacement is the replacement or partial replacement of characters of data attributes and values with predefined symbols.[21] Shuffling involves randomly reorganizing data so that the original attribute value stays in the dataset but could be linked to another record. The technique applies to situations where only one attribute is required for analysis without relating it to others.[22] Although, shuffling could allow for re-identification as data may be reorganized to uncover the original data.[23]

Noise addition, a popular anonymisation technique, entails making minor changes to dataset attributes, rendering them more imprecise.[24] Thus, the original data will be modified, however, data analysis could be adversely affected.[25] Generalisation, also a popular anonymisation technique, involves

16. Joana Ferreira Marques, Jorge Bernardino, 'Analysis of Data Anonymisation Techniques' (2020) KEOD 2 236-238 < https://www.scitepress.org/PublishedPapers/2020/101423/101423.pdf> accessed 24 March 2025.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid

25. Ibid.

making attributes more general, preventing the identification of individuals.[26] However, anonymisation is not foolproof when relying on this technique.[27] Generalisation can be applied through several methods such as K-Anonymity and L-Diversity. K-Anonymity anonymises data by rendering an individual's information in a dataset indistinguishable from a minimum number of other individuals.[28] As a result, re-identification is still possible, however, the risk is minimal.[29] L-Diversity is an addition to K-Anonymity where sensitive data linked to individuals is adequately varied to diminish inference when many individuals share the same sensitive data.[30] Therefore, even if re-identification is attempted, attributing data to a certain individual will remain speculative.[31] Nevertheless, L-Diversity is prone to probabilistic inference attacks.[32]

4. Potential Drawbacks of Anonymisation

4.1. Decreased Utility

Anonymisation may be used as a tool to relieve AI system developers from their GDPR obligations, as data would no longer be linked to identified or identifiable individuals. However, this tool may be accompanied by certain draw-

26. Ibid.

27. Ibid.

28. Utrecht University, 'K-anonymity, l-diversity and t-closeness' (*Utrecht University*, 30 May 2023) < https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html > accessed 26 March 2025.

29. Joana Ferreira Marques, Jorge Bernardino, 'Analysis of Data Anonymisation Techniques' (n 15).

30. Utrecht University, 'K-anonymity, l-diversity and t-closeness' (n 27).

31. Joana Ferreira Marques, Jorge Bernardino, 'Analysis of Data Anonymisation Techniques' (n 15).

32. Ibid.

backs which diminish its appeal. For instance, anonymising personal data may increase the difficulty of conducting data analysis as the lack of identification of training data decreases the amount of information available for analysis.[33] This is especially challenging in the context of medical data analysis where patient data is essential, and a high level of precision is necessary. Applying anonymisation techniques such as shuffling, noise addition, and generalisation may decrease the accuracy and reliability of the data including the identifying signatures and biological signals concerned in the analysis.[34]

Furthermore, delinking data from its identifiers such as a data subject's home address would render geographic comparative health research impossible.[35] Thus, when an AI system is intended for certain purposes, anonymisation may not be suitable as it could compromise the optimal functioning and use of an AI system. For example, shuffling would be unsuitable for medical research as several attributes are usually required for data analysis and links between the different attributes are needed to make precise and complex inferences for medical correlations and insights.[36] Noise addition would also undermine medical research as changes to dataset attributes, even if minimal, could greatly impact results of analysis in a field where great precision is needed.[37] Moreover, generalization could prevent the advancement of medical research which relies on the discovery of links by decreasing the amount of inferences which can be made. Thus, anonymisation cannot be regarded as a one-size-fits-all solution, as different applications of AI systems entail distinct data processing requirements.

---

33. Kerstin N Vokinger, Daniel J Stekhoven, Michael Krauthammer, 'Lost in Anonymisation — A Data Anonymisation Reference Classification Merging Legal and Technical Considerations' (2020) The Journal of Law, Medicine & Ethics 48(1) 228-231 < https://doi.org/10.1177/10731105209170> accessed 27 March 2025.

34. Ibid.

35. Ibid.

36. Joana Ferreira Marques, Jorge Bernardino, 'Analysis of Data Anonymisation Techniques' (n 15).

37. Ibid.

4.2. Re-identification Risks

Besides the potential to comprise the optimal use and functioning of an AI system, anonymisation is not free from re-identification risks. Several anonymisation techniques risk re-identification. Apart from suppression, which permanently deletes attributes preventing the data's retrieval, character replacement, shuffling, noise addition, K-Anonymity, and L-Diversity are susceptible to re-identification risks.[38] Despite anonymisation efforts, personal data can still be extracted even when information linking training data to data subjects is no longer found in the dataset, 'but can still be accessed by the controller or a third party.'[39] Additionally, re-identification is possible even when no identifying information can be accessed if technical means are available to de-anonymise data through other existing data.[40]

The European Data Protection Board (EDPB) has clarified that data can be linked to an individual even if it is technically organised or encoded so that its link with a data subject is not obvious from the onset.[41] This statement follows from the ability of software applications to 'easily identify, recognise and extract specific data'.[42] AI systems tend to amplify re-identification risks because model parameters constitute statistical links between training data and personal data, which can be directly or indirectly extracted through those statistical links or through querying.[43] For instance, reliance on L-Diversity may increase re-identification risks due to probabilistic inference. Thus, training

38. Ibid.

39. Philipp Hacker, 'A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act' (n 6).

40. Ibid.

41. European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (Opinion of the Board (Art. 64) (EDPB, 17 December 2024) 14-15.

42. Ibid.

43. Ibid.

data can only be considered anonymous if it is sufficiently proven through reasonable means that personal data cannot be extracted from the AI model and system outputs cannot be linked to data subjects whose data were used for model training through querying.[44]

The EDPB has stated that even AI systems which are not intended to produce personal data from training data, can still absorb personal data from the training dataset in the model parameters.[45] The data absorbed could vary from the original training data, however, the original information can still be stored.[46] Consequently, personal data can still be directly or indirectly extracted from the AI model, thus, the model cannot be considered anonymous in those cases.[47] Therefore, the training data should be anonymised from the onset to ensure personal data is not extracted. Furthermore, the EDPB guidelines on anonymisation techniques indicate that 'if it is not possible to single out, link and infer information from the supposedly anonymous dataset, the data may be considered anonymous.'[48] In the absence of such conditions, AI systems necessitate an extensive analysis of re-identification risks.

This analysis needs to consider every possible technique which could be reasonably expected to be used to identify data subjects, including the nature of the training data, AI model, and training techniques, the purpose of the AI model, the availability of additional information enabling re-identification, and the amount of resources needed to acquire such additional information, as well as the technological state-of-the-art at the time of processing and in the present.[49] Therefore, merely applying anonymisation techniques to personal data used for AI model training does not guarantee that this data is

44. Ibid.

45. European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (n 40), 13-16.

46. Ibid.

47. Ibid.

48. Ibid.

49. Ibid.

'truly anonymised', a rigorous assessment of re-identification risks is needed to ensure the effectiveness of anonymisation. The EDPB's assessment of re-identification risks evaluates an AI model's design, analysis, and testing, as well as its corresponding documentation.[50]

In the *Breyer* case, the Court of Justice of the European Union (CJEU) held that the risk of re-identification depends directly on the likelihood that a data controller will actually attempt to re-identify the data. The Court emphasised that 'it must be reasonably likely that the controller will use the strategies available to him to carry out the identification.'[51] Accordingly, where the likelihood of re-identification by the controller is low, the risk of re-identification cannot be said to arise. The CJEU further indicated that re-identification would require a legitimate interest on the part of the controller.[52] This requirement makes the de-anonymization of data more difficult, assuming it is done lawfully, as not every interest would justify such an action. For example, economic interests such as advertising would generally not constitute a sufficient basis for re-identification, whereas national security interests would more likely be regarded as legitimate. Therefore, an AI model's design, analysis, and testing, as well as its corresponding documentation and the likelihood that a data controller will actually attempt to re-identify the anonymised data constitute significant factors in assessing the effectiveness of anonymisation.

5. Conclusion

The GDPR imposes several obligations on controllers when they use pre-obtained personal data to train AI models. However, the nature of AI systems renders upholding those obligations more onerous. Anonymisation could be used as a tool to ease the tension between the GDPR's obligations and AI model training. Several techniques are available to render personal data anonymous,

50. European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (n 40), 17-19.

51. Ibid.

52. Ibid.

although these techniques vary in efficacy in regard to safeguarding an AI model's performance and decreasing the risks of re-identification. Advanced technical means and the availability of information to controllers and third parties allowing for re-identification may diminish the effectiveness of anonymisation. Moreover, sole reliance on anonymisation techniques is insufficient to guarantee the inapplicability of the GDPR over the anonymised data.

Instead, controllers must perform extensive re-identification analysis on the anonymised data to ensure that it is 'truly anonymous'. The *Breyer* case may be used to interpret part of this analysis in determining the likelihood of re-identification risks. Moreover, technical and organisational measures must be taken and continuously reviewed to ensure that anonymisation is still effective at de-linking the data subject from the training data. For instance, the risk of re-identification increases when insufficient effort has been made to select training data sources with a view of minimising the collection of personal data.[53] Implementing appropriate data filtering techniques prior to model training and methodological choices to reduce re-identification risk are also crucial for safeguarding the effectiveness of anonymisation.[54] For example, the choice between suppression and character replacement as anonymisation techniques carry different implications on re-identification risks.

For optimal risk assurance, the robustness of an AI model should be assessed through evaluating engineering governance measures and the frequency of conducting internal and external documentation audits.[55] These audits may assess code review reports and theoretical analysis relating to the suitability of adopted measures in decreasing the probability of reidentification.[56] Model testing and evaluation of the 'the scope, frequency, quantity and quality of tests that the controller has conducted on the model' is also crucial.[57] Record-keeping relating to the data processing activities of AI models should

53. Ibid.

54. Ibid.

55. Ibid.

56. Ibid.

57. Ibid.

be ensured, irrespective of the fact that the processed data is anonymised.[58] This is because documentation and risk analysis of processing activities are essential for proving to a data protection supervisory authority that personal data is not being processed.[59]

If the supervisory authority cannot determine an AI model's training data anonymity after evaluating the available documentation relating to that model, then the controller would have infringed its accountability obligation pursuant to Article 5(2) GDPR.[60] Thus, in order for a controller to comply with their accountability obligations under the GDPR in relation to documentation obligations, they must record information which relates to Data Protection Impact Assessments, including information that was used to decide whether the Assessment was unnecessary.[61] Moreover, communications with the Data Protection Officer must be documented and technical and organisational measures taken throughout an AI model's lifecycle contributing or reinforcing the absence of personal data in the model must be recorded, along with documentation proving an 'AI model's theoretical resistance to re-identification techniques'.[62] These measures help maintain the anonymity of data while enabling AI system providers to demonstrate to supervisory authorities that anonymised data falls outside the scope of GDPR obligations.

Bibliography

Primary Sources

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L119

58. Ibid.

59. Ibid.

60. Ibid.

61. Ibid.

62. Ibid.

Secondary Sources

Books

Tigard D, 'Chapter 1: Embedded ethics as preparatory regulation of technology: a new solution to the Collingridge Dilemma?' (2022) Novel Beings Edward Elgar Publishing <https://doi.org/10.4337/9781800889262.00008> accessed 18 September 2025

Journals

Mougiakou E, Papadimitriou S, Chrysafiadi K, Virvou M, 'Artificial intelligence in educational games and consent under general data protection regulation' (2025) Intelligent Decision Technologies 2025 0(0) < https://doi.org/10.1177/187249812513228> accessed 27 March 2025

Vokinger K, Stekhoven D, Krauthammer M, 'Lost in Anonymisation — A Data Anonymisation Reference Classification Merging Legal and Technical Considerations' (2020) *The Journal of Law, Medicine & Ethics* 48(1) 228-231 < https://doi.org/10.1177/10731105209170> accessed 27 March 2025

Aleksandr K, Kerikmäe T, 'Artificial intelligence and the GDPR: Inevitable nemeses?' (2020) *TalTech Journal of European Studies* 10 3 83 <https://doi.org/10.1515/bjes-2020-0022> accessed 27 March 2025

Mühlhoff R, Ruschemeier H, 'Regulating AI with Purpose Limitation for Models' (2024) Journal of AI Law and Regulation 1 1 <https://doi.org/10.21552/aire/2024/1/5> accessed 18 September 2025

El-Gazzar R, Stendal K, 'Examining How GDPR Challenges Emerging Technologies' (2020) *Journal of Information Policy* 1 10 237–275 <https://doi.org/10.5325/jinfopoli.10.2020.0237> accessed 27 March 2025

Brewer R, Westlake B, Hart T, Arauza O, 'The Ethics of Web Crawling and Web Scraping in Cybercrime Research: Navigating Issues of Consent, Privacy, and Other Potential Harms Associated with Automated Data Collection' (2021) Researching Cybercrimes Palgrave Macmillan Cham https://doi.org/10.1007/978-3-030-74837-1_22 accessed 27 March 2025

Ferreira Marques J, Bernardino J, 'Analysis of Data Anonymisation Techniques' (2020) KEOD 2 236-237 <https://doi.org/10.5220/0010142302350241> accessed 24 March 2025

Hacker P, 'A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act' (2021) *Law, Innovation and Technology* 13 (2) 257–301 <https://doi.org/10.1080/17579961.2021.1977219> accessed 26 March 2025

Reports

European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' Opinion of the Board Art. 64 (EDPB, 17 December 2024)

Sartor G, Lagioia F, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' PE 641.530 (Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA), 2020)

Websites

NOYB, 'AI hallucinations: ChatGPT created a fake child murderer' (*Noyb.eu*, 20 March 2025) <https://noyb.eu/en/ai-hallucinations-chatgpt-created-fake-child-murderer> accessed 28 March 2025

Chen M, 'What Is Reinforcement Learning?' (*Oracle.com*, 3 April 2024) <https://www.oracle.com/nl/artificial-intelligence/machine-learning/reinforcement-learning/> accessed 26 March 2025

Utrecht University, 'K-anonymity, l-diversity and t-closeness' (*Utrecht University*, 30 May 2023) <https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html> accessed 26 March 2025

About the author

Marina El Moufti

Marina El Moufti completed the LL.M. in Technology Law and Innovation and European Law in a Global Context at the University of Groningen. Her research interests lie at the intersection of artificial intelligence, data governance, and standardisation.

CHAPTER 9: THE USE OF AUTOMATED DECEPTION DETECTION FOR LAW ENFORCEMENT IN THE EU: REGULATORY AND TECHNICAL ASSESSMENT UNDER THE AI ACT

Natálie Binderová

1. Introduction

The concept of a 'lie' can be explained as a 'false statement made by an individual who is aware that the statement is probably not true'.[1] Lies have become so prevalent in our society that the distinction between truth and falsehood is increasingly fading.[2] As the research article by Alex Sebastião Constâncio et al. concluded, an average person's ability to detect lies is approximately 54%, occasionally exceeding 60%.[3] Consequently, the majority of individuals are only capable of identifying when they are being lied to with an accuracy rate of only fifty percent. Unsurprisingly, this gap in human abilities to detect deception created a demand for technology to bridge it.

The first ever technology narrowing this gap was a polygraph machine credited to Dr. James Mackenzie, whose invention was able to track a patient's irreg-

1. Jo Ann Oravec, 'From Polygraphs to Truth Machines: Artificial Intelligence in Lie Detection' [2024] 2(2) Critical Humanities 37 <https://mds.marshall.edu/cgi/viewcontent.cgi?article=1036&context=criticalhumanities> accessed 14 March 2025.

2. Ibid

3. Alex Sebastião Constâncio et al, 'Deception detection with machine learning: A systematic review and statistical analysis' [2023] PLOS ONE 2 <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0281323> accessed 14 March 202.

ular heartbeat, recording the output in ink.[4] Mackanzie's invention was later innovated by a psychologist and police officer on duty, John Larso, who in 1921 designed a device 'to simultaneously measure continuous changes in blood pressure, heart rate, and respiration rate to aid in the detection of deception.'[5] However, over the years, many states deemed polygraph evidence inadmissible in courts as its use raised several legal concerns related to the alienation of the right to remain silent, as the physiological cues could non-verbally reveal deceitful behaviour.[6]

Nevertheless, with the advancement of technology in the past few years, novel proposals for automated polygraphs leveraging Artificial Intelligence, also known as Automated Deception Detection (ADD), have emerged.[7] ADD most commonly utilises deep learning or machine learning models,[8] which try to discover various cues of deception such as 'eye gaze, body, gestures, facial expressions, and physical signals'.[9] It is important to note that ADD is not

4. Theodora Burbank, 'The Origins of the Polygraph' (HARVARD COUNTWAY LIBRARY, 18 February 2020) <https://countway.harvard.edu/news/origins-polygraph> accessed 14 March 2025.

5. John Synnott and others, 'A review of the polygraph: history, methodology and current status' [2015] 1(1) Crime Psychology Review 60 <https://www.tandfonline.com/doi/full/10.1080/23744006.2015.1060080#d1e134> accessed 14 March 2025.

6. Ewout H. Meijer and Peter J. van Koppen, 'Lie Detectors and the Law: The Use of the Polygraph in Europe' in David Canter and Rita Žukauskiene (eds), *Psychology and Law : Bridging the Gap* (Routledge 2016) 42 <https://ebookcentral.proquest.com/lib/rug/detail.action?docID=438519> accessed 14 March 2025.

7. Wasiq Khan et al, 'Deception in the eyes of deceiver: A computer vision and machine learning based automated deception detection' [2021] 169 Expert Systems With Applications 1 <https://www.sciencedirect.com/science/article/pii/S0957417420310289> accessed 14 March 2025.

8. Alex Sebastião Constâncio et al. (n 2) 21.

9. Sayde L. King and Tempest Neal, 'Applications of AI-Enabled Deception Detection Using Video, Audio, and Physiological Data: A Systematic Review' [2024] 12 IEEE Access

purely theoretical. It has been utilised in numerous states and across a variety of sectors. For example, the European Union conducted a trial of an advanced border control AI lie detector called iBorderCtrl[10], which was originally a part of the ETIAS system.[11] Moreover, according to an article by the Guardian, a tool called EyeDetect 'has been deployed as part of a pilot scheme in the UK for the rehabilitation of sex offenders.'[12]

Even though some studies have shown a successful deception detection rate between 65 and 75%,[13] in high-risk sectors, such as law enforcement, an erroneous conclusion can aid in destroying the lives of the innocent or setting a perpetrator free. This paper shall examine the future of AI Deception Detection tools used for law enforcement purposes in the EU. Moreover, it shall also discuss not only the current state of the art of ADD tools but also their ability to comply with technical and safety requirements under the AI Act.[14]

Section 1 outlines the technical architecture and operational processes of Automated Deception Detection (ADD) systems. Section 2 addresses the evidentiary cues upon which these systems are designed to rely, while Section 3 examines the provenance and reliability of training datasets, with emphasis

---

135208 <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10681404> accessed 14 March 2025.

10. European Commission, 'Intelligent Portable Border Control System' (European Commission) <https://cordis.europa.eu/project/id/700626> accessed 14 March 2025.

11. Ibid.

12. Amit Katwala, 'The race to create a perfect lie detector – and the dangers of succeeding' (*The Guardian*, 5 September 2019) <https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding> accessed 14 March 2025.

13. Wasiq Khan et al (n 7) 3.

14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L1689/1.

on bias and labelling accuracy. Section 4 considers the implications of profiling and automated decision-making. Section 5 situates ADD within the framework of the Artificial Intelligence Act, identifying their classification as high-risk when deployed in law enforcement. Section 6 analyses the compliance obligations arising under the Act, including requirements of governance, data quality, transparency, human oversight, and cybersecurity. The paper concludes with an assessment of the extent to which current ADD systems are capable of lawful deployment within the European Union.

2. Technical Description of ADD Systems

The research conducted by Alex Sebastião Constâncio et al. highlighted that both machine and deep learning are leveraged for the development of ADD systems.[15] Regarding machine learning, the literature review concluded that the best techniques for deception are 'decision trees, gradient boosting, neural networks, multi-view learning, random forest, and support vector machines (SVM).'[16] These techniques are later utilised in the deception detection pipeline, which is comprised of several key stages, namely: (1) pre-processing, (2) feature extraction, (3) training, and (4) detection. The process starts with the collection of training data, which can be obtained from local or publicly available datasets. Although optional, pre-processing helps improve data quality through annotation, noise reduction, and segmentation. After the refinement of quality, the data transforms through feature extraction, during which raw information is converted into meaningful representations, which can later be utilised by machine learning algorithms.[17]

Two phases of ADD systems can be distinguished:

1. **Training Phase:** In this phase, the AI algorithm learns the underlying relationships between the extracted features and their corresponding labels,

15. Alex Sebastião Constâncio et al. (n 2) 4.

16. Ibid 9.

17. Sayde L. King and Tempest Neal (n 9) 135210.

ultimately creating a robust deception detection model. Consequently, the model is trained.

2. **Detection Phase**: In this phase, the trained model is applied to new, unseen data, which undergoes the same pre-processing and feature extraction steps before being evaluated by the trained classification model. Lastly, the model then assigns a deception label, indicating whether the input data exhibits deceptive characteristics.[18]

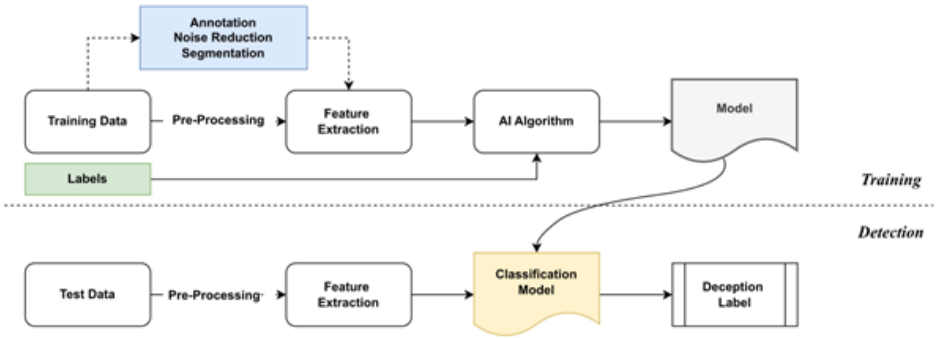


Figure: Workings of the ADD tool explained step by step[19]

Cues of Deception

The study of deceptive behaviour has been a subject of research for a considerable number of years, during which several features of deception have been identified.[20] In the domain of deception detection, 'feature classification methods' refer to the methods used for the classification of features extracted from data in the context of deception detection.[21] 'In this context, "features" typically

18. Ibid.

19. Ibid.

20. Wasiq Khan et al (n 7) 2.

21. Shanjita Akter Prome et al, 'Deception detection using machine learning (ML) and deep learning (DL) techniques: A systematic review' [2024] 6 Natural Language Processing

represent measurable attributes or patterns derived from various sources such as text, audio, or video data.'[22] ADD models look mostly for verbal and non-verbal features, such as facial cues, including micro-expressions, eye contact and facial tension,[23] hand and body gestures,[24] emotions such as guilt, fear and delight,[25] and linguistic patterns."[26]

Moreover, W. Khan highlights that the act of deceiving others has been proven to demand a greater cognitive load than the act of telling the truth. A key component of dishonesty is the fabrication of an elaborate narrative that needs to align with any subsequent information that the third-party observer may learn through further investigation.[27] Therefore, cognitive techniques can be employed by a deceitful person to trick their audience.[28]

Datasets and Training

The provenance of data is critical, as the quality and quantity of the input data highly influence the outcome of the Machine Learning.[29] The datasets should be diverse enough to represent the majority of the population in order to prevent the existence of bias in the output.[30] Therefore, the datasets should

---

Journal 6 <https://www.sciencedirect.com/science/article/pii/S2949719124000050> accessed 14 March 2025.

22. Ibid.

23. Ibid 9.

24. Sayde L. King and Tempest Neal (n 9) 135214.

25. Alex Sebastião Constâncio et al. (n 2) 15.

26. Wasiq Khan et al (n 7) 3.

27. Ibid.

28. Ibid.

29. Alex Sebastião Constâncio et al. (n 2) 17.

30. Ibid.

include individuals of different genders, races, ages, and individuals living with disabilities. In the area of criminology and forensics, ADD tools are currently trained on two different types of datasets:

1. Datasets containing mock data: contain data that has been collected through fabricated storylines, such as professional actors trying to realistically simulate specific scenarios.[31]
2. Datasets containing real-life data: contain data collected in collaboration with law enforcement or data depicting real court sessions or interrogations scraped from the Internet, such as the Real-Life Trial Dataset.[32] In current research, the use of mock data is prevalent over real-life data (70.15% to 29.85% ratio).[33]

In both cases, a hypothetical question arises of how the providers of ADD tools ensure that data is labelled correctly. This question currently remains unanswered, as it seems impossible to guarantee a high level of accuracy of the labelling, mainly in real-life scenarios. For example, the label of 'deceitful behaviour' in the Real-Life Trial Dataset depended on the outcome of the court proceedings, whereby a guilty verdict was equated with deceit, an assumption that is not necessarily valid in all cases.[34] Having in mind the state of the art of the datasets, it could be assumed that biased output is inevitable. This is mainly due to the lack of reports on ADD tools tested in real-world scenarios, together with the fact that the datasets are not large and diverse enough 'to provide a highly general classifier.'[35] Consequently, there is a need for additional research and pilot testing of ADD tools, which could help resolve the issues of possible bias and labelling.

---

31. Sayde L. King and Tempest Neal (n 9) 135210.

32. Ibid.

33. Alex Sebastião Constâncio et al. (n 2) 18.

34. Sayde L. King and Tempest Neal (n 9) 135215.

35. Alex Sebastião Constâncio et al. (n 2) 25.

Possible Profiling and Automated Decision-Making

Jo Ann Oravec reported that profiling of individuals has already been exploited for the purpose of enhancing deception detection.[36] Nevertheless, the case she is referring to concerns an ADD tool which detects deception only from voice evidence and does not extend to the analysis of video data.[37] From the rest of the literature reviews it is unclear whether any other ADD tools, more specifically the ones which utilise video analysis, utilise profiling. Furthermore, the current academic overview also does not specify whether the tools in question use automated decision-making processes, and to what extent human intervention is required in the detection process.

3. Classification of ADD tools under the AI Act[38]

The AI Act defines 'AI system' as 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.'[39] ADD tools fall within the definition of 'AI systems' as they leverage machine or deep learning AI to analyse data (like text or video) for the purposes of identifying signs of deception. They can be designed to work with varying levels of independence and can impact both physical environments such as law enforcement, and virtual ones such as gaming.[40]

---

36. Jo Ann Oravec (n 1) 38.

37. Rita Singh, Profiling Humans from their Voice (1 edn, Springer Singapore 2019) <https://link.springer.com/book/10.1007/978-981-13-8403-5> accessed 14 March 2025.

38. Artificial Intelligence Act (n 14).

39. Ibid Art 3 (1).

40. Sayde L. King and Tempest Neal (n 9) 135209.

For the purposes of this paper, the definitions of 'AI provider' and 'deployer' are those set out in the AI Act.

An AI provider is defined as:

> 'a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.'[41]

Secondly, an AI deployer is defined as:

> 'any natural or legal person, public authority, agency or other body that uses an AI system under its authority exclusively for professional activities,' which in this case is the law enforcement.[42]

The AI Act adopts a risk-based approach, meaning that the obligations for AI systems and their providers vary depending on the level of risk they pose. The regulation classifies AI systems into four categories:

1. Unacceptable-risk AI systems are considered extremely dangerous and are thus prohibited.
2. High-risk AI systems face strict regulatory requirements, including compliance assessments and ongoing oversight.
3. Limited-risk AI systems are required to meet transparency obligations, ensuring users are informed when interacting with AI-generated content or decisions.
4. Minimal-risk AI systems pose minimal regulatory concerns and are generally left unregulated.

It is evident from this approach that greater oversight is applied to high-risk AI

41. Artificial Intelligence Act (n 14) Art 3(3).

42. Ibid (4).

systems. In contrast, low-risk AI tools remain free from unnecessary regulatory burdens.[43]

The classification of ADD depends on the area of its application and the purpose of its use. The academia differentiates between high-stakes and lower-risk areas of deployment.[44] Nevertheless, the use of ADD by law enforcement is permitted, but the AI systems (ADD) are considered high risk.[45] This classification can be found in Article 6 (2) AI Act, which explicitly refers to AI systems mentioned in Annex III and labels them as high risk. Consequently, Annex III (6) (b) states:

> '6. Law enforcement, in so far as their use is permitted under relevant Union or national law:
> (...)
> (b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;'

Providers of high-risk AI systems inherently need to comply with the obligations laid down in Section 2 of the AI Act.[46] The obligations are as follows:

1. Establishment of Risk Management[47]

Article 9 states that providers must establish, implement, document, and maintain a continuous risk management system throughout the system's lifecycle.[48] As part of the risk management system, providers must analyse 'foreseeable

---

43. European Commission, 'AI Act' (Shaping Europe's digital future, 18 February 2025) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 28 March 2025.

44. Sayde L. King and Tempest Neal (n 9) 135211.

45. Artificial Intelligence Act (n 14) Art 6(2) Annex III (6)(b).

46. Ibid Art 8.

47. Ibid Art 9.

48. Ibid (1).

risks to health, safety, and fundamental rights.' In consequence, providers must accordingly adopt risk mitigation measures necessary to reduce or eliminate the identified risk. The risk remaining post the employment of mitigation measures must be considered 'acceptable'. Nevertheless, even if the remaining risk is deemed acceptable, the system must be continuously monitored. Furthermore, special attention needs to be paid to risks affecting more vulnerable groups, such as children or persons with certain disabilities.

The Article also calls for mandatory training before the employment of the system to ensure its regulatory compliance. The risk management, together with the measures, must be in accordance with other frameworks, such as the General Data Protection Regulation[49] or the Law Enforcement Directive.[50]

Compliance of ADD tool providers

In the event of incorrect or biased output from an ADD tool, several fundamental rights could be infringed upon. Primarily, as previously mentioned, the right against self-incrimination could be infringed,[51] causing an endangerment of the presumption of innocence.[52] Furthermore, the potential for ADD outputs to discriminate on the basis of factors such as race, age, gender, and so forth is contingent upon the origin of any inherent bias within the dataset. Hence,

49. 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) [2016] OJ L119/1.

50. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive) [2016] OJ L119/89.

51. Ewout H. Meijer and Peter J. van Koppen (n 6).

52. Charter of Fundamental Rights of the European Union [2012] OJ C326/391 Art 48 (2) EU.

infringing the right to non-discrimination.[53] Finally, it could be argued that ADD tools infringe the right to data protection,[54] as they are prone to invasive collection of data.[55]

It must be noted that the required risk mitigation and monitoring could present a challenge for the ADD tool providers, as they have leveraged the use of opaque 'black-box' processes, which could not allow for the deployer to inspect whether the risk has been mitigated.[56]

2. Compliance with strict governance and data quality requirements[57]

High-risk AI systems using trained models must rely on training, validation, and testing data sets that meet specified quality criteria and follow proper governance practices. Data sets must be relevant, representative, accurate, and complete for the system's intended purpose. Additionally, they have to account for the specific geographical, contextual, or behavioural settings in which the AI system will be used. Furthermore, providers will have to detect biases that can 'affect the health and safety of persons, have a negative impact on fundamental rights, or lead to discrimination prohibited under Union law.'[58] In regard to bias detection, special attention should be paid to special categories of data

53. Ibid Art 21.

54. Ibid art 8.

55. Jo Ann Oravec (n 1) 37.

56. Dana Rad et al, 'Neural Network Applications in Polygraph Scoring—A Scoping Review' [2023] 14(10) MDPI 6 <https://www.mdpi.com/2078-2489/14/10/564> accessed 14 March 2025.

57. Artificial Intelligence Act (n 14) Art 10.

58. Ibid Art (2)(f).

defined in Article 9(1) General Data Protection Regulation, which have to be securely protected and subject to appropriate safeguards.[59]

Compliance of ADD tool providers

As mentioned in the Section describing the technical workings of ADD, the current data sets are small and not diverse enough. Additionally, the labelling system of the data raises many questions. It is evident that these factors have the potential to result in an output that is both biased and inaccurate.

As previously mentioned, ADD is engaged in the processing[60] of facial, physiological, and emotional data, which can be classified as personal data, i.e. 'any information relating to an identified or identifiable natural person.'[61] Furthermore, it is notable that facial data, including eye movement, can be regarded as biometric data.[62] In addition, physiological data could be interpreted as health data.[63] Consequently, both types can be considered special categories of personal data.[64] Hence, ADD tool providers must comply with all the obligations related to special categories of sensitive data laid down in this Article.

To conclude, the requirements laid down under this Article will pose one of the biggest challenges to the ADD tool providers, who will need to invest in larger, more representative data and bias detection.

3. Mandatory technical documentation[65]

ADD tool providers must gather technical documentation confirming that their

59. Ibid (5)(c).

60. General Data Protection Regulation (n 49) Art 4 (2).

61. Ibid (1).

62. Ibid (14).

63. Ibid (15).

64. Ibid Art 9 (1).

65. Artificial Intelligence Act (n 14) Art 11.

system complies with all the requirements established in Section 2 (Articles 8-15 AI Act).[66] This documentation must be provided before the tool is deployed on the European market.[67]

4. Record-keeping[68]

To ensure an adequate level of traceability of systems' functioning is in line with its intended purpose, logging capabilities should be enabled by the provider over its whole lifetime.[69] These loggings should record events that may result in the emergence of a risk or a substantial modification.[70] Additionally, they should support post-market monitoring.[71]

5. Transparency of the operation of the high-risk AI system[72]

High-risk AI systems must be designed to ensure their operation is sufficiently transparent, allowing deployers to understand and appropriately use the system's output.[73] The provider must provide the deployer with 'concise, complete, correct and clear information' instructions[74] which shall include 'the identity and the contact details of the provider or their authorised represen-

66. Ibid (2).

67. Ibid (1).

68. Ibid Art 12.

69. Ibid (1).

70. Ibid (2)(a).

71. Ibid (2)(b).

72. Ibid Art 13.

73. Ibid (1).

74. Ibid (2).

tative'[75] and 'the characteristics, capabilities and limitations of performance'[76] Additionally, the provider must include information about the correct interpretation of the output, such as information about changes post-conformity assessment, human oversight measures, system resources and maintenance, and logging mechanisms.[77]

Compliance of ADD tool providers

It is to be assumed that the aforementioned transparency requirements will present a challenge for the ADD tool providers, considering the previously mentioned use of 'black-box' processes, which result in outputs from which the methodology used to reach the conclusions is not apparent.[78] The use of said black-boxes in ADD systems could have a detrimental impact on one's life, e.g. the output biased by discrimination could aid in the conviction of an innocent person. Hence, the AI Act calls for transparent systems and human oversight, which could intervene in specific situations.

6. Presence of Human oversight[79]

Any high-risk AI systems must be designed and developed with appropriate human-machine interface tools to ensure effective oversight by natural persons during their use.[80] This oversight should 'minimise the risks to health, safety or fundamental rights which may emerge when the system is used for its intended purpose.'[81]

---

75. Ibid 3(a).

76. Ibid 3(b).

77. Ibid 3(c)-(f).

78. Dana Rad et al (56) 6.

79. Artificial Intelligence Act (n 14) Art 14.

80. Ibid (1).

81. Ibid (2).

The measures ensuring human oversight can be either 'built-in technical safeguards' incorporated by the provider[82] or 'operational oversight mechanism' identified by the provider and implemented by the deployer.[83] Therefore, the law enforcement personnel overseeing the ADD tool must be according to paragraph 4 able to:

(a) Understand how the system works and spot any issues,

(b) Avoid blindly trusting the system's recommendations, having in mind the possible bias of the output,

(c) Correctly interpret the system's output,

(d) Decide, depending on the specific situation, whether to use the AI system and follow or ignore the system's output.

(e) Safely stop or intervene in the system if needed.[84]

Compliance of ADD tool providers

The findings of the research undertaken for the present paper do not provide a comprehensive understanding of the human factor's role in the implementation and use of ADD tools. Considering the severity of impact on human lives caused by the use of ADD systems by law enforcement, it is probable that human factor will be present. Nevertheless, certain academics have voiced concerns that more automation will lead to less transparency in the system due to the reduction of human oversight.[85]

7. Accurate, robust, and cybersecure design[86]

Lastly, ADD tool providers must be designed to ensure accuracy, robustness, and cybersecurity, and maintain these qualities consistently throughout their

82. Ibid (3)(a).

83. Ibid (3)(b).

84. Art (4).

85. Jo Ann Oravec (n 1) 3.

86. Artificial Intelligence Act (n 14) Art 15.

lifecycle.[87] High-risk AI systems must be as resilient as possible to errors, faults, or inconsistencies, especially from interactions with humans or other systems. If systems continue learning after their deployment, they should be designed to minimise the risk of biased outputs affecting future operations and include measures to address feedback loops.

Moreover, high-risk AI systems must be resilient to unauthorised attempts to alter their performance or outputs. Hence, cybersecurity measures should be appropriate to the system's risks, including protections against data poisoning, model poisoning, adversarial attacks, confidentiality breaches, and model flaws. When implementing the cybersecurity measures, other relevant frameworks, such as the General Data Protection Regulation,[88] shall be consulted.[89]

Conclusion

In light of the current state of the art of ADD tools, it appears highly improbable that they will be utilised by law enforcement agencies within the European Union in the near future. This results from the technical inability of ADD tool providers to comply with all the requirements stipulated in Section 2 of the AI Act, and therefore, prevents them from the deployment and sale of said tools on the European market. The current tools lack transparency, which could result in infeasible risk management and fundamental rights infringement. Moreover, the current data sets do not comply with the strict governance and data quality requirements, possibly leading to incorrect and biased input. To conclude, ADD tool providers will need to improve their design to be accurate, robust and cybersecure, taking into account the sensitive nature of the data processed by the tools.

---

87. Ibid, (1).

88. i.e. ADD is engaged in the processing of facial, physiological and emotional data within the meaning of article 4(2) , which can be classified as personal data. If the provider of the ADD tools is established in the Union, or if it processes the personal data of data subjects in the Union despite being established elsewhere, the GDPR applies to its processing activities.

89. General Data Protection Regulation (n 49) Art 25.

Bibliography

Primary Sources:

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive) [2016] OJ L119/89.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L1689/1.

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) [2016] OJ L119/1.

Secondary Sources

Alex Sebastião Constâncio et al, 'Deception detection with machine learning: A systematic review and statistical analysis' [2023] PLOS ONE <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0281323> accessed 14 March 202

Amit Katwala, 'The race to create a perfect lie detector – and the dangers of succeeding' (The Guardian, 5 September 2019) <https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding> accessed 14 March 2025

Dana Rad et al, 'Neural Network Applications in Polygraph Scoring—A Scoping Review' [2023] 14(10) MDPI <https://www.mdpi.com/2078-2489/14/10/564> accessed 14 March 2025.

European Commission, 'Intelligent Portable Border Control System' (European Commission) <https://cordis.europa.eu/project/id/700626> accessed 14 March 2025

Ewout H. Meijer and Peter J. van Koppen, 'Lie Detectors and the Law: The Use of the Polygraph in Europe' in David Canter and Rita Žukauskiene (eds), *Psy-*

chology and Law : Bridging the Gap (Routledge 2016) <https://ebookcentral.proquest.com/lib/rug/detail.action?docID=438519> accessed 14 March 2025

A. Oravec, 'From Polygraphs to Truth Machines: Artificial Intelligence in Lie Detection' [2024] 2(2) Critical Humanities <https://mds.marshall.edu/cgi/viewcontent.cgi?article=1036&context=criticalhumanities> accessed 14 March 2025

John Synnott and others, 'A review of the polygraph: history, methodology and current status' [2015] 1(1) Crime Psychology Review <https://www.tandfonline.com/doi/full/10.1080/23744006.2015.1060080#d1e134> accessed 14 March 2025

Rita Singh, Profiling Humans from their Voice (1 edn, Springer Singapore 2019) <https://link.springer.com/book/10.1007/978-981-13-8403-5> accessed 14 March 2025

Sayde L. King and Tempest Neal, 'Applications of AI-Enabled Deception Detection Using Video, Audio, and Physiological Data: A Systematic Review' [2024] 12 IEEE Access <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10681404> accessed 14 March 2025

Shanjita Akter Prome et al, 'Deception detection using machine learning (ML) and deep learning (DL) techniques: A systematic review' [2024] 6 Natural Language Processing Journal <https://www.sciencedirect.com/science/article/pii/S2949719124000050> accessed 14 March 2025

Theodora Burbank, 'The Origins of the Polygraph' (HARVARD COUNTWAY LIBRARY, 18 February 2020) <https://countway.harvard.edu/news/origins-polygraph> accessed 14 March 2025

Wasiq Khan et al, 'Deception in the eyes of deceiver: A computer vision and machine learning based automated deception detection' [2021] 169 Expert Systems With Applications <https://www.sciencedirect.com/science/article/pii/S0957417420310289> accessed 14 March 2025

About the author

Natálie Binderová

Natálie Binderová completed the LLM Technology Law and Innovation programme at the University of Groningen during the academic year 2025-2026. She is currently working at Pwc Czech Republic as a Responsible AI Consultant.

CHAPTER 10: THE LEGAL AND ETHICAL CHALLENGES POSED BY AI-ASSISTED POLICE REPORTS IN THE CRIMINAL PROCEDURE

Konstantina Kelesidi

1. Introduction

The emergence of Artificial Intelligence (AI) has enabled the automation of tedious tasks in both the public and private sectors. In the realm of law enforcement, AI has facilitated, *inter alia*, the identification of suspects through facial recognition technology[1] and the prevention of crimes by identifying crime patterns through area-based predictive policing.[2] These are only a few examples, as the applications of AI continue to expand through the development of quantum and edge computing.[3]

Additionally, Large Language Models (LLMs)[4] are AI models that 'mimic' human language by analysing and generating texts. Their performance depends on training on large datasets. One particular application of LLM, AI-assisted report writing, has been adopted in several police departments in

1. European Union Agency for Law Enforcement Cooperation (Europol), *AI and policing the benefits and challenges of artificial intelligence for law enforcement* (2024) 23-25 <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf#page=5.32> accessed 23 March 2025

2. Ibid 15-16.

3. Ibid 49-50.

4. Ibid 30.

the United States of America.[5] Draft One, developed by Axon, is an AI tool used for drafting police reports with promises of high quality and time efficiency in report writing. However, such applications must be met with significant caution; The European Union Agency for Law Enforcement Cooperation (EUROPOL) emphasizes that, despite being regarded as 'a treasure trove of possibilities', Generative AI is contingent on 'its judicious and ethical application' in the context of responsible innovation.[6] The latter statement applies to all applications of AI, and more importantly, in critical areas such as law enforcement, where it must be used rigorously.

Given the above, this paper will examine the legal and ethical challenges of AI-assisted reports in the context of law enforcement. Therefore, the paper explores the research questions 'To what extent AI-assisted police reports undermine the criminal procedure and 'Does Draft One classify as a high-risk AI system under the AI Act?'. The methodology used to answer these research questions is a case study on the AI tool 'Draft One' utilised by US police for police reporting. The first section of the paper will present how exactly AI is employed in drafting police reports and particularly how Draft One works. The second and third section will discuss the benefits of this AI-assisted police report writing and the risks of inaccuracy, bias, and hallucinations that affect the parties involved in a criminal case. In the fourth section, an assessment will be carried out on the impact on the fundamental rights to a fair trial, and presumption of innocence. Lastly, AI-assisted police reports will be examined under the relevant European Union (EU) legal framework.

2. The Role of Police Reports in the Criminal Justice System and How Draft One Works

To begin with, it is crucial to define police reports and their importance in criminal proceedings. Police reports can be defined as the official written accounts

5. American Civil Liberties Union (ACLU), *Police Departments Shouldn't Allow Officers to Use AI to Draft Police Reports* (2024) 1 <https://assets.aclu.org/live/uploads/2024/12/Automated-Police-Reports-1291.pdf> accessed 25 March 2025.

6. EUROPOL (n 1) 30.

documenting incidents and interactions between law enforcement officers and the public.[7] Police reports are of central importance within the criminal justice system, fulfilling a multifaceted role. Their role is to keep a record of events of criminal value serving as a 'fact-finding' instrument, and, in some cases, as an important piece of evidence in court.[8] Given the above, police reports are an integral part of the criminal procedure, and when considered in conjunction with other forms of evidence, these reports contribute to the establishment of a comprehensive and nuanced understanding of the criminal activity in question.

Recently, an AI tool called Draft One[9] was developed by the American tech company, Axon, which specializes in producing technology for law enforcement.[10] What is fascinating about Draft One is that it enables police officers to draft their reports without engaging in any writing themselves. How it works is that the system first has to transcribe audio from the police officer's body-worn camera during the interaction with suspects, witnesses, and afflicted persons.[11] This is done by wearing an activated body camera produced by Axon that transmits the audio to Axon's platform 'Axon Evidence' immediately after the deactivation of the body-worn cameras.[12] The police officer has to then log in into their account, select the relevant recording, and initiate the generative narration. Before the start of the generative narration, the system asks some

7. ACLU (n 5) 1.

8. Andrew Guthrie Ferguson, 'Generative Suspicion and the Risks of AI-assisted Police Reports' [2024] Northwestern Law Review 42 (forthcoming).

9. See also Ian T. Adams, 'Large Language Models and Artificial Intelligence for Police Report Writing, [2024] CrimRxiv1, 4 <https://doi.org/10.21428/cb6ab371.779603ee>. Truleo Narrative provides a similar AI tool.

10. Axon, 'Overview' (*Axon.com*, 2025) <https://www.axon.com/company> accessed 23 March 2025.

11. Ferguson (n 8) 17.

12. Ibid 17-18.

basic questions for the police officer in order to provide some context.[13] These include: 1) the type of crime, ranging from violent crimes to just pure informational reports; 2) the severity of the incident by defining the charge; 3) whether an arrest took place. The system then deploys OpenAI's GPT-4 model to generate the report in first person, as if the police officer wrote it themselves. Although the report is drafted entirely by the AI system, police officers can have an input by reviewing and editing the generative narration before finalizing the report, especially when the existing ambiguities do not allow the system to proceed to the submission.[14]

3. The Benefits of AI-assisted Police Reports

Axon pledges that automation in police report writing will considerably reduce the time spent by police officers on this task.[15] In fact, Axon and police officers who have tested the AI tool claim a time saving of up to 82%.[16] The automation of reports can greatly alleviate the 'administrative burden and paperwork' that police officers have to undertake, taking into account the increased rates of crime and consistent issues with understaffing of the police departments.[17] Consequently, it enables a greater allocation of time to more significant and collective tasks, thus facilitating an increased focus on more arduous facets

13. Ibid.

14. Axon (n 10).

15. Axon, 'Draft One Demo' (*Axon.com*, 2025) <https://my.axon.com/s/draft-one?language=en_US> accessed 23 March 2025.

16. Ian T. Adams *et al*, 'No man's hand: artificial intelligence does not improve police report writing speed' [2024] J Exp Criminol 1, 4 <https://doi.org/10.1007/s11292-024-09644-7> accessed 26 March 2025.

17. Ibid; Carl Dement and Melissa Inglis 'Artificial intelligence-assisted criminal justice reporting: An exploratory study of benefits, concerns, and future directions' [2024] Criminology & Criminal Justice 1, 9 <https://doi.org/10.1177/17488958241274296> accessed 26 March 2025.

of criminal proceedings, such as responding to citizens on emergency calls.[18] Additionally, it elevates the quality of police reporting,[19] by improving the form and essence of police reporting. This entails correcting typographical and grammatical errors and preventing indecipherable and incoherent texts attributed to common human errors.[20]

This type of standardization of the police reports could contribute to the consistency and comprehensiveness in the documentation process across different departments, and facilitate interoperability between different police departments.[21]

4. The Risks of AI-assisted Police Reports

Despite the benefits of LLMs, concerns have been expressed regarding potential inaccuracies, and bias. The following part examines some of the risks relating to AI-assisted police reports.

a. Inaccuracies and Omissions from Insufficient Training Data

The first risk that arises is the potential inaccuracy resulting from poorly trained AI systems. To elaborate, every crime has its own peculiarities that require different reporting details.[22] An example brought by Andrew Guthrie Ferguson suggests that an AI system trained solely on 'traffic stops', which do not involve goods and the act of stealing, might ignore details on the price and value of a property that was stolen in a case of theft.[23] Such omissions can exclude crucial information that determines the severity of the crime in question. This calls

18. Ian T. Adams *et al* (n 16) 4.

19. Ibid 3.

20. Ibid 12.

21. Carl Dement and Melissa Inglis (n 17) 10.

22. Ferguson (n 8) 29.

23. Ibid 28.

into question whether AI systems such as Draft One are trained on diverse data that includes many types of crimes. Failure to include a diverse range of offences may result in the system failing to recognise the unique demands of each crime and to filter the important and/or unimportant details tailored to specific crimes. Furthermore, the GPT-4 model is trained on unstructured data scraped from the internet via its '*GPTbot web crawler*', which further questions the quality of its dataset, and whether these sources are not reliable, but also familiarised with technical terminology used by officers.[24]

b. Inaccuracies and Omissions from Transcription Errors

Moreover, factual information and events are up to human interpretation. AI systems, such as Draft One, do not have information, for example, about: the environment; the body language of the people involved; or misleading statements made by the police officer. A police officer can, therefore, purposefully make a wrongful statement to hide their misconduct, which could manipulate the narration.[25]

Furthermore, Draft One does not have a visual representation of the interaction. The only data being transferred stems from the audio, which is transmitted and used to generate the report, as well as the input provided by the police officers regarding the essential details of the incident, without further elaboration. Thus, the AI system makes the executive decision on what information is included, the context, and the order[26] of the information that is provided in the report.[27] Technical issues may exacerbate this issue, as important informa-

---

24. Claudio Novell *et al*, 'Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity' (2024) 55 Computer Law & Security Review 1, 9-10 <https://doi.org/10.1016/j.clsr.2024.106066> accessed 26 March 2025. Limitations to the scraping techniques are set with opt-out mechanisms.

25. Alec Karakasanis, 'The Body Camera: The Language of Our Dreams' (2024) 4 Yale Journal of Law & Liberation 1, 6.

26. See Ferguson (n 8) 37. The order of the events generated by AI can be crucial in determining someone's innocence, which may be altered for coherence reasons by the AI.

27. Ferguson (n 8) 33-34.

tion may not be recorded due to the body camera deactivating by mistake, or external factors such as background noise that may affect the accuracy of the transcription.[28] When it comes to 'legal contexts', such transcription errors are not rare in Automatic Speech Recognition (ASR),[29] which are used for speech-to-text conversions.

c. Bias

Biases are a prominent concern regarding AI which are a direct cause of non-representative training datasets. If AI models are mainly trained on white individuals, standard accents, or male voices, they may develop 'gender, racial, cultural, and ideological biases',[30] potentially infringing the rights of the 'under-represented demographics'.[31] The same applies to viewpoints and ideologies that can be reinforced in the AI system. These disparities can be further amplified by the algorithms themselves, attributed to their 'mathematical assumptions' and 'statistical properties'.[32] Given the above, in the context of law enforcement, such biases can be detrimental by influencing the decision-making in the criminal procedure or increasing the suspicion of an individual.[33]

---

28. Ibid 34.

29. Radina Stoykova *et al*, 'The AI Act in a law enforcement context: The case of automatic speechrecognition for transcribing investigative interviews' (2024) 9 Forensic Science International: Synergy 1, 3 <https://doi.org/10.1016/j.fsisyn.2024.100563> accessed 26 March 2025.

30. Ibid *2.*

31. Ibid *7.*

32. Xiahua Wei *et al*, 'Addressing Bias in Generative AI: Challenges and Research Opportunities in Information Management' (2025) 62 Information & Management 1, 4 <https://doi.org/10.1016/j.im.2025.104103> accessed 26 March 2025.

33. Anuj A. Jain, 'Ethical AI: A Policy Framework to regulate Bias in Large Language Models' (The University of Texas, 2024) 12.

d. Hallucinations

The predictive and speculative nature also raises questions regarding the reliability of these systems. Past cases have indicated that such hallucinations can evolve into issues with legal significance. Fictitious citations in lawsuits and false accusations of criminal acts have underscored the need for a rigorous approach to LLMs.[34] Hallucinations are 'hypotheses in which the model generates incorrect, nonsensical, or unreal'.[35] LLM's outputs are unpredictable 'due to its reliance on probabilistic methods' that can deviate from the input data and prompts,[36] resulting in untruthful, fabricated narratives. This raises the question of the accuracy of the AI-assisted police reports, when minor inaccuracies turn into significant ones that are often hard to uncover even with the assistance of AI tools.[37] It is a subject of debate whether hallucinations of LLMs can be fully eliminated, given that they are designed to generate content by mathematically predicting and estimating responses through 'pattern matching'.[38] This becomes evident when an incomplete prompt is entered into the chatbot and tries to 'guess' the rest of the sentence. Similarly, it can attempt to guess the 'context' and other details of an incident by drawing patterns from similar situations.

---

34. Molly Bohannon, 'Lawyer Used ChatGPT in Court—And Cited Fake Cases. A Judge Is Considering Sanctions' (*Forbes*, 8 July 2023) <https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/> accessed 25 March 2025. In the Roberto Mata v Avianca Inc case in the US, a lawyer used AI-generated citations; See also Noyb, 'AI hallucinations: ChatGPT created a fake child murderer' (*Noyb,* 20 March 2025) <https://noyb.eu/en/ai-hallucinations-chatgpt-created-fake-child-murderer> accessed 25 March 2025.

35. Nicola Fabiano, 'AI Act and Large Language Models (LLMs): When critical issues and privacy impact require human and ethical oversight' [2024] arXiv <https://doi.org/10.48550/arXiv.2404.00600> accessed 25 March 2025.

36. Claudio Novelli *et al* (n 24) 6.

37. Ibid.

38. Ferguson (n 8) 35.

5. Evaluating the Impact on the Right to a Fair Trial and Presumption of Innocence

The aforementioned concerns suggest potential violations of fundamental rights and freedoms. The deployment of AI in the realm of law enforcement is a sensitive subject, and there is a lot of mistrust within society, as errors attributed to AI are held to a more stringent standard compared to human errors. Technological advancements such as AI are often met with scepticism solely because they are 'foreign' to us due to a lack of AI literacy.[39] However, as discussed above, even if we set aside unfamiliarity with the AI, the issues regarding bias and inaccuracy are considerable.

In the event that hallucinations could incriminate an individual, this would have implications for the right to a fair trial, and presumption of innocence as enshrined under Articles 47 and 48 of the Charter of Fundamental Rights of the European Union, respectively. Deploying AI in the criminal justice system can have adverse effects, questioning the fairness of the criminal procedure, especially when accountability and liability involving AI constitute a grey area. Even if safeguards are put into place, such as reviews by police officers, the opportunity to complete ambiguities, or the chance to revisit the incident from the video footage from the body-worn cameras to counter-check the facts reported, the burden of proof of their innocence should not be shifted due to AI errors. Proving such innocence demands time, effort, and financial resources that undermine the effectiveness of the justice system and deprive individuals of fair and impartial legal protection.

As mentioned above, police reports can be admissible in court to attest to facts of the incident or complement and support other existing evidence. Although police reports only present facts of incidents, the risk of AI influencing the decision-making process in court or being used to press charges could affect 'people's innocence, guilt, and punishment'.[40] This implies that while AI might assist in drafting or the collection of information, the final interpreta-

39. Carl Dement and Melissa Inglis (n 17) 8.

40. ACLU (n 5) 1.

tions and observations in the report must be made by police officers exercising their judgment and discretion.[41]

To substantiate the above, AI-assisted could compromise public trust, considering the existing mistrust in law enforcement, perpetuate the existing issues with biases in law enforcement,[42] and possibly create chilling effects for individuals who seek justice. Moreover, an experimental trial carried out by a team of scholars with the cooperation of the Manchester Police Department in the US concluded that Draft One is not as time-efficient as claimed by police officers and Axon.[43] This raises issues regarding the legitimacy of AI systems in light of the potential for such systems to compromise fundamental rights, thereby challenging the very purpose of their existence.

6. Regulating AI-assisted Police Reports under EU Law

This section will analyse the applicable legal framework in the EU with respect to AI-assisted police reports and the associated legal challenges in light of the risks examined in the previous section of this paper.

a. Data Protection Issues under LED

Firstly, data protection issues may arise under the Law Enforcement Directive (LED).[44] To elaborate, voice recordings are protected as a special category of personal data due to their ability to reveal sensitive information about an individual relating to their 'health or emotional status', 'racial or ethnic origin', and

41. Tomasz Sroka 'Artificial intelligence and the right to a fair trial', in M. Balcerzak, J. and Kapelańska-Pręgowska (eds), *Developing Standards for a Changing World (Edward Elgar Publishing* 2024*)* 250, 276 <https://doi.org/10.4337/9781035337934.00022> accessed 26 March 2025.

42. Ferguson (n 8) 46.

43. Ian T. Adams et al (n 16) 3.

44. LED applies to law enforcement as lex specialis according to article 1(1).

'social status'.[45] Therefore, strict safeguards apply under Article 10 of the LED that guarantee the 'rights and freedoms' of the data subjects.[46] Particularly, the processing of special categories of personal data is allowed only 'where strictly necessary'. In the recent case of *Criminal proceedings against V.S.,* the European Court of Justice raised the standard of 'strictly necessary', emphasizing that Article 10 of the LED should be applied rigorously and in limited cases.[47]

Whilst the processing of voice recordings may be necessary in instances where law enforcement wishes to verify the recordings to identify discrepancies in the written report,[48] such processing via AI tools appears unnecessary in terms of generating police reports and the completion of such administrative tasks by law enforcement. Therefore, it fails to justify the necessity of processing voice recordings, especially compared to the disproportionate risks associated with it. Similarly, issues arise concerning the principle of data accuracy under Article 4(1)(d) of the LED. LLMs are susceptible to 'generate content that is factually inaccurate' due to hallucinations, undermining the lawfulness of the data processing under LED.[49]

45. Radina Stoykova et al (n 29) 7.

46. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (LED), and repealing Council Framework Decision 2008/977/JHA OJ L 119, art. 10 (1).

47. Case C-205/21 *Criminal proceedings against VS* [2023]; See also Markus Naarttijärvi, 'AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity', in Eduardo Gill-Pedro and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions* 331, 341.

48. Ferguson (n 8) 46.

49. Claudio Novell et al (n 24) 6.

b. Inconsistencies under the AI Act

Secondly, the AI Act takes a risk-based approach to determine the requirements of AI systems and obligations of providers and deployers of AI systems.[50] According to the risk they pose, the AI systems are divided as follows: unacceptable, high-risk, limited, and minimal.[51] If an AI system is classified as high risk under article 6 of the AI Act it is required to ensure: a) high-quality data sets; b) technical documentation with all the necessary information for competent authorities to assess compliance with the regulation; c) enable record-keeping; ensure transparency and provide information to users; d) human oversight; and e) an appropriate level of robustness, accuracy and cybersecurity.[52]

Prohibited practices under Article 5 of the AI Act are exhaustively listed, including 'social scoring' and 'real-time remote biometric identification for law enforcement purposes in publicly accessible spaces', without any reference to AI tools for administrative tasks intended for law enforcement. Furthermore, General-Purpose AI (GPAI), classified as a limited risk, must be able to operate a variety of tasks and in various fields.[53] In this case, AI systems such as Draft One are only intended to be used by law enforcement for the sole purpose of drafting police reports and therefore cannot be classified as limited risk under the definition of GPAI.

It is unclear whether such AI system can be, also, classified as high-risk, as according to article 6 (2) combined with the referred to section 8(a) of Annex III 'AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and

50. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act) [2024] OJ L, 2024/1689.

51. Radina Stoykova et al (n 29) 3.

52. AI Act, art. 10, 11, 12, 13, 14, and 15.

53. AI Act, article 3 (66); recital 97.

in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution'. In light of this, it is unclear whether police officers assist in researching and applying the law on behalf of the judicial authority, as police reports are not always invoked as evidence, and police officers do not interpret the law. On the contrary, they are part of the executive branch and operate independently from the judiciary.

Similarly, it is unclear whether these AI systems fall under the scope of section 6 (c) of Annex III. According to this section, 'AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences'. However, AI-assisted police reports do not proceed to the assessment of evidence, such as footage from the body-worn cameras.[54] Rather, they just state factual information without analysing or suggesting legal actions, for instance, whether charges should be pressed.

Given the above, the AI Act has received criticism from the academic community, *inter alia*, for being incapable of facing the risks associated with Generative AI.[55] Considering the rationale for classifying AI systems based on their impact on fundamental rights, the effectiveness of the AI Act is called into question. If Draft One is not classified as a high-risk or limited risk AI system, that means General-Purpose AI (GPAI), such as ChatGPT,[56] is subjected to greater scrutiny and held to higher standards by requiring transparency,[57] compared to AI systems that are intended for law enforcement and could influence criminal procedures by charging suspects and making sentencing decisions. This is further reinforced by: 1) Article 6 (3) of the AI Act which mandates the requirements for

54. Radina Stoykova et al (n 29) 4.

55. Claudio Novell et al (n 24) 14.

56. Tambiama Madiega, 'General-purpose artificial intelligence' (*European Parliament,* 2023) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf> accessed 26 March 2025.

57. See European Commission, 'AI Act' <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 28 March 2025. Transparency requirements entail the disclosure and labelling of AI-generated content.

high-risk AI systems do not apply 'if a high risk system does not pose a significant risk of harm to…fundamental rights',[58] and 2) recital 28 of the AI Act that mandates practices under Article 5 of the AI Act are prohibited on the basis that they are harmful to fundamental rights enshrined in the Charter, including the right to fair trial and the presumption of innocence.[59]

While there is no evidence that Axon's Draft One is used in law enforcement agencies within the EU, this technology underlines the shortcomings of the current EU legal regime to address the risks associated with it. While LED sheds light on current data protection challenges regarding processing voice recordings for the purpose of generating AI-assisted police reports, the AI Act is ill-equipped to address the issues associated with the development and deployment of such AI systems. In light of the inconsistencies of the AI Act, the classification of a similar AI tool for AI-assisted police reporting as a minimal-risk AI system with no further requirements and obligations for providers will compromise the fundamental rights of persons and the integrity of the European criminal justice system. LLMs such as Axon's Draft One, designed for AI-assisted police reporting, may appear harmless at first glance, should be approached with caution and stringency. More importantly, such technology needs to be reconsidered by classifying it as a high-risk AI system under the AI Act and explicitly addressing the risks of LLMs used in the context of law enforcement.

Given the above, it is imperative that guidelines be published by the European Commission to clarify uncertainties in the interpretation of the AI Act regarding high-risk systems, as well as to extend the exhaustive list of high-risk AI systems to similar LLMs in the context of law enforcement. Nonetheless, adherence to obligations and requirements related, for example, to transparency, biases, accuracy, and the quality of datasets, for high-risk AI systems, should not just be part of the due diligence of providers and deployers of AI systems used for generating police reports.

58. See also AI Act, recitals 28; 67; 93; 157.

59. European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689' C (2025), 2.

7. Conclusion

AI inevitably continues to reshape established practices across sectors, including in law enforcement. Its current applications, such as Axon's Draft One for police reporting highlights risks such as bias, inaccuracies, and hallucinations that question the lawfulness of data processing under LED. LLM-powered AI tools used for police reporting can potentially incriminate individuals due to inaccuracies and false statements generated by them. Ultimately, the persons affected are those involved in the criminal cases, whose rights to a fair trial and presumption of innocence are put at stake. Under the current interpretation of the AI Act, Axon's Draft One is classified as a minimal risk AI system and subjected to no requirements if deployed in EU law enforcement. These challenges showcase the contradictions and shortcomings of the AI Act. Unless these legal uncertainties are explicitly addressed, the legitimacy of criminal proceedings and fundamental rights of persons in the EU remain inadequately safeguarded.

Bibliography

Primary sources

Charter of Fundamental Rights in European Union [2012] OJ C 326, OJ C 326

European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689' C (2025)

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119

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, and repealing Directive 95/46/EC (GDPR) OJ L 119

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU,

(EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 2024/1689

Secondary Sources

American Civil Liberties Union (ACLU), Police Departments Shouldn't Allow Officers to Use AI to Draft Police Reports (2024) 1 <https://www.aclu.org/documents/aclu-on-police-departments-use-of-ai-to-draft-police-reports> accessed 25 March 2025

Ferguson A.G., 'Generative Suspicion and the Risks of AI-assisted Police Reports' [2024] Northwestern Law Review 42 (forthcoming)

European Union Agency for Law Enforcement Cooperation (Europol), AI and policing The benefits and challenges of artificial intelligence for law enforcement (2024) <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing> accessed 23 March 2025

Adams I.T., 'Large Language Models and Artificial Intelligence for Police Report Writing', [2024] CrimRxiv1, 4 <https://doi.org/10.21428/cb6ab371.779603ee> accessed 23 March 2025

Axon, 'Overview' (*com*, 2025) <https://www.axon.com/company> accessed 23 March 2025

Axon, 'Draft One Demo' (*com*, 2025) <https://my.axon.com/s/draft-one?language=en_US> accessed 23 March 2025

Bohannon M., 'Lawyer Used ChatGPT In Court—And Cited Fake Cases. A Judge Is Considering Sanctions' (*Forbes*, 8 July 2023) <https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/> accessed 25 March 2025

Ian T. Adams *et al*, 'No man's hand: artificial intelligence does not improve police report writing speed' [2024] J Exp Criminol <https://doi.org/10.1007/s11292-024-09644-7> accessed 26 March 2025

Dement C and Inglis M, 'Artificial intelligence-assisted criminal justice reporting: An exploratory study of benefits, concerns, and future directions' [2024] Criminology & Criminal Justice <https://doi.org/10.1177/17488958241274296> accessed 26 March 2025

Fabiano N., 'AI Act and Large Language Models (LLMs): When critical issues and privacy impact require human and ethical oversight' [2024] arXiv <https://doi.org/10.48550/arXiv.2404.00600> accessed 25 March 2025

Jain A.A., 'Ethical AI: A Policy Framework to regulate Bias in Large Language Models' (The University of Texas, 2024)

Karakasanis A., 'The Body Camera: The Language of Our Dreams'(2024) 4 Yale Journal of Law & Liberation

Madiega T., 'General-purpose artificial intelligence' (*European Parliament,* 2023) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)745708> accessed 26 March 2025

Naarttijärvi M., 'AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity', in Eduardo Gill-Pedro and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions*

Noyb, 'AI hallucinations: ChatGPT created a fake child murderer' (*Noyb,* 20 March 2025) <https://noyb.eu/en/ai-hallucinations-chatgpt-created-fake-child-murderer> accessed 25 March 2025

Novell C. *et al*, 'Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity' (2024) 55 Computer Law & Security Review 1, <https://doi.org/10.1016/j.clsr.2024.106066> accessed 26 March 2025

Sroka T. 'Artificial intelligence and the right to a fair trial', in M. Balcerzak, J. and Kapelańska-Pręgowska (eds), *Developing Standards for a Changing World (Edward Elgar Publishing* 2024*)* <https://doi.org/10.4337/9781035337934.00022> accessed 26 March 2025

Stoykova R. *et al*, 'The AI Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews' (2024) 9 Forensic Science International: Synergy <https://doi.org/10.1016/j.fsisyn.2024.100563> accessed 26 March 2025

Wei X. *et al*, 'Addressing Bias in Generative AI: Challenges and Research Opportunities in Information Management' (2025) 62 Information & Management <https://doi.org/10.1016/j.im.2025.104103> accessed 26 March 2025

About the author

Konstantina Kelesidi

Konstantina Kelesidi is a EU qualified lawyer and has completed the LL.M. Technology Law and Innovation programme at the University of Groningen during the academic year 2025-2026. She is currently pursuing a career in data protection and AI governance.

PART III. DATA SPACES AND GLOBAL CHALLENGES

CHAPTER 11: CONSENT AS A CATALYST? THE GDPR, THE DGA, AND THE ROLE OF DATA ALTRUISM ORGANIZATIONS IN FOSTERING EUROPEAN INNOVATION

Paulina Anna Ryszkowska

1. Introduction

For decades, the European Union (EU) has recognised the potential of data sharing in driving innovation.[1] Although the PSI Directive, later revised as the Open Data Directive (ODD), laid a solid foundation by opening up publicly-held data, the rapid growth of the data economy soon demanded a broader and more comprehensive framework.[2] Particularly private sectors, despite an increasing concentration of valuable data, had no EU-level data-sharing incentives.[3]

1. Mar Negreiro, 'Re-use of public sector information' (*European Parliament* 2019) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628312/EPRS_BRI(2018)628312_EN.pdf> accessed 23 March 2025, p 1.

2. Mirelle van Eechoud, 'Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research' (European Commission 2022) <https://op.europa.eu/en/publication-detail/-/publication/a313139b-1147-11ed-8fa0-01aa75ed71a1> accessed 23 March 2025, p 8-9; Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive) [2019] OJ L 172/56.

3. Commision, 'A European Strategy for Data' (Communication) COM (2020)16 final p 7.

Recognising these limitations, the EU has shifted its focus towards the development of Common European Data Spaces, designed to encourage secure data sharing across public and private sectors for the reasons of general interest.[4] One measure in particular, i.e. data altruism established under the Data Governance Act (DGA), was recognised as the next step in fully facilitating a citizen-centric data economy.[5] As opposed to forcing the opening of agency data, the framework aims to popularise individual acts of trust-based, voluntary data donation for the mutual benefit of progressing scientific research and innovation.[6]

In this context, trust is achieved through establishing registered Data Altruism Organisations (DAOs), responsible for managing the altruistically-donated data, subject to obtaining prerequisite consent.[7] The DGA also envisions that, past the point of collection, all data processed by DAOs will be anonymised, allowing the organisations to operate without prejudice to the General Data Protection Regulation (GDPR).[8] The application of this framework has led to a number of practical challenges. Noteworthy is the current subjective definition of personal data and the concurrent anonymisation issues,[9] which have resulted in the GDPR being unintentionally, yet *de facto,* applicable for DAOs.

---

4. Ibid p 16-17.

5. The Open Data Directive initially introduced this goal in its recitals. Subsequently, the reference to data altruism as a step forward has been made.Open Data Directive, recital 8 and 14; Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2018] OJ L 152/1, recital 5.

6. Data Governance Act, recital 46 and art 2(16).

7. Ibid.

8. Data Governance Act, art 1(3).

9. Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (0829/14/ENWP216, European Commission 2014), p 3; also endorsed later by the European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (EDPB 2024), p 15-16.

Various doctrinal sources have elaborated on the possible consequences of this regulatory overlap. Tackling the issue on a literary level suggests a full convergence between the DGA and the GDPR, with the latter taking primacy in conflict cases.[10] However, some deem this belief vastly naive.[11] Particularly, inconsistencies regarding the definition of consent across both regulations prove to be problematic.[12] In this context, two alternative solutions are put forward. First, that the GDPR as well as the DGA consent standards will be applied independently within DAOs, creating a more robust framework.[13] Second, that the GDPR standard will be applied within the DGA consent form, creating coherence.[14] However, both of these approaches presume that under this regulatory interplay DAOs will ultimately bring a certain added value towards empowering European research and innovation.

This paper examines the effects of the DGA-GDPR regulatory interplay in shaping the DAO governance framework, arguing that the lack of clarity surrounding fundamental concepts, particularly consent, hinders both trust and the effective implementation of data-sharing initiatives, ultimately questioning the added value of DAOs in driving European innovation. Chapter 1 will explore

---

10. Corina Kruesz and Felix Zopf, 'The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU' (2021) 7 Eur Data Prot L Rev 569, p 575.

11. Maria Christofidou and Others, 'Data altruism and the "consent" question: a study into the "consent" models used under the GDPR and how the data altruism mechanism can act as a potential solution for the research community in the reuse of health data' (2024) 11 Regulatory Science 2024-2025, p 9; Cruesz and Zopf (n 10) p 572; Gauthier Chassang and Lisa Feriol, 'Data Altruism, Personal Health Data and the Consent Challenge in Scientific Research: A Difficult Interplay between EU Acts' (2024) 10 European Data Protection Law Review 57, p 5.

12. Winfried Veil, 'Data Altruism: How the EU is screwing up a good idea' [2021] Algorithm Watch <https://algorithmwatch.org/en/data-altruism> accessed 24 March 2025, p 5; Chassang and Feriol (n 11) p 5; Christofidou and Others (n 11) p 9.

13. Christofidou and Others (n 11) p 8-9.

14. Kruesz and Zopf (n 10) p 570.

the general applicability of GDPR within the data altruism framework. Following, Chapter 2 will delve into the discrepancies concerning the concept of consent focusing on three particular issues: the multiplicity of legal bases under the GDPR, the scope of consent under both Regulations and the ambiguity regarding meeting its formal requirements. Lastly, Chapter 3, based on the findings from previous sections, will examine the added value that DAOs bring towards fostering innovation through enabling scientific research in the EU.

2. Applicability of the GDPR within the Data Altruism Framework

To examine the interplay of the GDPR and the DGA consents, one should first gain understanding of the scope of GDPR's applicability to the data altruism framework. Article 1(3) of the DGA states that *'This Regulation is without prejudice to Regulation (EU) 2016/679 [...]. In the event of a conflict between this Regulation and Union law on the protection of personal data, the relevant Union or national law on the protection of personal data shall prevail.'*[15] Additionally, the main text of the DGA contains numerous references to the GDPR, for example within the definitions of 'consent', or 'processing'.[16] This stipulates the full applicability and primacy of the GDPR so long as the data processing activity falls under its scope.[17] Even though primary data anonymisation is put forward as the default mechanism to avoid issues of conflict,[18] the difficulties relating to its achievement, as expressed by the EDPB,[19] bring the assumption that DAOs will likely be required to consider GDPR requirements when conducting its commended tasks.

Looking further into the scope of this legal co-existence, DAOs are most

15. Data Governance Act, art 1(3).

16. Ibid art 2.

17. Kruesz and Zopf (n 10) p 573.

18. Data Governance Act, recital 15.

19. EDPB (n 9) p 15-16.

likely to qualify as data controllers under the GDPR, determining the purposes and means of personal data processing.[20] For example, this can be seen in DAOs autonomy to decide on granting access to their datasets based on their own policies, specifying the nature of processing activities allowed.[21] The requirement of the DGA that DAOs pursue an objective of 'general interest' may, however, yield instances of lowered GDPR responsibilities, in accordance with Article 89 GDPR 'public interest' or 'scientific research', should the meaning of these concepts be deemed synonymous.[22]

It can thus be concluded that, unless the DGA's 'general interest' can fall under the scope of Article 89 GDPR (subject to a later determination), DAOs bear responsibility for ensuring comprehensive compliance with data protection obligations in relation to the processing of personal data. Particularly important within this context is ensuring the lawful basis of processing. This factor, alongside safeguarding data subject rights, is deemed critical for fostering data subject trust.[23] That, in turn, becomes a prerequisite for fostering innovation via data altruism, as endorsed in the DGA itself.[24]

3. The Consent Requirement

3.1. The GDPR has Multiple Legal Bases

To ensure lawful processing, the GDPR allows for the use of multiple legal

20. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, art 4(7).

21. Data Governance Act, art 21(1); Kruesz and Zopf (n 10) p 574.

22. Data Governance Act, art 18; General Data Protection Regulation, recital 33 and art 89.

23. Francesca Perucci and Eric Swanson, 'Building Trust and Facilitating Use of Data' (2024) 40 *Statistical Journal of the IAOS* 71, p 74.

24. Data Governance Act, recital 5.

bases under Article 6 and 9.[25] From a historical perspective, consent used to be the main basis for processing in scientific research, stemming from the wording of Recital 33 GDPR.[26] A shift was seen in 2020, when the European Data Protection Board (EDPB) clarified that alternative legal bases of Article 6 and 9 GDPR may effectively be used for research purposes, so long as they are justified and accompanied by sufficient safeguards.[27] Since then, relying on alternative legal bases has become a widely accepted practice.[28] Notably, the basis of public interest has been heavily relied upon in this context, including within data sharing organisations.[29] On the contrary, the DGA's definition of 'data altruism' defines the process as: *"the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data [...] where they make their data available for objectives of general interest as provided for in national law"*.[30] This wording unambiguously suggests that consent should once again become the pivotal, if not the only possible, legal basis for data processing. Multiple recitals and provisions in the DGA, such as Article 21(3) or Recital 50, further confirm this assumption, obliging DAOs to provide tools for

25. General Data Protection Regulation, art 6 and 9.

26. General Data Protection Regulation, recital 33; Christofidou and Others (n 11) p 7.

27. European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (EDPB, 2020) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 24 March 2025, para 154.

28. Christofidou and Others (n 11) p 7.

29. The term 'data sharing organisations' used in this context refers to public or private entities with an essentially equivalent role to what the DGA frames as 'Data Altruism Organisations', that have been active since before the DGA's enforcement, operating mainly under the GDPR for data protection and fostering trust in data sharing; Ana Koiava, 'Challenges of GDPR Compliance with the Data Altruism Concept under DGA: Lessons from the Estonian X-Road Model' (Master's thesis, Tallinn University of Technology 2024), p 37-38.

30. Data Governance Act, art 2(16).

obtaining consent from the data subject or permissions to process data made available by data holders.[31]

The choice to embed consent as a central element of DAO governance can be traced back to a core principle of the EU data protection acquis, i.e. restoring control to data subjects;[32] this becoming particularly relevant for concepts such as data altruism, where gaining data subject trust is foundational. Even when considered at a literal level, data altruism cannot be realized without consent. Cambridge dictionary defines 'altruism' as *doing acts that help others although one does not get anything by doing those acts*.[33] Accordingly, even if one were to critique the DGA's legal definition of data altruism, the terminology itself presupposes a selfless act (on the part of the data subject). This semantic connotation renders the reliance on alternative legal bases under Article 6 GDPR conceptually incompatible, as consent constitutes the only legal basis affording sufficient data subject autonomy to adopt an altruistic stance.

Another source justifies this consent rule as an ethical standpoint, deeming the alternative GDPR legal bases as incompatible with the object of data altruism due to the wide (unclear) variety of purposes for which the altruistic data could be processed.[34] This reasoning is also justifiable from a teleological standpoint. Considering the DGA's objectives, DAOs are supposed to function as a neutral facilitator in enabling data sharing practices in the EU.[35] Whereas other companies, platforms, or research entities that collect and process data for their own purposes must establish a lawful basis under the GDPR to con-

31. Data Governance Act, recital 50 and art 21(3).

32. Claudia Quelle, 'Not just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann and Others (eds), *Privacy and Identity Management. Facing up to Next Steps* (IFIP Advances in Information and Communication Technology 2016), p 141.

33. 'Cambridge Academic Content Dictionary' (*Cambridge Dictionary*, 20 August 2025) <https://dictionary.cambridge.org/dictionary/english/altruism> accessed 24 August 2025

34. Chassang and Feriol (n 11) p 10.

35. Data Governance Act, recital 29.

duct its commercial activities, DAOs, as neutral facilitators, lack an autonomous purpose capable of justifying recourse to alternative bases such as 'legitimate interest' or 'contractual necessity'.[36] Accordingly, DAOs reliance on consent can be seen as more than a mere policy preference, viewing it as a structural necessity flowing from their intermediary character under the DGA's commitment to foster trust and transparency in data sharing.

It could nevertheless be contended that such a framework imposes limitations, not only upon DAOs themselves, but also upon the wider ecosystem of EU data-sharing organisations. The emphasis on trustworthiness, inherent to the role of DAOs, risks re-establishing consent as the 'golden standard' for data processing in scientific research.[37] Such a development is not without concern, given that both the applicability and the practical attainability of GDPR-compliant consent in the context of data altruism have already been subject to sustained contestation within the academic discourse.[38] Highlighted are two arguments: the inconsistent relationship between the consent concepts across the GDPR and the DGA and the issue of defining specificity.

3.2. The Concept of Consent

The concept of consent for data altruism under the DGA presents inherent ambiguities. The Act's definition directly references Article 6 GDPR.[39] Consequently, the logical assumption would be that the consent to be obtained by the DAOs should meet the GDPR standard, i.e. be freely given, specific,

36. László Bencze and Others, 'Report on lessons learned to be applied and recommendations for data altruism practices in the implementation of construction of national and European health data spaces (including broad consent)' (Deliverable 8.2, TEHDAS Consortium Partners 2023) p 22-24.

37. Chassang and Feriol (n 11) p 14; Veil (n 12) p 7.

38. Chassang And Feriol (n 11) p 15; Koiava (n 29) p 40; Lusine Vardanyan and Hovsep Kocharyan, 'The GDPR and the DGA Proposal: Are They in Controversial Relationship?' (2022) 9 European Studies 91, 99.

39. Data Governance Act, art 2(5).

informed and unambiguous, according to its most recent interpretation.[40] Looking at the DAO governance framework, however, one cannot oversee the inherent hostilities that the full applicability of this notion brings.

DAOs process both personal and non-personal data and, for both of them, a form of consent is required.[41] The DGA wording distinguishes between obtaining consent (personal data) and permission (non-personal data).[42] Nevertheless, there is a persistent ambiguity regarding their functional differentiation.[43] As far as the DGA's text is concerned, the 'permission' needs to meet an overwhelmingly similar standard to the one required for data subject consent. For example, both the data holder and the data subject need to be provided with the same information before sharing the data.[44] They also are granted the same right to withdraw the consent, and are able to dictate the purposes for which their data will be used.[45] To obtain the consent or permission, DAOs are required to utilize the same European Data Altruism Consent Form (EDACF) as well.[46] Subsequently, the distinction in treatment between personal and non-personal data under the data altruism framework becomes unclear. Should DAOs seek GDPR-compliant consent from data holders as well? What is the functional difference between the GDPR consent and the EDACF? It should also be noted that, pursuant to the considerations made in the previous sections, DAOs are, in principle, required to obtain consent for any further processing activity regarding either type of data.[47] Should both consent standards be then

40. General Data Protection Regulation, art 4(11).

41. Data Governance Act, art 2(16).

42. Ibid.

43. Koiava (n 29) p 36.

44. Data Governance Act, art 21.

45. Data Governance Act, art 21(2) and (3); Data Governance Act, art 23.

46. Data Governance Act, art 25.

47. See Chapter 1.

applied for personal data?[48] If the differences in applicability of the GDPR consent and the EDACF are not sufficiently clarified, DAOs could be met with an unreasonable administrative burden in ensuring compliance.[49] This, in turn, could decrease their efficiency and the ability to boost scientific research and innovation.[50]

Within this context, the value of introducing EDACF in the first place becomes debatable. The EU already has a well-developed notion of consent under the GDPR – a Regulation that is supposed to foster data subject trust itself. With the creation of a second consent form, similarly applicable to personal data, one could argue that the trust in data sharing outside of DAOs could suffer significantly, with the mere GDPR compliance being viewed as 'below the industry standard'.[51] Conversely, the lack of clarity in the functional applicability of both the consent forms creates significant compliance hurdles for DAOs, particularly as their non-registered competitors would not have to consider this issue.[52] It is thus disputed whether simply requiring the existing GDPR consent could not have provided for a more effective framework, ensuring a more equal level-playing field while keeping the robust image of the GDPR.[53]

3.3. The Scientific Research Exception

Arguably, the compliance burden could be lowered by utilizing the scientific

48. Koiava (n 29) p 36.

49. Ibid. p 40.

50. 'Administrative Simplification' (*OECD,* 2021) <https://www.oecd.org/en/topics/sub-issues/administrative-simplification.html> accessed 24 March 2025.

51. Veil (n 12) p 7.

52. Koiava (n 29) p 36.

53. Max von Grafenstein, 'Reconciling Conflicting Interests in Data through Data Governance An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR) (2022) 2 HIIG Discussion Paper Series, p 32

research exception found under Article 5(1)(b) in conjunction with Article 89 GDPR.[54] On this matter, the DGA's stance seems convergent. Under Recital 50, DAOs are required to comply with the GDPR when obtaining data subject consent, but are permitted to make use of the scientific research exception for further processing, so long as ethical standards are effectively utilised.[55]

The problem becomes complicated once the main text of the DGA is examined. Under Article 21(2), DAOs are prohibited from using the data for other objectives than those of general interest for which the data subject or data holder allows the processing.[56] This seemingly contradicts or, in the very least, limits the applicability of Article 5(1)(b) GDPR.[57] To ensure consistency, 'general interest' would have to have an essentially equivalent meaning to 'scientific research' or 'public interest' under the GDPR. Nonetheless, the legislator deliberately opted for using a different term, pointing towards the existence of certain divergencies between the concepts.[58] To that end, the DGA provides a mere non-exhaustive list of examples regarding what 'general interest' could be. While the decision to leave a broad definition allows for future flexibility and makes data altruism meaningful beyond the GDPR, it also carries the capability to diminish data subject trust in altruism.[59] It has been argued, since before the official publication of the DGA, that an additional list of limitations or examples of what general interest is not could reconcile these two interests.[60] It could also carry an additional positive effect on fostering data subject trust by empowering individuals to make better-informed decisions on altru-

54. General Data Protection Regulation, art 5(1)(b) and 89.

55. Data Governance Act, recital 50.

56. Data Governance Act, art 21(2).

57. Kruesz and Zopf (n10), p 576.

58. Chassang and Feriol (n11), p 5.

59. Tea Mustać, 'Data Altruism by Default: An Alternative to Consent for Personal Data Processing in Machine Learning'(CEP project, 2024), p 8.

60. Koiava (n 29) p 33; Kruesz and Zopf (n 10) p 570.

istically sharing their data for the general interest.[61] Unfortunately, such limitations have never found their way into the published text, leaving DAOs with legal uncertainty as to the (extent of the) applicability of the scientific research exception.

The referral to national 'general interest' objectives exacerbates the challenge of establishing a Single European Data Market as well.[62] Without an EU-wide, autonomous interpretation of 'general interest', DAOs are likely to encounter significant difficulties in navigating intra-EU data transfers, as they would need to account for the divergent interpretations of each Member State to maintain trust and transparency.[63] Unlike the issues addressed in Schrems II, which concerned the adequacy of third-country data protection, the present fragmentation originates within the EU itself, posing an internal barrier to the free flow of data in the EU.[64] As a by-product, data altruism practices among organisations are also likely to diverge, further undermining the establishment of an effective and harmonised framework for EU-wide data sharing.[65]

When turning to potential solutions, the EDACF re-emerges as a key reference point. Its modular approach could help define a more uniform definition of a 'general purpose' and make it easier for DAOs to obtain lawful consent.[66] However, subject to the considerations made in the previous section, EDACF's

---

61. Koiava (n 29) p 33.

62. The DGA has been established as part of the European Strategy for Data. One of the main goals of said strategy is the creation of the Single European Data Market; Marianne Bårtvedt van Os and Others, 'Presentation of a first set of data altruism definitions, use cases and findings' (*Towards European Health Data Space* 2021) <https://tehdas.eu/app/uploads/2021/09/tehdas-presentation-of-a-first-set-of-data-altruism-definitions-use-cases-and-findings.pdf> accessed 24 March 2025, p 3.

63. Dwayne Ansah and Iryna Susha, 'Exploring Data Altruism as Data Donation: A Review of Concepts, Actors and Objectives' (16th IFIP WG 8.5 International Conference, Ghent, September 2024) , p 181; Koiava (n 29) p 32.

64. Case C-311/18 *Schrems II* [2020] EU:C:2020:559, para 105 and 203.

65. Kruesz and Zopf (n 10) p 571.

66. Data Governance Act, art 25(2); Koiava (n 29) p 36.

overall value in contributing towards an effective data altruism framework is arguable.[67] Even if it would help resolve some of the consent problems, such as defining 'general interest', it would only do so for the DGA. The ambiguous relationship between the GDPR and the DGA under data altruism would remain unaffected.

4. The Added Value of DGAs in Fostering Scientific Research and Innovation

As argued before, the DAOs will likely need to ensure GDPR compliance in their processing activities. Due to the subjective definition of personal data, this compliance is likely to spread over a majority of its tasks. On the contrary, the DGA and the GDPR have failed to achieve sufficient coherence across their provisions, capturing DAOs within a legally-uncertain governance framework. As opposed to their non-registered counterparts, DAOs can only rely on consent when processing personal data for altruism. They're also required to obtain an essentially equivalent 'permission' regarding non-personal data from the data holders. The sole concept of consent fails to provide sufficient clarity to enable its efficient use. The framework establishes two consent forms but does not establish the functional differences or, alternatively, measures for convergence between them. This creates both legal uncertainty and an additional compliance burden for the DAOs.

It should also be noted that this paper has only highlighted the issues of consent and ensuring the applicable legal basis for data processing. Looking from a broader perspective, DAOs are likely to meet more obstacles in further stages of conducting their activities. One direct effect of failing to meet lawful consent is the limited possibility to exercise data subject rights.[68] Other issues surround

67. See section 2.2.

68. General Data Protection Regulation, art 15-22; Adrianna Michałowicz, 'Data Sharing for the Common Good – Remarks on the Data Altruism Framework Established under the Data Governance Act' (2024) 17 Yearbook of Antitrust and Regulatory Studies 209, p 228.

fulfilling the accountability obligation,[69] establishing a form of legal personality under the national law,[70] or the complex oversight and reporting framework.[71] On the other hand, the risk of non-compliance poses an even greater threat, as it may trigger the full scope of fines under both the GDPR and the DGA.[72]

On this note, one can start questioning the added value that DAOs bring to fostering scientific research and innovation. The initiative to register beyond, in principle, being considered more trustworthy is arguably low.[73] On the contrary, the legal uncertainty restricts transparency and will likely lead to more instances of non-compliance than within the non-registered data sharing organisations.[74] Notwithstanding, being portrayed by the EU as the 'golden standard' of data altruism, the existence of DAOs might *de facto* reduce the data subjects' trust in such initiatives.[75] Ultimately, without trust, less data will be shared altruistically, and any shared data will be harder to access – an outcome that could significantly hinder Europe's innovative performance.

5. Conclusion

This paper has demonstrated that Data Altruism Organisations (DAOs) bring little to no added value to fostering scientific research and innovation in the EU. While intended to facilitate trustworthy data-sharing, DAOs face significant

69. General Data Protection Regulation, art 5(2) and 28(1); Koiava (n 29) p 31; Michałowicz (n 66) p 227.

70. Magdalena Jacolik, 'Data Altruism or Voluntary Data Sharing in the Economy' (2022) 14 Przegląd Prawniczy Uniwersytetu Im. Adam Mickiewicza 339, p 349.

71. Veil (n 12) p 7.

72. Kruesz and Zopf (n 10) p 577.

73. Veil (n 12) p 6-7.

74. Scott Baker and Alex Raskolnikov, 'Harmful, Harmless, and Beneficial Uncertainty in Law' [2017] Journal of Legal Studies 281, p 281.

75. Veil (n 12) p 7.

legal and administrative burdens that outweigh any potential benefits. The requirement to rely solely on consent for personal data processing, combined with the ambiguity between GDPR and DGA consent frameworks, creates unnecessary complexity. On the other hand, the European Data Altruism Consent Form fails short of its potential to effectively address these issues, as the scope of its applicability remains unclear and unreasonably bureaucratic.

Moreover, the undefined concept of 'general interest' fragments the EU data market, as national interpretations create legal uncertainty in cross-border data sharing. These challenges deter participation in data altruism initiatives, while non-registered entities operate with greater flexibility. Ultimately, instead of fostering data-driven innovation, DAOs introduce additional obstacles without a clear competitive advantage. Unless significant regulatory refinements are made, DAOs will remain an impractical and ineffective tool for advancing the EU innovative ambitions.

Bibliography

Primary sources

Case C-311/18 *Schrems II* [2020] EU:C:2020:559

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive) [2019] OJ L 172/56

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2018] OJ L 152/1

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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Secondary sources

—— 'Administrative Simplification' (*OECD,* 2021) <https://www.oecd.org/en/topics/sub-issues/administrative-simplification.html> accessed 24 March 2025

Ansah D and Susha I, 'Exploring Data Altruism as Data Donation: A Review of Concepts, Actors and Objectives' (16th IFIP WG 8.5 International Conference, Ghent, September 2024)

Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (0829/14/EN

WP216, European Commission 2014)

Baker S and Raskolnikov A, 'Harmful, Harmless, and Beneficial Uncertainty in Law' [2017] Journal of Legal Studies 281

Bencze L and Others, 'Report on lessons learned to be applied and recommendations for data altruism practices in the implementation of construction of national and European health data spaces (including broad consent)' (Deliverable 8.2, TEHDAS Consortium Partners 2023)

Bårtvedt van Os M and Others, 'Presentation of a first set of data altruism definitions, use cases and findings' (Towards European Health Data Space 2021) <https://tehdas.eu/tehdas1/results/tehdas-probes-matrix-of-data-altruism-definitions/> accessed 24 March 2025

Commision, 'A European Strategy for Data' (Communication) COM (2020)16 final

Chassang G and Feriol L, 'Data Altruism, Personal Health Data and the Consent Challenge in Scientific Research: A Difficult Interplay between EU Acts' (2024) 10 European Data Protection Law Review 57

Christofidou M and Others, 'Data altruism and the "consent" question: a study into the "consent" models used under the GDPR and how the data altruism mechanism can act as a potential solution for the research community in the reuse of health data' (2024) 11 Regulatory Science 2024-2025

European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (EDPB, 2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> accessed 24 March 2025

European Data Protection Board, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (EDPB 2024)

Jacolik M, 'Data Altruism or Voluntary Data Sharing in the Economy' (2022) 14 Przegląd Prawniczy Uniwersytetu Im. Adam Mickiewicza 339

Negreiro M, 'Re-use of public sector information' (European Parliament 2019) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)628312> accessed 23 March 2025.

Kruesz C and Zopf F, 'The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU' (2021) 7 Eur Data Prot L Rev 569

Koiava A, 'Challenges of GDPR Compliance with the Data Altruism Concept under DGA: Lessons from the Estonian X-Road Model' **(**Master's thesis, Tallinn University of Technology 2024), p 37-38.

Michałowicz A, 'Data Sharing for the Common Good – Remarks on the Data Altruism Framework Established under the Data Governance Act' (2024) 17 Yearbook of Antitrust and Regulatory Studies 209

Mustać T, 'Data Altruism by Default: An Alternative to Consent for Personal Data Processing in Machine Learning'(CEP project, 2024)

Perucci F and Swanson E, 'Building Trust and Facilitating Use of Data' (2024) 40 Statistical Journal of the IAOS 71

Quelle C, 'Not just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann and Others (eds), *Privacy and Identity Management. Facing up to Next Steps* (IFIP Advances in Information and Communication Technology 2016)

Vardanyan L and Kocharyan H, 'The GDPR and the DGA Proposal: are They in Controversial Relationship?' (2022) 9 European Studies 91

Veil W, 'Data Altruism: How the EU is screwing up a good idea' [2021] Algorithm Watch <https://algorithmwatch.org/en/data-altruism> accessed 24 March 2025

Von Grafenstein M, 'Reconciling Conflicting Interests in Data through Data Governance An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR) (2022) 2 HIIG Discussion Paper Series

About the author

Paulina Anna Ryszkowska

Paulina Ryszkowska completed the LLM Technology Law and Innovation programme at the University of Groningen during the academic year 2025-2026. She is currently attending an exchange programme at the University of Osaka, Japan, and works as a research assistant for a HORIZON Europe research project on institutional ethics reviews.

CHAPTER 12: THE EUROPEAN HEALTH DATA SPACE AND MEDICAL AI DEVICES

Mariam Ibraham

1. Introduction

Artificial Intelligence has the potential of transforming healthcare, however, its success highly depends on access to high quality and diverse health data. Its capacity to analyse large volumes of complex data and generate clinical predictions renders it a powerful instrument for enhancing the quality of healthcare. For instance, AI systems are now capable of detecting early signs of conditions such as sepsis in intensive care units, and identifying cancerous tissue in mammograms with a degree of precision that sometimes surpasses human radiologists. Moreover, the automation of routine processes such as scheduling, billing, and electronic recordkeeping allows clinicians to dedicate more time to patient care, enhancing both efficiency and quality of service in healthcare.

Despite these advancements, the adoption of AI in healthcare remains constrained by a number of critical challenges. Among these are the opacity of many AI models, which function as 'black boxes' and resist clinical interpretation; the potential for algorithmic bias, which can reinforce existing health inequalities; and the risks associated with poor data quality, privacy breaches, and legal ambiguity. Consequently, the realisation of AI's potential depends not only on technological innovation but also on the establishment of robust governance frameworks that address issues of data quality, privacy, transparency, and accountability.

In this context, the European Health Data Space (EHDS) has emerged as a key instrument intended to support the development and regulation of the use of AI in the medical sphere in the European Union. By creating a secure and standardised framework for accessing and sharing health data across member states, the EHDS seeks to address fundamental barriers to the effective use of AI in healthcare, including inconsistent data quality, lack of interoperability, and fragmented access to large-scale, diverse datasets. Crucially, it also rein-

forces existing regulations concerning data protection, cybersecurity, and sets safeguards for the responsible secondary use of health data.

At the same time, AI in healthcare cannot be discussed in isolation from the legal framework that governs it. The Medical Devices Regulation (MDR) and the EU AI Act set the standards for when and how AI qualifies as a medical device and impose obligations on developers, providers, and users. Thus, to understand how the EHDS impacts medical AI, one must also situate it within this broader regulatory framework.

Under Article 2(1) MDR, a medical device includes 'any instrument, apparatus, appliance, software or other article' intended by the manufacturer for medical purposes such as diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease. Recital 19 MDR clarifies that software in its own right can qualify as a medical device if it serves such medical purposes, while software used for general lifestyle or wellness is not covered. Thus, AI systems are regulated as medical devices only when they perform or support medical functions. Under the AI Act, any AI system qualifying as a medical device under the MDR or IVDR is automatically considered high-risk.[1] This dual regime means that medical AI devices must comply with both MDR obligations (safety, performance, CE-marking, clinical evaluation) and AI Act requirements (risk management, data governance, transparency, human oversight, robustness). As such, a medical AI device under EU law is any AI-based software that meets the MDR's definition of a medical device and is thereby also governed as a high-risk AI system under the AI Act.

This paper adopts a doctrinal legal analysis, focusing on the interpretation of the EHDS and its interaction in governing medical AI devices. It combines this with policy analysis of the risks and challenges of AI in healthcare, particularly bias, accountability, and data quality. This paper argues that while the EHDS offers a critical foundation for mitigating certain risks associated with

1. Joint Artificial Intelligence Board and Medical Device Coordination Group, *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)* (MDCG 2025-6 and AIB 2025-1, June 2025) , <https://health.ec.europa.eu/document/download/b78a17d7-e3cd-4943-851d-e02a2f22bbb4_en?filename=mdcg_2025-6_en.pdf&utm_source=chatgpt.com> accessed 5 September 2025

medical AI, particularly those related to data quality, privacy, cybersecurity, and accountability, it remains insufficient in addressing other systemic concerns. In particular, issues such as algorithmic bias, data shift, tool misuse, and the persistent opacity of AI systems are not comprehensively tackled within the current scope of the EHDS. Therefore, although the EHDS is a step in the right direction, reliance on additional regulatory measures, technical standards, and interdisciplinary oversight will be required to ensure that AI in healthcare develops in a manner that is not only effective but also fair, transparent, in compliance with fundamental rights.

2. Uses of AI in Healthcare

AI is transforming healthcare by making it more efficient and patient-centred. Examples include improving diagnostics or optimising hospital resources, allowing healthcare professionals to deliver better care while reducing administrative burdens. However, its successful adoption depends on building patient trust and ensuring data quality when training these systems.

One of AI's important functions is in optimising healthcare resources. Predictive models help hospitals forecast patient admissions and manage resources like beds, staff, and equipment.[2] By analysing trends, these systems ensure that resources are available when and where they're needed, reducing waste and improving patient care. In addition to resource management, AI plays a significant role in reducing costs and administrative workloads.[3] Automating routine tasks such as scheduling, billing, and electronic health record management allows doctors and nurses to spend more time with patients.[4]

Furthermore, AI's ability to improve diagnostics and enable early disease detection is one of its most promising applications.[5] In intensive care units,

2. 'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025

3. Ibid

4. Ibid

5. Ibid

AI systems can detect early warning signs of sepsis, a life-threatening condition, hours before symptoms appear, allowing for quicker intervention.[6] Similarly, AI-powered mammograms can identify early signs of breast cancer with high accuracy, sometimes outperforming human radiologists.[7] These advancements not only improve the patients' medical experience but also reduce the need for costly and invasive treatments.[8]

Despite its potential, medical AI devices face several hurdles. One major challenge is building trust in these models, as many of them operate as 'black boxes'.[9] Without clear explanations for AI-generated recommendations, healthcare professionals may be hesitant to rely on them. Ensuring data quality and privacy is another significant concern. AI relies on large, diverse datasets, but medical records are often inconsistent or incomplete. Strict privacy regulations further complicate the use of patient data, limiting AI's ability to learn from a wide range of cases. Financial and infrastructural barriers also pose challenges, as implementing AI requires significant investment, particularly in public hospitals that may lack the necessary funding. Additionally, AI raises complex legal and regulatory questions. If an AI system makes an error, it remains unclear whether the responsibility lies with the developer, the hospital, or the clinician. Establishing clear legal frameworks will be essential to addressing these liability concerns and ensuring the safe and ethical deployment of AI in healthcare.

3. Risks and Challenges of AI in Healthcare

As discussed, the use of AI in healthcare has the potential to become revolutionary, but this comes with significant risks. These include technical and clin-

6. Ibid

7. Ibid

8. Ibid

9. George Maliha and others, 'Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation' (2021) 99 The Milbank Quarterly 629, 638; Zach Harned and others, 'Machine vision, medical AI, and malpractice' [2019] Harv. J.L. & Tech. Dig, 4

ical data-related errors, biases that perpetuate health inequities, privacy and security vulnerabilities, and legal and ethical challenges in accountability and transparency.[10] Addressing these concerns is critical to ensuring AI's safe and effective use in healthcare.

Despite being trained on extensive datasets, AI models can still make errors that may lead to patient harm. Three primary sources contribute to these errors. First, inaccuracies in input data can distort AI predictions, leading to incorrect diagnoses or treatment recommendations.[11] Second, AI models can struggle with dataset shift: when real-world clinical data differs from the data used for training.[12] This can happen due to differences in population demographics, hospital protocols, or equipment, resulting in a drop in accuracy. For instance, a U.S.-based AI system trained to detect pneumonia performed well on data from two hospitals but significantly declined in accuracy when tested on a third, revealing hospital-specific biases.[13] Lastly, AI models may fail to adapt to unexpected environmental changes. In medical imaging, for example, AI could mistakenly classify harmless artifacts as medical anomalies, leading to unnecessary procedures or misdiagnoses.[14]

Another major challenge in medical AI tools adoption is its potential misuse. Clinicians, nurses, and patients may not fully understand how or when to use AI tools, leading to errors in medical assessments.[15] Many AI systems are designed by data scientists with limited clinical input, forcing healthcare professionals to adapt to complex technology that may not align with real-world

10. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 277

11. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 278

12. Ibid; Adarsh Subbaswamy and Suchi Saria, 'From development to deployment: dataset shift, causality, and shift-stable models in health AI' (2020) 21 Biostatistics 345, 345

13. Ibid (n 9)

14. Ibid

15. Ibid, 279

workflows. Involving end-users, such as clinicians, technicians, and patients, throughout AI development can lead to more intuitive and reliable systems.[16]

Bias in AI algorithms further complicates medical decision making, as it can reinforce existing disparities. AI models trained on biased datasets may unintentionally discriminate against certain groups based on race, gender, or socioeconomic status.[17] For example, it has been studied that in the United States, black patients' pain complaints are often taken less seriously than those of white patients, a bias that could be reflected and reinforced by AI models trained on historical data.[18] Similarly, gender bias in pain management has been documented, with female patients' symptoms more frequently dismissed as psychological.[19] Geographic bias also arises when AI is trained on data from specific regions, making it less effective for populations in different locations.[20] Addressing these biases requires diverse datasets, interdisciplinary development teams, and continuous monitoring to ensure AI tools remain fair and equitable.

The use of AI in healthcare also raises privacy concerns. Sensitive patient data, if misused or exposed, could lead to privacy violations and unauthorised access by third parties.[21] A key issue is informed consent, as patients often struggle to understand how their data is used. Complex consent forms and

16. Ibid

17. Ibid, 280; Anke Samulowitz and others, 'Brave Men and Emotional Women: A Theory-Guided Literature Review on Gender Bias in Health Care and Gendered Norms towards Patients with Chronic Pain' [2018] Pain Research and Management 1, 2

18. Ziad Obermeyer and others, 'Dissecting racial bias in an algorithm used to manage the health of populations' (2019)366 Science 447, 447

19. Anke Samulowitz and others, 'Brave Men and Emotional Women: A Theory-Guided Literature Review on Gender Bias in Health Care and Gendered Norms towards Patients with Chronic Pain' [2018] Pain Research and Management 1, 2

20. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 281

21. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 282

opaque AI algorithms can further limit patient autonomy.[22] Additionally, AI health platforms and big data research introduce new risks, as patients may not fully grasp the extent of data sharing across organisations. Security risks are also significant. Cyberattacks on AI systems could lead to data breaches, identity theft, or even manipulation of medical AI devices, potentially endangering patients.[23]

Lastly, lack of transparency is one of the biggest obstacles to AI adoption in healthcare. As aforementioned, many AI models function as 'black boxes', meaning their decision-making processes are unclear to both clinicians and patients.[24] Transparency involves two key aspects: traceability (documenting how AI models are developed and used) and explainability (ensuring AI decisions can be understood and justified).[25] However, many healthcare AI tools lack both, making it difficult to assess their reliability or hold them accountable when errors occur.[26] Accountability also remains a major unresolved issue. If an AI diagnosis leads to harm, it is unclear whether responsibility lies with

22. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 282

23. Lucy Hocking and others, 'Reuse of health data by the European pharmaceutical industry' [2019] RAND 1, 60; Maximilian Kiener, 'You may be hacked and other things doctors should tell you' (*The Conversation*, 3 November 2020) < https://theconversation.com/you-may-be-hacked-and-other-things-doctors-should-tell-you-148946> accessed 27 March 2025

24. George Maliha and others, 'Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation' (2021) 99 The Milbank Quarterly 629, 638; Zach Harned and others, 'Machine vision, medical AI, and malpractice' [2019] Harv. J.L. & Tech. Dig, 4

25. Guang Yang and others, 'Unbox the Black box for the Medical Explainable AI via Multimodal and Multicentre Data Fusion: A MiniReview, Two Showcases and Beyond' [2022] Information Fusion 29, 29; Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 283

26. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 285

the doctor using the tool, the developers who created it, or the hospital that deployed it.[27] Without clear legal frameworks, healthcare providers may hesitate to adopt AI, fearing legal repercussions.[28] The complexity of AI development, where multiple actors, from data scientists to healthcare providers, contribute to a system, further complicates accountability.

While AI holds immense promise for improving healthcare, its risks must be carefully managed. Clinical and technical errors, biases, security threats, and legal uncertainties all pose challenges to its safe implementation. Ensuring AI is transparent, fair, and accountable requires collaboration between policymakers, healthcare professionals, and AI developers. By addressing these concerns, AI can be integrated responsibly into healthcare, ultimately improving patient outcomes and system efficiency.

4. The European Health Data Space (EHDS) and Medical AI Devices

The European Health Data Space (EHDS) is set to revolutionise how AI systems are developed, trained, and deployed in healthcare. By creating a structured, secure, and standardised framework for health data access and sharing across the EU, the EHDS could provide the foundation for more accurate and reliable medical AI devices.

A key barrier to AI adoption in healthcare is the inconsistent quality of electronic health records. Medical data is often unstructured, incomplete, or varies across hospitals and countries. These inconsistencies make it difficult to apply AI models at scale without significant effort in data cleaning and quality control. Improving data standardisation and interoperability across healthcare sys-

27. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 285

28. Helen Smith, 'Clinical AI: opacity, accountability, responsibility and liability' (2020) 26 AI & SOCIETY 535, 536

tems is essential to maximise AI's effectiveness.[29] AI models, particularly those used in medical diagnosis, treatment recommendations, and predictive analytics, require vast datasets to ensure accuracy and fairness.[30] The EHDS facilitates this by allowing researchers and innovators to access a wide range of health data for secondary use (such as research and development) while maintaining strict data protection standards.[31] For example, a company developing an AI diagnostic tool for detecting lung cancer from radiology scans can securely access anonymised medical images from hospitals across multiple EU countries. This access allows the AI model to be trained on a diverse set of data, improving its accuracy and reducing biases that might arise from using only localised datasets.

AI in healthcare operates under strict ethical and regulatory guidelines to ensure patient safety and privacy. The EHDS builds upon existing EU data regulations such as the General Data Protection Regulation (GDPR), the Data Governance Act, and the Network and Information Systems Directive. These regulations ensure that AI tools comply with stringent data protection and cybersecurity measures.[32] By providing a clear legal and ethical framework for the secondary use of health data, the EHDS reduces legal uncertainties for AI developers, allowing them to focus on innovation while maintaining

29. Apoorva Muley and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276, 282

30. 'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025

31. 'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025; Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1, art 53(e)(ii)

32. 'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025

compliance. This structured approach also increases public trust in medical AI devices.[33]

As mentioned in the previous chapter, a major concern with the use of AI in healthcare is ensuring that algorithms perform fairly across different population groups. Bias in AI models, resulting from underrepresentation of certain demographics, can lead to inaccurate diagnoses or disparities in treatment recommendations. With the EHDS, AI developers gain access to broader and more diverse health datasets, allowing them to test and refine their algorithms to ensure equitable performance across different patient groups. However, there is still a risk that AI systems trained using EHDS data could be biased. For example, if a medical AI system is developed in one EU country and primarily trained on its own national data, while also using some EHDS data, it may not fully represent the diversity of patients across the EU. Additionally, if the data within the EHDS itself contains biases, this could amplify the problem. Since AI systems using EHDS data will operate on a much larger scale, any bias in the training data could affect more patients across the EU. This could lead to disparities in healthcare based on factors like race, gender, or socioeconomic status, potentially worsening inequalities between different EU countries.

Additionally, trust is a critical factor in the adoption of AI in healthcare. The EHDS establishes a secure environment where health data can be shared for research and innovation while ensuring that data privacy and patient rights remain a top priority. This fosters confidence among healthcare providers, patients, and regulators, encouraging greater collaboration and investment in medical AI tools. By providing a robust, transparent, and efficient system for accessing and utilising health data, the EHDS lays the groundwork for a future where AI plays a central role in improving healthcare outcomes across Europe.

4.1. The Effect of the European Health Data Space (EHDS) on AI Risks in Healthcare

Considering the risks associated with AI in healthcare, the EHDS provides partial but not comprehensive mitigation. The key risks examined include inaccu-

33. 'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025

rate training data, data shift (where AI systems fail in unfamiliar situations), misuse of AI tools, bias in training data, privacy and data protection concerns, cybersecurity threats, transparency issues, and accountability challenges. Of these eight risks, the EHDS effectively mitigates four: inaccurate training data, privacy risks, cybersecurity threats and accountability. However, four critical risks, bias, data shift, misuse of AI tools, and transparency, remain unaddressed within the scope of the EHDS regulations.

Bias in training data remains a major concern, as the EHDS does not provide direct mechanisms to counteract historical inequalities that can be found in healthcare datasets. Importantly, bias does not only arise from flawed datasets; even robust and accurate datasets can reflect underlying human and systemic biases. Additionally, geographic bias also arises when AI is trained on data from specific regions, making it less effective for populations in different locations. This could be a problem with EHDS if there is more data available from a certain country, leading to AI models that perform better for patients in that country while being less accurate elsewhere. Similarly, data shift, which occurs when AI models encounter new or evolving medical conditions that differ from their training data, remains unaddressed by EHDS regulations.

Another gap lies in the responsible use of medical AI tools. The EHDS does not establish specific guidelines to prevent misuse by healthcare practitioners, increasing the risk of misdiagnoses or inappropriate treatment recommendations. However, under current medical practice, AI systems function as decision-support tools. Responsibility ultimately rests with the clinician, who must interpret AI outputs in light of professional judgment. EU law reinforces this human oversight requirement: under Article 14 AI Act, high-risk AI systems, including medical AI, must be designed to allow effective human oversight. This ensures that they cannot function as fully autonomous clinical decision-makers; responsibility and final judgment remain with healthcare professionals. Transparency also remains a challenge, as the EHDS does not introduce explicit frameworks to ensure explainability and interpretability of AI decisions in clinical settings. Despite these limitations, the EHDS significantly enhances data privacy and cybersecurity. It ensures that individuals can opt out of sec-

ondary data use in a simple and reversible manner.[34] Strict rules prevent personal data from being downloaded, and researchers, companies, or public institutions can only access pseudonymised data when anonymised data is insufficient.[35] Re-identifying data subjects is strictly prohibited, and data processing is limited to highly secure environments, mitigating cybersecurity threats.[36] These measures are essential given the sensitivity of health data.

The EHDS also mitigates accountability risks by establishing clear rules on how health data can be used. For instance, the regulation prohibits the use of health data for decisions that could be harmful to individuals or for marketing purposes.[37] This ensures that AI tools are not misused for unethical or commercially driven objectives, reinforcing accountability in instances where AI tools aid in crucial decision-making.

Additionally, health data can only be used for secondary purposes if explicitly permitted by a designated health data access body, with strict limitations on its use, such as prohibiting decisions that could harm individuals or be exploited for marketing.

While the EHDS strengthens data privacy and security, addressing its remaining gaps will be essential for the safe and effective integration of AI into the European healthcare system. Ensuring AI models are trained on diverse datasets and relying on complementary regulations will be crucial to maintaining patient trust and safety. Though this paper focuses solely on the EHDS, other regulations such as the AI Act, the Medical Devices Regulation, and the GDPR may help mitigate the risks it does not fully address.

34. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1, art 71

35. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1, art 66 (3)

36. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1, art 73

37. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1, art 54

AI risk	Mitigated by EHDS	Not Mitigated by EHDS
Inaccurate training data	The EHDS provides a large, high-quality dataset, reducing the risk of inaccurate or insufficient data	
Data shift	–	Not addressed
Misuse of AI Tools	–	Not addressed
Bias in training data	–	Not addressed
Privacy and Data Protection	Users can opt out of secondary data use. Only pseudonymised data is accessible when anonymised data is insufficient. Re-identification is strictly prohibited	
Cybersecurity/ Cyberattacks	Data processing occurs in secure, high-privacy environments. Access requires a permit from a health data access body	
Transparency	–	Not addressed
Accountability	Data use is strictly regulated. AI tools cannot make harmful or marketing-driven decisions	

5. Conclusion

Artificial intelligence is expected to play a transformative role in healthcare, offering efficiencies across clinical, operational, and administrative domains. From improving diagnostic accuracy and enabling earlier disease detection to optimising hospital resource allocation and reducing administrative burdens, AI has the potential to enhance patients' medical experience. However, these opportunities are accompanied by significant risks, including clinical errors, algorithmic bias, data privacy concerns, and challenges around transparency and accountability. The safe and effective integration of AI into healthcare systems depends on the extent to which these risks are understood, anticipated, and managed.

The European Health Data Space (EHDS) represents a major policy initiative aimed at creating a secure, standardised, and ethically governed framework for health data sharing and secondary use across the European Union. By improving the quality and accessibility of health data, the EHDS addresses sev-

eral barriers to trustworthy use of AI for medical devices. Specifically, it mitigates risks related to inaccurate training data, privacy violations, cybersecurity threats, and the misuse of health data for unethical or commercially driven purposes. It also introduces mechanisms for regulatory oversight and ensures that patients retain a degree of control over their personal data through opt-out options.

Nonetheless, the EHDS falls short of comprehensively addressing all critical risks associated with AI in healthcare. Notably, it does not directly resolve concerns related to algorithmic bias, data shift, the misuse of AI tools in clinical workflows, or the lack of transparency and explainability in medical AI tools. These limitations point to the need to rely on complementary frameworks, such as the EU AI Act and the Medical Devices Regulation, that can provide more targeted regulation in these areas. In addition, ongoing collaboration between data scientists, healthcare professionals, policymakers, and patients is essential to ensure that AI systems are designed with real-world clinical needs, fairness, and ethical considerations in mind.

In conclusion, while the EHDS lays an important foundation for safer and more equitable AI deployment in healthcare, it is not a universal remedy. A comprehensive regulatory and ethical ecosystem is required to fully realise the benefits of AI while safeguarding against its potential harms. Future efforts must focus on enhancing data diversity, ensuring responsible use, and promoting algorithmic transparency to support the development of AI systems that are not only technically robust but also socially and ethically aligned with the values of modern healthcare.

Bibliography

Joint Artificial Intelligence Board and Medical Device Coordination Group, Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA) (MDCG 2025-6 and AIB 2025-1, June 2025) , <https://health.ec.europa.eu/document/download/b78a17d7-e3cd-4943-851d-e02a2f22bbb4_en?filename=mdcg_2025-6_en.pdf&utm_source=chatgpt.com> accessed 5 September 2025

'Artificial Intelligence in healthcare' <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 27 March 2025

Harned Z and others, 'Machine vision, medical AI, and malpractice' [2019] Harv. J.L. & Tech. Dig

Hocking L and others, 'Reuse of health data by the European pharmaceutical industry' [2019] RAND 1, 60

Kiener M, 'You may be hacked and other things doctors should tell you' (*The Conversation*, 3 November 2020) <https://theconversation.com/you-may-be-hacked-and-other-things-doctors-should-tell-you-148946> accessed 27 March 2025

Maliha G and others, 'Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation' (2021) 99 The Milbank Quarterly 629, 638

Muley A and others, 'Risk of AI in Healthcare: A Comprehensive Literature Review and Study Framework' (2023) 21 Asian Journal of Medicine and Health 276

Obermeyer Z and others, 'Dissecting racial bias in an algorithm used to manage the health of populations' (2019)366 Science 447

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L327/1

Samulowitz A and others, 'Brave Men and Emotional Women: A Theory-Guided Literature Review on Gender Bias in Health Care and Gendered Norms towards Patients with Chronic Pain' [2018] Pain Research and Management 1

Smith H, 'Clinical AI: opacity, accountability, responsibility and liability' (2020) 26 AI & SOCIETY 535

Subbaswamy A and Saria S, 'From development to deployment: dataset shift, causality, and shift-stable models in health AI' (2020) 21 Biostatistics 345

Yang G and others, 'Unbox the Black box for the Medical Explainable AI via Multimodal and Multicentre Data Fusion: A Mini Review, Two Showcases and Beyond' [2022] Information Fusion 29

About the author

Mariam Ibraham

Mariam Ibrahim completed the LL.M. in Technology Law and Innovation at the University of Groningen. She is currently undertaking a traineeship at the European Union Intellectual Property Office, contributing to the Digital Innovation Department's work on data protection and cybersecurity.

CHAPTER 13: PATENTS, DATA PRIVACY, AND INNOVATION WITHIN THE EUROPEAN HEALTH DATA SPACE

Darina Pitkevica

1. Introduction

In the wake of a global pandemic, where access to data, innovation, and equitable healthcare determined the pace of recovery and survival, the European Union (EU) took a decisive step: to create a common health data infrastructure capable of reshaping the region's biomedical future. The European Health Data Space (EHDS), introduced as part of the EU's broader Digital Europe strategy, is not just a regulation – it is a vision for a different future.[1] One that aspires to unify the fragmented landscape of health data governance, empower individuals with control over their personal health information, and stimulate a new wave of cross-border innovation in healthcare delivery and medical research.[2] But as with all visions that seek to centralise power, data, and ambition, the EHDS raises fundamental legal and ethical questions, particularly in the context of intersection with patents, data privacy, and the tension between private rights and public interest.

1. European Commission, 'A European Strategy for Data' (2020) COM/2020/66 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066> accessed 22 March 2025; Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2026 on the European Health Data Space and amending Directive 2012//24/EU and Regulation (EU) 2024/2847 (EHDS Regulation) [2025] OJ L 2025/327.

2. European Commission, 'What is the EHDS Regulation About' (2025) <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en#:~:text=The European Health Data Space,health data across the EU.> accessed 20 March 2025.

This paper explores these dimensions through the specific and timely lens of vaccine development. The COVID-19 pandemic showcased the stakes involved: vast pools of sensitive personal health data became essential fuel for vaccine trials and epidemiological research, while intellectual property (IP) protections sparked global controversy over access, affordability, and fairness. The EHDS enters this terrain with bold promises but uncertain mechanisms.

With a targeted focus on vaccines as a case study, this paper navigates the intersections between the European legal framework for patents and data protection, the evolving governance of the EHDS, and the broader implications for medical innovation and global health equity. Structured as a legal essay rather than a purely doctrinal analysis, it aims to be not only informative but also interrogative, and cover the underlying assumptions that shape the modern health governance in the EU. Ultimately, this should be viewed as a story of paradoxes: of data that is both personal and collective, of vaccines that are both scientific triumphs and political instruments, and of a digital future that promises empowerment while threatening intrusion.

2. The European Health Data Space: A New Digital Health Ecosystem

I. EHDS Origins and Objectives

The EHDS Regulation emerged from a long-standing ambition to harness the digital single market in the service of health.[3] Yet, its timing was no coincidence. The devastation wrought by the COVID-19 pandemic exposed the fragmentation of health data governance across the EU and depicted all of the missed opportunities for collective, data-driven responses.[4] Vaccine distribution, epidemiological tracking, and cross-border research efforts were all hampered by national silos, divergent privacy regimes and incompatible digital

3. Ibid.

4. Scott L Greer, Anniek de Ruijter, Eleanor Brooks, *The Palgrave Handbook of EU Crises* 'The COVID-19 Pandemic: Failing Forward in Public Health' (Palgrave Macmillan, 2020) 747 <https://doi.org/10.1007/978-3-030-51791-5_44> accessed 20 March 2025.

infrastructures.[5] In this context, the EHDS is not only a regulatory intervention but also a move to supranational health sovereignty in the digital age.

The core objectives of the EHDS are twofold.[6] First, to empower individuals with access to and control over their own electronic health data across the EU – a promise grounded in the ethos of digital citizenship and the free movement of persons.[7] Second, and the more ambitious one, to enable the secondary use of health data for such purposes as research, innovation, policy-making, and regulation.[8] It is this second pillar that is more legally and ethically fraught, and where the implications for innovation, particularly in areas like vaccine development, become most profound.

II. Legal and Technical Framework

At its base, the EHDS is envisioned as a horizontal data space operating in synergy with the Data Governance Act (DGA), the Data Act, and the General Data Protections Regulation (GDPR).[9] However, unlike these instruments, the EHDS is sector-specific.[10]

---

5. Ibid 754-755.

6. Luca Marelli and others, 'The European Health Data Space: Too big to succeed?' (2023) 135 Health Policy 2-3 <https://doi.org/10.1016/j.healthpol.2023.104861> accessed 20 March 2025.

7. Ibid.

8. Ibid.

9. European Commission (n 2), 'How will the EHDS ensure data protection and security'; Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L2023/2854.

10. Ibid.

Under the EHDS Regulation, Member States (MS) are required to ensure that health data is made available for both primary and secondary use.[11] The latter involves a central role for new entities in the form of Health Data Access Bodies (HDAB), which would oversee data permits, ensure GDPR compliance, and supervise secure data processing environments.[12]

While the legal scaffolding borrows heavily from the GDPR's risk-based approach, it also creates new complexities. The EHDS carves out a distinct legal basis for data processing under Article 6(1)(e) and Article 9(2)(i) GDPR, grounding secondary use in tasks carried out in the public interest or for scientific research.[13] However, critics have pointed out that these justifications remain vague and open-ended, potentially clashing with individual rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU.[14]

III. Data Governance Model

Apart from the new rights and obligations, one of the most innovative features of the EHDS is its multi-level governance model. At the EU level, the European Commission, together with the newly created EHDS Board is to provide strategic oversight.[15] And at the national level, the aforementioned HDABs are to

11. EIT Health ThinkTank, *Implementing the European Health Data Space Across Europe* (2024) 9 <https://eithealth.eu/wp-content/uploads/2024/04/EIT_Health_ThinkTank_Implementing_the_EHDS_across_Europe_23.04.24.pd> accessed 22 March 2025.

12. Ibid 8, 20, 110.

13. GDPR (n 9), arts 6(1)(e) and 9(2)(i).

14. EDRI, 'EU's Proposed Health Data Regulation Ignores Patients' Privacy Rights' (2023) <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/> accessed 22 March 2025; Charter of Fundamental Rights of the European Union [2012] OJ C326/391 arts 7-8.

15. J Scott Marcus and others, *The European Health Data Space* (IPOL Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament Policy Department Studies, 2022) 41 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4300393> accessed 22 March 2025.

serve as gatekeepers and monitors.[16] Crucially, the EHDS envisions a public-private interface, allowing research organisations, pharmaceutical companies, and health technology developers to request access to anonymised or pseudonymised data for specified purposes.[17]

At this point, the line between public health objectives and commercial interests becomes increasingly blurred. For instance, the EHDS explicitly allows data use by private entities for developing medical products and AI applications – a move welcomed by the life sciences industry but met with scepticisms by civil society advocates concerned about data commodification.[18] Despite these tensions, the EHDS represents a paradigm shift in how the EU approaches digital health innovation. Traditionally, medical research, particularly in the field of vaccinology, has relied on long, expensive clinical trials and siloed data from national health registries.[19] The EHDS aims to streamline this process, offering researchers access to large, diverse, and cross-border data sets that can accelerate vaccine development, efficacy monitoring, and adverse effect tracking. Moreover, the EHDS is being framed as a key pillar of European strategic autonomy in health.[20] As the EU seeks to reduce dependence on non-European pharmaceutical and biotech supply chains, it recognises that data is the new infrastructure.[21] In this sense, the EHDS is not merely a health initiative but also

16. Ibid.

17. Ibid 20-21.

18. EHDS Regulation (n 1), rec 61 and art 53(e).

19. World Health Organization, 'How are Vaccines Developed?' (2020) <https://www.who.int/news-room/feature-stories/detail/how-are-vaccines-developed> accessed 22 March 2025.

20. European Commission (n 1), 'A European Strategy for Data'.

21. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Pharmaceutical Strategy for Europe (2020) COM/2020/761 'Secure the supply of medicines across the EU and avoid shortages' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0761> accessed 22 March 2025.

a part of a geopolitical strategy, one that tries to position Europe at the lead of ethical, privacy-conscious innovation.

3. IP in the Light of EHDS

I. The Role of Patents in Medical Innovation

IP rights play an important role in the medical research and development sector. Specifically patents, by their design, serve as the cornerstone of the pharmaceutical innovation system, granting inventors a time-limited monopoly in exchange for public disclosure of an invention.[22] The underlying intention of patents is to incentivise high-risk, high-cost research and development.[23] Vaccines, despite their global public health relevance, are of no exception.

In the context of EU, patents are primarily governed by the European Patent Convention (EPC) and enforced at the national level.[24] Additionally, the recently implemented Unified Patent Court (UPC) also promises to streamline this system for participating EU MSs.[25] And finally, the Supplementary Protection Certificate (SPC) regime further extends patent protection specifically for pharmaceuticals, recognising the regulatory delay often involved in bringing such products to market.[26]

---

22. Caroline A Grenshaw, 'Patents and Patients: Who is the Tragedy of the Anticommons Impacting and Who is Bearing the Cost of High-Priced Biotechnological Research?' (2008) 9(2) Minnesota Journal of Law, Science & Technology 916 <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1281&context=mjlst> accessed 25 March 2025.

23. Ibid.

24. Convention on the Grant of European Patents (European Patent Convention) (adopted 5 October 1973, entered into force 7 October 1977) 1065 UNTS 199.

25. Agreement on a Unified Patent Court (adopted 19 February 2013, entered into force 1 June 2023) [2023] OJ C175/1.

26. Council Regulation (EC) No 469/2009 of 6 May 2009 concerning the supplementary protection certificate for medicinal products [2009] OJ L152/1.

Despite this architecture, the patent system remains a subject of intense ethical and legal scrutiny, especially when life-saving technologies are at stake. It is arguable that patent monopolies contribute to market exclusion, price inflation, and delayed access in lower-income regions.[27] The EHDS, with its ethos of data solidarity and innovation sharing, now offers a novel challenge to this multi-layered puzzle.

II. Vaccine Patent Framework and Corresponding Issues

The controversy surrounding vaccine patents reached a crescendo during the COVID-19 pandemic, as the EU, along with the US and other wealthier nations, rejected calls at the World Trade Organisation to waive IP protections under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[28] The issue of opposing interests became more apparent through the fact that, within the EU, vaccine patents often exist in tandem with public funding.[29] For example, BioNTech Pfizer and Moderna received substantial financial support

27. John Sulston, *Cut the Cost* (Oxfam GB, 2001) 'The cost of illness: why prices matter', 'Patents and prices: the threat to public health' <https://www.iatp.org/sites/default/files/Cut_the_Cost_-_Patent_Injustice_How_World_Trad.htm> accessed 25 March 2025.

28. EESC, 'TRIPS Waiver' (2021) https://www.eesc.europa.eu/en/news-media/news/trips-waiver-end-deadlock-covid-vaccine-patents-workers-group-statement> accessed 25 March 2025. See also, Elaine Ruth Fletcher, 'World Trade Organisation Enters COVID Pandemic Fray With Dispute Brewing Over Patent Rights' (2020) *Health Policy Watch: Independent Global Health Reporting* <https://healthpolicy-watch.news/world-trade-organization-enters-covid-pandemic-fray-with-dispute-brewing-over-patent-rights/> accessed 25 March 2025; Medecins Sans Frontieres Access Campaign, 'No Patents, No Monopolies in a Pandemic' (2022) <https://msfaccess.org/no-patents-no-monopolies-pandemic> accessed 25 March 2025.

29. Massimo Florio and others, *Mapping of Long-Term Public and Private Investments in the Development of COVID-19 Vaccines* (European Parliament Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, 2023) <https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740072/IPOL_STU(2023)740072_EN.pdf> accessed 25 March 2025.

from European and national institutions during early stages.[30] However, the resulting patents remained in private hands, and contractual terms governing pricing, distributions, and transparency were often shielded by commercial confidentiality clauses.[31] This duality between public risk and private reward has reignited calls to rethink the role of IP rights in biomedical innovation. Furthermore, the Data Act and the EHDS Regulation together hint at a new legal frontier: one in which data, rather than molecules, become the primary asset in pharmaceutical research and development.

III. Conflicts Between Open Science and Patent Protection

The EHDS proposes to make health data more accessible for secondary use, including to pharmaceutical companies conducting research.[32] However, access does not necessarily mean openness. Under current EU legal framework, data that leads to a patentable invention (such as a novel vaccine) does not automatically become open science. Indeed, the very logic of the patent system is to enclose knowledge within exclusive boundaries. This creates a potential moral and legal dissonance where companies may gain privileged access to publicly governed health data under the EHDS and subsequently patent outputs derived from that data, in such a way restricting downstream access. The fear, voiced by scholars and NGOs, is that the EHDS could inadvertently enable a form of 'data extraction' – a process where private actors mine public health datasets to generate commercialised outputs without proportional reinvestment into the public health system.[33] To address this imbalance, new legal tools have been proposed, for instance, data-sharing clauses in

30. Ibid 21.

31. WIPO, 'Exploring COVID-19 Vaccine Patents' <https://www.wipo.int/en/web/patent-analytics/exploring-covid-19-vaccine-patents> accessed 25 March 2025.

32. Cheryl Barton, 'Finalising the European health Data Space' (2024) 48(1) Pharmaceutical Technology <https://www.pharmtech.com/view/finalizing-the-european-health-data-space> accessed 25 March 2025.

33. Luca Marelli and others (n 6), 2-3.

grant agreements, equitable access conditions for EHDS data users, or patent pool models that could function under the EHDS umbrella.[34]

The stakes are particularly high for vaccines, which often require global deployment under urgent timelines. The EHDS offers a potential platform for real-time monitoring of vaccine effectiveness, variant tracking, and post-market safety surveillance. These are all valuable functions but they also reinforce the information asymmetry between data controllers, such as the EU institutions and national health systems, and data users, such as researchers and pharma firms.

Patent law, by granting exclusive commercial rights, can further distort this asymmetry. The danger is a scenario where vaccine developers use EHDS-facilitated data access to optimise proprietary products, whilst retaining exclusive rights over distribution, pricing, and production, potentially sidelining public health objectives. This risk was made visible during the pandemic, when the EU faced vaccine supply shortages and opaque contractual negotiations with pharmaceutical companies.[35]

However, there are possible ways to counterbalance such dynamics. The EHDS could further incorporate conditional access regimes, requiring that patentable innovations derived from EHDS data include non-exclusive licensing provisions, or that patent holders submit to transparency obligations regarding pricing and distribution models. Although, politically sensitive, such measures would align the EHDS with a more equity-focused innovation model and also further support the EU Data Strategy.

---

34. MedTech Europe, *MedTech Europe's position on the proposed European Health Data Space Regulation* (2023) 12-13 <https://www.medtecheurope.org/wp-content/uploads/2023/02/230222-ehds-position-paper-final.pdf> accessed 25 March 2025.

35. European Parliament, *Motion for a Resolution on EU Transparency in the Development, Purchase and Distribution of COVID-19 Vaccines* (2021) B9-0519/2012 <https://www.europarl.europa.eu/doceo/document/B-9-2021-0519_EN.html> accessed 25 March 2025.

4. Data Privacy in the EHDS: Legal Foundations and Ethical Concerns

I. GDPR and the EHDS

At the heart of the EHDS lies a paradox: the more valuable health data becomes for innovation, the more its protection as a fundamental right becomes both politically sensitive and legally complex. To battle any data processing problems, the EHDS cannot operate in a legal vacuum, it must coexist with the GDPR. The GDPR's protections are rooted in individual autonomy, consent, and the principle of data minimisation.[36] In contrast, the EHDS seeks to maximise the secondary use of health data for scientific research, public health monitoring, and policy evaluation.[37] While the GDPR allows such secondary use under specific derogations, the boundaries of these provisions remain contestable and context-dependent.

Critically, the EHDS introduces a new category of governance entities (HDABs) which are tasked with authorising data access requests, ensuring GDPR compliance, and maintaining secure processing environments.[38] However, the legal basis for their authority, particularly over pseudonymised data, is still under debate. In the absence of clear case law, questions persist about whether the EHDS creates a de facto loophole in the GDPR's protections by shifting decisions about sensitive data access away from individuals and towards institutional gatekeepers.

II. Corresponding Risks of Secondary Use of Health Data and Cross-Border Sharing

Nowhere is the conflict between individual rights and collective goals more acute than in the issue of consent. The GDPR makes consent the default legal

36. GDPR (n 9), arts 5-6.

37. EHDS Regulation (n 1), arts 33-35.

38. Ibid 37-38.

basis for processing personal data, particularly when it is sensitive, such as health data.[39] However, in the context of the EHDS, obtaining specific, informed consent for each use of data in research or innovation is impractical, especially, when dealing with large-scale datasets aggregated across borders and institutions.

The EHDS therefore relies heavily on the pseudonymisation and anonymisation of data to enable secondary use without explicit consent.[40] Yet, these safeguards are not completely foolproof. As recent studies in reidentification risk have shown, even anonymised health data can be vulnerable to reverse engineering, particularly when combined with other datasets.[41] For example, genomic data used in vaccine research, such as for mRNA vaccine personalisation or epidemiological modelling, poses inherent risks of traceability due to its uniquely identifiable nature.[42] Moreover, the EHDS regulation does not standardise the thresholds for anonymisation or the technical methods for risk assessment, leaving much discretion to MSs and HDABs.

Finally, the ambition of the EHDS is to facilitate borderless data flows, however, cross-border sharing of sensitive data introduces its own privacy risks, especially when data is transferred to third countries or private actors operating across jurisdictions. Vaccine research further exemplifies these challenges. Multinational consortia, which often involves both public institutions and pharmaceutical companies, requires access to health data from across the EU and sometimes beyond. While the GDPR contains mechanisms for international

39. GDPR (n 9), art 6(1)(a) and 9(2)(a).

40. EHDS Regulation (n 1), recitals 31-32 and art 44. See also, European Data Protection Board, *Guidelines 01/2025 on Pseudonymisation* (2025) 23–24 <https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf> accessed 26 March 2025.

41. Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques 0829/14/EN WP216* (2014) 8-10 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 25 March 2025.

42. Melissa Gymrek and others, 'Identifying Personal Genomes by Surname Inference' (2013) 339(6117) Science 321-324 <https://www.science.org/doi/10.1126/science.1229566> accessed 26 March 2025.

data transfers (e.g., adequacy decisions, standard contractual clauses), the legal uncertainty surrounding third country access has only intensified following the Schrems II judgement, which invalidated the EU – US Privacy Shield.[43] The EHDS gestures toward these concerns, mandating that data processing must occur within secure processing environments and that international transfers must comply with the GDPR rules. However, given the geopolitical importance of vaccine research and the dominant role of non-European tech and pharma companies, the EHDS may struggle to enforce meaningful safeguards once data crosses the EU borders, especially if another pandemic ever worsens the situation.

III. Public-Private Collaboration and Data Access in Vaccine Research

Within the EU, institutions such as the European Medicines Agency (EMA) and the European Centre for Disease Prevention and Control (ECDC) played central roles in coordinating surveillance data and regulatory fast-tracking during COVID-19.[44] At the same time, companies like BioNTech, Moderna, and AstraZeneca leveraged a complex ecosystem of clinical, epidemiological, and genomic data to design and adapt their vaccines.[45] Much of this data was

43. C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Schrems* [2020] ECLI:EU:C:2020:559.

44. European Medicines Agency, 'COVID-19 Guidance: Evaluation and Marketing Authorisation' <https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/coronavirus-disease-covid-19/covid-19-public-health-emergency-international-concern-2020-23/guidance-medicine-developers-other-stakeholders-covid-19/covid-19-guidance-evaluation-marketing-authorisation> accessed 25 March 2025.

45. WHO, 'Statement for Healthcare Professionals: How COVID-19 Vaccines are Regulated for Safety and Effectiveness (Revised March 2022)' (2022) <https://www.who.int/news/item/17-05-2022-statement-for-healthcare-professionals-how-covid-19-vaccines-are-regulated-for-safety-and-effectiveness> accessed 25 March 2025.

derived from public health systems, often collected without specific consent for vaccine research and development.[46]

The EHDS is designed, at least in part, to normalise and regulate this kind of accelerated data-enabled research, but in doing so, it inherits the controversies of the pandemic era.[47] If vaccine development is to remain fast, collaborative, and responsive, the EHDS must institutionalise data-sharing mechanisms that are robust and trustworthy. However, it must also guard against the structural imbalances revealed by the pandemic, namely, that public systems bore the risks and collected the data, while private entities capture the IP and profits.

One of the most polarising debates during COVID-19 crisis centred on vaccine equity and the proposal to waive IP protection under the TRIPS Agreement to allow broader manufacturing of COVID-19 vaccines.[48] The EU eventually supported a watered-down compromise at the WVO, which many critics deemed inadequate.[49] In this context, a twofold lesson can be brought for the EHDS. First, if public data contributes to private vaccine innovation, there should be reciprocal obligations, whether in the form of licensing conditions, price controls, or open-access publication. Second, any innovation ecosystem that relies on centralised data infrastructures, like the EHDS, should confirm the distributional consequences of exclusivity regimes. Patents, in this case, become not just legal instruments but vectors of inequality, especially when combined with proprietary data access and trade secrecy. An EHDS that ignores these dynamics will risk entrenching a model in which the EU citizens' health data fuels innovations that are neither affordable nor globally accessible.

---

46. Marcel Verweij and others, 'Public Health Ethics in a Pandemic' (2020) 13(2) Public Health Ethics 125-126 <https://edepot.wur.nl/541022> accessed 26 March 2025.

47. J Scott Marcus (n 15), 13.

48. EESC Workers' Group (n 28).

49. WTO Ministerial Decision on the TRIPS Agreement WT/MIN(22)/30 (22 June 2022) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/30.pdf> accessed 25 March 2025. See also, Doctors Without Borders, 'Lack of Real IP Waiver on COVID-19 tools is a Disappointing Failure for People' (2022) <https://www.doctorswithoutborders.ca/lack-of-a-real-ip-waiver-on-covid-19-tools-is-a-disappointing-failure-for-people/> accessed 24 March 2025.

To be clear, this is not a call to abandon patents or commercial incentives. Innovation, particularly in vaccine development, depends on a delicate balance between exclusivity and openness. The EHDS has the potential to recalibrate this balance by changing the inputs to innovation. It lowers the barriers to accessing rich, qualitative, diverse health data that can inform early-stage research, identify target populations, and reduce duplication in clinical trials. However, this potential comes with new responsibilities. If companies gain a data advantage through EHDS access, they should not resist when facing calls for corresponding obligations, such as pre-registration of trials, transparency in algorithmic models, or even data dividend schemes. This approach and logic would reflect a movement toward 'data justice' where those who contribute data, often unknowingly, are not merely protected but also empowered and rewarded.[50]

5. The Future of Innovation Regulation

Lastly, one of the central criticisms facing the EHDS is the risk of it becoming another layer of bureaucratic inertia in an already over-regulated European data environment. While each regulation serves a valid purpose, their interaction remains imperfectly harmonised, especially for researchers and developers seeking to access data across borders. Similarly to other regulatory acts, the EHDS is facing criticism concerning the slowing down of the innovation sector.[51] There is uncertainty over how HDABs will function, what standards will govern anonymisation, and how swiftly data requests will be processed.[52] This

50. Matthias Braun, Patrik Hummel, 'Data Justice and Solidarity' (2022) 3 Patterns 3-5 <https://doi.org/10.1016/j.patter.2021.100427> accessed 26 March 2025. See also, Bridget Pratt and Susan Bull, 'Equitable Data Sharing in Epidemics and Pandemics' (2021) 22 BMC Medical Ethics 9 <https://link.springer.com/article/10.1186/s12910-021-00701-8> accessed 26 March 2025.

51. DIGITALEUROPE, *Position Paper on the European Health Data Space Proposal* (2023) 16-17 <https://cdn.digitaleurope.org/uploads/2023/01/DIGITALEUROPEs-Position-Paper-on-the-European-Health-Data-Space-proposal-1.pdf> accessed 26 March 2025.

52. J Scott Marcus (n 15), 41-42.

showcases the overall need for greater legal clarity and procedural efficiency in order to avoid the very fragmentation that EHDS seeks to resolve.

However, this critique should not lead to deregulation. Rather, the challenge lays in facilitation of building a governance system that is not only protective of rights but also adaptive, responsive, and still innovation-friendly. One possible solution is the implementation of regulatory sandboxes, in such a way also supporting the Commission's proposed innovation agenda.[53] In practice, these would work as experimental environments where new data use models can be tested under regulatory supervision without the full weight of compliance obligation.[54] Such approach has recently been put forward also within the Artificial Intelligence Act.[55]

The EHDS now attempts to institutionalise the lessons of emergency into a sustainable, long-term model for health data governance. But sustainability requires legitimacy, and legitimacy cannot be built without equity. The principle of data solidarity, which appears in EU digital strategy documents, conferences, and other conversations, must be given operational form.[56] As mentioned above, this could mean tiered access models that prioritise public institutions

53. EHDS Regulation (n 1), art 40; European Commission, A New European Innovation Agenda COM (2022) 332 final, section 2.2.2 'Flagship on enabling deep tech innovation through experimentation spaces and public <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0332> accessed 26 March 2025.

54. Ibid.

55. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L 2024/1689, art 57.

56. Healthy Europe, 'Using Data for the Greater Good' (2024) <https://www.healthyeurope.info/using-data-for-the-greater-good/> accessed 26 March 2025. See also, Barbara Prainsack and others, *White Paper: Data Solidarity* (Governing Health Futures: The Lancet & Financial Times Commission, 2022) 4-6 <https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf> accessed 25 March 2025.

and non-profits, community consent mechanisms that supplement individual data rights, or solidarity-based licensing models, where IP generated from EHDS data is subjected to equitable access terms.

In the long run, the EHDS offers an opportunity to craft a new legal and ethical blueprint for health innovation in the digital age. It can be a model not only for the EU but also for other regions. However, to fulfil this role, the EHDS regime will have to clarify its relationship to existing EU laws, like the aforementioned GDPR, embed public interest conditions into data access protocols, create enforcement mechanisms that ensure compliance with privacy obligations and equity-based innovation principles, and invest in infrastructure and digital literacy, ensuring that all populations are capable to meaningfully participate and benefit from the EHDS. Finally, the EHDS must resist becoming a technocratic system focusing solely on infrastructure and interoperability.[57] The true test, in the context of the fuller picture, will be whether it can rebalance the power asymmetries of the already existing innovation ecosystem, making data not only more available, but also more justly governed.

6. Conclusion

The EHDS stands as a regulatory initiative seeking to reconcile individual privacy with collective innovation and the economic interest with public good. Its emergence is a pivotal moment in the EU health governance, one where the management of data, knowledge, and power becomes as vital as the regulation of medicine itself. This paper has traced the potential of the EHDS through specific lens of vaccine development and the coexisting IP protection. The EHDS now has the opportunity to institutionalise the best lessons of the pandemic by not ignoring the worst. Ultimately, the EHDS cannot succeed by technology or legislation alone. Its legitimacy depends on how it distributes access, how it shares benefits, and how it respects the autonomy of the individuals whose data it seeks to mobilise. It must become the engine not only for efficient innovation but also for ethical redistribution, ensuring that the publicly governed health data is not locked behind paywalls or patent forests, thus contributing to a more just, data-driven innovation landscape.

57. Luca Marelli and others (n 6).

Bibliography

Primary Sources

Agreement on a Unified Patent Court (adopted 19 February 2013, entered into force 1 June 2023) [2013] OJ C175/1

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

Convention on the Grant of European Patents (European Patent Convention) (adopted 5 October 1973, entered into force 7 October 1977) 1065 UNTS 199

Council Regulation (EC) No 469/2009 of 6 May 2009 concerning the supplementary protection certificate for medicinal products [2009] OJ L152/1

Court of Justice of the European Union, 'Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)' [2020] C-311/18, ECLI:EU:C:2020:559

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2022/868 (Data Governance Act) [2022] OJ L152

Regulation (EU) 2023/2854 (Data Act) [2023] OJ L2023/2854

Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L1689

Regulation (EU) 2025/327 on the European Health Data Space [2025] OJ L327

WTO Ministerial Decision on the TRIPS Agreement WT/MIN(22)/30 (17 June 2022)

Secondary Sources

Commission Documents

European Commission, 'A European Strategy for Data' COM(2020) 66 final

European Commission, 'Pharmaceutical Strategy for Europe' COM(2020) 761 final

European Commission, 'A New European Innovation Agenda' COM(2022) 332 final

Journal Articles and Academic Sources

Braun M and Hummel P, 'Data Justice and Solidarity' (2022) Patterns 3

Grenshaw CA, 'Patents and Patients: Who is the Tragedy of the Anticommons Impacting and Who is Bearing the Cost of High-Priced Biotechnological Research?' (2008) 9(2) Minnesota Journal of Law, Science & Technology

Greer SL, de Ruijter A and Brooks E, 'The COVID-19 Pandemic: Failing Forward in Public Health' in The Palgrave Handbook of EU Crises (Palgrave Macmillan 2020)

Gymrek M and others, 'Identifying Personal Genomes by Surname Inference' (2013) 339 Science 321

Marelli L, Neresini F and Vayena E, 'The European Health Data Space: Too big to succeed?' (2023) 135 Health Policy 104861

Marcus JS and others, 'The European Health Data Space' (2022) IPOL Policy Department Study

Pratt B and Bull S, 'Equitable Data Sharing in Epidemics and Pandemics' (2021) BMC Medical Ethics 22

Taylor L, 'What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally' (2017) 4 Big Data & Society

Verweij M and others, 'Public Health Ethics in a Pandemic' (2020) 13(2) Public Health Ethics 125

Other Web Sources

Barton C, 'Finalising the European Health Data Space' (2024) 48(1) Pharmaceutical Technology

DigitalEurope, 'DIGITALEUROPE's Position Paper on the European Health Data Space Proposal' (2023)

EDRi, 'EU's Proposed Health Data Regulation Ignores Patients' Privacy Rights' (2023)

European Data Protection Board, 'Guidelines 01/2025 on Pseudonymisation' (January 2025)

European Medicines Agency, 'EMA initiatives for acceleration of development support and evaluation procedures for COVID-19 treatments and vaccines' (2022)

European Parliamentary Research Service, 'The European Health Data Space Proposal: A Legal and Policy Analysis' (2023) PE 729.489

European Parliament, 'COVID-19 vaccines: how the EU ensured safe and effective vaccines' (2022)

Fletcher ER, 'World Trade Organisation Enters COVID Pandemic Fray With Dispute Brewing Over Patent Rights' (2020) Health Policy Watch

Florio M, Gamba S and Pancotti C, 'Mapping of long-term public and private investments in the development of COVID-19 vaccines' (2023) European Parliament Policy Department Study

Initiative for Medicines, Access, and Knowledge (I-MAK), 'About Us' (2025)

Malinina J, 'EU's Lack of Transparency Around COVID-19 Vaccine Negotiations is Damaging Public Trust' (2021) Transparency International

MedTech Europe, ‘MedTech Europe’s position on the proposed European Health Data Space Regulation’ (2023)

Médecins Sans Frontières Access Campaign, ‘No Patents, No Monopolies in a Pandemic’ (2022)

Oxfam GB, ‘Cut the Cost: Patent Injustice’ (2001)

Transparency International, ‘EU’s Lack of Transparency Around COVID-19 Vaccine Negotiations’ (2021)

WIPO, ‘Exploring COVID-19 Vaccine Patents’ (2022)

About the author

Darina Pitkevica

Darina Pitkevica graduated with distinction (cum laude) from the LLM in Technology Law and Innovation at the University of Groningen in the 2025-2026 academic year. She subsequently commenced an internship as a legal researcher at the European Centre for Certification and Privacy (ECCP), focusing on data protection, regulatory assessment, and certification criteria development, and has since transitioned into a full-time role.

CHAPTER 14: AI, COMPETITION, AND GEOPOLITICS: EUROPE'S NEED FOR DIGITAL INDEPENDENCE

Luke Crofton Arbuthnot

1. Introduction

The current market for the development of Artificial Intelligence (AI) technology exists in a wider digital ecosystem of highly concentrated and entrenched incumbents based primarily out of the United States of America (US).[1] These firms core business model is the collection, synthesis, and processing of personal data for behavioural analysis and prediction, with the aim of '*nudging, coaxing and tuning behaviour towards profitable outcomes*'.[2] By leveraging network effects and extensive analysis of personal user data obtained from their 'data ecosystems',[3] these incumbents have solidified their dominance. They arguably now '*constitute a sweeping political-economic*[4] *institutional order that*

1. 'Topic: Google, Amazon, Meta, Apple, and Microsoft (GAMAM)' (*Statista*) <https://www.statista.com/topics/4213/google-apple-facebook-amazon-and-microsoft-gafam/> accessed 24 March 2025.

2. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019* (Profile Books 2019).

3. Peter van de Waerdt, *Data Is Power: On the Fundamental Connections between Data Protection Law and Competition Law as Applied to the Digital Market* (University of Groningen 2024) 89.

4. *For a clear display of this 'political-economic' order one can see:* 'Which Tech Titans Attended Donald Trump's Inauguration?' (*euronews*, 12:41:06 01:00) <https://www.euronews.com/next/2025/01/18/donald-trumps-inauguration-which-tech-leaders-will-be-attending-and-who-will-skip-it> accessed 24 March 2025.

exerts oligopolistic control over most digital information and communication spaces, systems, and processes'.[5] Advances in AI technologies are further entrenching their market power, as their dominant position in providing core products and services on the digital market serve as a key competitive advantage.

While there may be much competition 'downstream'[6] regarding the varying ways in which AI systems can be practically deployed, these are built on a consolidated set of 'upstream'[7] inputs. These inputs, or the means of AI production, rely on cloud computing power, access to data, access to capital, ecosystem control and technical expertise. All these assets within the AI value chain are currently, directly or indirectly, majority owned and controlled by current Big Tech incumbents.

Viewing this as a critical issue of sovereignty for the EU, this opinion paper adopts an analytical framework that factors in 'strategic autonomy' and 'data autonomy'.[8] While competition, data protection, and consumer protection law are useful mechanisms for safeguarding the Union's values against Big Tech, they have inherent limits. The broader implications of digital dependence,

---

5. Shoshana Zuboff, 'Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization' (2022) 3 Organization Theory 26317877221129290, 1.

6. *In the context of the AI value chain, 'downstream' refers to the later stages of AI development, deployment, and commercialisation. It involves the application of AI models to real-world products and services, as well as the ways in which these models are distributed, integrated with other products/ services, and monetised.*

7. *Upstream in the AI value chain refers to the early stages of AI development, where foundational technologies, resources, and infrastructure are created.*

8. EU strategic autonomy (EU-SA) refers to the capacity of the EU to act autonomously – that is, without being dependent on other countries – in strategically important policy areas. These can range from defence policy to the economy, and the capacity to uphold democratic values. See Mario Damen, 'EU Strategic Autonomy Monitor'; Oskar J Gstrein, 'Data Autonomy: Recalibrating Strategic Autonomy and Digital Sovereignty' (2023) 28 European Foreign Affairs Review 379 <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\EERR\EERR2023028.pdf> accessed 25 March 2025.

including its impact on European sovereignty and regulatory capacity, must be considered in any legal regime governing key digital infrastructure, products and services. Consequently, this paper argues that a geopolitically aware regulatory stance, one that prioritises digital independence, is essential to address the structural challenges posed by US Big Tech.

This opinion paper highlights the need to ensure that Big Tech does not become Big AI, particularly in the European context. It argues that both ex ante and ex post regulatory measures should be rigorously applied to AI incumbents to ensure that the current 'super-dominance' of US Big Tech does not translate into equivalent dominant positions in the emergent AI market. This is imperative because unchecked dominance by a few major tech firms could and is stifling competition, limiting innovation, and harming consumer welfare and fundamental right protections in the AI market. Moreover, in a geopolitical context, control over AI productive assets and development is increasingly seen as a determinant of global influence, making it critical that Europe prevents its digital economy from being dependent on a handful of US tech giants. This paper offers some examples of potential AI conduct that may be precluded under EU competition law. This paper also acknowledges and highlights potential future enforcement challenges of such competition and regulatory moves given the recent changes in the USA administration's views towards the domestic and foreign regulation of its national technology gatekeepers.[9]

In highlighting these challenges, it is argued that European regulation of what are primarily US technology incumbents can no longer be viewed through a purely competition, consumer/ data protection and privacy lens. Regulation

9. 'EU Risks More Trump Tariffs in Looming Big Tech Crackdown' (*POLITICO*, 19 March 2025) <https://www.politico.eu/article/big-tech-crackdown-europe-donald-trump-tariffs-united-states-digital-competition/> accessed 24 March 2025; 'Are Tariffs Big Tech's New Tool against EU Regulation?' (*Brookings*) <https://www.brookings.edu/articles/are-tariffs-big-techs-new-tool-against-eu-regulation/> accessed 24 March 2025; 'Trump Fires Back at EU Tech Regulation' (9 March 2025) <https://www.lemonde.fr/en/economy/article/2025/03/09/trump-fires-back-at-eu-tech-regulation_6738972_19.html> accessed 24 March 2025; Richard Manfredi, 'Two Weeks In: Key Trump Administration Developments in Tech Policy' (*Gibson Dunn*, 5 February 2025) <https://www.gibsondunn.com/two-weeks-in-key-trump-administration-developments-in-tech-policy/> accessed 24 March 2025.

of the digital ecosystem *must* also factor in the need to ensure the Union's digital sovereignty and 'strategic autonomy'. If Europe is to compete in this new data-driven century it will need its own technological infrastructure, research and production base, particularly in the domain of AI.

2. The Upstream Market for AI: Concentrated and Entrenched Incumbents

As previously stated there is much competition 'downstream' in the AI value chain but vital 'upstream' AI assets are owned and controlled by current tech incumbents. These assets can be divided into the following categories: cloud computing power, access to data, access to capital, ecosystem control and technical expertise.[10]

Regarding the first category, a limited number of giants dominate the computing infrastructure necessary to develop, train and host advanced AI models and their downstream applications.[11] For instance, Amazon, Microsoft and Google collectively account for ~ two thirds of the cloud computing market,[12] while the partnership of US based Nvidia and Taiwanese TSMC control an estimated 80-90% of the market for AI specialised semiconductor design and manufacturing.[13] While there are attempts underway to reduce this reliance on

10. Max von Thun and Daniel Hanley, 'Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All' (Social Science Research Network, 17 October 2024) 8 <https://papers.ssrn.com/abstract=4990780> accessed 16 March 2025.

11. Christophe Carugati, 'The Generative AI Challenges for Competition Authorities' (2024) 59 Intereconomics 14, 14.

12. 'Infographic: Amazon and Microsoft Stay Ahead in Global Cloud Market' (*Statista Daily Data*, 27 February 2025) *With Google in a far behind third place. See* <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers> accessed 24 March 2025.

13. Trevor Jennewine, 'Nvidia Sells Graphics and AI Chips, but 15% of Sales Come From Other Multi-Hundred-Billion Dollar Markets' (*The Motley Fool*, 22 January 2024)

Nvidia and TSMC, these have been spearheaded by already dominant Big Tech firms.[14] The end result of this is that concentration in computing infrastructure necessarily entails the '*centralization of AI research and commercialization around dominant firms*.'[15]

As to data access, AI models[16] require massive amounts of reasonably high quality data to be trained on. While much of this data can be described as publicly accessible,[17] theoretically being available to any market players to access, current tech incumbents have a clear advantage. They are able to collect, organise, clean, label and prepare such data for model training purposes more efficiently due to their dominant digital market positions.[18] In addition, the large amounts of proprietary, highly personalised and higher quality[19] data accessible and usable by Big Tech through their networked ecosystems and extensive first and third party surveillance capabilities, grant those firms, such as Google, Microsoft and Meta, decisive market advantages compared to players who can only access publicly accessible information.[20] Downstream,

---

<https://www.fool.com/investing/2024/01/22/nvidia-sells-ai-chips-15-sales-from-other-markets/> accessed 24 March 2025.

14. Jai Vipra, 'Computational Power and AI' (*AI Now Institute*, 27 September 2023) <https://ainowinstitute.org/publication/policy/compute-and-ai> accessed 24 March 2025.

15. von Thun and Hanley (n 10) 10.

16. *AI models include large language models (LLMs) and large multimodal models (LMMs).*

17. *Barring questions and issues raised regarding copyright, privacy and data protection in which, for example, Big Tech players have inherent advantages in meeting regulatory burdens and the negotiation of contracts.*

18. von Thun and Hanley (n 10) 10.

19. *Such as cultural/ behavioural trends and speech patterns garnered from social media platforms and analysis of users.*

20. Fabio Morreale and others, 'The Unwitting Labourer: Extracting Humanness in AI Training' (2024) 39 AI & SOCIETY 2389; Lauren Leffer, 'Your Personal Information Is Probably

these advantages reinforce incumbents' dominance as their AI models and services, being the most advanced, attract greater adoption. This in turn provides them with access to larger volumes of training data, further widening the gap between them and less prominent AI providers in a 'data feedback loop'.[21]

Big Tech incumbents, as a result of decades of unchallenged dominance, have also gained enormous financial resources and capital, allowing them to both defend their monopolistic positions and expand their market reach further. With data being described as 'the new oil',[22] these technology firms have leveraged their vast cash reserves[23] to maintain a competitive edge through research and development, benefiting from significant economies of scale. Their ability to invest heavily in AI research far exceeds that of smaller competitors, enabling them to drive innovation while reinforcing their dominance. This

---

Being Used to Train Generative AI Models' (*Scientific American*, 1 March 2025) <https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/> accessed 24 March 2025.

21. von Thun and Hanley (n 10) 11.

22. *While not a fully accurate statement (oil is finite in comparison to the theoretical infinite amount of data capable of being generated) it captures the centrality and value of data in the current technological revolution.* 'Is Data the New Oil? Competition Issues in the Digital Economy | Think Tank | European Parliament' <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)646117> accessed 24 March 2025; 'You May Have Heard Data Is the New Oil. It's Not' (*World Economic Forum*, 10 January 2018) <https://www.weforum.org/stories/2018/01/data-is-not-the-new-oil/> accessed 24 March 2025.

23. See the following data from companiesmarketcap.com for GAMMA cash on hand statistics. 'Microsoft (MSFT) – Cash on Hand' <https://companiesmarketcap.com/microsoft/cash-on-hand/> accessed 24 March 2025; 'Alphabet (Google) (GOOG) – Cash on Hand' <https://companiesmarketcap.com/alphabet-google/cash-on-hand/> accessed 24 March 2025; 'Meta Platforms (Facebook) (META) – Cash on Hand' <https://companiesmarketcap.com/meta-platforms/cash-on-hand/> accessed 24 March 2025; 'Apple (AAPL) – Cash on Hand' <https://companiesmarketcap.com/apple/cash-on-hand/> accessed 24 March 2025; 'Amazon (AMZN) – Cash on Hand' <https://companiesmarketcap.com/amazon/cash-on-hand/> accessed 24 March 2025.

financial strength also allows them to engage in cross-subsidisation, absorbing losses over a longer period of time in high-risk AI ventures that would be untenable for less capitalised firms.[24] By doing so, they can exert greater control over AI's development trajectory, ensuring that the most cutting-edge advancements emerge within their ecosystems. Furthermore, Big Tech is supplanting traditional venture capitalists, funding promising AI start-ups while maintaining strict oversight.[25]

AI does not operate in isolation but is embedded within broader data ecosystems controlled by these dominant firms. From search engines like Google and Bing to smartphones running iOS and Android, integrated AI services can further entrench incumbents' influence. Operating systems such as Windows and macOS, internet browsers like Chrome and Edge, and social media and messaging platforms such as Facebook, WhatsApp and Instagram all integrate AI-driven functionalities.[26] IoT devices, such as Amazon's Alexa home assistant, also rely on AI to process user interactions.[27] This integration is facilitated by proprietary software development kits (SDKs) and application programming interfaces (APIs), ensuring seamless interoperability within their ecosystems. This ecosystem control is a decisive factor in a firm's ability to commercialise AI

24. Reijer Hendrikse and others, 'The Big Techification of Everything' (2022) 31 Science as Culture 59, 6.

25. George Hammond, 'Big Tech Outspends Venture Capital Firms in AI Investment Frenzy' *Financial Times* (29 December 2023).

26. 'Meet Your New Assistant: Meta AI, Built With Llama 3' (*Meta*, 18 April 2024) <https://about.fb.com/news/2024/04/meta-ai-assistant-built-with-llama-3/> accessed 24 March 2025; 'Gemini – Chat to Supercharge Your Ideas' (*Gemini*) <https://gemini.google.com> accessed 24 March 2025; 'Https://Www.Microsoft.Com/En-Us/Edge/Features/Copilot' <https://www.microsoft.com/en-us/edge/features/copilot> accessed 24 March 2025; 'Apple Intelligence' (*Apple*) <https://www.apple.com/apple-intelligence/> accessed 24 March 2025.

27. Panos Panay, 'Introducing Alexa , the next Generation of Alexa' (26 February 2025) <https://www.aboutamazon.com/news/devices/new-alexa-generative-artificial-intelligence> accessed 24 March 2025.

at scale.[28] By embedding AI across platforms used by millions, even billions, of users, Big Tech can transform new AI models into instantly marketable products. By capitalising on network effects, economies of scale, data feedback loops, and integration, these interconnected service ecosystems reinforce their owners' dominance. This is achieved through locking in users and creating significant barriers (moats) that make it difficult for outside businesses to compete.[29] The UK Competition and Markets Authority (CMA) highlights this dominance of Big Tech across the AI value chain.[30] Cloud dominance further strengthens their gatekeeping role, as they provide not only proprietary AI solutions but also the infrastructure that third-party AI developers depend on. This dual position allows them to shape the future of AI while ensuring that the most critical innovations remain within their control.[31]

28. von Thun and Hanley (n 10) 13.

29. Daniel Hanley, 'A Topology of Multisided Digital Platforms' (Social Science Research Network, 20 June 2020) <https://papers.ssrn.com/abstract=3651606> accessed 24 March 2025.

30. 'AI Foundation Models: Update Paper' (*GOV.UK*, 16 April 2024) <https://www.gov.uk/government/publications/ai-foundation-models-update-paper> accessed 24 March 2025.

31. von Thun and Hanley (n 10) 14.



Presence of Big Tech incumbents across the AI model value chain: *Competition and Markets Authority (UK)*[32]

Finally, developing advanced AI models requires highly specialised and scarce expertise, making skilled labour one of the most valuable assets in the industry. Studies have highlighted a persistent talent crunch, with demand for AI researchers, engineers, and data scientists far outstripping supply.[33] Big Tech firms, with their vast financial resources, can outcompete smaller players by offering higher salaries, research funding, and exclusive projects.[34] This

32. 'AI Foundation Models Update Paper' (Competition and Markets Authority 2024) <https://assets.publishing.service.gov.uk/media/661941a6c1d297c6ad1dfeed/Update_Paper__1_.pdf> accessed 26 March 2025.

33. 'New McKinsey Survey Reveals the AI Tech-Talent Landscape' <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-reinvents-tech-talent-opportunities> accessed 24 March 2025; 'AI Skills Gap Must Be Addressed Urgently, Say 72% of IT Leaders in Red Hat Survey' (5 December 2023) <https://www.redhat.com/en/about/press-releases/ai-skills-gap-must-be-addressed-urgently> accessed 24 March 2025.

34. Hammond (n 25); Mark Sullivan, 'Big Tech Is on a Generative AI Hiring Spree' (*Fast Company*, 15 April 2024) <https://www.fastcompany.com/91092373/big-tech-is-on-a-generative-ai-hiring-spree> accessed 24 March 2025.

ability to absorb and poach top talent consolidates technical expertise within a handful of dominant incumbents, creating what Zuboff describes as a '*technological high priesthood*', a concentrated elite with exclusive control over AI's development and deployment, further entrenching their market power.[35]

3. Identified Potential Anti-competitive Practices

This section examines (by no means exhaustively) some potential anti-competitive practices by Big Tech in the AI market under competition law, focusing on Article 102 TFEU,[36] along with the Digital Markets Act (DMA)[37] and the Merger Control Regulation.[38] The AI market could see incumbents acting in an exclusionary and anti-competitive manner, by leveraging network effects, ecosystem power and control over processing power and data moats. It should be prefaced that any analysis of Big Tech's dominant position in the digital and AI market should be approached through the lens of viewing them as 'data ecosystems', rather than through the lens of a strictly defined single market. This is because of the network effects that allow these firms to pool massive quantities of personal data from different products and services. This is a '*vital element in determining an undertaking's market power under EU competition law*'.[39] It is even more essential to recognise this when it comes to the AI market. As discussed previously, these firm's access to data places them at a structural advantage, reinforcing their dominance and limiting the ability of

35. Zuboff (n 2).

36. Treaty on the Functioning of the European Union (TFEU) [2008] OJ C 115/47.

37. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) 2022 (OJ L).

38. Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) (Text with EEA relevance) 2004 (OJ L).

39. van de Waerdt (n 3) 250.

competitors to challenge their position. The AI market is not confined to a single, well-defined sector but is instead deeply integrated across multiple digital markets, amplifying the competitive concerns associated with Big Tech's control over key resources. The regulatory response must therefore account for the interconnected nature of these data ecosystems and the far-reaching implications of AI-driven market power. As such the Commission:

> '*should also not hesitate to counter the concentration of power in the emerging AI stack market, where control over infrastructure and technology is increasingly in the hands of a few dominant players.*'[40]

Exclusionary conduct may encompass strategies such as bundling, tying and self-preferencing to erect barriers to entry and exclude rivals.[41] Such conduct is not new within digital markets.[42] Tying and bundling are likely to be and already are a common occurrence in the AI market, with incumbents being able to link new AI products/ services with existing core products/ services.[43] This can be seen with the tying and bundling of large language models by both Google and Microsoft into their core offerings. Google, for example, has integrated Gemini into its dominant search engine, email service, internet browser, certain applications and mobile operating system. While Microsoft has integrated Copilot into its browser and productivity applications.

These cases arguably involve elements of self-preferencing. The AI market

---

40. Christoph Schmon, 'Saving the Internet in Europe: Fostering Choice, Competition and the Right to Innovate' (*Electronic Frontier Foundation*, 25 March 2025) <https://www.eff.org/deeplinks/2025/03/saving-internet-europe-fostering-choice-competition-and-right-innovate> accessed 27 March 2025.

41. Aysem Diker Vanberg, 'Generative AI & Competition Law Concerns: The New Kid on the Block!' [2024] COM&IP Insight 1, 2.

42. Rosario Baratta, 'European Commission Fines Microsoft for Non-Compliance with Browser Choice Commitments: A First Timer' (2013) 4 Journal of European Competition Law & Practice 415; *Google LLC and Alphabet Inc v European Commission* [2024] ECJ Case C-48/22 P; *Microsoft Corp v Commission of the European Communities* [2007] GC Case T-201/04.

43. Diker Vanberg (n 41) 2.

currently features a diverse range of AI agents and large language models (LLMs), including many open-source options.[44] These models can be deployed locally (for smaller-scale models) or hosted on cloud services provided by various companies. However, Google and Microsoft restrict the integration of third-party AI within their core offerings, effectively favouring their own models over competitors. This can be seen to be the use of market dominance by Big Tech incumbents in search engines, browsers, mobile operating systems, and productivity applications to establish a stronghold in the emerging market for virtual AI companions and assistants. This practice echoes the Google Shopping case, where the CJEU held that the company used its search engine dominance to disadvantage competitors by prioritising its own services, constituting abuse of dominance under 102 TEFU.[45] In practice, there is no technical barrier to allowing third-party LLM agents to integrate with operating systems and search engines. This has been demonstrated by Brave Browser[46] (based on Google's Chromium), which enables users to select their preferred AI model for both the browser and Brave Search, including the option to use locally downloaded models.[47]

Applying the CJEU's jurisprudence on tying and bundling and self-preferencing in the digital market, it is possible that the current approach of incumbents could constitute an abuse of dominance under Article 102 TFEU. The Digital Markets Act may also provide a potential remedy through its interoperability requirements. Under Article 6 (7) DMA, gatekeepers must allow third-party providers to interoperate with their operating systems, virtual assistants, and cloud services, ensuring that competition in AI services is not unfairly

44. Bertin Martens, 'Why Artificial Intelligence Is Creating Fundamental Challenges for Competition Policy' (Bruegel Policy Brief 2024) Research Report 16/2024 3 <https://www.econstor.eu/handle/10419/302296> accessed 23 March 2025.

45. *Google LLC and Alphabet Inc v European Commission* (n 42).

46. 'The Browser That Puts You First' (*Brave*) <https://brave.com/> accessed 27 March 2025.

47. 'Brave Leo AI' (*Brave*) <https://brave.com/leo/> accessed 27 March 2025; 'Finally! Brave Brings Local AI to the Browser' (*It's FOSS News*, 25 September 2024) <https://news.itsfoss.com/brave-browser-local-ai/> accessed 27 March 2025.

restricted.[48] Enforcing these provisions could prevent dominant firms from entrenching their position in the AI sector and promote a more competitive and diverse AI assistant market. The Commission has taken the preliminary view that Alphabet self-preferences its own services over those of third parties, thereby failing to comply with the DMA.[49] Any Commission action should factor in AI self-preferencing as well.

Competition concerns also arise regarding the vast data assets held by Big Tech incumbents, as discussed in the previous section. Companies like Google, Microsoft, and Meta benefit from extensive data generated by internet users, which provides a competitive advantage in training AI models. In the case of Google and Meta, they have actively incentivised, or compelled, users and content creators to allow their data to be scraped. For instance, Google has reportedly penalised websites that block data scraping for AI search purposes by reducing their visibility in search results and in Gemini summaries at the top of the search page.[50] Such conduct raises concerns about Google's ability to reinforce its dominance by leveraging its control over search infrastructure to extract valuable data for AI development, while simultaneously locking competitors out of its data assets.

Under the DMA, Google is designated as a gatekeeper (Article 3 DMA). The Commission could use its enforcement powers to mandate greater data-sharing obligations, ensuring that Google does not exploit its exclusive access to scraped web data to gain an unfair advantage in the AI market. This could include requiring Google to provide third-party access to its training datasets

48. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) art 6 (7).

49. 'Commission Sends Preliminary Findings to Alphabet under the Digital Markets Act' (*European Commission – European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_811> accessed 27 March 2025.

50. 'Google's AI Search Gives Sites Dire Choice: Share Data or Die' *Bloomberg.com* (15 August 2024) <https://www.bloomberg.com/news/articles/2024-08-15/google-s-search-dominance-leaves-sites-little-choice-on-ai-scraping> accessed 27 March 2025.

under fair, reasonable, and non-discriminatory (FRAND) terms. Such an approach would mitigate Google's ability to leverage its economies of scale and its privileged position in search to entrench itself as a dominant AI provider. By enforcing data-sharing requirements on firms that have access to large troves of data, the DMA could help level the playing field, ensuring that AI development is not monopolised by a handful of firms with disproportionate access to training data.

In the context of 'killer acquisitions', the European Commission could assess whether the acquisition of an AI company significantly alters competition in the AI market under the EU Merger Regulation. The Commission could examine if the acquisition strengthens a dominant position, particularly when the acquirer holds a gatekeeping role in related markets such as search engines or cloud services. For example, if a dominant player like Google or Microsoft acquires an AI startup with unique technology, the Commission should evaluate whether the acquisition stifles competition by removing a potential competitor, reducing innovation, or restricting access to essential AI resources. Under Article 2(3) of the EU Merger Regulation, the Commission could block or impose conditions on acquisitions that substantially harm competition, considering both horizontal and vertical effects, such as the potential for excluding rivals or restricting access to critical AI models, data, or infrastructure. However, the partnership between OpenAI and Microsoft[51] shows that some agreements may fall outside the scope of EU merger control rules due to challenges in demonstrating a change of control. This suggests that European merger control may not always capture every anti-competitive concentration. However, since June 2024, the EU Commission has been reviewing the exclusivity agreements between OpenAI and Microsoft to determine if they prevent other companies from entering the generative AI market. In such cases, the Commission could still act under Article 102 TFEU to address any anti-competitive effects.[52]

This section examined some potential examples of anti-competitive conduct

51. Microsoft Corporate Blogs, 'Microsoft and OpenAI Evolve Partnership to Drive the next Phase of AI' (*The Official Microsoft Blog*, 21 January 2025) <https://blogs.microsoft.com/blog/2025/01/21/microsoft-and-openai-evolve-partnership-to-drive-the-next-phase-of-ai/> accessed 27 March 2025.

52. Diker Vanberg (n 41) 4.

by Big Tech in the AI market, focusing on practices under Article 102 TFEU, the Digital Markets Act, and the Merger Control Regulation. However, these examples represent only a fraction of the broader issue. Any analysis of the competitive dynamics of the market for AI must also factor in data protection concerns as this is a crucial element to the functioning of the digital market.[53] The next section will address the importance of Europe's technological sovereignty in mitigating these concerns, particularly in reducing reliance on foreign providers.

4. Enforcement Challenges in Light of Geopolitical Realities

Any discussion of applying European competition measures to Big Tech gatekeepers would be remiss without consideration of the wider geopolitical landscape. Competition law does not operate in a vacuum but is inevitably shaped by political dynamics.[54] In the case of regulating Big Tech, this is particularly pronounced due to close ties between dominant technology firms and the United States government.[55] This raises fundamental questions about the feasibility and effectiveness of European regulatory efforts.

Both *ex ante* and *post facto* regulatory measures can, in theory, curb anti-competitive behaviour. However, their efficiency and efficacy at sufficiently

53. van de Waerdt (n 3) 249.

54. See Tim Büthe, The Politics of Market Competition: Trade and Antitrust in a Global Economy in Lisa L Martin, *The Oxford Handbook of the Political Economy of International Trade* (Oxford University Press 2015).

55. US 'Big Tech' has always had very close institutional and personal ties to elements of the US National Security State. Under Donald Trump's second administration these ties appear to be growing stronger. See the following for some examples and commentary. Andrea Coveri, Cozza ,Claudio and Dario and Guarascio, 'Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus' Review of Political Economy 1; Jay Peters, 'Former Head of NSA Joins OpenAI Board' (*The Verge*, 13 June 2024) <https://www.theverge.com/2024/6/13/24178079/openai-board-paul-nakasone-nsa-safety> accessed 26 June 2024; Zuboff (n 2) ch 4 The Moat Around the Castle.

deterring abuse of dominance remains an open question. Protracted and resource intensive[56] legal proceedings often allow incumbents to entrench their market dominance further during proceedings, limiting the effectiveness of enforcement actions when they are finally levied. Additionally, while regulatory penalties may impose financial costs, they may not necessarily deter unlawful conduct when Big Tech firms are able to absorb penalty costs. The emerging risk of punitive actions being met with political and economic retaliation from the US, no longer a hypothetical scenario under the second Trump administration, further complicates regulatory approaches.[57] This is even more pronounced in the context of regulating AI technology and firms with the US and Trump specifically stating the paramount importance of continued American leadership in AI to maintain the economic and national security of the US.[58] With Big Tech and AI incumbents asking the Trump administration to '*assertively engage foreign governments to deter adoption of detrimental AI policies that weaken US AI leadership*',[59] it is clear that there is fast becoming a geopolitical clash over how AI should be regulated, with US dominance in AI giving its firms leverage over European regulation, with efforts to assert digital sovereignty facing corporate and political resistance.

The key issue at present is Europe's reliance on US tech firms for essential

56. Jasper van den Boom and others, 'Towards Market Investigation Tools in Competition Law: The Case of the Netherlands' (2023) 14 Journal of European Competition Law & Practice 553, 556.

57. 'Are Tariffs Big Tech's New Tool against EU Regulation?' (n 9); Anupriya Datta, 'Trump Threatens to Launch Tariff Attack on EU Tech Regulation' (*Euractiv*, 22 February 2025) <https://www.euractiv.com/section/tech/news/trump-threatens-to-launch-tariff-attack-on-eu-tech-regulation/> accessed 25 March 2025; 'Can EU Laws Hold against Big Tech's Power Play?' (*ctech*, 20 February 2025) <https://www.calcalistech.com/ctechnews/article/vglbleori> accessed 25 March 2025.

58. 'Artificial Intelligence for the American People' <https://trumpwhitehouse.archives.gov/ai/> accessed 25 March 2025.

59. Jacob Wulff Wold, 'Big Tech Is Asking Trump to Fight EU AI Regulation' (*Euractiv*, 24 March 2025) <https://www.euractiv.com/section/tech/news/big-tech-is-asking-trump-to-fight-eu-ai-regulation/> accessed 26 March 2025.

digital public and private services and products. Big Tech's dominance extends beyond consumer markets, underpinning critical infrastructure, cloud services, and digital platforms essential to European economies. This creates a paradox: **how can Europe effectively address abusive market practices of US Big Tech when it is structurally dependent on the very firms it seeks to regulate?**[60]

The durability of transatlantic alliances can clearly no longer be taken for granted. While the US and Europe have historically maintained close economic and security ties, the current US administration has highlighted growing divergences in their strategic priorities and interests.[61] Europe's reliance on US controlled digital infrastructure exposes it to significant vulnerabilities, ranging from national security risks[62] to the potential for service disruptions at moments of geopolitical tension. Many public and private institutions and most individuals in Europe continue to depend on US technology firms, leaving the bloc exposed to external leverage.[63] There is also the already apparent risk that

60. Gstrein (n 8) 381.

61. Andrew Roth, 'Stunning Signal Leak Reveals Depths of Trump Administration's Loathing of Europe' *The Guardian* (25 March 2025) <https://www.theguardian.com/world/2025/mar/25/stunning-signal-leak-reveals-depths-of-trump-administrations-loathing-of-europe> accessed 25 March 2025.

62. Laura Poitras, Marcel Rosenbach and Holger Stark, 'Secret NSA Documents Show How the US Spies on Europe and the UN' *Der Spiegel* (26 August 2013) <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> accessed 25 March 2025; ibid; James Ball and Nick Hopkins, 'GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief' *The Guardian* (20 December 2013) <https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner> accessed 4 December 2024; Reuters, 'NSA Tapped German Chancellery for Decades, WikiLeaks Claims' *The Guardian* (8 July 2015) <https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel> accessed 25 March 2025; Bruce Sterling, 'So, It Was the NSA in the Greek Phones All Along' *Wired* <https://www.wired.com/beyond-the-beyond/2015/10/nsa-greek-phones-along/> accessed 25 March 2025.

63. For example, the European cloud market is dominated by Amazon Web Services (AWS),

US technology firms may simply elect to exclude Europe from certain products and services, which could stifle innovation and hurt the blocs global economic competitiveness. This is already the case with Meta and Apple delaying and holding off on releasing certain AI products and services within the bloc.[64]

If Europe is serious about asserting digital sovereignty, it must confront these dependencies. So long as US tech giants control the infrastructure that underpins Europe's digital economy and society, any attempt to enforce competition law will be shackled by political and economic realities far beyond the legal framework. Without a decisive shift, Europe will remain vulnerable, not just to corporate dominance, but to the geopolitical leverage that comes with it.

5. Conclusions: Europe's Need for Strategic Digital Autonomy

Given the risks associated with reliance and dependency on foreign countries for critical and core technological infrastructure, software, products and services, there are initiatives within the EU towards achieving 'strategic autonomy' and 'data autonomy' when applied to the digital domain. Although past efforts

---

Microsoft, and Google. One has to look at the prevalence of Microsoft and Google software in European public and private institutions and consumer reliance on Microsoft, Google and Apple services and products to see how dependent Europe is on US Big Tech. Will McCurdy published, 'European Cloud Market Is Being Dominated by Three Big Players' (*TechRadar*, 30 September 2022) <https://www.techradar.com/news/european-cloud-market-is-being-dominated-by-three-big-players> accessed 25 March 2025.

64. 'Meta AI Finally Comes to Europe after a Year-Long Delay, but with Some Limitations' (*Business Today*, 21 March 2025) <https://www.businesstoday.in/technology/news/story/meta-ai-finally-comes-to-europe-after-a-year-long-delay-but-with-some-limitations-468809-2025-03-21> accessed 27 March 2025; Rohan Goswami, 'Apple Intelligence Won't Launch in EU in 2024 Due to Antitrust Regulation, Company Says' (*CNBC*, 21 June 2024) <https://www.cnbc.com/2024/06/21/apple-ai-europe-dma-macos.html> accessed 27 March 2025.

have seen mixed success,[65] shifting relations with the United States during Donald Trump's presidency have made the issue more pressing. For example, the Dutch Parliament recently urged an 'end to dependence on US software companies.'[66] A day later, dozens of European tech firms urged the European Commission to create a sovereign fund to invest in European technology, including cloud infrastructure. They also called for a 'Buy European' mandate, which would require Member State governments to prioritise European companies in procurement tenders. This would boost demand and encourage businesses to invest in local technology.[67]

The term strategic and data autonomy should be understood to refer to European owned and controlled technological infrastructure. This is arguably fast becoming a necessary precondition for the enforcement of competition rules and other regulatory concerns such as data protection. The effectiveness of enforcement mechanisms hinges not just on legal authority but on Europe's ability to impose meaningful consequences. As it stands, punitive actions against dominant US-based firms remain limited by Europe's dependence on their products, services, and infrastructure. Without viable European alternatives, any attempt to curb Big Tech's dominance risks being undermined by economic and political constraints.

A shift towards open-source software could reduce reliance on proprietary systems controlled by foreign tech giants. Governments and public and private institutions could prioritise open-source solutions such as Linux over Windows, fostering technological self-sufficiency and digital sovereignty. A proof of concept of this can be seen in the German Federal State of Schleswig-Holstein's adoption of Linux and open document standards (amongst other open source

65. For example, see discussion of the Gaia-X federated cloud system in Gstrein (n 8) 385.

66. Toby Sterling, 'Dutch Parliament Calls for End to Dependence on US Software Companies' *Reuters* (19 March 2025) <https://www.reuters.com/world/europe/dutch-parliament-calls-end-reliance-us-software-2025-03-18/> accessed 25 March 2025.

67. Foo Yun Chee and Foo Yun Chee, 'Airbus Leads Call for Europe to Create Sovereign Infrastructure Fund, Buy European' *Reuters* (17 March 2025) <https://www.reuters.com/business/aerospace-defense/airbus-others-call-sovereign-infrastructure-fund-buy-european-2025-03-17/> accessed 25 March 2025.

initiatives) in public administration to replace Windows.[68] Widespread adoption of privacy-focused services based out of Europe, such as the emerging competitor to Google's ecosystem Proton,[69] or public open-source initiatives,[70] could further strengthen Europe's digital sovereignty while ensuring its values. Regarding AI especially, open-sourced models are key to reducing Europe's dependence on foreign controlled systems. Proprietary AI, dominated by US firms, dictates access and development. By investing in open-source AI and European cloud infrastructure, Europe can foster competition, transparency, and innovation while safeguarding its digital sovereignty.[71] Without this, reliance on external providers will continue to undermine Europe's technological and regulatory autonomy.

Establishing an interoperable, open-data framework would also help level the playing field for European tech firms. Restricting the monopolisation of key data assets by dominant platforms and encouraging data sharing could promote competition while ensuring European businesses and researchers have access to critical data for innovation. The EU has taken steps in this direction through regulatory initiatives such as the Data Act, Data Governance Act, and the Open Data Directive, all of which aim to create a fairer, more accessible and sovereign data economy.[72] A key element of this strategy is the creation

68. 'Schleswig-Holstein.de – Linux Plus 1 – Die Open Innovation Und Open Source Strategie Des Landes Schleswig-Holstein (Stand: November 2024)' <https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Downloads/_dateien/open-source-strategie.pdf> accessed 25 March 2025.

69. 'Learn about Proton and Our Vision for a Better Internet' (*Proton*) <https://proton.me/about-test-31012025-b/> accessed 25 March 2025.

70. For example: 'France and Germany Unveil Docs, a Homegrown Alternative to Google Docs' (*TechSpot*, 20 March 2025) <https://www.techspot.com/news/107225-france-germany-unveil-docs-collaborative-tool-rival-us.html> accessed 25 March 2025.

71. 'A Call to Protect Open-Source AI in Europe | LAION' <https://laion.ai/notes/letter-to-the-eu-parliament> accessed 26 June 2024.

72. 'A European Strategy for Data | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 27 March 2025.

of Common European Data Spaces, which seek to increase the availability of data for use across the economy and society. These frameworks are designed to decentivise dominant firms from monopolising critical data assets, while fostering a more competitive and innovation-driven digital environment.

Political momentum for a 'Eurostack' initiative appears to be increasing. Both the German and French governments have expressed support for the proposal, which aims to lessen the Union's reliance on US technologies by developing a sovereign European technological infrastructure encompassing the entire value chain, including semiconductors, cloud services, platforms, social media, and AI.[73] However, at the time of writing, no final agreement has been reached between Member States on the specifics of the initiative. The concept remains vague, with divergent approaches, some emphasising public investment and others private, which highlights underlying political divisions among Member States and political parties.[74] The Commission has offered only cautious support and has yet to propose any concrete measures.[75]

It is this paper's view that the EU must commit to long-term investment in homegrown technology firms, infrastructure and AI ventures through initiatives such as the EU Chips Act and the proposed sovereign tech fund and Eurostack initiative. A 'Buy European' mandate, encouraging public institutions and businesses to prioritise European digital products and services, could provide the necessary support for domestic firms to compete with Silicon Valley

73. Théophane Hartmann, 'European Industry Big Win: Germany, France Both Support Sovereign EU-Based Tech Infrastructure' (*Euractiv*, 10 April 2025) <https://www.euractiv.com/section/tech/news/european-industry-big-win-germany-france-both-support-sovereign-eu-based-tech-infrastructure/> accessed 16 April 2025.

74. Théophane Hartmann, 'Rival Report to Knafo's on EU Tech Sovereignty: More Content, More Cautious' (*Euractiv*, 15 March 2025) <https://www.euractiv.com/section/tech/news/rival-report-to-knafos-on-eu-tech-sovereignty-more-content-more-cautious/> accessed 19 April 2025.

75. Théophane Hartmann, 'Von Der Leyen Expresses Timid Support for Eurostack Tech Sovereignty Project' (*Euractiv*, 9 April 2025) <https://www.euractiv.com/section/tech/news/von-der-leyen-expresses-timid-support-to-sovereign-eurostack-project/> accessed 16 April 2025.

giants. True strategic autonomy will require more than individual member states acting in isolation. A cohesive EU-wide strategy, ensuring alignment between regulatory frameworks, industrial policy, and digital infrastructure development, is essential. Without coordination, fragmented efforts will fail to counteract the entrenched power of foreign Big Tech firms. With the forthcoming Chips Act 2.0 and a proposed 'five pillar AI Continent Action Plan', reducing the continent's dependency on the United States specifically in the field of artificial intelligence appears to be a key priority on the Commission's legislative agenda.[76] With regard to cloud computing sovereignty, it is essential to avoid 'sovereignty washing', where US cloud providers partner with European firms to present their services as European-based.[77] This practice has raised concerns, including from France's Digital Minister, and is currently being addressed by members of the European Parliament.[78]

Achieving digital sovereignty is not simply a matter of economic competitiveness. It is a fundamental issue of legal and political independence. If Europe is serious about enforcing competition law, protecting fundamental rights and

---

76. Jacob Wulff Wold, 'Virkkunen Confirms a Chips Act 2.0 and Outlines AI Action Plan' (*Euractiv*, 26 March 2025) <https://www.euractiv.com/section/tech/news/virkkunen-confirms-a-chips-act-2-0-and-outlines-ai-action-plan/> accessed 27 March 2025.

77. This is vital for considering the limitations of European control over data, as the US CLOUD Act allows American authorities to access data held by US-based cloud providers, even when the data is stored outside the United States. Gretchen Ramos, 'Application of the CLOUD Act to EU Entities' <https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo>; Nationaal Cyber Security Centrum, 'De werking van de CLOUD-Act bij dataopslag in Europa – Expertblogs – Nationaal Cyber Security Centrum' (16 August 2022) <https://www.ncsc.nl/actueel/weblog/weblog2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa> accessed 19 April 2025.

78. Théophane Hartmann, 'EPP, SD, Renew Table 309 Changes to Controversial EU Tech Sovereignty Report' (*Euractiv*, 22 March 2025) <https://www.euractiv.com/section/tech/news/epp-sd-renew-table-309-changes-to-controversial-eu-tech-sovereignty-report/> accessed 19 April 2025; Théophane Hartmann, 'Against US Digital "predators," France Digital Minister Calls for a European "Pack Hunt"' (*Euractiv*, 15 April 2025) <https://www.euractiv.com/section/tech/news/against-us-digital-predators-france-digital-minister-calls-for-a-european-pack-hunt/> accessed 16 April 2025.

maintaining sovereign democratic control over its digital future, it must first ensure that it has the technological capacity to autonomously stand on its own. This is even more critical in the context of AI. The development of advanced AI systems, as stated previously, is deeply intertwined with access to computing power, data, infrastructure, technical expertise and capital. These all largely remain concentrated in the hands of US technology firms. Without independent European capabilities in AI research, cloud computing, and semiconductor manufacturing, the bloc risks becoming permanently dependent on foreign providers for one of the most transformative technologies of the century. This dependence not only weakens Europe's ability to regulate AI effectively but also exposes it to geopolitical risks, including supply chain disruptions and policy shifts in the US and elsewhere.

If Europe wants to maintain control over its own digital and geopolitical destiny, it must make reducing reliance on external AI providers and the broader digital infrastructure that enables their dominance an urgent and absolute priority.

Bibliography

'A Call to Protect Open-Source AI in Europe | LAION' <https://laion.ai/notes/letter-to-the-eu-parliament> accessed 26 June 2024

'A European Strategy for Data | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 27 March 2025

'AI Foundation Models Update Paper' (Competition and Markets Authority 2024) <https://www.gov.uk/government/publications/ai-foundation-models-update-paper> accessed 26 March 2025

'AI Foundation Models: Update Paper' (*GOV.UK*, 16 April 2024) <https://www.gov.uk/government/publications/ai-foundation-models-update-paper> accessed 24 March 2025

'AI Skills Gap Must Be Addressed Urgently, Say 72% of IT Leaders in Red Hat Survey' (5 December 2023) <https://www.redhat.com/en/about/press-releases/ai-skills-gap-must-be-addressed-urgently> accessed 24 March 2025

'Alphabet (Google) (GOOG) – Cash on Hand' <https://companiesmarketcap.com/alphabet-google/cash-on-hand/> accessed 24 March 2025

'Amazon (AMZN) – Cash on Hand' <https://companiesmarketcap.com/amazon/cash-on-hand/> accessed 24 March 2025

'Apple (AAPL) – Cash on Hand' <https://companiesmarketcap.com/apple/cash-on-hand/> accessed 24 March 2025

'Apple Intelligence' (*Apple*) <https://www.apple.com/apple-intelligence/> accessed 24 March 2025

'Are Tariffs Big Tech's New Tool against EU Regulation?' (*Brookings*) <https://www.brookings.edu/articles/are-tariffs-big-techs-new-tool-against-eu-regulation/> accessed 24 March 2025

'Artificial Intelligence for the American People' <https://trumpwhitehouse.archives.gov/ai/> accessed 25 March 2025

Ball J and Hopkins N, 'GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief' *The Guardian* (20 December 2013) <https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner> accessed 4 December 2024

Baratta R, 'European Commission Fines Microsoft for Non-Compliance with Browser Choice Commitments: A First Timer' (2013) 4 Journal of European Competition Law & Practice 415

Blogs MC, 'Microsoft and OpenAI Evolve Partnership to Drive the next Phase of AI' (*The Official Microsoft Blog*, 21 January 2025) <https://blogs.microsoft.com/blog/2025/01/21/microsoft-and-openai-evolve-partnership-to-drive-the-next-phase-of-ai/> accessed 27 March 2025

'Brave Leo AI' (*Brave*) <https://brave.com/leo/> accessed 27 March 2025

'Can EU Laws Hold against Big Tech's Power Play?' (*ctech*, 20 February 2025) <https://www.calcalistech.com/ctechnews/article/vglbleori> accessed 25 March 2025

Carugati C, 'The Generative AI Challenges for Competition Authorities' (2024) 59 Intereconomics 14

Centrum NCS, 'De werking van de CLOUD-Act bij dataopslag in Europa – Expertblogs – Nationaal Cyber Security Centrum' (16 August 2022) <https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa> accessed 19 April 2025

Chee FY and Chee FY, 'Airbus Leads Call for Europe to Create Sovereign Infrastructure Fund, Buy European' *Reuters* (17 March 2025) <https://www.reuters.com/business/aerospace-defense/airbus-others-call-sovereign-infrastructure-fund-buy-european-2025-03-17/> accessed 25 March 2025

'Commission Sends Preliminary Findings to Alphabet under the Digital Mar-

kets Act' (*European Commission – European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_811> accessed 27 March 2025

Coveri A, Cozza, Claudio and and Guarascio D, 'Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus' Review of Political Economy 1

Damen M, 'EU Strategic Autonomy Monitor'

Datta A, 'Trump Threatens to Launch Tariff Attack on EU Tech Regulation' (*Euractiv*, 22 February 2025) <https://www.euractiv.com/section/tech/news/trump-threatens-to-launch-tariff-attack-on-eu-tech-regulation/> accessed 25 March 2025

Diker Vanberg A, 'Generative AI & Competition Law Concerns: The New Kid on the Block!' [2024] COM&IP Insight 1

'EU Risks More Trump Tariffs in Looming Big Tech Crackdown' (*POLITICO*, 19 March 2025) <https://www.politico.eu/article/big-tech-crackdown-europe-donald-trump-tariffs-united-states-digital-competition/> accessed 24 March 2025

'Finally! Brave Brings Local AI to the Browser' (*It's FOSS News*, 25 September 2024) <https://news.itsfoss.com/brave-browser-local-ai/> accessed 27 March 2025

'France and Germany Unveil Docs, a Homegrown Alternative to Google Docs' (*TechSpot*, 20 March 2025) <https://www.techspot.com/news/107225-france-germany-unveil-docs-collaborative-tool-rival-us.html> accessed 25 March 2025

'Gemini – Chat to Supercharge Your Ideas' (*Gemini*) <https://gemini.google.com> accessed 24 March 2025

'Google's AI Search Gives Sites Dire Choice: Share Data or Die' *Bloomberg.com* (15 August 2024) <https://www.bloomberg.com/news/articles/2024-08-15/google-s-search-dominance-leaves-sites-little-choice-on-ai-scraping> accessed 27 March 2025

Goswami R, 'Apple Intelligence Won't Launch in EU in 2024 Due to Antitrust Regulation, Company Says' (*CNBC*, 21 June 2024) <https://www.cnbc.com/2024/06/21/apple-ai-europe-dma-macos.html> accessed 27 March 2025

Gstrein OJ, 'Data Autonomy: Recalibrating Strategic Autonomy and Digital Sovereignty' (2023) 28 European Foreign Affairs Review <https://doi.org/10.54648/eerr2023028> accessed 25 March 2025

Hammond G, 'Big Tech Outspends Venture Capital Firms in AI Investment Frenzy' *Financial Times* (29 December 2023)

Hanley D, 'A Topology of Multisided Digital Platforms' (Social Science Research Network, 20 June 2020) <https://papers.ssrn.com/abstract=3651606> accessed 24 March 2025

Hartmann T, 'Rival Report to Knafo's on EU Tech Sovereignty: More Content, More Cautious' (*Euractiv*, 15 March 2025) <https://www.euractiv.com/section/tech/news/rival-report-to-knafos-on-eu-tech-sovereignty-more-content-more-cautious/> accessed 19 April 2025

——, 'EPP, SD, Renew Table 309 Changes to Controversial EU Tech Sovereignty Report' (*Euractiv*, 22 March 2025) <https://www.euractiv.com/section/tech/news/epp-sd-renew-table-309-changes-to-controversial-eu-tech-sovereignty-report/> accessed 19 April 2025

——, 'Von Der Leyen Expresses Timid Support for Eurostack Tech Sovereignty Project' (*Euractiv*, 9 April 2025) <https://www.euractiv.com/section/tech/news/von-der-leyen-expresses-timid-support-to-sovereign-eurostack-project/> accessed 16 April 2025

——, 'European Industry Big Win: Germany, France Both Support Sovereign EU-Based Tech Infrastructure' (*Euractiv*, 10 April 2025) <https://www.euractiv.com/section/tech/news/european-industry-big-win-germany-france-both-support-sovereign-eu-based-tech-infrastructure/> accessed 16 April 2025

——, 'Against US Digital "predators," France Digital Minister Calls for a European "Pack Hunt"' (*Euractiv*, 15 April 2025) <https://www.euractiv.com/section/tech/news/against-us-digital-predators-france-digital-minister-calls-for-a-european-pack-hunt/> accessed 16 April 2025

Hendrikse R and others, 'The Big Techification of Everything' (2022) 31 Science as Culture 59

'Copilot in Edge' <https://www.microsoft.com/en-us/edge/features/copilot> accessed 24 March 2025

'Infographic: Amazon and Microsoft Stay Ahead in Global Cloud Market' (*Statista Daily Data*, 27 February 2025) <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers> accessed 24 March 2025

'Is Data the New Oil? Competition Issues in the Digital Economy | Think Tank | European Parliament' <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)646117> accessed 24 March 2025

Jennewine T, 'Nvidia Sells Graphics and AI Chips, but 15% of Sales Come From Other Multi-Hundred-Billion Dollar Markets' (*The Motley Fool*, 22 January 2024) <https://www.fool.com/investing/2024/01/22/nvidia-sells-ai-chips-15-sales-from-other-markets/> accessed 24 March 2025

'Learn about Proton and Our Vision for a Better Internet' (*Proton*) <https://proton.me/about-test-31012025-b/> accessed 25 March 2025

Leffer L, 'Your Personal Information Is Probably Being Used to Train Generative AI Models' (*Scientific American*, 1 March 2025) <https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/> accessed 24 March 2025

Manfredi R, 'Two Weeks In: Key Trump Administration Developments in Tech Policy' (*Gibson Dunn*, 5 February 2025) <https://www.gibsondunn.com/two-weeks-in-key-trump-administration-developments-in-tech-policy/> accessed 24 March 2025

Martens B, 'Why Artificial Intelligence Is Creating Fundamental Challenges for Competition Policy' (Bruegel Policy Brief 2024) Research Report 16/2024 <https://www.econstor.eu/handle/10419/302296> accessed 23 March 2025

Martin LL, *The Oxford Handbook of the Political Economy of International Trade* (Oxford University Press 2015)

'Meet Your New Assistant: Meta AI, Built With Llama 3' (*Meta*, 18 April 2024) <https://about.fb.com/news/2024/04/meta-ai-assistant-built-with-llama-3/> accessed 24 March 2025

'Meta AI Finally Comes to Europe after a Year-Long Delay, but with Some Limitations' (*Business Today*, 21 March 2025) <https://www.businesstoday.in/technology/news/story/meta-ai-finally-comes-to-europe-after-a-year-long-delay-but-with-some-limitations-468809-2025-03-21> accessed 27 March 2025

'Meta Platforms (Facebook) (META) – Cash on Hand' <https://companiesmarketcap.com/meta-platforms/cash-on-hand/> accessed 24 March 2025

'Microsoft (MSFT) – Cash on Hand' <https://companiesmarketcap.com/microsoft/cash-on-hand/> accessed 24 March 2025

Morreale F and others, 'The Unwitting Labourer: Extracting Humanness in AI Training' (2024) 39 AI & SOCIETY 2389

'New McKinsey Survey Reveals the AI Tech-Talent Landscape' <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-reinvents-tech-talent-opportunities> accessed 24 March 2025

Panay P, 'Introducing Alexa , the next Generation of Alexa' (26 February 2025) <https://www.aboutamazon.com/news/devices/new-alexa-generative-artificial-intelligence> accessed 24 March 2025

Peters J, 'Former Head of NSA Joins OpenAI Board' (*The Verge*, 13 June 2024) <https://www.theverge.com/2024/6/13/24178079/openai-board-paul-nakasone-nsa-safety> accessed 26 June 2024

Poitras L, Rosenbach M and Stark H, 'Secret NSA Documents Show How

the US Spies on Europe and the UN' *Der Spiegel* (26 August 2013) <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> accessed 25 March 2025

published WM, 'European Cloud Market Is Being Dominated by Three Big Players' (*TechRadar*, 30 September 2022) <https://www.techradar.com/news/european-cloud-market-is-being-dominated-by-three-big-players> accessed 25 March 2025

Ramos G, 'Application of the CLOUD Act to EU Entities' <https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo>

Reuters, 'NSA Tapped German Chancellery for Decades, WikiLeaks Claims' *The Guardian* (8 July 2015) <https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel> accessed 25 March 2025

Roth A, 'Stunning Signal Leak Reveals Depths of Trump Administration's Loathing of Europe' *The Guardian* (25 March 2025) <https://www.theguardian.com/world/2025/mar/25/stunning-signal-leak-reveals-depths-of-trump-administrations-loathing-of-europe> accessed 25 March 2025

'Schleswig-Holstein.de – Linux Plus 1 – Die Open Innovation Und Open Source Strategie Des Landes Schleswig-Holstein (Stand: November 2024)' <https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Projekt/open-source-strategie> accessed 25 March 2025

Schmon C, 'Saving the Internet in Europe: Fostering Choice, Competition and the Right to Innovate' (*Electronic Frontier Foundation*, 25 March 2025) <https://www.eff.org/deeplinks/2025/03/saving-internet-europe-fostering-choice-competition-and-right-innovate> accessed 27 March 2025

Sterling B, 'So, It Was the NSA in the Greek Phones All Along' *Wired* <https://www.wired.com/beyond-the-beyond/2015/10/nsa-greek-phones-along/> accessed 25 March 2025

Sterling T, 'Dutch Parliament Calls for End to Dependence on US Software Companies' *Reuters* (19 March 2025) <https://www.reuters.com/world/europe/dutch-parliament-calls-end-reliance-us-software-2025-03-18/> accessed 25 March 2025

Sullivan M, 'Big Tech Is on a Generative AI Hiring Spree' (*Fast Company*, 15 April 2024) <https://www.fastcompany.com/91092373/big-tech-is-on-a-generative-ai-hiring-spree> accessed 24 March 2025

'The Browser That Puts You First' (*Brave*) <https://brave.com/> accessed 27 March 2025

'Topic: Google, Amazon, Meta, Apple, and Microsoft (GAMAM)' (*Statista*) <https://www.statista.com/topics/4213/google-apple-facebook-amazon-and-microsoft-gafam/> accessed 24 March 2025

'Trump Fires Back at EU Tech Regulation' (9 March 2025) <https://www.lemonde.fr/en/economy/article/2025/03/09/trump-fires-back-at-eu-tech-regulation_6738972_19.html> accessed 24 March 2025

van de Waerdt P, *Data Is Power: On the Fundamental Connections between Data Protection Law and Competition Law as Applied to the Digital Market* (University of Groningen 2024)

van den Boom J and others, 'Towards Market Investigation Tools in Competition Law: The Case of the Netherlands' (2023) 14 Journal of European Competition Law & Practice 553

Vipra J, 'Computational Power and AI' (*AI Now Institute*, 27 September 2023) <https://ainowinstitute.org/publication/policy/compute-and-ai> accessed 24 March 2025

von Thun M and Hanley D, 'Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All' (Social Science Research Network, 17 October 2024) <https://papers.ssrn.com/abstract=4990780> accessed 16 March 2025

'Which Tech Titans Attended Donald Trump's Inauguration?' (*euronews*, 12:41:06 01:00) <https://www.euronews.com/next/2025/01/18/donald-trumps-inauguration-which-tech-leaders-will-be-attending-and-who-will-skip-it> accessed 24 March 2025

Wold JW, 'Big Tech Is Asking Trump to Fight EU AI Regulation' (*Euractiv*, 24 March 2025) <https://www.euractiv.com/section/tech/news/big-tech-is-asking-trump-to-fight-eu-ai-regulation/> accessed 26 March 2025

——, 'Virkkunen Confirms a Chips Act 2.0 and Outlines AI Action Plan' (*Euractiv*, 26 March 2025) <https://www.euractiv.com/section/tech/news/virkkunen-confirms-a-chips-act-2-0-and-outlines-ai-action-plan/> accessed 27 March 2025

'You May Have Heard Data Is the New Oil. It's Not' (*World Economic Forum*, 10 January 2018) <https://www.weforum.org/stories/2018/01/data-is-not-the-new-oil/> accessed 24 March 2025

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

——, 'Surveillance Capitalism or Democracy? The Death Match of Institutional

Orders and the Politics of Knowledge in Our Information Civilization' (2022) 3 Organization Theory 26317877221129290

Google LLC and Alphabet Inc v European Commission [2024] ECJ Case C-48/22 P

Microsoft Corp v Commission of the European Communities [2007] GC Case T-201/04

Treaty on the Functioning of the European Union (TFEU) [2008] OJ C 115/47

Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) (Text with EEA relevance) 2004 (OJ L)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) 2022 (OJ L)

About the author

Luke Crofton Arbuthnot

Luke Crofton Arbuthnot completed the LLM in Technology Law and Innovation (cum laude) at the University of Groningen in 2026. He is a Certified Information Privacy Professional and pursuing qualification as an English and Welsh Solicitor, with the aim of working in the technology, media and telecommunications practice area.

CHAPTER 15: TRACING FLIGHT LINES BETWEEN TIMES: A MINIMAL INSIGHT INTO THE CONTEMPORARY REALITY OF DATA COLONIALISM IN LATIN AMERICA

Eduardo Aguirre Mercado

> *Decolonizing is tracing flight lines between times and strange stories [...] learning to coexist with the fractured stories of the past, yes, but also with the new possibilities that emerge.*[1]
>
> Name Villa del Ángel.

1. Introduction

Colonialism and data protection are opposites. The former implied discrimination based on what the GDPR considers sensitive data nowadays, such as race and ethnicity.[2] Additionally, as Latin America shows, colonialism was all about exclusion from resources that derived from this discrimination. Acade-

1. Name Villa del Ángel y Animal Político. '¿Puede "Avatar: La Legenda de Aang" enseñarnos a decolonizar? ¿La descolonización es un proceso creativo?'. (*Instagram,* 29 October 2024) <https://www.instagram.com/reel/DBsEnczMg2o/?igsh=MWwyMTlwc2kzZHdxZQ==>, accessed 3 March 2025.

2. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, art 9.

mic Norma Castillo Palma described the following context in Spanish colonies between the 15th and the 19th centuries:[3]

> The Spaniards [constituted], in some way, a kind of privileged estate. Only noble Indians were equated with the Spaniards, which allowed them to dress in their own manner, carry weapons, ride horses, and attend prestigious schools—in other words, enjoy the same privileges as the Spaniards. However, in practice, many Spaniards of plebeian origin were considered superior to [indigenous nobles], which should not have happened according to the conventions of the time. Thus, the Indians were considered free but vassals of the King of Spain, which obligated them to pay tribute due to their classification as destitute. Meanwhile, slaves and their descendants were excluded because slavery was regarded as disgraceful. Consequently, as indigenous people intermingled with slaves or remained within their own groups, over time, by the late 18th century, an individual's status came to be identified with their skin color.[4]

As Palma highlighted, ethnicity and social status were enough for colonizers to place a person in particular schools, clothing, and jobs. However, while there was oppression towards Indigenous people and slaves based on their characteristics (a.k.a. pre-20th-century processing of personal data), Spanish colonizers exploited Indigenous knowledge and culture to obtain benefits and development in several fields, such as agriculture, tool production, and techniques of fishing.[5] Can there be parallels between these historical injustices and the modern development of new technologies?

---

3. David Bushnell and Robert A. Kittleson, 'History of Latin America' (*Britannica,* March 17th, 2025) <https://www.britannica.com/place/Latin-America> accessed 18 March 2025.

4. Norma Castillo Palma, 'La discriminación por el color de piel, la raza o el origen es un rezago colonial.' (*PUCP*, 26 June 2017) < https://puntoedu.pucp.edu.pe/voces-pucp/la-discriminacion-por-el-color-de-piel-la-raza-o-el-origen-es-un-rezago-colonial/> accessed 18 March 2025.

5. Prof. Dr. Corinne Hofman (Leiden University), 'Indigenous knowledge was key to the European colonisation of the Americas.' (*Universiteit Leiden*, 13 February 2018) <https://www.universiteitleiden.nl/nexus1492/news/indigenous-knowledge-was-key-to-the-european-colonisation-of-the-americas> accessed 18 March 2025;'a.k.a.' stands for 'also known as.'

Academics Nick Couldry and Ulises Mejías defined the term '*data colonialism*' as the '*process by which governments, non-governmental organizations[,] and corporations claim ownership of and privatize the data that is produced by their users and citizens*.'[6] To exemplify this phenomenon in a contemporary example, Harvard Law Review mentioned the case of Getty Images v. Stability AI in the United States. In 2023, Getty Images claimed to the District Court of Delaware that Stability AI—creators of the artificial intelligence (*AI*) art generator Stable Diffusion—had '*copied more than 12 million images from its database "without permission… or compensation… as part of its efforts to build a competing business*",' infringing on copyright and trademark protections.[7] Beyond the elements of abuse and violation of consent this case displays, this is an incident of data colonialism because it exemplifies the concentration of data within the servers of a Global North company.[8] However, data colonialism also shows that the discussion around the development of AI and new technologies should not be limited to how they affect intellectual property and entrepreneurship. It should also analyse how new technologies deepen existing systemic inequalities and prove that colonialism is a current problem rather than a historical one.

Couldry and Mejías mentioned that traditional colonialism has four main characteristics: *'(I) the appropriation of resources; (II) the formation of new social orders; (III) an extreme concentration of wealth; and (IV) the creation of ideologies to justify the appropriative practices*.'[9] The motif behind the term '*data colonial-*

---

6. 'Data Colonialism and Data Sets' (*Harvard Law Review,* 22 June 2023) <https://harvardlawreview.org/blog/2023/06/data-colonialism-and-data-sets/>, accessed 18 March 2025.

7. James Vincent, 'Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement.' (*The Verge*, 6 February 2023) <https://www.theverge.com/2023/2/6/23587393/ai-art-copyright-lawsuit-getty-images-stable-diffusion> accessed 18 March 2025.

8. Stability AI. 'Privacy Policy'. (*Stability AI,* 31 July 2025) <https://stability.ai/privacy-policy> accessed 20 September 2025.

9. Dieter Decraene, '"Data Colonialism" and the ubiquitous appropriation of human life.'

ism' comes from the idea that modern authorities and companies extract data under these conditions: they value profit and dominance over the welfare of consumers, data subjects, and art creators alike. To analyse data colonialism's development in Latin America, this essay will briefly examine: (i) how new technologies have mined resources, data, and knowledge in the region; (ii) how they exclude indigenous perspectives in their design; and (iii) how opacity in their algorithms has contributed to the extractive and violent concentration of data in a neocolonialist manner. To examine these points, this essay will undertake a literature review that analyses (i) the academic and philosophical reflection from worldwide authors, including Global South writers, and (ii) the recompilation of quantitative studies that prove data colonialism has negative quantifiable consequences for Global South countries and communities.

2. Colonialism over Resources, Data, and Knowledge

New technologies are not distant from the colonial resource extraction that history books describe. After all, as Couldry and Mejías have pointed out, one of the principal phenomena that colonialism displays is '*land grab*.'[10] For instance, in 2023, Microsoft-backed OpenAI extracted water from the '*Raccoon and Des Moines rivers in central Iowa[,] to cool a powerful supercomputer as it helped teach its AI systems how to mimic human writing*.'[11] In general, from 2021 to 2022, Microsoft's water consumption rose 34% from 2021 to 2022 due to its devel-

---

(*KU Leuven,* 26 July 2022) < https://www.law.kuleuven.be/citip/blog/data-colonialism-and-the-ubiquitous-appropriation-of-human-life/> accessed 26 July 2022.

10. Tech Won't Save Us. 'The Threat of Data Colonialism w/Ulises A. Mejías & Nick Couldry.' (24 October 2024) <https://open.spotify.com/episode/6JWjztgf6sLIjMahnetBEm?trackId=0fQuzbQNLcD1ofo7B2NcFI> accessed 18 March 2025.

11. Matt O'Brian and Hannah Fingerhut, 'Artificial intelligence technology behind ChatGPT was built in Iowa — with a lot of water.' (*AP,* 9 September 2023) < https://apnews.com/article/chatgpt-gpt4-iowa-ai-water-consumption-microsoft-f551fde98083d17a7e8d904f8be822c4> accessed 18 March 2025.

opment of AI.[12] The amount of water Microsoft used in 2022 is enough to fill '*2,500 Olympic-sized swimming pools*', or to supply 155,251 people with water in a year.[13] Further tying AI-driven water extraction to colonialism, ChatGPT also extracts water from Mexican states, like Querétaro, to install data centers. As AI expert, Ana Valdivia, stated, *'[d]ata centers are extracting drinking water for their economic businesses, whereas* [people] *walk almost a day to water his beans and nixtamal [used to make tortillas]*.'[14] Additionally, AI chips require more energy and minerals to be produced.[15] This rapid growth puts into question where AI developers will extract the necessary resources to satisfy global demand, which may increase the extraction of valuable resources beyond the Global North.

Beyond its production, new technologies are also extractive by design. For example, social media in Latin America has skyrocketed. Nineteen countries in the region have noticed a penetration of over 50% in social media as of 2023.[16] What do Facebook, Instagram, TikTok, YouTube, X, WeChat, and WhatsApp all have in common in the region? They all store their users' names, phone numbers, locations, devices, operative systems, browsers, IP addresses, and their use of further websites and apps.[17] This is colonialism because it concentrates the generation of global data—which universally expresses all aspects of the

12. Ibid.

13. O'Brian and Fingerhut (n 10); calculated based on information found in: This N That. 'Water Consumption Statistics.' (*PRB Magazine*, 30 September 2022) <https://www.prb-plus.com/water-consumption-statistics/> accessed 18 March 2025.

14. Gerry McGovern, Sue Branford, 'Critics fear catastrophic energy crisis as AI is outsourced to Latin America.' (*Mongabay,* 21 March 2024) <https://news.mongabay.com/2024/03/critics-fear-catastrophic-energy-crisis-as-ai-is-outsourced-to-latin-america/> accessed 18 March 2025.

15. Ibid.

16. Ricardo DiCarlo and Álvaro Moncada Niño, 'Herencia del pasado, desafíos del presente. Colonialismo de datos contemporáneo.' (*SCIELO Uruguay*, 1 June 2024) <http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301-15132024000101203> accessed 18 March 2025.

17. Ibid.

users' personality, such as political ideals, music taste, relationships, and lifelong text messages, among other data—in servers controlled by China and the Global North. Organizations like UNESCO have reported this data extraction has a differentiated impact on Global South countries, since it fosters existing inequalities, strengthens their digital dependency on Global North countries that concentrate online platforms, and brings an inequality of regulation in cross-border data flows.[18]

When it comes to Indigenous extraction of data, it has sometimes functioned to the preservation of Indigenous languages and cultures in Latin America. For example, AI helped to create an educational app to teach the Mixtec language in Oaxaca, Mexico.[19] Furthermore, Google Arts & Culture helped to develop Woolaroo, an app aimed at recognising objects portrayed in phone cameras and naming them in the Mayan and Tepehuan languages, spoken by over 800,000 people.[20] However, examples outside of Latin America show the risks of AI being in contact with Indigenous legacy.

OpenAI's Whisper harvested 1,381 hours of Māori-language audio. While Reuters pointed out this could be beneficial to preserve Indigenous languages, Māori ethicist Karaitiana Taiuru affirmed that '*[d]ata is like [...] land and natural resources*,' warning that if '*Indigenous peoples don't have sovereignty of their own data, they will simply be re-colonised in this information society*.'[21] These examples show that, even though AI systems are not always properly trained to

18. Bitange Ndemo, 'Addressing digital colonialism: A path to equitable data governance'. (*UNESCO Inclusive Policy Lab,* 8 August 2024) <https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance> accessed 20 September 2024.

19. Edin Noé López, 'Inteligencia artificial, TICs y pueblos indígenas.' (*BID*, 20 February 2024) <https://blogs.iadb.org/igualdad/es/culturas-milenarias-y-tic/> accessed 18 March 2025.

20. Ibid.

21. Rina Chandran, 'FEATURE-Indigenous groups in NZ, US fear colonisation as AI learns their languages.' (*Reuters,* 3 April 2023) < https://www.reuters.com/article/business/media-telecom/feature-indigenous-groups-in-nz-us-fear-colonisation-as-ai-learns-their-languag-idUSL8N2UQ0EC/> accessed 19 March 2025.

fully comprehend Indigenous language and use Indigenous data with consent, deployers still show a will to exploit massive amounts of information relating to several Indigenous cultures around the world. Neocolonialism in a fully digital landscape.

To prevent these exploitations in the region, deployers who work in Latin America must ensure the consent of Indigenous communities while extracting the latter's data and knowledge. In the spirit of avoiding these incidents in the region, intergovernmental organizations (IGOs) have launched efforts to recognize Indigenous knowledge in '*medicine, agriculture,* [and] *astronomy*', amongst other topics, while proposing public policies incorporating Indigenous perspectives and ethical guidelines into AI regulation.[22] An example is the report *Artificial Intelligence Focused on Indigenous Peoples: Perspectives from Latin America and the Caribbean*, issued by the United Nations Economic, Social, and Cultural Organization (UNESCO). The report issued recommendations for governmental institutions, civil society, tech companies, academia, and other IGOs, which include (i) promoting Indigenous communities' access to Information and Communications Technology (ICT); (ii) letting Indigenous communities develop technology through fostering new spaces of open innovation; (iii) using open lines of code to increase the existing content in Indigenous languages; (iv) undertaking interdisciplinary research on the development of AI from Indigenous-led academic communities; and (v) involving international organisms in the monitoring, capacitation and job-creation on Indigenous-led tech use and development.[23]

The report stands out because it introduced the concept of '*artificial wisdom*': the idea that, beyond intelligence, AI systems must represent the technological necessities in a fast-changing society, learning '*from past experiences and self-correct*;' exhibiting '*ethical, compassionate, and unbiased behavior*;' and perceiving '*human emotions to assist users in regulating them and making wise decisions*.'[24] The report also suggests the application of ethical design in all the

22. UNESCO. 'Inteligencia artificial centrada en los pueblos indígenas: perspectivas desde América Latina y el Caribe' (unesdoc.unesco.org, 2023), p 6.

23. UNESCO (n 22) p. 6.

24. Ibid, p 23.

stages of AI development, as well as the everlasting respect for Indigenous sovereignty in these processes.[25] UNESCO's contributions are compelling because they tie the design of ethical AI systems directly to anticolonial practices.

3. Innovative Technologies: Exclusion of Indigenous Perspectives

Yásnaya Elena –a recognised linguist from Ayutla Mixe, Mexico– came up with the concept of *tequiology.* In Nahuatl, the Aztec language spoken before the Spaniards arrived in modern-day Mexico City, the word *tequitl* stands for a '*collaborative effort*' to build necessary mechanisms for survival and thrive, from water management systems to cultural representation through artistic pieces.[26] Subsequently, tequiology regards technology as a modern means of union amongst Indigenous communities, '*not as consumable goods, but as means of resisting colonial imposition* [amid] *an unprecedented climate crisis*.'[27] Yásnaya's observations are also relevant because they highly contrast Indigenous perspectives in Latin America with current debates happening in the Global North, namely Europe. Yásnaya is critical of the concept of development and '*perpetual economic growth*', since it uses technology, not as a means to improve collective well-being, but as a tool to promote massive consumption.[28] In comparison, reports such as *The Future of European Competitiveness* have criticized European laws, like the General Data Protection Regulation (GDPR), for preventing wealth accumulation through electronic databases and under-

25. Ibid, p 24.

26. Yásnaya Elena Aguilar Gil, 'A modest proposal to save the world'. (*Rest of World,* 9 December 2020) <https://restofworld.org/2020/saving-the-world-through-tequiology/> accessed 3 March 2025.

27. Ibid.

28. Ibid; European Commission. 'The future of European competitiveness Part A | A competitiveness strategy for Europe.' (commission.europa.eu, 2024).

mining '*the EU's digital goals*.'[29] Indigenous perspectives similar to Yásnaya's do not denounce an impediment to innovation but address the lack of social, not profit-oriented drive behind technological development.

Beyond the aforementioned UNESCO report, outside Latin America, Indigenous activists—among them Native Americans—have developed self-managed guidelines that voice their concerns further than organizations such as UNESCO. For example, in 2020, Indigenous communities from Aotearoa, Australia, North America, and the Pacific drafted the Indigenous Protocol and Artificial Intelligence, whose purpose is to introduce the Guidelines for Indigenous-centered AI Design and to make '*non-Indigenous technologists and policy-makers [...] start a productive conversation with Indigenous communities about how to enter into collaborative technology development efforts*.'[30] As part of the papers that complemented the Protocol, Dr. Noelani Arista stated that technology often leaves '*Native people out of its imaginary.*'[31] Arista also highlighted a double-morality contradiction that exemplifies the modern unfairness of data colonialism.

There are no compulsory educational programs in place that will teach Native children to code, or create through the mediums of VR, AR, video gaming, or imagine futures through the intricacies of AI shaped by Native norms. [Cultivating data sovereignty] will require [a] deep study of language, history, social relations, and customary [knowledge] which have often been negatively impacted by colonial processes. [However,] the textual, auditory, and film archives function already as a living source of artificial intelligence. The textual archives [...] are an unsynthesized mass of documents, comprised of compositions once maintained orally and committed to writing and print. Added to this mass are newly composed oral genres of chant, prayer, and song, letters, journals, newspapers, reports, the official business of government, [and] books.

29. European Commission (n 26), p. 69.

30. Jason Edward Lewis, 'Indigenous Protocol and Artificial Intelligence Position Paper.' (*CIFAR,* 2020) <https://spectrum.library.concordia.ca/id/eprint/986506/7/Indigenous_Protocol_and_AI_2020.pdf> accessed 18 March 2025, p 12.

31. Ibid, p 102.

Though [the] Hawaiian language is endangered in the world of everyday modern speech, it thrives on the page.[32]

As another example in the American continent, developer Corbett tried to incorporate the Cree language into its AI model. However, the algorithmic structure of English-language programming made it difficult to fully express grammatically and syntactically correct sentences. According to academic Yaw Ofosu-Asare, '*[t]o accommodate [Indigenous] languages, AI algorithms require substantial modification and a richer dataset, which is often lacking for [Indigenous] languages.*'[33] Arista's explanation is relevant in a Latin American context because it establishes how, despite having limited access to artificial intelligence, Indigenous communities often struggle to fight the data extraction that new technologies undertake from their cultural heritage. If not careful enough, Latin American communities may be added to the list of further examples.

Moreover, Latin America still faces a considerable digital gap. 200 million Latin Americans remain offline, which already reduces the ability of Indigenous communities to detect any abuse that they may collectively suffer with a massively increasing extraction of data at a regional level.[34] According to UNESCO, populations outside cities have less access to Internet, since '*urban households are 7% to 33% more likely (depending on the country) of having Internet connection compared to rural households*.'[35] Furthermore, language is one of the main factors that contribute to the digital gap. UNESCO has highlighted that Spanish dominates online content, stating that '*an estimated 40 million people in the region speak an indigenous language,* [which] *are grossly under-repre-*

32. Indigenous Protocol (n 28), p 103.

33. Yaw Ofosu-Asare, 'Cognitive imperialism in artificial intelligence: counteracting bias with indigenous epistemologies.' (*Springer Nature Link*, 19 September 2024) <https://link.springer.com/article/10.1007/s00146-024-02065-0> accessed 18 March 2025, p 9.

34. UNESCO. 'Policy Papers UNESCO: Digital Society: Gaps and Challenges for Digital Inclusion in Latin America and the Caribbean.' (unesdoc.unesco.org, 2024), p 5.

35. Ibid, p 12.

sented on the Internet.'[36] Additionally, UNESCO reported that, for a non-Spanish speaker, '*the likelihood of using the Internet diminishes between 8% (Ecuador) and 31% (Paraguay)*.'[37] Even though technology and colonialism might seem opposite due to their position in history, they are interlinked. While technology extracts massive amounts of data worldwide, it has not been able to provide equal benefits across the globe, especially for marginalized communities.

4. Opacity: Is It Also Colonialism?

There are risks to making AI algorithms fully open source, including '*upstream intellectual property concerns, viral software issues, and non-infringement warranties or intellectual property (IP) indemnity issues*.'[38] However, a consequence of not knowing how AI codes are wired is that they may promote discrimination without a traceable explanation. The risk with this discrimination is that it fosters practical experiences of modern, digital colonialism. For example, OpenAI's Terms of Use point out that their chatbots may produce '*incomplete, incorrect, or offensive Output that does not represent OpenAI's views*.'[39] ChatGPT has shown racial biases when describing fictional crime stories.[40] Furthermore, it has demonstrated gender bias in low-resource languages, such as Turkish and Malay, and it has further tied Muslims to terrorists in some of its answers.[41]

---

36. Ibid, p 12.

37. Ibid, p 12.

38. David Bahn and Dan Dresser, 'Liability and Control Risks with Open Source Software.' (*IEEEXplore*, 16-19 October 2006) <https://ieeexplore.ieee.org/abstract/document/4266334> accessed 19 March 2025.

39. 'Terms of Use' (*OpenAI,* 11 December 2024) < https://openai.com/policies/row-terms-of-use/> accessed 19 March 2025.

40. Craig Piers, 'Even ChatGPT Says ChatGPT Is Racially Biased.' (*SCIAM*, 7 February 2024) <https://www.scientificamerican.com/article/even-chatgpt-says-chatgpt-is-racially-biased/> accessed 19 March 2025.

41. Shangying Hua, Shuangci Jin, and Shengyi Jiang, 'The Limitations and Ethical Consid-

This displays a trait large language models may portray: toxicity. Toxic content in AI systems is based on '*biased and discriminatory training data and biased prompts datasets*', influenced mainly by the will of English-speaking input.[42] Aren't these outputs forming a new social order, like Couldry and Mejías warned data colonialism does? Aren't they creating ideologies, not necessarily to justify appropriative practices, but in the process of doing them? The social consequence of not exposing or regulating the functioning of AI algorithms is that their opacity becomes a tool for data colonialism to thrive.

Latin America is especially vulnerable to this. Neither Argentina, Colombia, Chile, Mexico, Peru, nor Brazil have a comprehensive approved AI Bill.[43] These countries have isolated bill proposals in their respective Congress or parliamentary bodies, but none have passed and most are not government-proposed.[44] Furthermore, according to the Latin American Intelligence Index, aside from the aforementioned countries, only Uruguay shows an AI readiness level superior to 50%. For example, Costa Rica shows a 33.41% level and Bolivia has a 15.1% level.[45] Therefore, Latin American countries lack a legal framework to identify high-risk AI systems, demand transparency from them, and draft legal dispositions that prevent the worst effects of data colonialism from happening.

---

erations of ChatGPT.' (2020) 6(1) Data Intelligence 219 <https://doi.org/10.1162/dint_a_00243>.

42. Ibid, 218.

43. Andrés Mosqueira & Shanty Emmanuel Rubio González, 'Foster innovation or mitigate risk? AI regulation in Latin America.' (*White & Case,* 18 November 2024) <https://www.whitecase.com/insight-our-thinking/latin-america-focus-2024-ai-regulation> accessed 18 March 2025.

44. Ibid.

45. Ibid.

5. Conclusion

New technologies can democratise societies but they also deepen their inequalities. Data colonialism established a relationship of dominance from the Global North to the Global South, ever since the extraction of resources needed to satisfy the technological demand that exists nowadays. As exemplified by Mexico, the amount of water and minerals needed to establish AI data centers and interconnected devices may create an unequal concentration of wealth that benefits dominant undertakings in Global North countries. Amid the climate crisis emergency, the development of these technologies may create sustainability issues. Furthermore, there are two problems: on the one hand, the input of data may be based on knowledge exploitation, linguistic deficiency, and extensive profiling of users' personalities, which is mostly concentrated on American and Chinese-based companies. However, on the other hand, when these technologies generate output, like AI, they may create discriminatory, biased content, which Latin America does not have the governmental or systemic framework to combat. The most useful guidance is to follow guidelines where Indigenous people have collaborated, where they exhort tech developers to follow the principles of tequiology. In Indigenous protocols, we can find a philosophical reflection concerning the elevation of AI to artificial wisdom, considering the ethical development of technology and the priority of collective benefit over profit and innovation. These observations may contrast with European debates on innovation, cybersecurity, and the protection of trade secrets. However, this essay shows that the debates around technology do change in light of existing inequalities. Tracing flight lines is, therefore, necessary to combine the protection of innovation and subjects' rights with the current issues that historically press Latin America and the Global South.

Bibliography

Aguilar Gil, Yásnaya Elena, 'A modest proposal to save the world' (*Rest of World,* 9 December 2020) <https://restofworld.org/2020/saving-the-world-through-tequiology/> accessed 3 March 2025.

Bahn, David and Dan Dresser, 'Liability and Control Risks with Open Source Software.' (*IEEEXplore*, 16-19 October 2006) <https://ieeexplore.ieee.org/abstract/document/4266334> accessed 19 March 2025.

Bushnell, David, and Robert A. Kittleson, 'History of Latin America' (*Britannica,*

March 17th, 2025) <https://www.britannica.com/place/Latin-America> accessed 18 March 2025.

Castillo Palma, 'La discriminación por el color de piel, la raza o el origen es un rezago colonial.' (*PUCP*, 26 June 2017) <https://puntoedu.pucp.edu.pe/voces-pucp/la-discriminacion-por-el-color-de-piel-la-raza-o-el-origen-es-un-rezago-colonial/> accessed 18 March 2025.

Chandran, Rina, 'FEATURE-Indigenous groups in NZ, US fear colonisation as AI learns their languages.' (*Reuters,* 3 April 2023) < https://www.reuters.com/article/business/media-telecom/feature-indigenous-groups-in-nz-us-fear-colonisation-as-ai-learns-their-languag-idUSL8N2UQ0EC/> accessed 19 March 2025.

'Data Colonialism and Data Sets' (*Harvard Law Review,* 22 June 2023) <https://harvardlawreview.org/blog/2023/06/data-colonialism-and-data-sets/> accessed 18 March 2025.

Decraene, David, '"Data Colonialism" and the ubiquitous appropriation of human life.' (*KU Leuven,* 26 July 2022) <https://www.law.kuleuven.be/citip/blog/data-colonialism-and-the-ubiquitous-appropriation-of-human-life/> accessed 26 July 2022.

DiCarlo, Ricardo and Álvaro Moncada Niño, 'Herencia del pasado, desafíos del presente. Colonialismo de datos contemporáneo.' (*SCIELO Uruguay*, 1 June 2024) <http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301-15132024000101203> accessed 18 March 2025.

European Commission. 'The future of European competitiveness Part A | A competitiveness strategy for Europe.' (commission.europa.eu, 2024)

Hofman, Corinne (Leiden University), 'Indigenous knowledge was key to the European colonisation of the Americas.' (*Universiteit Leiden*, 13 February 2018) <https://www.universiteitleiden.nl/nexus1492/news/indigenous-knowledge-was-key-to-the-european-colonisation-of-the-americas> accessed 18 March 2025.

Hua, Shangying, Shuangci Jin, and Shengyi Jiang, 'The Limitations and Ethical Considerations of ChatGPT.' (2020) 6(1) Data Intelligence 201–239 <https://doi.org/10.1162/dint_a_00243>.

Lewis, Jason Edward, 'Indigenous Protocol and Artificial Intelligence Position Paper.' (*CIFAR,* 2020) <https://spectrum.library.concordia.ca/id/eprint/986506/> accessed 18 March 2025.

López, Edin Noé, 'Inteligencia artificial, TICs y pueblos indígenas.' (*BID*, 20

February 2024) <https://blogs.iadb.org/igualdad/es/culturas-milenarias-y-tic/> accessed 18 March 2025.

McGovern, Gerry, and Sue Branford, 'Critics fear catastrophic energy crisis as AI is outsourced to Latin America.' (*Mongabay,* 21 March 2024) <https://news.mongabay.com/2024/03/critics-fear-catastrophic-energy-crisis-as-ai-is-outsourced-to-latin-america/> accessed 18 March 2025.

Mosqueira, Andrés & Shanty Emmanuel Rubio González, 'Foster innovation or mitigate risk? AI regulation in Latin America.' (*White & Case,* 18 November 2024) <https://www.whitecase.com/insight-our-thinking/latin-america-focus-2024-ai-regulation> accessed 18 March 2025.

Ndemo, Bitange, 'Addressing digital colonialism: A path to equitable data governance'. (*UNESCO Inclusive Policy Lab,* 8 August 2024) <https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance> accessed 20 September 2024.

Ofosu-Asare, Yaw, 'Cognitive imperialism in artificial intelligence: counteracting bias with indigenous epistemologies.' (*Springer Nature Link*, 19 September 2024) <https://link.springer.com/article/10.1007/s00146-024-02065-0> accessed 18 March 2025.

O'Brian, Matt and Hannah Fingerhut, 'Artificial intelligence technology behind ChatGPT was built in Iowa — with a lot of water.' (*AP,* 9 September 2023) <https://apnews.com/article/chatgpt-gpt4-iowa-ai-water-consumption-microsoft-f551fde98083d17a7e8d904f8be822c4> accessed 18 March 2025.

Piers, Craig, 'Even ChatGPT Says ChatGPT Is Racially Biased.' (*SCIAM*, 7 February 2024) <https://www.scientificamerican.com/article/even-chatgpt-says-chatgpt-is-racially-biased/> accessed 19 March 2025.

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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Stability AI. 'Privacy Policy'. (*Stability AI,* 31 July 2025) <https://stability.ai/privacy-policy> accessed 20 September 2025.

Tech Won't Save Us. 'The Threat of Data Colonialism w/Ulises A. Mejías & Nick Couldry.' (24 October 2024) <https://open.spotify.com/episode/6JWjztgf6sLIjMahnetBEm?trackId=0fQuzbQNLcD1ofo7B2NcFI> accessed 18 March 2025.

This N That. 'Water Consumption Statistics.' (*PRB Magazine*, 30 September 2022) <https://www.prbplus.com/water-consumption-statistics/> accessed 18 March 2025.

UNESCO. 'Inteligencia artificial centrada en los pueblos indígenas: perspectivas desde América Latina y el Caribe' (unesdoc.unesco.org, 2023).

UNESCO. 'Policy Papers UNESCO: Digital Society: Gaps and Challenges for Digital Inclusion in Latin America and the Caribbean.' (unesdoc.unesco.org, 2024).

Villa del Ángel, Name and Animal Político. '¿Puede "Avatar: La Legenda de Aang" enseñarnos a decolonizar? ¿La descolonización es un proceso creativo?'. *Instagram,* 29 October 2024. <https://www.instagram.com/reel/DBsEnczMg2o/?igsh=MWwyMTlwc2kzZHdxZQ==>, accessed 3 March 2025.

Vincent, James, 'Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement.' (*The Verge*, 6 February 2023) <https://www.theverge.com/2023/2/6/23587393/ai-art-copyright-lawsuit-getty-images-stable-diffusion> accessed 18 March 2025.

About the author

Eduardo Aguirre Mercado

Eduardo Aguirre Mercado completed the LLM in Technology Law and Innovation at the University of Groningen. He currently works as Data Protection Manager Associate at MyData-Trust in Mexico.