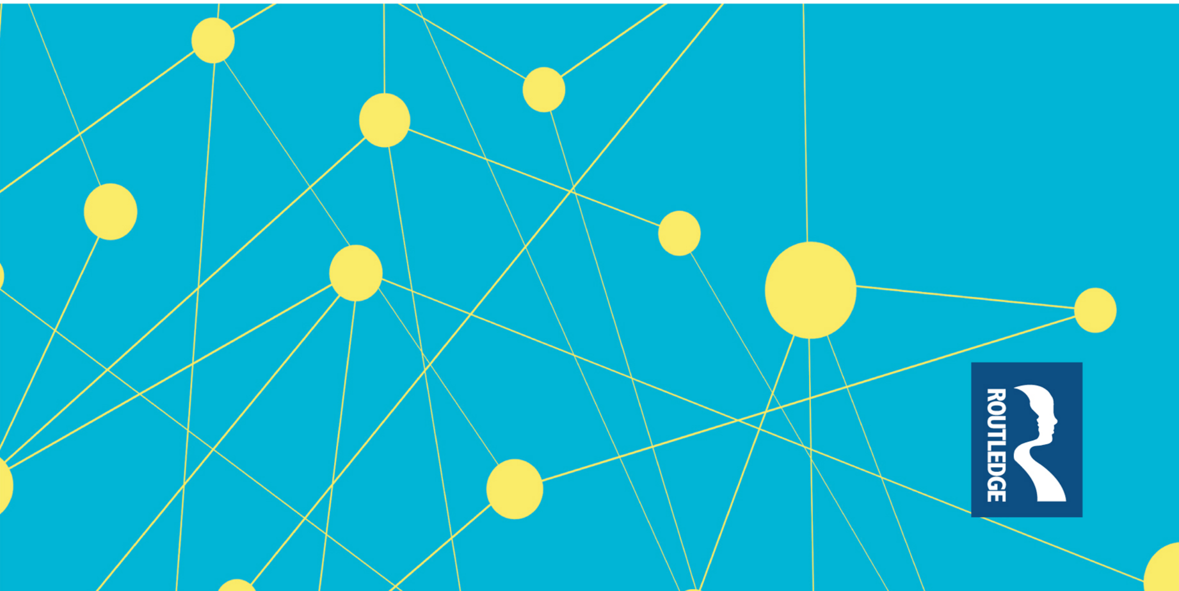
Routledge Research in the Law of Emerging Technologies

PRIVACY, DATA PROTECTION AND DATA-DRIVEN TECHNOLOGIES

Edited by
Martin Ebers and Karin Sein



Privacy, Data Protection and Data-driven Technologies

This book brings together contributions from leading scholars in law and technology, analysing the privacy issues raised by new data-driven technologies.

Highlighting the challenges that technology poses to existing European Union (EU) data protection laws, the book assesses whether current legal frameworks are fit for purpose, while maintaining a balance between supporting innovation and the protection of individuals' privacy. Data privacy issues range from targeted advertising and facial recognition, systems based on artificial intelligence (AI) and blockchain, and machine-to-machine (M2M) communication, to technologies that enable the detection of emotions and personal care robots.

The book will be of interest to scholars, policymakers and practitioners working in the fields of law and technology, EU law and data protection.

Martin Ebers is President of the Robotics & AI Law Society (RAILS) and Associate Professor of IT Law at the University of Tartu (Estonia). He taught and presented at more than 100 international conferences, is a member of several national and international research networks and published 16 books and over 120 articles in the field of law and technology, especially artificial intelligence, as well as in commercial, private, European, comparative and international law. His latest books include *Algorithms and Law* (2020), *Algorithmic Governance and Governance of Algorithms* (2021), *Contracting and Contract Law in the Age of Artificial Intelligence* (2022) and the *Stichwortkommentar Legal Tech* (2023).

Karin Sein is a Professor of Civil Law in the Faculty of Law of the University of Tartu, Estonia. Her main research interests cover domestic and European contract law, consumer law, private international law and international civil procedure and also law and digitalisation. In recent years, she has provided expertise for the Estonian Ministry of Justice on implementing European consumer protection directives into Estonian contract law. During the Estonian EU Presidency in July–December 2017, she was acting as Chair for the Council Working Group for the Proposals of the Directive on Digital Content and of the Directive on Sale of Consumer Goods.

Routledge Research in the Law of Emerging Technologies

Regulating Artificial Intelligence
Binary Ethics and the Law
Dominika Ewa Harasimiuk and Tomasz Braun

Cryptocurrencies and Regulatory Challenge
Allan C. Hutchinson

Regulating Artificial Intelligence in Industry
Edited by Damian M. Bielicki

The Law of Global Digitality
Edited by Matthias C. Kettemann, Alexander Peukert and Indra Spiecker gen. Döhmann

Internet of Things and the Law
Legal Strategies for Consumer-Centric Smart Technologies
Guido Noto La Diega

Regulating the Metaverse
A Critical Assessment
Ignas Kalpokas and Julija Kalpokienė

The Regulation of Digital Technologies in the EU
Act-ification, GDPR Mimesis and EU Law Brutality at Play
Vagelis Papakonstantinou and Paul de Hert

Privacy, Data Protection and Data-driven Technologies
Edited by Martin Ebers and Karin Sein

For more information about this series, please visit: www.routledge.com/Routledge-Research-in-the-Law-of-Emerging-Technologies/book-series/LAWTECHNOLOGY

Privacy, Data Protection and Data-driven Technologies

Edited by Martin Ebers and Karin Sein

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2025
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Ebers, Martin, 1970- editor. | Sein, Karin, 1974- editor.
Title: Privacy, data protection, and data-driven technologies / edited by
Martin Ebers and Karin Sein.
Description: Abingdon, Oxon [UK] ; New York, NY : Routledge, 2024. |
Series: Routledge research in law of emerging technologies |
Includes bibliographical references and index.
Identifiers: LCCN 2024016100 (print) | LCCN 2024016101 (ebook) |
ISBN 9781032614472 (hardback) | ISBN 9781032820682 (paperback) |
ISBN 9781003502791 (ebook)
Subjects: LCSH: Privacy, Right of—European Union countries. |
Data protection—Law and legislation—European Union countries. |
European Parliament. General Data Protection Regulation. |
Technological innovations—Law and legislation—European Union
countries. | Blockchains (Databases)—Law and legislation—European
Union countries.
Classification: LCC KJE6071 .P755 2024 (print) | LCC KJE6071 (ebook) |
DDC 342.2408/58—dc23/eng/20240412
LC record available at https://lccn.loc.gov/2024016100
LC ebook record available at https://lccn.loc.gov/2024016101

ISBN: 978-1-032-61447-2 (hbk)
ISBN: 978-1-032-82068-2 (pbk)
ISBN: 978-1-003-50279-1 (ebk)

DOI: 10.4324/9781003502791

Typeset in Times New Roman
by Apex CoVantage, LLC

Contents

Contributors

Tommaso Corno is an Italian journalist and recent graduate of the Dickson Poon School of Law at King's College London. Having completed an LLB in Politics, Philosophy and Law in 2023, his interest in European jurisdictions will soon bring him to pursue Masters of Laws in Université Paris II Panthéon-Assas and La Sapienza in Rome as part of the *Juriste Européen* programme. His focus is on technological regulation, in particular within the field of artificial intelligence.

Mateja Durovic is a professor in contract and commercial law, and Co-Director of the Centre for Technology, Ethics, Law and Society (TELOS) at King's College London. Previous to this, he was an assistant professor (2015–2017) at the School of Law, City University of Hong Kong. The work of Dr. Durovic was published in leading law journals (*European Review of Private Law*, *European Review of Contract Law*, *Journal of Consumer Policy*) and by most prominent publishers (Oxford University Press, Hart Publishing). He is a member of the European Law Institute, Society of Legal Scholars and Society for European Contract Law.

Martin Ebers is President of the Robotics & AI Law Society (RAILS) and Associate Professor of IT Law at the University of Tartu (Estonia). He taught and presented at more than 100 international conferences, is a member of several national and international research networks and published 16 books and over 120 articles in the field of law and technology, especially artificial intelligence, as well as in commercial, private, European, comparative and international law. His latest books include *Algorithms and Law* (2020), *Algorithmic Governance and Governance of Algorithms* (2021), *Contracting and Contract Law in the Age of Artificial Intelligence* (2022) and the *Stichwortkommentar Legal Tech* (2023).

Federico Galli is a junior assistant professor at the Department of Legal Studies, University of Bologna. In 2021, he obtained a PhD in law, science and technology from the University of Bologna and in computer science from University of Luxembourg. During this period, he has gained research experiences in the field of computer law (in particular, privacy, data protection law, contract, and consumer law of AI) and in law and ethics of AI. He has published on Italian and international journals. He is currently involved in several projects in legal and ethical issues of computation and in legal informatics.

Giorgia Guerra is assistant professor in comparative private law at the School of Law of the University of Verona (Italy). She teaches comparative legal systems (law school program), and transnational and comparative law and technology (data science program). She has held the national qualification (habilitation) as second-level professor (associate) since August 2021. She has an extensive track record of publications with leading international publishers, particularly on disruptive technologies. Her latest book is *Redesigning Protection for Consumer Autonomy: The Case-study of Dark Patterns in European Private Law* (FrancoAngeli, 2023).

Mykyta Petik holds an LL.B degree from Taras Shevchenko Kyiv National University (2016), an LL.M degree from Ghent University (2017, cum laude), and an MA in IT law degree from Tartu University (2018, MFA scholarship). He is currently pursuing a PhD degree as an MSCA scholar at KU Leuven CiTiP focusing on privacy and cybersecurity in 5G networks. His professional experience includes consulting Estonian, U.S., and Ukrainian companies in matters of information technology and intellectual property law and working as a Senior Privacy Specialist for a major international company.

Kärt Pormeister is a legal scholar and practitioner whose work focuses on data protection and health law. Kärt obtained a LLM in health law as a Fulbright scholar from the University of Houston (Texas, USA). Her PhD thesis focused on transparency in genetic research, and after completing her PhD, Kärt served as the legal counsel of the Estonian Biobank. Prior to this, Kärt taught law at the University of Tartu and Tallinn University, and has practiced law both in the private sector as an attorney and in the public sector as a lawyer for the State Agency of Medicines.

Vera Lúcia Raposo is currently an assistant professor of law and technology at Nova School of Law in Lisbon, Portugal, where she is the leading researcher at FutureHealth, focused on the use of new technologies in healthcare. She was also a supervisor at the Centre for Medical Ethics and Law, University of Hong Kong and a collaborator of the National Yang Ming Chiao Tung University School of Law in Taiwan. She is the author of more than 100 studies, particularly in digital law (AI, data protection, metaverse) and biomedical law, many of which were published in indexed journals.

Peter Rott is a professor of civil law, commercial law and information law at the University of Oldenburg. Prior to this, he held positions as lecturer at the University of Sheffield, junior professor at the University of Bremen, associate professor at the University of Copenhagen, professor at the University of Kassel and visiting professor at the University of Ghent. Peter specialises in European private law and in German and European consumer law. Currently, he focuses on the effects of digitalisation on private law, on sustainable consumer law and on the enforcement of consumer law.

Galileo Sartor is a PhD student at Swansea University, Wales, Department of Computer Science. He obtained a bachelor's degree in computer engineering from the University of Bologna in 2019. His current research includes the analysis of risk-based approaches in socio-technical systems and AI- and logic-based knowledge representation in the legal context. He has published in Italian and international journals and is currently involved in projects in legal informatics and AI and law.

Karin Sein is a Professor of Civil Law in the Faculty of Law of the University of Tartu, Estonia. Her main research interests cover domestic and European contract law, consumer law, private international law and international civil procedure and also law and digitalisation. In recent years, she has provided expertise for the Estonian Ministry of Justice on implementing European consumer protection directives into Estonian contract law. During the Estonian EU Presidency in July–December 2017, she was acting as Chair for the Council Working Group for the Proposals of the Directive on Digital Content and of the Directive on Sale of Consumer Goods.

Gerald Spindler was a fully tenured professor of civil law, commercial and economic law, comparative law, and multimedia and telecommunication law at the University of Göttingen, mainly occupied with legal issues regarding e-commerce, i.e., Internet and telecommunication law. He was elected as a fully tenured member of the German Academy of Sciences, Göttingen, in 2004. He has published more than 20 books, commentaries and more than 400 papers in law reviews, as well as expert legal opinions. He was elected as general rapporteur for the bi-annual German Law Conference regarding privacy and personality rights on the Internet (2012).

Paul Vogel studied law at the University of Würzburg. Between 2017 and 2022, he was a graduate assistant at the Chair of Prof. Hilgendorf. As of 2018, he completed postgraduate studies in European Law at the University of Würzburg for which he attained a Master of Laws in European Law (LL.M. Eur.). He completed his legal clerkship from 2020–2022, graduating as a fully qualified lawyer in 2022. In his dissertation, he dealt with the compatibility of artificial intelligence with applicable data protection law. Since 2022, he is working as an attorney at the German law firm Noerr.

Wojciech Wiewiórowski is the European Data Protection Supervisor, the EU's independent data protection authority.

Monika Zalnieriute is a Senior Fellow at the Lithuanian Centre for Social Sciences. Monika's research on law and technology has been published widely and has been drawn upon by international organizations such as the Council of Europe, World Bank, the European Parliament and the World Health Organization. Monika's work has been translated into Mandarin, Russian and German, and has also appeared in international media outlets *such as BBC and the Guardian*. She is the co-editor of *Money Power and AI* (Cambridge University Press, 2023) and *Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press, 2024).

Preface

Privacy and data protection are cornerstones in any democratic society based on the rule of law and fundamental rights. Data protection is one of the last lines of defence for persons. The EU Charter is for everybody, not just EU citizens, and so Arts. 7 and 8 of the Charter on the rights to privacy and to data protection are there for all.

Neither privacy nor data protection are absolute rights, however; therefore, important objectives of general interest, such as internal security or public health, may justify limitations on its exercise. However, such limitations should be necessary and proportionate, and in any event must respect the essence of the fundamental rights and freedoms. The EU Court of Justice has provided us with a clear guidance in this regard – in a nutshell – the more serious interference with fundamental rights requires the more serious justification and stronger safeguards, and vice versa. Against this background, the actual policy challenge is to translate the legal requirements into practical steps and measures.

The authors of this book have been observing carefully how data protection and its application grows, develops and changes – not only in itself, but predominantly due to ever-changing context in which it is applied. This context, or rather contexts, are influenced in particular in recent years by a rapid technological advancement. In these observations we all make in the data protection community, there are two types of temptations: (1) to maintain the unwavering faith in effectiveness of data protection concepts irrespectively of the matter which they are facing, or (2) to approach each new technological development with an undocumented conviction that new regulatory approaches are immediately necessary.

The book does not fall into the trap of both fallacies. Instead, it engages with both, attempting to find evidence-based answers (be they normative or empirical); not shying away from questioning general views when evidence supports, and, equally, not afraid of reinforcing them when the analysis confirm.

An assessment of the realisation of the fundamental rights to privacy and to data protection in various sectors, or in different applications of technology, is key to understand whether the data protection laws in fact protect well the “data protection right.” Data protection being conceived as a framework law poses that its functioning in different aspects is key to determine whether a specific regulation or a specific intervention is needed or not. These are never instead of data protection laws, but on top of it, and the book is a welcome and much needed contribution in this regard, given how new technologies, or even certain “hype” around them, require careful attention and diligent analysis.

The book identifies such contexts both on the level of technologies and areas, e.g., biobanking or health data, where the EU lawmaker – especially in recent years – has focused its regulatory initiatives. And not coincidentally. The approaches taken by the EU lawmaker are par excellence a very good exemplification of data protection not precluding as such the creation of instruments aimed at achieving specific policy objectives through a use of data, as long as a tailor-made structure in place respects and ensures the fundamental rights to privacy and data protection.

The authors also reflect on and recognise the national contexts. These indeed cannot be overestimated. The EU nature of data protection laws (or new regulations such as AI Act) should not diminish our attention to the national contexts, be it in designing the letters of law on EU level, and not less importantly in terms of the governance structures and practical implementation and enforcement aspects – especially when a country has a pioneer experience in subject matter, as is the case with Estonia.

The constraints of the procedural nature of data protection law, and a critical take presented in the book on the limitations this procedural nature brings, remain an interesting and valuable angle, sometimes forgotten in the public debate that expects from data protection solving somehow all the problems of the digital world. Such limitations, however, remain for me “a feature, not a bug” – an opportunity to approach the variety of challenges stemming from different areas, different applications of technology, in a largely coherent (even if not perfect) way, a methodology, a mind-set, that does not preclude further regulatory interventions.

I would like to thank warmly all the contributors to this book, with special appreciation to Prof. Martin Ebers and Prof. Karin Sein.

Wojciech Wiewiórowski
European Data Protection Supervisor

Acknowledgements

This book is part of the “Geriatronics” project, a lighthouse initiative of the Munich Institute of Robotics and Machine Intelligence (MIRMI) at the Technical University Munich (TUM). The contributions in this book are mainly based on the presentations given at a two-day conference on “Privacy, Data Protection and New Technologies” held in Tallinn, Estonia, on 16–17 June, 2022, and funded by the ENLIGHT network. We would like to express our gratitude to Ms Tiina Jaksman, the coordinator of ENLIGHT in Tartu University, for her great help. We would also like to thank those who helped us to edit this book, especially Ms. Valeria Argento, Mr. Gabriel Udoh and Mr. Daniel Hauck.

During the production process of this book, a number of developments have taken place at the European level. In particular, the AI Act has been under negotiation since April 2021 and was not formally adopted until early 2024. While Chapter 1 was able to take this legislative development into account, the other chapters were already completed in mid-2023. Readers should therefore be aware of the changes made in the political agreement as enacted into law. Nevertheless, most of the legal observations are still relevant, as the AI Act is a horizontal instrument that applies in addition to existing EU data protection law.

Martin Ebers
Karin Sein

Part I

Introduction

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1 Data-driven Technologies

Challenges for Privacy and EU Data Protection Law*

Martin Ebers and Karin Sein

1.1 Introduction

The General Data Protection Regulation (GDPR),[1] which came into force in 2018, has become a landmark in the field of privacy and data protection, setting legally binding standards for the European Union (EU) and beyond.[2] Although the GDPR attempts to keep pace with technological and socio-economic changes – notably, by following the principle of technology neutrality[3] and providing for flexible, openly worded principles and articles – concerns have been growing in recent years as to whether the regulation is being outpaced by new technological developments and their use of data.[4]

Indeed, data-driven technologies introduce new privacy risks that are currently not (explicitly) addressed by European data protection law. The specific characteristics of data-driven technologies pose significant challenges to current data protection law, in particular due to: (i) their functional dependence on large amounts of (personal) data and on the quality of the data; (ii) their lack of transparency, which makes it difficult to understand how data-driven systems operate, including how data are processed and for what purpose; (iii) the complexity of data processing activities and the multiplicity of actors involved, which raises the question of how to identify and control data controllers and processors; (iv) the ability of some data-driven systems to continuously "learn" and "adapt" their behavior leading to new unpredictable risks; and (v) their (partially) autonomous behavior, which may affect privacy without direct human intervention.

Against this backdrop, this book – consisting of chapters by leading scholars in law and technology – analyzes the manifold privacy issues raised by data-driven

* This work is part of the "Geriatronics" project, a lighthouse initiative of the Munich Institute of Robotics and Machine Intelligence (MIRMI) at the Technical University Munich (TUM).

[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 [2016] OJ L119/1.

[2] On the so-called Brussels effect of the GDPR, cf., A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[3] Cf., Recital 15 GDPR.

[4] eg A Voss, 'Position Paper on Fixing the GDPR: Towards Version 2.0' (2021) <www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf> accessed 5 January 2024.

DOI: 10.4324/9781003502791-2

technologies, ranging from systems based on artificial intelligence (AI) and blockchain, machine-to-machine (M2M) communication and social robots, to behavioral advertising, biometrics and technologies that enable the detection of emotions.

This introduction builds on the findings of the book by first discussing the general conceptual shortcomings and limits of the GDPR (Section 1.2), followed by an overview of the various issues that arise when applying EU data protection law to data-driven technologies (Section 1.3) and an analysis of the (often unclear and incoherent) relationship between the GDPR and EU digital law (Section 1.4). The final section (Section 1.5) draws conclusions and provides recommendations on how the EU data protection legal framework could be improved to take sufficient account of data-driven technologies.

1.2 Conceptual Flaws and Limits of the GDPR

1.2.1 The "One-Size-Fits-All" Approach

One of the most imminent conceptual shortcomings of the GDPR is its "one-size-fits-all" approach. As is well known, the regulation does not distinguish between different use-cases or sectors (e.g., retail, health or finance) or technologies (e.g., AI or blockchain). Rather, it strives to protect everything at the same time.

Unlike much other recent EU legislation in the field of digital law,[5] the GDPR lacks a risk-based approach that tailors the choice and design of regulatory instruments based on the level of risk, following the rule: "the higher the risk, the stricter the rules." Instead, it treats most data processing activities uniformly, regardless of their level of risk. Admittedly, the GDPR also contains few elements of a risk-based approach. For example, the regulation distinguishes between "normal" and "sensitive" personal data, with the latter category of data receiving a higher level of protection under Art. 9 GDPR. In addition, when imposing administrative fines, the supervisory authorities must take into account the circumstances of each case; in particular, the nature, gravity and duration of the infringement, having regard to the nature, scope or purpose of the processing concerned, the number of data subjects affected and the level of the damage suffered by them (Art. 83[2] GDPR). Other than that, the articles of the GDPR do not take into account the severity of the breach. To the extent that *personal data* is processed, the entire body of the GDPR is applicable, with all its obligations and rights, regardless of the nature, gravity or duration of the infringement.

[5] Cf., G De Gregorio and P Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59(2) *Common Market Law Review* 473. See also R Gellert, 'The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?' (2021) 3(2) *Journal of Ethics and Legal Technologies* 15; M Tzanou, 'Addressing Big Data and AI Challenges: A Taxonomy and Why the GDPR Cannot Provide a One-Size-Fits-All Solution' in M Tzanou (ed), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Routledge 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654119> accessed 5 January 2024.

However, the GDPR leaves the assessment of risk and choice of mitigation measures to the data controller and processor.[6] This is evident with regard to the responsibilities of data controllers. According to Art. 24 GDPR, data controllers are required to implement "appropriate" technical and organizational measures "[t]aking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons." However, there is no specification as to definite or mandatory risk thresholds. Accordingly, to comply with the GDPR, data controllers must conduct a thorough assessment of the risks to the fundamental rights of data subjects when processing personal data and implement appropriate mitigation strategies.[7] In addition, data controllers are primarily responsible for conducting a Data Protection Impact Assessment (DPIA) prior to processing if it is likely to result in a high risk to the rights and freedoms of natural persons (Art. 35[1] GDPR). Also, by Art. 35(4)(5) GDPR, supervisory authorities may require a DPIA if they consider that a particular processing operation poses a high risk and the processor has not yet carried out a DPIA, either by publishing a public list of processing operations for which a DPIA is required or of processing operations for which a DPIA is not required. For many data-driven technologies, however, such a list does not exist,[8] making it difficult for processors to assess the need for a DPIA. In such cases, controllers should proactively assess the risks and, if uncertain, seek guidance from privacy experts or consult the relevant supervisory authority.

The rise of data-driven technologies raises the question as to whether this approach is still appropriate. The European Court of Justice (ECJ) has recently taken a strict stance on claims for damages under Art. 82 GDPR by increasing the liability risk for companies handling personal data.[9] To manage this increased liability risk, adopting a risk-based approach can serve as a mitigating factor. After all, different data processing activities carried out by different actors in different sectors for different purposes pose very different risks to the right to privacy and other fundamental rights. A one-size-fits-all approach that treats all types of data processing activities with similar rigor often leads to higher costs and burdens without effectively targeting particularly high-risk activities. In contrast, a codified risk-based regime – taking into account the specific risks and providing for appropriately tiered obligations and rights[10] – would be much better suited to address the specific risks of different technologies in different sectors.

[6] De Gregorio and Dunn (n 5) 476.

[7] Ibid., 478.

[8] The ongoing debate concerns the question whether or not the legislator should include a specific list of technologies in Art. 35(5) GDPR and continuously update it as new technologies emerge.

[9] Case C-300/21 *UI v Österreichische Post* ECLI:EU:C:2023:370; Case C-340/21 *VB v Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986. According to the latter judgment, the mere fear of a possible misuse of personal data is capable, in itself, of constituting non-material damage.

[10] Strongly opposed to such a graduated approach, cf., Art. 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' adopted on 30 May 2014, 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/

This approach involves organizations assessing and prioritizing potential risks to data subjects' rights and freedoms. Entities can demonstrate a proactive commitment to data protection by identifying and addressing high-risk processing activities. Such measures may be considered favorably in the event of legal challenges. This approach aligns with the GDPR's objective of promoting accountability and ensuring that organizations take appropriate measures to protect the privacy of individuals.

Implementing robust risk assessments and adopting measures to mitigate identified risks can help organizations demonstrate compliance and a commitment to protecting personal data. Incorporating privacy impact assessments when necessary not only enhances legal defensibility, but also aligns with the GDPR's principles of accountability and proportionality.

1.2.2 The Individual Rights Approach

Another problematic feature is the GDPR's exclusive focus on individual rights, which shapes both its scope and remedies. The regulation only applies to personal data of known and identifiable individuals, not to anonymous or anonymized data.[11] Moreover, the remedies for GDPR violations are primarily designed as individual rights,[12] granting data subjects exclusive rights, particularly with respect to access and deletion of their personal data.

This approach dates back to the origins of privacy and data protection law. Historically, privacy has focused on giving individuals control over their personal information. However, in today's digital age when data is continuously and automatically collected and stored, establishing individual control is challenging. Moreover, the combination of individual data with other datasets in the realm of Big Data raises concerns about harm to groups, particularly in vulnerable contexts.[13]

Machine learning (ML) models used for profiling make the limits of data protection law based on individual rights even more apparent. As most of the data

files/2014/wp218_en.pdf> accessed 5 January 2024: "It is important to note that – even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'."

[11] Cf., Recital 26 GDPR.

[12] This becomes evident in the light of Art. 80(1) GDPR. Even the representation of data subjects requires that the mandated body is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data. Furthermore, a successfully lodged complaint requires infringement of the data subjects' rights. This becomes even clearer with regard to Art. 80(2) GDPR, according to which non-profit organizations can litigate data protection rights without being mandated, only if they consider that the rights of a data subject have been infringed as a result of the processing. According to the ECJ, this requires that the rights of *identified* or *identifiable* natural persons have been infringed; Case C-319/20 *Meta Platforms Ireland Limited, Formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* ECLI:EU:C:2022:322.

[13] L Kammourieh and others, 'Group Privacy in the Age of Big Data' in L Taylor, L Floridi and B van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 37.

that drives AI systems is either directly linked to a person, or (if pseudonymized) is at least identifiable by an algorithm, the GDPR applies regularly both when AI is under development (since it governs the collection and use of data in generating ML models) and under certain limited conditions when it is used to analyze or reach decisions about individuals. However, there are no data protection rights or obligations concerning the ML models themselves in the period after they have been built but before any decisions have been made about using them. As a rule, ML models do not contain any personal data, but only information about groups and classes of persons. Although algorithmically designed group profiles may have a big impact on a person, (ad hoc) groups are not recognized as holders of privacy rights. Hence, automated data processing by which individuals are clustered into groups or classes (based on their behavior, preferences, and other characteristics) creates a loophole in data protection law.[14]

To illustrate, an algorithm that filters content can discriminate against someone based on their race, gender, or sexual orientation without identifying the person.[15] The algorithm only needs access to these characteristics or their proxy data. The individual can remain anonymous and still be discriminated against. In addition, statistical data about human behavior can be used in general ways, such as redesigning the interface of some services or adjusting the timing of notifications. However, this generic use may intentionally or unintentionally increase the addictive nature of such services, which may be harmful to the mental health of users.[16]

These examples show that the GDPR – with its concept of individual rights and remedies – is reaching its limits in the age of Big Data. Thus, many scholars have proposed ways to fill these gaps, such as recognizing some form of "group privacy,"[17] a new right "to reasonable inferences"[18] or a right to "predictive privacy."[19] Arguably, in order to protect citizens and groups from unfair Big Data (group) profiles and inferences, it is not necessary to provide such protections in the GDPR itself. After all, data protection law is primarily concerned with the unjustified *disclosure* of data and not so much with the harmful *use* of data. As a result, other regulations such as the recently adopted AI Act, in combination with other laws (competition law, civil law, non-discrimination law, or criminal law) could and should primarily address the harmful use of data, thus creating a comprehensive legal framework.

[14] M Ebers, 'Regulating AI and Robotics: Ethical and Legal Challenges' in M Ebers and S Navas (eds), *Algorithms and Law* (Cambridge University Press 2020) 63.

[15] P Pałka, 'Harmed While Anonymous' (2023) *Technology and Regulation* 22 <https://techreg.org/article/view/13829> accessed 5 January 2024.

[16] Ibid.

[17] L Floridi, 'Group Privacy: A Defence and an Interpretation' in L Taylor, L Floridi and B van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 83 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3854483> accessed 5 January 2024.

[18] S Wachter and B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review* 1.

[19] R Mühlhoff, 'Predictive Privacy: Towards an Applied Ethics of Data Analytics, Ethics and Information Technology' (2021) 23 *Ethics and Information Technology* 675 <https://link.springer.com/article/10.1007/s10676-021-09606-x> accessed 5 January 2024.

1.2.3 The "Prohibition Principle" in Private Law Relationships

Some authors have argued that the so-called prohibition principle[20] can be seen as an inherent flaw of the GDPR insofar as it applies to private law relationships. The GDPR treats any processing of personal data as a potential risk. According to Art. 6 GDPR and also Art. 8(2)(1) CFR (Charter of Fundamental Rights),[21] processing of personal data is prohibited unless there is a specific legal ground (such as consent or statutory permission) justifying it. Whereas most scholars agree that the "prohibition principle" is legitimate as far as vertical relationships between citizens and administrative institutions are concerned, such a restrictive legal concept of data protection has been criticized as being ill-equipped to regulate horizontal data transactions.[22]

Indeed, the "prohibition principle" is in tension with the general objective of Art. 1(3) GDPR regarding the promotion of the free movement of data. One could argue that it also conflicts with the very foundations of private law, which is based on the principle of party autonomy, thus stressing the freedom to act according to one's own will. Yet, private law has a lot of restrictions on party autonomy, especially where fundamental rights and vulnerable parties are concerned, such as, e.g., in consumer, labor and even insurance law. Data protection law follows this regulatory model and reverses this rule/exception relationship. Since the processing of personal data is generally prohibited, private parties who contract for the commercial use of personal data always run the risk of violating data protection law. Some lawyers have therefore described the "prohibition principle" as a straightforward "interventionist paternalism"[23] that creates an "informational heteronomy" ("informationelle Fremdbestimmung"),[24] leading to a hypertrophic protection of fundamental rights accompanied by a loss of freedom for data controllers and data subjects.[25] Others, however, argue that the "prohibition principle" is not only mandatory due to Art. 8(2)(1) CFR, but that it can also be combined with the proposed risk-based approach.[26]

[20] A Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (2019) *Neue Juristische Wochenschrift* 1 argues that the legal terms "prohibition principle" and "prohibition subject to authorization" are not suitable for data protection law because they do not acknowledge the fundamental rights basis of data protection law.

[21] Charter of Fundamental Rights of the European Union [2016] OJ C202/389.

[22] Cf., K von Lewinski, *Die Matrix des Datenschutzrechts* (Mohr Siebeck 2014) 46; H P Bull, *Sinn und Unsinn des Datenschutzrechts* (Mohr Siebeck 2015) 1; A Sattler, 'Personenbezogene Daten als Leistungsgegenstand' (2017) 72(21) *Juristen Zeitung* 1036; J Reinhardt, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in M Albers and I Sarlet (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022) 55.

[23] C Krönke, 'Datenpaternalismus' (2016) 55 *Der Staat* 319; Bull (n 22); von Lewinski (n 22) 46.

[24] Von Lewinski (n 22) 46 ("informationelle Fremdbestimmung"). See also Bull (n 22).

[25] C Herresthal, 'Grundrechtecharta und Privatrecht' (2014) *Zeitschrift für Europäisches Privatrecht* 238.

[26] B Buchner and T Petri, 'Art. 6 Rechtmäßigkeit der Verarbeitung' in J Kühling and B Buchner (eds), *DS-GVO-BDFG* (4th edn, C.H. Beck 2024) para 14; cf., also B Buchner, *Informationelle Selbstbestimmung im Privatrecht* (Mohr Siebeck 2006) 175ff (individual rights to personal data as a necessary requirement for an efficient distribution of data as an economic good). Prohibition principle is also welcomed by Hornung, see G Hornung, 'Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012' (2012) *Zeitschrift für Datenschutz* 101.

The apparent conflict between data protection law on the one hand, and the needs of the modern data economy for data exchange contracts on the other hand, cannot be resolved by the Member States. National legislators are not allowed to create national divergent provisions on consent requirements in contract law (cf., Art. 6[2] GDPR) and hence national rules on mistake, duress etc., usually employed in order to guarantee the free will of the person, are not applicable. However, in cases of certain categories of sensitive data, national legislators are permitted to foresee more stringent rules for consent (Art. 9[4] GDPR). The adoption of a common European data obligation law (beyond the Data Act)[27] is also very unlikely in the near future, as the years of negotiations on the GDPR have resulted in little interest in revising the European requirements for the protection of personal data.[28] Additionally, both the ECJ and the European Data Protection Board (EDPB) tend to interpret the key concepts of "informed consent,"[29] "performance of contract"[30] and "legitimate interest"[31] restrictively in practice. However, an alternative way forward would be expanding and reformulating certain statutory legal bases and hence relying less on consent as the expression of personal autonomy.

1.2.4 The Primacy of Consent

Although the GDPR provides for six equally adequate legal bases, the most important provision for the processing of personal data in practice is "informed consent" (Art. 6[1][a] GDPR). This concept is also subject to strong criticism, mainly because, often, users do not have a clear understanding of what they are agreeing to. Also, they often have no choice but to consent, as refusal would exclude them from the use of certain services. Therefore, critics argue that the notion of individual control over personal data is an illusion, as data controllers exploit this concept by shifting their responsibilities to users through complex and extensive privacy statements. Some legal scholars even view consent as fiction that gives companies a blank check to process data,[32] because they often confront and overwhelm users

[27] Cf., thereto Section 1.4.3.

[28] Sattler (n 22) 1036.

[29] Case C-61/19 *Orange România SA v. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Persona* ECLI:EU:C:2020:901; Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* ECLI:EU:C:2019:801; EDPB Guidelines 05/2020 on consent under Regulation 2016/679 15.

[30] Case C-252/21 *Meta vs Bundeskartellamt* ECLI:EU:C:2023:537; EDPB, Guidelines 2/2019 on the processing of personal data under Art. 6(1)(b) GDPR in the context of the provision of online services to data subjects, 9.

[31] Case C-252/21 *Meta vs Bundeskartellamt* ECLI:EU:C:2023:537; Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme* ECLI:EU:C:2017:336, cf., EDPB, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, 16.

[32] D J Solove, 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law' (2024) 104 *Boston University Law Review* 593; N Richards and W Hartzog, 'The Pathologies of Digital Consent' (2019) 96 *Washington University Law Review* 1461, 1476–1491; G Hornung and S

with privacy banners (e.g., cookie banners), leading them to agree to an overload of consents as a condition for accessing certain services. This not only undermines the original idea of informed consent but also gives a few large companies a competitive advantage over small to medium-sized enterprises (SMEs) and start-ups. Such companies can obtain consent (often automatically)[33] for all their services in a centralized manner (e.g., through terms and conditions) and use the collected data for innovation and product development.

Against this backdrop, several solutions are being discussed. Some have called for a strict interpretation of Art. 6(1)(a) GDPR.[34] In addition, the notion of "informed consent" could be further strengthened by applying EU (and national) consumer law, in particular by reviewing pre-formulated data processing clauses in light of the Unfair Contract Terms Directive (UCTD) 93/13/EEC.[35] According to Recital 42 GDPR, a pre-formulated declaration of consent "should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms." This implies that a pre-formulated data processing consent clause must comply not only with the GDPR, but also with the requirements of the UCTD – i.e., both the fairness requirement under Art. 3 UCTD and the transparency requirement under Art. 5 UCTD.[36]

Others argue that a strict interpretation of the concept of "informed consent" may stifle technological innovation.[37] As some chapters in this book make clear,[38] it is almost impossible to require consent for every data processing operation, especially in the case of automated networked services. Against this backdrop, some scholars argue that the concept of "informed consent" should be replaced by "technological consent," i.e., agreement technologies[39] that automate the consent procedure based on privacy preferences. In addition, many advocate giving data subjects the right to actively choose whether to pay for a service indirectly through their data or directly through monetary payments.[40]

Schomberg, 'Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Governance Acts' (2022) *Computer und Recht* 508–516 with further references.

[33] Cf., G Guerra, Chapter 2 in this book.

[34] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679,15.

[35] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

[36] Accordingly, national courts review pre-formulated consent clauses also against the provisions transposing the UCTD. For Germany, see OLG Köln, judgment of 03.11.2023–6 U 58/23 Rn 37; S Ernst, 'Die Einwilligung nach der Datenschutzgrundverordnung' (2017) 3 *Zeitschrift für Datenschutz* 110.

[37] Voss (n 4).

[38] Cf., G Guerra, Chapter 2; M Petik, Chapter 5; M Ebers, Chapter 9.

[39] Cf., C Santos and others, *Artificial Intelligence and Law* 2019 1(2ff); H Billhardt and others, 'Agreement Technologies for Coordination in Smart Cities' (2018) 8(5) *Applied Sciences Article* 816 1 (2ff with overview on applications at 6ff); M Luck and P McBurney, 'Computing as Interaction: Agent and Agreement Technologies' (2008) *IEEE SMC Conference on Distributed Human-Machine Systems* 1; see also S Ossowski (ed), *Agreement Technologies. Second International Conference, AT 2013, Beijing, China, August 1–2, 2013. Proceedings* (Springer 2013).

[40] P Hacker, *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB* (Mohr Siebeck 2020) 621 footnote 442.

Alternatively, there have also been calls to replace consent as the primary means of justifying data processing with the "legitimate interest" test.[41] According to these opinions, such a test would provide a more robust data protection framework and enhance legitimacy in contrast to the current legal regime, which primarily emphasizes the intended purposes of data collection and use. Nevertheless, it remains unclear how this test will be carried out and what criteria will determine whether an interest is legitimate. Art. 6(1)(f) GDPR gives supervisory authorities and the courts considerable leeway for a flexible ex-post assessment in individual cases. Hence, private data controllers who base their business model on legitimate interest face a great deal of legal uncertainty, as they cannot say ex ante whether the courts will give higher priority to the interests of data controllers (general freedom of action, freedom of contract, freedom of profession) or to the right to the protection of personal data in their ex-post assessment of individual cases.

An alternative strategy to overcome the current reliance on consent as the primary legal basis for data processing in private law is to rely more on statutory legal bases – by creating specific legal grounds for data processing or by expanding existing ones.

1.2.5 Unclear Responsibilities

A further problem with the GDPR, as interpreted by the ECJ, is the unclear responsibilities of data processors and controllers in the context of data-driven technologies. Since these technologies typically collect and store personal data in a decentralized manner, they involve multiple actors. Additionally, according to the judicial interpretation of "control", joint controllers only require a low threshold of influence over the means. The decisive criterion is that the individual concerned enables the collection and transfer of personal data, possibly linked to some input that such a joint controller has as to the parameters.[42] This confirms earlier warnings that as more individuals become data creators, they also become controllers, and raises questions about the controllers' liability.[43]

However, these broad interpretations of control not only fail to achieve the goal of providing comprehensive and efficient protection for data subjects, but also prove problematic from a political economy perspective. Furthermore, such far-reaching definitions hinder the effectiveness of the law itself, as the intricate

[41] L Moerel and C Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 5 January 2024. See moreover D J Solove and W Hartzog, 'Kafka in the Age of AI and the Futility of Privacy as Control' (2024) 104 *Boston University Law Review* (forthcoming), with the proposal to replace the "individual control model" based on consent with the "societal structure model" which seeks to protect privacy by regulating the behavior of organizations that collect, use and disclose personal data, rather than relying solely on individual empowerment.

[42] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* ECLI:EU:C:2018:388.

[43] M Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11(4) *International Data Privacy Law* 333; G Spindler, Chapter 8, in this book, under 3.3.1.

network of responsibilities lacks clarity and precision, thereby making enforcement challenging and leaving gaps in the protection of individuals' data rights.[44]

A possible solution could be a new control test: instead of asking if a controller controls the data and software used, one could devise a de minimis threshold of influence over the means of the processing. According to this, only entities that influence both the objectives and methods beyond the simple selection of a platform or service and facilitating another party's processing should be considered controllers,[45] so a company or state authority that chooses to keep personal data in a certain cloud should not be considered a controller and hence liable. Such an approach would, however, create false incentives whereby controllers could outsource certain high-risk activities to other entities and thereby escape liability for data breaches. This can be illustrated by the recent case decided by the ECJ in which the Lithuanian National Public Health Centre commissioned a private company with the development of a COVID-19 app and provided instructions regarding its development but later tried to evade liability on the ground that it did not process personal data itself.[46] Moreover, a new control test is not necessary to avoid an unreasonably high risk of liability. If a controller has no real influence over the data processing, they could often prove that he or she is not 'in any way responsible' for the breach and hence not financially liable for the damages under Art. 82(3) GDPR. The same applies to administrative fines: as confirmed by the recent judgments of the ECJ, the imposition of a fine under Art. 83 GDPR requires wrongful conduct on the part of the data controller.[47] Controllers with no or minimal influence can rarely be accused of intentional or negligent conduct.

1.2.6 Regulatory Burdens

An additional issue that is often pointed out is the regulatory burden of GDPR compliance, which can be particularly hard on SMEs. Some studies have shown that the GDPR has had noteworthy implications for the European common market. Notably, businesses subject to the GDPR have reportedly experienced an 8% decline in profits, with small companies bearing a nearly double average reduction.[48] Another study examining data from 4.1 million apps on the Google Play Store between 2016 and 2019 came to the conclusion that the GDPR triggered the exit of approximately one-third of available apps.[49] Moreover, in the quarters following

[44] Finck (n 43) 333; F N Wittner, *Verantwortlichkeit in komplexen Ökosystemen. Attempt to Further Develop Data Protection in the Context of Distributed Processing Reality* (Mohr Siebeck 2022).

[45] Finck (n 43) 347.

[46] Case C-683/21 *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija* ECLI:EU:C:2023:949.

[47] Ibid.; Case C-807/21 *Deutsche Wohnen SE v Staatsanwaltschaft Berlin* ECLI:EU:C:2023:950.

[48] C Chen, C B Frey and G Presidente, 'Disrupting Science' (2022) *Oxford Martin School Working Paper* <www.oxfordmartin.ox.ac.uk/downloads/academic/Disrupting-Science-Upload-2022-4.pdf> accessed 5 January 2024.

[49] R Janßen, R Keßler, M E Kummer and J Waldfogel, 'GDPR and the Lost Generation of Innovative Apps' (2022) *NBER Working Paper 30028* <www.nber.org/system/files/working_papers/w30028/w30028.pdf> accessed 5 January 2024.

its implementation, the entry of new apps significantly decreased by half. While the GDPR aims to enhance consumer protection and safety, it also brings to light potential constraints on product choice in the market, particularly as consumer and safety laws may limit the availability of certain products. Furthermore, concerns have been raised about how the GDPR has contributed to an increase in digital market concentration, suggesting a complex interplay between regulatory efforts and market dynamics in the European digital landscape.[50]

A solution to mitigate this economic impact could be the risk-based approach discussed previously or the inclusion of more exemptions.

1.2.7 Enforcement Gaps

Finally, policymakers and academics alike assert that there is a significant mismatch between the GDPR's legal framework and its actual enforcement, despite the fact that the regulation allows for both public and private enforcement.[51] Due to this gap between the law in the books and the law in action, some of the GDPR's strongest supporters have even warned that it risks becoming a "fantasy law."[52]

Indeed, the GDPR has been enforced differently across the EU in the past. While some Member States (such as Spain, Italy, France and Germany) have been very proactive in issuing fines,[53] public enforcement in other countries, notably Ireland, has been so weak that the European Parliament in 2021 voted in favor of a resolution calling on the European Commission to open infringement proceedings against Ireland for failing to enforce the GDPR.[54] The main reason for this disparity is the

[50] G A Johnson, S K Shriver and S G Goldberg, 'Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686> accessed 5 January 2024.

[51] European Parliament, *Press Release*, 25.3.21, Parliament Calls for Improved Implementation and Enforcement of the GDPR <www.europarl.europa.eu/news/en/press-room/20210322IPR00527/parliament-calls-for-improved-implementation-and-enforcement-of-the-gdpr> accessed 5 January 2024; F Lancieri, 'Narrowing Data Protection's Enforcement Gaps' (2022) 74 *Maine Law Review* 16 <https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1753&context=mlr> accessed 5 January 2024.

[52] Lancieri (n 51).

[53] Spain has issued the highest number of fines, with 277 (212 of which were issued in 2021), followed by Italy (88), Romania (62), Hungary (44), and Germany (32). In terms of the total fine amount, Italy leads with €84 million, followed by France (€57 million), Germany (€49 million), the UK (€44 million), and Spain (€32 million). Recently, Luxembourg joined these ranks by issuing the largest fine to date on Amazon, amounting to €746 million. Cf., I Heine, '3 Years Later: An Analysis of GDPR Enforcement' (*Center for Strategic and International Studies*, 13 September 2021) <www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement> accessed 5 January 2024; cf., J Ruohonen and K Hjerppe, 'The GDPR Enforcement Fines at Glance' (2022) 106 *Information Systems* 101876. See also EDPB, Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Art. 3(2) GDPR.

[54] L Bertuzzi, 'MEPs Call for Infringement Procedure Against Ireland' (20 May 2021) *Euractiv* <www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/> accessed 5 January 2024.

one-stop-shop (OSS) mechanism introduced by the GDPR,[55] under which multinational companies are only subject to the regulator in the jurisdiction where the organization has its main or only branch. Countries such as Ireland, where many big tech companies are headquartered, have therefore long been able to refrain from strict GDPR enforcement in order to protect their domestic economy. Estonia, in turn, has been very modest in issuing fines or administrative orders due to the lack of resources of the national enforcement authority, as well as to the unclear legislation on the requirements of applying administrative fines.[56]

However, this has recently changed. On 13 April 2023, the EDPB issued a binding dispute resolution decision[57] against the Irish data protection authority, directing it to impose fines on Meta Platforms Ireland Limited for Meta's transfers of personal data to the United States since 16 July 2020. As a result, Ireland imposed the largest ever GDPR fine on Meta, amounting to €1.2 billion.[58]

At the same time, the ECJ strengthened the mechanisms of private enforcement of the GDPR in a couple of cases. In *Natsionalna agentsia za prihodite*[59] the Court ruled that the mere fear of a possible misuse of personal data may, in itself, constitute non-material damage. This broad interpretation of Art. 82 GDPR will most likely have a deterrent effect, encouraging companies to step up their efforts to comply with EU data protection law. Furthermore, in *Meta Platforms Ireland*,[60] the ECJ emphasized that the GDPR does not preclude the bringing of additional representative actions in the field of consumer protection, and that consumer protection associations are entitled to bring actions against infringements of the GDPR on the basis of the Unfair Commercial Practices Directive (UCPD) 2005/29[61] and the Injunctions Directive 2009/22.[62] The latter Directive has now been replaced by the Representative Action Directive (RAD) 2020/1828,[63] which explicitly states in

[55] Cf., Art. 56(1) GDPR.

[56] K Sein, 'The Growing Interplay of Consumer and Data Protection Law' in H-W Micklitz and C Twigg-Flesner (eds), *The Transformation of Consumer Law and Policy in Europe* (Bloomsbury 2023) 154. See also K Sein, Chapter 3, in this book, on the innovative data-sharing platform created by the state in order to allow citizens to share their personal data held in public databases.

[57] EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted on 13 April 2023.

[58] <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en> accessed 5 January 2024.

[59] Case C-340/21 *VB v Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986.

[60] Case C-319/20, *Meta Platforms Ireland Limited, Formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* ECLI:EU:C:2022:322, para 79.

[61] European Parliament and Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 (Unfair Commercial Practices Directive).

[62] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version) [2009] OJ L110/30.

[63] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.

Art. 2(1), Annex I No. 56, that the Directive also applies to representative actions brought against infringements of the GDPR that harm or may harm the collective interests of consumers. Last but not least, competition law can also contribute to a more efficient enforcement of data protection law. According to the ECJ's judgment in *Meta Platforms and Others*,[64] national competition authorities may find an abuse of a dominant position (Art. 102 TFEU) when the company's general terms and conditions for the processing of personal data infringe the GDPR.

In the meantime, the European Commission has also reacted to the enforcement deficits that have become apparent in the past. In July 2023, the Commission published a proposal for a GDPR Procedural Regulation[65] to set up concrete procedural rules for the authorities when applying the GDPR in cases which affect individuals located in more than one Member State. In particular, the proposal introduces an obligation for the lead data protection authority to send a "summary of key issues" to their counterparts concerned, identifying the main elements of the investigation and its views on the case, thereby allowing them to provide their views early on. By this, the proposal aims to reduce disagreements and facilitate consensus among authorities from the initial stages of the process.

1.3 GDPR and Data-driven Technologies

In addition to the conceptual shortcomings and limits of the GDPR discussed previously, there is the question of how new, data-driven technologies can comply with EU data protection law. Critics from politics point out that the GDPR is incompatible with many emerging technologies and rather prevents them from reaching their full potential.[66] This is probably not generally true. Yet, as various chapters of our book show, data-driven technologies – such as AI systems, blockchain technology, social robots, M2M communication in Internet of Things (IoT) environments and smart cities, behavioral advertising and biometrics – do indeed raise a number of data protection issues.

1.3.1 AI Systems

AI systems process a significant amount of data, which is likely to include personal data, triggering the application of the GDPR. Therefore, when applied to certain AI applications, including large language models, their training may conflict with EU data protection law. This became particularly clear at the end of March 2023, when the Italian data protection authority decided to impose a temporary restriction on OpenAI's

[64] Case C-252/21 *Meta v Bundeskartellamt* ECLI:EU:C:2023:537, para 62. At the same time, the ECJ developed criteria to assure a coherent GDPR application on interactions between competition and data protection authorities, paras 53ff.

[65] European Commission, Proposal for a Regulation laying down additional procedural rules relating to the enforcement of GDPR, COM(2023) 348 final. Cf., thereto EDPB-EDPS, Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679.

[66] Voss (n 4) 9.

processing of Italian users' data due to alleged GDPR violations.[67] While this ban has since been lifted, the EDPB set up a task force in April 2023 to cooperate and exchange information on the enforcement of EU laws against ChatGPT maker OpenAI.[68]

Indeed, the training of AI models may violate the general principles of the GDPR, above all the principles of transparency (Art. 5[1][a] GDPR), purpose limitation (Art. 5[1][b] GDPR) and data minimization (Art. 5[1][c] GDPR). Of these, purpose limitation is especially problematic. According to this principle, data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. The purpose must be stated at the time of data collection. Importantly, the purpose limitation principle is at odds with the way Big Data is collected and used, which is characterized by the collection of large amounts of data, while the methods of analysis and the specific purpose of the data processing are only determined during or after collection. Furthermore, the purpose limitation principle requires the purpose to be clearly stated. A purpose statement such as "to improve the service" is not considered specific enough.[69] In practice, however, neither the data controller nor the data subject will often know at the time of data collection what precise purposes the processing may serve in the future.

Finding a legal ground for processing data to train AI systems[70] and complying with the GDPR's information duties[71] are other key challenges for AI system developers. Moreover, it is currently unclear whether and how data subjects can exercise their rights of access, rectification and erasure in relation to training datasets.[72]

[67] <www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english> accessed 5 January 2024.

[68] <https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en> accessed 5 January 2024.

[69] Recital 39 GDPR; M Finch and A Biega, 'Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems' (2021) *Max Planck Institute for Innovation and Competition (research paper series)* 1 <www.utupub.fi/bitstream/handle/10024/174974/Aho_Sami_progradu.pdf;jsessionid=0753DB2A519AD776DDBF1503DE5DDE70?sequence=1> accessed 5 January 2024. See also Art. 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN 16.

[70] Cf., P T Kramcsák, 'Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?' (2022) *Computer Law & Security Review* 1 <www.sciencedirect.com/science/article/abs/pii/S026736492200108X> accessed 5 January 2024.

[71] Cf., L Mitrou, 'Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?' (2018) 53 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> accessed 5 January 2024.

[72] B Custers and A S Heijne, 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' (2022) 46 *Computer Law & Security Review* 1; S Cabral, 'Forgetful AI: AI and the Right to Erasure under the GDPR' (2020) 6 *The European Data Protection Law Review* 378; T Li, E Fosch Villaronga and P Kieseberg, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 *Computer Law & Security Review* 12; T Li, 'Algorithmic Destruction' (2022) 75(3) *SMU Law Review* <https://ssrn.com/abstract=4066845> accessed 5 January 2024; L Floridi, 'Machine Unlearning: Its Nature, Scope, and Importance for a "Delete Culture"' (2023) *Philosophy & Technology* <https://ssrn.com/abstract=4455976> accessed 5 January 2024.

Another key provision of the GDPR that is highly relevant for AI systems is Art. 22 GDPR, according to which the adoption of a "decision based solely on automated processing" (Art. 22[1] GDPR) is only permitted if: (i) the decision is necessary for the conclusion or performance of a contract; (ii) it is authorized by EU or Member State law; or (iii) it is based on the data subject's explicit consent (Art. 22[2] GDPR). In the recent *Schufa* judgment,[73] the ECJ interpreted the term "decision based solely on automated processing" very broadly. According to the Court, the provision does not only cover those transactions that have direct legal effects vis-à-vis the data subject without any human intervention. Rather, Art. 22(1) GDPR also covers prior automated predictions (such as credit scoring) made by a particular company (Schufa), provided that a third company (bank) subsequently "draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person."[74]

The *Schufa* ruling is likely to have far-reaching consequences for companies that use AI systems to generate scores that "strongly" influence legally relevant decisions, regardless of whether these decisions are made by those companies themselves or by third parties. Since such predictions fulfill the criteria of Art. 22(1) according to the ECJ, they will henceforth require a justification under Art. 22(2) GDPR and trigger the data subject's rights under Arts. 15(1)(h) and 22(3) GDPR.

All these considerations show how difficult it is for providers and users of AI systems to comply with the GDPR. Arguably, the recently adopted AI Act has not brought clarity, but rather created more problems, as the AI Act applies additionally to the GDPR.[75] Against this backdrop, some critical voices perceive European data protection law as an "obstacle" to the development and use of AI systems,[76] while others highlight that despite these problems, it is quite possible for developers and users to navigate and comply with the requirements of the GDPR.[77]

1.3.2 Blockchain Technology

Significant data protection issues also arise with blockchain technology – a distributed ledger technology based upon a peer-to-peer network which forms the basis for cryptocurrencies and smart contracts.

[73] Case C-634/21 *OQ v Land Hessen* ECLI:EU:C:2023:957.

[74] Ibid., para 73.

[75] Cf., Art. 2(7) AI Act; additionally, Recital 10 AI Act clarifies "that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling." On the relationship between the AI Act and data protection law see more generally Section 1.4.4.

[76] Cf., C Lawson-Hetchley, 'The Potential Impact of the Future AI Act on the GDPR' (Master's thesis, University of Oslo 2022) <www.duo.uio.no/bitstream/handle/10852/101369/1/The-potential-impact-of-the-future-AI-Act-on-the-GDPR.pdf> accessed 5 January 2024; <www.euractiv.com/section/5g/interview/gdpr-could-obstruct-ai-development-mep-says/> accessed 5 January 2024.

[77] A Vogel, Chapter 6, in this book; G Sartor, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (2020) *European Parliamentary Research Service* <www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 5 January 2024.

In most cases, blockchains process personal data within the meaning of Art. 4(1) GDPR.[78] Although blockchain generally only assigns a pseudonym to data whose concrete assignment leads to persons outside blockchain, pseudonymized data is personal data because such data relates at least to an identifiable natural person.[79]

One key feature of blockchain technology is that the data stored on blockchain is secured against modification and deletion. Once data is stored in a decentralized block, it is impossible to delete or alter. Another characteristic is that blockchains are often decentralized as peer-to-peer networks without their own administrators or servers, with which in principle anyone can therefore participate.

Both features are in conflict with the GDPR. First, the fact that data on blockchain cannot be deleted or modified is hardly compatible with the requirements of Art. 16 GDPR (right to rectification) and Art. 17 GDPR (right to erasure). Second, decentralized blockchains make it difficult to assign responsibility and accountability, whereas the GDPR is based on the assumption that for each personal data point, there is at least one person – the data controller – to whom data subjects can turn to enforce their rights under EU data protection law.

Other questions arise in relation to the data minimization principle. Data is replicated on many different computers, and distributed ledgers are constantly growing, so how the purpose limitation principle can be complied with when data is not only processed once for a specific purpose but continues to be processed after it has been placed on the chain, remains in contention.

Accordingly, Chapter 8 of this book concludes that the provisions of the GDPR and blockchain technology can hardly be reconciled.

1.3.3 Social Robots, Especially Medical and Care Robots

Another technology that raises many open questions under the GDPR is social robotics – i.e., physically embodied, (partially) autonomous agents that communicate and interact with humans on an emotional level. Chapter 7 and Chapter 9 focus, in particular, on medical and care robots, which are designed to assist users, family members or professional caregivers, in providing physical, cognitive or emotional support.

Social robots may have impacts on privacy, especially, in three ways: facilitating direct surveillance, introducing new access points to traditionally protected spaces and leading to new varieties of highly sensitive personal information.[80] The inherent vulnerability of some users (patients, care recipients) raises specific questions concerning the relationship between data processors and data subject,

[78] M Finck, *Blockchain and the General Data Protection Regulation* (European Parliament 2019) 14ff; J Schrey and T Thalhofer, ‘Rechtliche Aspekte der Blockchain’ (2017) *Neue Juristische Wochenschrift* 1431.

[79] G Spindler, Chapter 8, in this book.

[80] M Ebers, Chapter 9, in this book.

especially with regard to information duties and transparency requirements, informed consent and legal capacity.[81] In addition, human users often develop an emotional and empathic bond with personal (care) robots, considering them as friends or even partners.[82] This well-known "anthropomorphization effect" might lead to significant misconceptions about data processing and challenge the very concept of informed consent. On the other hand, the cooperative nature of human–robot interaction offers a number of opportunities to protect privacy in new ways. Against this backdrop, Chapter 9 discusses novel solutions on how personal (care) robots can comply with the GDPR, especially design options, data anonymization methods and the cutting-edge ideas of dynamic consent and conversational privacy.

Additional issues arise in relation with the reuse of personal data, in particular health data. As Chapter 7 shows, the GDPR imposes many restrictions on the processing of health data, and especially on the repurposing of such data. On the other hand, the envisaged regulation on a European Health Data Space (EHDS)[83] aims to facilitate the use, reuse, and repurposing of health data for AI systems in healthcare. Accordingly, the question arises as to how this new piece of legislation will relate to the GDPR. A number of issues remain to be clarified in this regard, not least the legal basis for data processing.[84]

1.3.4 M2M Communication, Especially in IoT Environments and Smart Cities

With the proliferation of IoT devices and 5G networks, data generation activities are increasing, particularly in M2M communications, which poses legal challenges under the GDPR (and also the ePrivacy Directive[85] and the proposed ePrivacy Regulation[86]), particularly with regard to the principles of transparency and data minimization, as well as the concept of informed consent. The shift to real-time data processing in M2M, especially in IoT and smart city applications, requires

[81] Ibid.; C Ho, 'Privacy and Transparency in Human-Robot Interaction' in W Barfield, Y Weng and U Pagallo (eds), *Cambridge Handbook on Law, Policy, and Regulations for Human-Robot Interaction* (Cambridge University Press, 2024) 589.

[82] M Scheutz, 'The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots' in P Lin, K Abney and G A Bekey (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (The MIT Press 2012) 205; K Ishii, 'Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects' (2019) 34 *AI and Society* 509 with further references, 515.

[83] European Commission, Proposal for a regulation of the European Parliament and of the Council establishing the Union Health Data Space, COM(2022) 197 final.

[84] V L Raposo, Chapter 7, in this book.

[85] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[86] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

robust data protection measures. The integration of 5G and edge computing further emphasizes the need for GDPR compliance. Although 5G has promising aspects, there is a need for a comprehensive examination of privacy (and also security) vulnerabilities in M2M communications, including technical, societal, ethical and regulatory dimensions. At the same time, it is important that legal frameworks are dynamic and adaptable to the evolving 5G technology.

The cornerstone of data protection – consent – faces challenges in balancing operational efficiency with the stringent requirements of the GDPR, creating the need for a nuanced approach. A broader application of GDPR principles and industry-wide standards for managing consent in M2M environments could be a solution.[87] Advanced and dynamic consent procedures and notifications are critical to upholding individual rights within M2M-generated data in 5G.[88] This may require regulatory adjustments. Overall, the interplay between M2M communications and 5G networks within EU data protection standards remains a dynamic area of focus as both technologies continue to evolve.

1.3.5 Behavioral Advertising

Online Behavioral Advertising (OBA) practices have several market and societal implications. They process large amounts of data to personalize advertisements by predicting the potential customers' behavior and to make online marketing more effective. Data protection law therefore applies in many cases, but numerous questions remain. Generally speaking, OBA raises issues regarding compliance with data protection principles, challenges in distinguishing between data controllers and processors, the complex issue of obtaining valid consent, lack of enforcement on profiling and automated decision-making prohibitions, and insufficient accountability among data controllers in cases of cross-border transfers.[89] These shortcomings are the result of a lack of coherence between EU data protection law with regard to the use of consent in online advertising.

To address this regulatory impasse, there are essentially two regulatory options. The first option focuses on techno-legal reforms to reinstate data protection in OBA and ensure that users can more effectively have consent and control of their personal data.[90] These options include privacy-friendly interfaces, user-accessible options, and

[87] M Petik, Chapter 5, in this book.

[88] Ibid.; E Del Re, 'Which Future Strategy and Policies for Privacy in 5G and Beyond?' (2020) *IEEE 3rd 5G World Forum (5GWF)* 236 <https://doi.org/10.1109/5gwf49715.2020.9221371> accessed 5 January 2024.

[89] F Galli and G Sartor, Chapter 11, in this book.

[90] See, eg, E Hsiao, 'Ethical Design: Obligations of a UX Designer That Are Never Talked about Enough' (*BoorCamp UX Design*, 8 December 2022) <https://bootcamp.uxdesign.cc/ethical-design-obligations-of-a-ux-designer-thats-never-talked-about-enough-452692529a2b> accessed 5 January 2024; N Lawrence, 'UI/UX Design: 5 Major Ethics' (*UX Planet*, 24 January 2022) <https://uxplanet.org/ui-ux-design-5-major-ethics-116a7fc14df7> accessed 5 January 2024. Studies and courses are also emerging to teach ethical design to UX students, see G N Vilaza and P Bækgaard, 'Teaching User Experience Design Ethics to Engineering Students: Lessons Learned' (2022) 4 *Frontiers in Computer Science* 793879.

controlled browser gatekeeping mechanisms. The second option – preferred by the authors of Chapter 11 – proposes a new approach to data regulation,[91] namely, to regulate data use in OBA, dissecting different options – substantive prohibitions, the disclosure of ad selection criteria and the regulatory attitudes necessary for effective oversight.

1.3.6 Biometrics: Facial Recognition and Emotional AI

The processing of biometric data also raises questions under the GDPR. A typical example is that of facial recognition technologies (FRT), which are used for various purposes, including policing and law enforcement, welfare and banking. While a biometric identification system (BIS) identifies natural persons on the basis of biometric data, a biometric categorization system (BCS) is able to assign a natural person to specific categories, such as sex, age, ethnic origin or sexual or political orientation.[92] An emotion recognition system (ERS), on the other hand, tries to detect different emotions through the integration of information from facial expressions, body movement, gestures and speech.[93]

The use of biometrics has sparked concerns around the world.[94] While many organizations and lawmakers advocate for strict(er) regulation or bans,[95] the GDPR has been criticized for its non-specific and general approach towards the use of biometrics[96] and for its heavy reliance on procedural safeguards, which may not be sufficient to counteract the expansion of state and corporate power enabled by this technology.[97]

Against this backdrop, the regulation of biometrics was one of the most contentious issues during the negotiations on the AI Act. In its proposal, the European Commission advocated prohibiting (with notable exceptions) real-time remote biometric systems used in publicly accessible spaces for law enforcement purposes,[98] while other forms of BIS were (partially) recognized as high-risk AI

[91] F Galli and G Sartor, Chapter 11, in this book.

[92] Cf., Art. 3(40) AI Act; C Wendehorst and Y Duller, 'Biometric Recognition and Behavioural Detection' *Study Requested by the JURI and PETI Committees of the European Parliament, PE 696.968*, August 2021 56ff, available 28 July 2022 at: <www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf> accessed 5 January 2024.

[93] Cf., Art. 3(39) AI Act.

[94] T Madiega and H Mildebrath, *Regulating Facial Recognition in the EU* (European Parliament 2021) 32–34.

[95] V L Raposo, '(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation' (2023) 32 *Information & Communications Technology Law* 45; J Vincent, 'Automatic Gender Recognition Tech Is Dangerous, Say Campaigners: It's Time to Ban It' (*The Verge*, 14 April 2021) <www.theverge.com/2021/4/14/22381370/automatic-gender-recognition-sexual-orientation-facial-ai-analysis-ban-campaign> accessed 5 January 2024; cf., M Zahn, 'Controversy Illuminates Rise of Facial Recognition in Private Sector' (*ABC News*, 8 January 2023) <https://abcnews.go.com/Business/controversy-illuminates-rise-facial-recognition-private-sector/story?id=96116545> accessed 5 January 2024.

[96] M Zalnieriute, Chapter 12 in this book.

[97] Ibid., Section 12.6.

[98] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM(2021) 206 final, Art. 5(1)(d).

systems.[99] BCS and ERS, on the other hand, were only subject to transparency obligations[100] and were not necessarily considered high-risk under the Commission's proposal,[101] even though these systems have a history of bias.

In contrast, the European Parliament insisted in its negotiating position[102] for a full ban of: (i) real-time remote BIS in publicly accessible spaces; (ii) "post" remote BIS, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorization; (iii) BCS using sensitive characteristics; and (iv) ERS in law enforcement, border management, workplaces and educational institutions.

The compromise agreement reached on 8 December 2023 took a middle course, according to the press releases of the Council[103] and the European Parliament.[104] Recognizing the potential threat to citizens' rights, the co-legislators agreed to prohibit in Art. 5(1) AI Act the following: (i) untargeted scraping of facial images from the Internet or CCTV footage to create or expand facial recognition databases; (ii) ERS in workplaces and educational institutions; (iii) BCS that use sensitive characteristics; and (iv) real-time remote BIS in publicly accessible spaces for the purpose of law enforcement, unless and in so far as such use is strictly necessary under certain conditions.

1.4 The GDPR and Its Relationship to EU Digital Law

Since 2018, the European legislature has adopted and proposed new legal acts regulating issues related to digitalization and data economy that will interact with the GDPR in cases when personal data is being processed, the most recent of these being the proposed Financial Data Access Regulation.[105] The texts of these legal acts are characterized by the difficulty of the EU legislature to reconcile the aims of data protection and data economy/innovation, as these aims are partially contradictory. There are structural controversies such as the principle of data minimization versus the interest in large data pools.[106] In a recently published position paper on the GDPR, the Council of the European Union stressed that any new EU legislation containing provisions on the processing of personal data should be consistent with the GDPR and with ECJ case law.[107]

[99] Annex III.1.a. AI Act Proposal of the European Commission.

[100] Art. 52 AI Act Proposal of the European Commission.

[101] Critically discussed in M Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' <www.mdpi.com/2571-8800/4/4/43> accessed 5 January 2024; N A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991> accessed 5 January 2024.

[102] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts, P9_TA(2023)0236.

[103] Council of the EU, Press Release 986/23 of 9 December 2023.

[104] European Parliament, Press Release 20231206IPR15699, of 9 December 2023.

[105] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access and Amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM(2023) 360 final.

[106] D Tolks, 'Die finale Fassung des Data Governance Act' (2022) *Multimedia und Recht* 444.

[107] Council of the European Union, Council position and findings on the application of the General Data Protection Regulation (GDPR), 15507/23, 17 November 2023, para 40.

As Specht-Riemenschneider observes, “regulatory addressees will regularly find themselves in the situation of acting contrary to data protection law or of acting contrary to the obligations under the data law.”[108] Although the GDPR has been called an elephant in the room for data economy, it is also argued that it should not be considered an antagonist to data exchange but rather an expression of the standards to which the exchange of personal data in the EU must adhere.[109]

Subsequent sections describe the complicated interplay of the GDPR with the most important EU digital law legislative initiatives: Data Governance Act,[110] Digital Services Act,[111] Data Act[112] and the very recently adopted AI Act,[113] as well as the EHDS proposal[114] that is still in the negotiation phase. It highlights certain inconsistencies as well as issues that have been solved during the legislative process.

1.4.1 GDPR and Data Governance Act

The Data Governance Act (DGA) – applicable since September 2023 – regulates conditions, structures and procedures of data use for individuals, public bodies and traders. Its relationship with the GDPR is set forth in Art. 1(3) DGA, stating that the Act is without prejudice to data protection law. It further clarifies that in case of a conflict between the DGA and European or national data protection law, the latter has priority. It is, however, quite tricky to determine when there is a conflict between these regimes, as the GDPR has many open clauses that entitle the EU legislature to adopt further regulation and, in some cases, the provisions of the DGA could be considered such further regulation and thus a filler of the GDPR’s opening clauses.[115]

[108] L Specht-Riemenschneider, ‘Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO’ (2023) *Zeitschrift für Europäisches Privatrecht* 638.

[109] C Wendehorst, ‘Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy’ in S Lohsse, R Schulze and D Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos/Hart Publishing 2017); B P Paal and M Fenik, ‘Access to Data in the Data Act Proposal’ (2023) *Zeitschrift für Digitalisierung und Recht* 249.

[110] 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 L152/1.

[111] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[112] 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 L1.

[113] While the AI Act had not yet been published in the Official Journal of the EU, at the time of writing this chapter, the authors have taken into account the final version which was approved by the European Parliament (March 13, 2024), by the Council (May 21, 2024) and finally signed into law (June 13, 2024), PE-CONS 24/1/24 REV 1, available at: https://data.consilium.europa.eu/doc/document/PE-24-2024-REV-1/en/pdf.

[114] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022)197 final.

[115] L Specht-Riemenschneider (n 108). It is further unclear whether the GDPR and the DGA are parallelly applicable to mixed datasets. R Gellert and I Graef, ‘The European Commission’s Proposed

For example, it has been argued that Art. 12(a) and (e) DGA that regulate the provision of data intermediation services should be understood as a Union law within the meaning of Art. 6(4) GDPR setting forth the compatibility test for the further use of personal data.[116] This interpretation would mean that the original legal basis for data processing is enough, and a new legal basis is not needed for data processing under Art. 12(a) and (e) DGA. Article 1(3) DGA states that the DGA does not create a legal basis for personal data processing, nor does it affect any of the rights and obligations set out in the EU data protection law. Therefore, the aforementioned Art. 12(d) and (e) DGA are not to be seen as independent legal bases but only as additional requirements for certain data processing activities that must be met in addition to the legal basis of the GDPR.[117]

As the DGA aims to strengthen the trust of market actors in data intermediaries,[118] one of the crucial issues is how data intermediaries – including the Personal Information Management Systems (PIMS) – can foster the exchange of personal data to manage the consent and support data subjects in exercising their data-related rights. On this, several authors have argued that the answer to these questions should be found in the data protection law and not the DGA. However, it is still unclear whether (for instance) the possibility of the data holder to mandate data trustees can be contractually excluded.[119] The DGA does not provide any rules on that issue and simply sets further requirements in addition to the requirements of the GDPR.[120]

The interplay of the DGA and GDPR is also reflected in the important issue of liability of data intermediaries. Under the DGA, data intermediaries have a fiduciary duty toward individuals to ensure that they act in the best interest of the data subjects. Before the adoption of the DGA, it was discussed whether it should set out rules on the liability of data trustees for data breaches that the trustee should have foreseen.[121] In the final version, this important issue – that also arises in the case of the Estonian consent service[122] – is left to the national liability regimes.[123] Hence, the validity of contractual liability restrictions also depends on national contract law. However, if the data intermediary breaches this fiduciary duty, such intermediary may be qualified as a joint controller within the meaning of Art. 26 GDPR and, hence, be liable for the material and immaterial damages inflicted to the data subject under Art. 82 GDPR.[124]

Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing' *TILEC Discussion Paper No DP2021–006* (2021) 16.

[116] L Specht-Riemenschneider (n 108).

[117] Ibid., 638, 658.

[118] See recitals 4 and 5 DGA.

[119] H Richter, 'Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing' (2023) 72 *GRUR International* 458; Tolks (n 106) 444.

[120] L Specht-Riemenschneider (n 108) 656.

[121] H Richter (n 119) 467.

[122] K Sein, Chapter 3 in this book.

[123] Recital 33 DGA.

[124] J Kühling, 'Der datenschutzrechtliche Rahmen für Datentreuhänder' (2021) *Zeitschrift für Digitalisierung und Recht* 26.

1.4.2 GDPR and Digital Services Act

The Digital Services Act (DSA) aims to foster a safe, predictable and trusted online environment by laying down harmonized rules on the provision of intermediary services. As providing digital intermediary services is inextricably linked to processing personal data, the regimes of DSA and GDPR become intertwined. Similar to other EU digital law acts, its interplay with the data protection law is characterized by the "without prejudice" rule in Art. 2(4)(g) DSA. Again, it is prone to create uncertainties as to its consequences. First, it is unclear whether provisions of the DSA can create a legal obligation and hence a legal basis for data processing within the meaning of Art. 6(1)(c) GDPR. Presumably, this is the case – provided that the requirements in Art. 6(3) GDPR are met.[125] Furthermore, certain provisions of the DSA stress that the compliance with its obligations places no obligation on online platform providers to process more personal data than they already have.[126]

Second, the DSA will interact with data protection law (as well as EU consumer law) in cases of dark patterns. According to Art. 25(2) DSA, the prohibition of dark patterns in Art. 25(1) DSA does not apply to practices covered by the UCPD or the GDPR. Consequently, it will only be applicable to such dark patterns that do not rely upon processing of personal data. This provision, leading to the mutual exclusivity of the DSA and GDPR (and UCPD) will be counterproductive to the aim of fighting dark patterns as its unclear content will render enforcement overly complicated and hence ineffective.[127]

Finally, Arts. 26, 28 and 38 DSA complement the rules of the GDPR on profiling, forbidding presenting advertisements based on profiling using special categories of personal data or the personal data of minors and obliging the very large online platforms and very large online search engines to provide at least one recommender system not based on profiling. Hence, the protection of privacy in the EU is not restricted to the GDPR but is also fostered by certain digital law acts. At the same time, it should be noted that this additional layer of protection only applies to these players that are not micro and small-sized enterprises, whereas the rules of the GDPR continue to apply to all data controllers, notwithstanding their size.

Last but not least, the complicated relationship between the GDPR and the DSA becomes obvious in case of liability of intermediary services providers. According to Art. 2(4) GDPR, these rules remain untouched by the GDPR. Yet, in turn, under Art. 2(4)(g) DSA, its provisions are without prejudice to the GDPR. Consequently, both regimes are applicable in parallel and hence the online platform providers cannot rely upon the safe harbor privileges of the DSA in case of data protection breaches.

[125] S Schwamberger, 'Zusammenspiel und Friktionen mit anderen Rechtsakten' in B Steinrötter (ed), *Europäische Platformregulierung* (Nomos 2023) 273.

[126] See Art. 28(3) and recitals (71) and (77) DSA.

[127] See, in detail, the European Law Institute, Response to the European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law (2023) 9–10. It rightly suggests deleting Art. 25(2) DSA.

1.4.3 GDPR and Data Act

The recently adopted Data Act (DA) regulates, inter alia, the access rights of users as well as the contractual relationships between different actors of the data economy. Both the new DA as well as the GDPR break up the de facto monopoly of data holders by requiring a legal basis (GDPR) or user's permission (DA) for the use of data.[128] The Commission's DA proposal was criticized as to its unclear relationship with EU data protection rules – most importantly with the GDPR. While many of these critical points have been addressed and solved during the legislative procedure, some are still left open. For example, originally, even the question of whether the DA applies at all to personal data was disputed in the legal literature.[129] Yet, the final text of Art. 1(2) DA clearly states that the Act applies both to personal and non-personal data. Indeed, in the case of IoT,[130] data is usually connected with a person and hence qualifies as personal data within the meaning of the GDPR. It should also be kept in mind that the protection of personal data under the GDPR goes way beyond the protection of the product and related services data under the DA.[131]

The criticism about the unclear meaning of Art. 1(2) (third sentence) of the Commission's proposal declaring that the DA does not affect the applicability of the GDPR[132] is taken into account and reflected in Art. 1(3) of the final text – which states that in case of contradictions the data protection rules should take precedence. In addition, Art. 1(5) DA clarifies the relationship of the data access and data portability rules of DA and GDPR, stating that these regimes are complementary.

In the case of the data access rights under the DA, it has been questioned whether (for instance) Art. 3(1) DA constitutes an independent legal basis for data processing or should at least be qualified as a legal obligation within the meaning of Art. 6(1)(c) GDPR.[133] Although plausible at the first sight, the EDPS and EDPB have correctly pointed out the privacy risks associated with such interpretation. For example, in case of employer-owned smart products, this could lead to a violation of data subjects' rights when the employer provides its employees with a virtual voice assistant and uses its right of direct access under Art. 3(1) DA to monitor their search history.[134] Moreover, in case of sensitive personal data, such interpretation would be contrary to Art. 9 GDPR. The final texts of Art. 4(12) and Art. 5(7) DA rightly provide that, if the user is not the data subject whose personal data is requested, any personal data generated by the use

[128] B J Hartmann, R McGuire and H Schulte-Nölke, 'Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act)' (2023) *Recht Digital* 49.

[129] B Steinrötter, 'Verhältnis von Data Act und DS-GVO' (2023) *GRUR International* 216.

[130] See Recital 14 DA listing IoT objects (connected products) such as household and medical appliances or cars: data created by these smart objects will in most cases qualify as personal data and hence lead to the parallel applicability of the GDPR.

[131] S Assion and L Willecke, 'Der EU Data Act. Die neuen Regelungen zu vernetzten Produkten und Diensten' (2023) *Multimedia und Recht* 805.

[132] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)' COM (2022) 68 final, 4.

[133] B Steinrötter, 'Verhältnis von Data Act und DS-GVO' (n 129) 220.

[134] EDPB and EDPS, Joint Opinion 2/2022 on the Proposal of the Data Act, 10.

of a product or related service may only be made available by the data holder if there is a valid legal basis.[135] Consequently, Arts. 4 and 5 DA can constitute a legal basis for personal data processing only in cases when the data subject is the user. In other cases, i.e., when the user is not the data subject but an employer, the user must prove that he/she has a legal basis for the data transfer – like the consent of the data subject.

Finally, it has been rightly pointed out that after the enactment of the Data Act, distinguishing between personal and non-personal data will become vitally important, as an incorrect classification will lead to a violation of either the DA or the GDPR.[136] This will become extremely complicated in case of mixed datasets and mean considerable legal uncertainty for data holders.

1.4.4 GDPR and AI Act

The recently adopted AI Act is a horizontal instrument[137] that applies in addition to existing EU legislation. Article 2(7) AI Act clarifies that the regulation does not affect EU data protection law,[138] in particular the GDPR, the LED[139] or the EUDPR.[140] Accordingly, AI systems the use personal data must comply with both the AI Act and EU data protection law. This is only logical, as the GDPR, the LED and the EUDPR establish a detailed and comprehensive system for the protection of personal data in the EU. The AI Act, on the other hand, does not contain explicit preconditions for AI systems to comply with the GDPR requirements in order to

[135] Recital 7 DA further explains that:

> Where the user is not the data subject, this Regulation does not create a legal basis to provide access to personal data or make it available to a third party and should not be understood as conferring any new right on the data holder to use personal data generated by the use of a product or related service. In these cases, it could be in the interest of the user to facilitate meeting the requirements of Article 6 of Regulation (EU) 2016/679. As this Regulation should not adversely affect the data protection rights of others, including the data subject, the data holder can comply with requests inter alia by anonymizing personal data or transferring only personal data relating to the user.

[136] D Bomhard and M Merkle, 'Der Entwurf eines EU Data Acts' (2022) *Recht Digital* 168.

[137] Cf., M Ebers, 'Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act' in L A DeMatteo, C Poncibò and M Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022) 13.

[138] Explicitly excluded are, according to Art. 2(7)(2) AI Act, data processing for the purpose of ensuring bias detection in high-risk AI systems (Art. 10[5] AI Act) and data processing in AI regulatory sandboxes (Art. 59 AI Act).

[139] 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 [2016] OJ L119/89.

[140] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

enter the European market – although both the EDPS and the EDPB asked the co-legislators to include such a requirement in the AI Act. In particular, both bodies recommended that the certification of high-risk AI systems should expressly include a verification of compliance with the GDPR.[141] In contrast, Recital 63 AI Act points out that the fact that an AI system is classified as a high-risk AI system

> should not be interpreted as indicating that the use of the system is lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons.

Additionally, Recital 63 clarifies that the AI Act "should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant" unless it is specifically provided for otherwise in the AI Act.

As the AI Act and EU data protection law apply in parallel, both the EDPB and the EDPS pointed out that it is important for the AI Act to clearly avoid any inconsistencies and possible conflicts with the GDPR, the LED and the EUDPR.[142] Indeed, several concepts and provisions of the AI Act overlap with EU data protection law, potentially leading to legal uncertainties, diverse interpretations and contradictions. For example, both the GDPR and the AI Act impose transparency obligations, but the scope and the requirements are regulated differently under the two acts.[143] Another example is the requirement for human intervention and/or human oversight. While the GDPR requires human intervention for decisions based solely on automated processing, including profiling (Art. 22[3] GDPR), the AI Act requires human oversight for high-risk AI systems (Art. 14 AI Act).

In addition, the AI Act carries the risk of creating parallel enforcement structures with data protection authorities, which could also lead to legal uncertainty.[144] While the EDPB and the EDPS stressed that the national data protection authorities should be entrusted with the enforcement of the AI Act,[145] Art. 70 AI Act leaves

[141] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act), 18 June 2021, para 23; EDPS, Opinion 44/2023 on the Proposal for AI Act in the light of legislative, 23 October 2023, para 27.

[142] EDPB-EDPS, Joint Opinion 5/2021, para 57.

[143] The GDPR establishes the principle of transparency to facilitate the exercise of data subjects' rights under Art. 15–22, including the right to erasure, to rectification and to data portability. In contrast, the AI Act contains transparency obligations only for high-risk AI systems (Art. 13 AI Act) and for other certain AI systems (Art. 50 AI Act). Moreover, Art. 13 AI Act focuses on the interests of the deployer of an AI system rather than on the final user and/or data subject.

[144] P Hajduk, 'AI Act and GDPR: On the Path Towards Overlap of the Enforcement Structures' (*RAILS-Blogpost*, 1 October 2023) <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/> accessed 5 January 2024.

[145] EDPB-EDPS, Joint Opinion 5/2021, para 48.

the designation of competent authorities to the Member States.[146] This will most likely lead to the authorization of different entities with overlapping competences, as shown by the example of the recently created Spanish Agency for the Supervision of AI.[147]

1.4.5 The GDPR and the European Health Data Space Act

While the previously discussed legal acts were cross-sectoral, the new EHDS Act proposal would only cover a narrow sector of medical data, aiming at encouraging innovation and research and thereby facilitating better healthcare. Yet, as is also the case with the previously discussed legislation, the EHDS is characterized by the complicated interplay with data protection law. In their joint opinion on the proposal, the EDPB and the EDPS note that the EHDS will add yet another layer to the already extremely complex set of provisions under the EU and national law on health data processing and call for further clarification.[148]

Most importantly, there is considerable legal uncertainty as to the EHDS Act's linkage with the legal bases for personal data processing under the GDPR. In several instances, the EHDS does not seem to be in line with the requirement of the GDPR that every data processing must have a legal basis. For example, the EDPB and the EDPS note that Art. 4(1) EHDS Proposal, which grants every health professional access to the electronic health data of natural persons under their treatment, is not in line with the data minimization and purpose limitation principles, since access is not granted independently of whether it is necessary and only on a need-to-know basis.[149]

Similarly, there is a problem with the legal basis requirement under Art. 34(1)(f) EHDS Proposal which obliges health data access bodies to grant access to electronic health data whereby the intended purpose of processing is "development and innovation activities for products or services contributing to public health or social security or ensuring high levels of quality and safety of healthcare, of medicinal products or of medical devices." According to the Commission's proposal, the EHDS is meant to complement it and function as "the Union law" within the meaning of Art. 9(2) GDPR. Recital 37 EHDS Proposal states that "[t]his Regulation also meets the conditions for such processing pursuant to Arts. 9(2)(h),(i),(j) of the Regulation (EU) 2016/679," indicating that by meeting the purpose of development and innovation activity, the data user automatically satisfies the legal basis requirement under Art. 9(2)(h), (i) or (j) GDPR as well. Hence the proposal

[146] See also Recital 157 AI Act: "This Regulation is without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise the application of Union law protecting fundamental rights, including equality bodies and data protection authorities."

[147] <https://decrypt.co/153482/spain-just-created-the-first-european-ai-supervision-agency> accessed 5 January 2024.

[148] EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space 3.

[149] Ibid., 17.

proceeds from the assumption that the user does not need to prove compliance with Art. 9 GDPR separately.[150] Yet, it has been demonstrated that while in many cases, Art. 9(2)(j) GDPR is an appropriate legal basis for development and innovation activities with health data, and in exceptional cases, reliance on Art. 9(2)(h) and Art. 9(2)(i) is also possible, this is not necessarily so in all cases where health data is used for development and innovation activities.[151] Therefore, it is plausible to conclude that the EHDS Proposal, as it currently stands, does not fully comply with the legal basis requirement of Art. 9 GDPR.

The EDPB and the EDPS have also expressed the view that to guarantee the protection of personal data, the EHDS should be further circumscribed when there is a sufficient connection with public health and/or social security within the meaning of Art. 34(1) EHDS, and that the criteria of the GDPR should additionally be taken into account when deciding upon issuance of the data access permit.[152] Moreover, the EDPB and the EDPS recommend excluding wellness applications and other digital applications, as well as wellness and behavior-related health data from Art. 33(1)(f) EHDS, or at least subjecting them to the requirement of consent. Should these applications remain within the scope of the EHDS, they further recommend including a reference to the ePrivacy Directive.[153] Finally, there is a need for legal clarity on the interplay between the data subject's rights under the EDHS and under the GDPR.[154]

1.5 Conclusions and Outlook

Data protection is and remains a vital component of responsible and ethical innovation. We should only allow technology that complies with our core values and ethical principles, and we should not modify these principles just because there is new technology available on the market. As Gerald Spindler stresses in his Chapter 8 of this book on blockchain and data protection, when discussing the right to be forgotten in case of blockchain technology: "Thus, the argument with regard to Art. 17 GDPR that deletion is fundamentally unreasonable cannot be accepted either, because the technology is deliberately used here."[155] His reference to Steinrötter that otherwise the legal system would always have to capitulate when persons deliberately maneuver themselves into a situation that makes it impossible to enforce

[150] Artt 33(1), 45(1, 2), 45(4), 46(1) EHDS; M Shabani and S Yilmaz, 'Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS' (2022) *Technology and Regulation* 128; S Slokenberga, 'Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject That the Proposed EHDS Regulation Promises to Bring Along' (2022) *Technology and Regulation* 135.

[151] M Kruus, 'Development and Innovation Activities with Health Data: On What Legal Basis? Examples of Estonia, Finland, and the EHDS Proposal' (2023) *European Journal of Health Law* 97.

[152] EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space 3.

[153] Ibid., 4, 9.

[154] Ibid., 4.

[155] G Spindler, Chapter 8, in this book.

the law[156] (e.g., by using certain technology) is of utmost importance. Instead of constantly changing the law, we should try to develop and deploy technology that complies with existing law.

Nevertheless, new technologies are leading us to rethink certain central issues of privacy law. First, a risk-based approach may be better suited to the era of Big Data and data-intensive technologies than the current "one-size-fits-all" approach. Estonia's recent example of a major data leak – which potentially affected more than 10,000 individuals when a genetic testing laboratory fell victim to a cyber-attack – is a good illustration of the high risks to privacy posed by evolving technologies. The leaked data arguably included paternity tests, fertility tests and tests related to genetic conditions.[157] At the same time, it also shows that technology could be of cure and prevention. The head of the Estonian Data Protection Inspectorate argued that the consequences of the leak could have been mitigated if the health data had been encrypted or pseudonymized.[158] Therefore, investing more in privacy-enhancing technology and raising awareness about the importance of its use, especially for high-risk data, would be an important step forward.

Second, technological developments have highlighted, more clearly, the problem of the primacy of consent over other legal bases for data processing. Although this problem existed before the era of Big Data and AI, it is now impossible to ignore. As a result, we should rely more on statutory legal bases (and possibly modify them in certain cases) in order to take into account the public interest in innovation. Similarly, the Estonian biobanking example shows that the "one-size-fits-all" approach to consent for data processing under the GDPR is not feasible when it comes to biobanks and genetic research.[159] Additionally, when consent is used as a legal basis, there is an increasing need to use dynamic consent models.[160]

Another problem related to the data-driven technologies and the protection of personal data is the growing intertwining of data protection and data law. The new EU legal initiatives concerning digitalization and data create new legal challenges and uncertainties regarding the coherence of the instruments and their interrelationship with the data protection framework. These inconsistencies are rooted in the difficulty to reconcile the aims of data protection and data economy/innovation. On a positive note, some of them have already been corrected during the legislative process. However, some still remain and can only be fully resolved through case law. In addition, the Council of the EU has recently encouraged the EDPB to adopt specific opinions and guidelines to clarify how the provisions of the GDPR should be applied together

[156] B Steinrötter, 'Datenschutzrechtliche Probleme beim Einsatz der Blockchain' (2021) *Zeitschrift für Bankrecht und Bankwirtschaft* 373.

[157] ERR, 'Paternity and Fertility Tests Among Data Stolen in Asper Biogene Cyberattack' (15 December 2023) <https://news.err.ee/1609195705/paternity-and-fertility-tests-among-data-stolen-in-asper-biogene-cyberattack> accessed 5 January 2024.

[158] Ibid.

[159] See K Pormeister, Chapter 4 in this book.

[160] Cf., thereto M Ebers, Chapter 9 in this book.

with, inter alia, the DMA, the DSA, the DGA, the DA, the AI Act, etc.[161] Such guidelines would be essential for legal certainty, especially if they take into account – as the Council suggests – the development of the digital economy in the Union and the need to support innovation and the development of new technologies.[162] Otherwise, it would often be extremely complicated for data controllers to ensure compliance with all these legal frameworks at the same time. This would be even more complex in the case of mixed datasets.

Finally, we should also recognize the limits of data protection law in protecting individuals and groups from the unfair use of Big Data. It is not the task of data protection law to address all possibilities of misuse of personal data. Specific technology-oriented regulations, such as the recently adopted AI Act, and other areas of law – such as competition law, civil law, anti-discrimination law and criminal law – should primarily address the harmful use of personal data and ensure that we as citizens can benefit from the development of technology while preserving our privacy.

Bibliography

Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN 16

Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (30 May 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> accessed 5 January 2024

Assion S and Willecke L, 'Der EU Data Act. Die neuen Regelungen zu vernetzten Produkten und Diensten' (2023) *Multimedia und Recht* 805

Bertuzzi L, 'MEPs Call for Infringement Procedure against Ireland' (*Euractiv*, 20 May 2021) <www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/> accessed 5 January 2024

Billhardt H and others, 'Agreement Technologies for Coordination in Smart Cities' (2018) 8(5) *Applied Sciences* Article 816

Bomhard D and Merkle M, 'Der Entwurf eines EU Data Acts' (2022) *Recht Digital* 168

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

Buchner B, *Informationelle Selbstbestimmung im Privatrecht* (Mohr Siebeck 2006)

Buchner B and Petri T, 'Art. 6 Rechtmäßigkeit der Verarbeitung' in Kühling J and Buchner B (eds), *DS-GVO-BDFG* (4th edn, C.H. Beck 2024)

Bull HP, *Sinn und Unsinn des Datenschutzrechts* (Mohr Siebeck 2015)

Cabral S, 'Forgetful AI: AI and the Right to Erasure under the GDPR' (2020) 6 *The European Data Protection Law Review* 378

Chen C, Frey CB and Presidente G, 'Disrupting Science' (Oxford Martin School Working Paper 2022) <www.oxfordmartin.ox.ac.uk/downloads/academic/Disrupting-Science-Upload-2022-4.pdf> accessed 5 January 2024

[161] Council of the European Union, Council position and findings on the application of the General Data Protection Regulation (GDPR), 15507/23, 17 November 2023, para 41.

[162] Council of the European Union, Council position and findings on the application of the General Data Protection Regulation (GDPR), 15507/23, 17 November 2023, para 20.

Custers B and Heijne AS, 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' (2022) 46 *Computer Law & Security Review* 1

De Gregorio G and Dunn P, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59(2) *Common Market Law Review* 473

Del Re E, 'Which Future Strategy and Policies for Privacy in 5G and Beyond?' (2020) *IEEE 3rd 5G World Forum (5GWF)* 236 <https://doi.org/10.1109/5gwf49715.2020.9221371> accessed 5 January 2024

Ebers M, 'Regulating AI and Robotics: Ethical and Legal Challenges' in Ebers M and Navas S (eds), *Algorithms and Law* (Cambridge University Press 2020) 37

Ebers M, 'Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act' in DeMatteo LA, Poncibò C and Cannarsa M (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022) 321

Ebers M and others, 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' <www.mdpi.com/2571-8800/4/4/43> accessed 5 January 2024

EDPB, Binding Decision 01/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art. 65 GDPR), adopted on 13 April 2023

EDPB, Guidelines 02/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects

EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679

EDPB, Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR

EDPB, Study on the Enforcement of GDPR Obligations against Entities Established Outside the EEA But Falling under Article 3(2) GDPR

EDPB and EDPS, Joint Opinion 02/2022 on the Proposal of the Data Act

EDPB and EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space

EDPB-EDPS, Joint Opinion 05/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 18 June 2021

EDPB-EDPS, Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Additional Procedural Rules Relating to the Enforcement of Regulation (EU) 2016/679

EDPS, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the Light of Legislative, 23 October 2023

Ernst S, 'Die Einwilligung nach der Datenschutzgrundverordnung' (2017) 3 *Zeitschrift für Datenschutz* 110

ERR, 'Paternity and Fertility Tests among Data Stolen in Asper Biogene Cyberattack' (15 December 2023) <https://news.err.ee/1609195705/paternity-and-fertility-tests-among-data-stolen-in-asper-biogene-cyberattack> accessed 5 January 2024

European Law Institute, 'Response to the European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law' (2023)

Finch M and Biega A, 'Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems' (2021) *Max Planck Institute for Innovation and Competition* (Research Paper Series) 1 <www.utupub.fi/bitstream/handle/10024/174974/Aho_Sami_progradu.pdf;jsessionid=0753DB2A519AD776DDBF1503DE5DDE70?sequence=1> accessed 5 January 2024

Finck M, 'Blockchain and the General Data Protection Regulation' (Study for the European Parliament, Panel for the Future of Science and Technology, PE 634.445, European Parliament 2019)

Finck M, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11(4) *International Data Privacy Law* 333

Floridi L, ‘Group Privacy: A Defence and an Interpretation’ in Taylor L, Floridi L and van der Sloot B (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3854483> accessed 5 January 2024

Floridi L, ‘Machine Unlearning: Its Nature, Scope, and Importance for a “Delete Culture”’ *Philosophy & Technology* (2023) <https://ssrn.com/abstract=4455976> accessed 5 January 2024

Gellert R, ‘The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission’s Proposed Artificial Intelligence Act: Business as Usual?’ (2021) 3(2) *Journal of Ethics and Legal Technologies* 15

Gellert R and Graef I, ‘The European Commission’s Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing’ (TILEC Discussion Paper No DP2021-006 2021) 16

Hacker P, *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB* (Mohr Siebeck 2020)

Hajduk P, ‘AI Act and GDPR: On the Path towards Overlap of the Enforcement Structures’ (*RAILS-Blogpost*, 1 October 2023) <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/> accessed 5 January 2024

Hartmann BJ, McGuire R and Schulte-Nölke H, ‘Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act)’ (2023) *Recht Digital* 49

Heine I, ‘3 Years Later: An Analysis of GDPR Enforcement’ (*Center for Strategic and International Studies*, 13 September 2021) <www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement> accessed 5 January 2024

Herresthal C, ‘Grundrechtecharta und Privatrecht’ (2014) *Zeitschrift für Europäisches Privatrecht* 238

Ho C, ‘Privacy and Transparency in Human-Robot Interaction’ in Barfield W, Weng Y and Pagallo U (eds), *Cambridge Handbook on Law, Policy, and Regulations for Human-Robot Interaction* (Cambridge University Press, 2024) 589

Hornung G, ‘Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012’ (2012) *Zeitschrift für Datenschutz* 101

Hornung G and Schomberg S, ‘Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Governance Acts’ (2022) *Computer und Recht* 508

Hsiao E, ‘Ethical Design: Obligations of a UX Designer That Are Never Talked about Enough’ (*BoorCamp UX Design*, 8 December 2022) <https://bootcamp.uxdesign.cc/ethical-design-obligations-of-a-ux-designer-thats-never-talked-about-enough-452692529a2b> accessed 5 January 2024

Ishii K, ‘Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects’ (2019) 34 *AI and Society* 509

Janßen R, Keßler R, Kummer ME and Waldfogel J, ‘GDPR and the Lost Generation of Innovative Apps’ (NBER Working Paper 30028 2022) <www.nber.org/system/files/working_papers/w30028/w30028.pdf> accessed 5 January 2024

Johnson GA, Shriver SK and Goldberg SG, ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’ (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686> accessed 5 January 2024

Kammourieh L and others, ‘Group Privacy in the Age of Big Data’ in Taylor L, Floridi L and van der Sloot B (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 37

Kramcsák PT, ‘Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?’ (2022) *Computer Law & Security Review* 1 <www.sciencedirect.com/science/article/abs/pii/S026736492200108X> accessed 5 January 2024

Krönke C, 'Datenpaternalismus' (2016) 55 *Der Staat* 319

Kruus M, 'Development and Innovation Activities with Health Data: On What Legal Basis? Examples of Estonia, Finland, and the EHDS Proposal' (2023) *European Journal of Health Law* 97

Kühling J, 'Der datenschutzrechtliche Rahmen für Datentreuhänder' (2021) *Zeitschrift für Digitalisierung und Recht* 26

Lancieri F, 'Narrowing Data Protection's Enforcement Gaps' (2022) 74 *Maine Law Review* 16 <https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1753&context=mlr> accessed 5 January 2024

Lawrence N, 'UI/UX Design: 5 Major Ethics' (*UX Planet*, 24 January 2022) <https://uxplanet.org/ui-ux-design-5-major-ethics-116a7fc14df7> accessed 5 January 2024

Lawson-Hetchley C, 'The Potential Impact of the Future AI Act on the GDPR' (Master's Thesis, University of Oslo 2022) <www.duo.uio.no/bitstream/handle/10852/101369/1/The-potential-impact-of-the-future-AI-Act-on-the-GDPR.pdf> accessed 5 January 2024; <www.euractiv.com/section/5g/interview/gdpr-could-obstruct-ai-development-mep-says/> accessed 5 January 2024

Li T, 'Algorithmic Destruction' (2022) 75(3) *SMU Law Review* <https://ssrn.com/abstract=4066845> accessed 5 January 2024

Li T, Fosch Villaronga E and Kieseberg P, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 *Computer Law & Security Review* 12 <www.sciencedirect.com/science/article/abs/pii/S0267364917302091> accessed 5 January 2024

Luck M and McBurney P, 'Computing as Interaction: Agent and Agreement Technologies' (IEEE SMC Conference on Distributed Human-Machine Systems 2008)

Madiega T and Mildebrath H, *Regulating Facial Recognition in the EU* (European Parliament 2021)

Mitrou L, 'Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"? (2018) 53 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914> accessed 5 January 2024

Moerel L and Prins C, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 5 January 2024

Mühlhoff R, 'Predictive Privacy: Towards an Applied Ethics of Data Analytics, Ethics and Information Technology' (2021) 23 *Ethics and Information Technology* 675 <https://link.springer.com/article/10.1007/s10676-021-09606-x> accessed 5 January 2024

Ossowski S (ed), *Agreement Technologies: Second International: Conference, AT 2013, Beijing, China, August 1–2, 2013: Proceedings* (Springer 2013)

Paal BP and Fenik M, 'Access to Data in the Data Act Proposal' (2023) *Zeitschrift für Digitalisierung und Recht* 249

Pałka P, 'Harmed While Anonymous' (2023) *Technology and Regulation* <https://techreg.org/article/view/13829> accessed 5 January 2024

Raposo VL, '(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation' (2023) 32 *Information & Communications Technology Law* 45

Reinhardt J, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in Albers M and Sarlet I (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022) <www.springerprofessional.de/realizing-the-fundamental-right-to-data-protection-in-a-digitize/20213844> accessed 5 January 2024

Richards N and Hartzog W, 'The Pathologies of Digital Consent' (2019) 96 *Washington University Law Review* 1461

Richter H, 'Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing' (2023) 72 *GRUR International* 458

Roßnagel A, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (2019) *Neue Juristische Wochenschrift* 1

Ruohonen J and Hjerppe K, 'The GDPR Enforcement Fines at Glance' (2022) 106 *Information Systems* 101876

Santos C and others, *Artificial Intelligence and Law* (2019) 1(2) <https://doi.org/10.1007/s10506-019-09259-8> accessed 5 January 2024

Sartor G, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' *European Parliamentary Research Service* (2020) <www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 5 January 2024

Sattler A, 'Personenbezogene Daten als Leistungsgegenstand' (2017) 72(21) *Juristen Zeitung* 1036

Scheutz M, 'The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots' in Lin P, Abney K and Bekey GA (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (The MIT Press 2012)

Schrey J and Thalhofer T, 'Rechtliche Aspekte der Blockchain' (2017) *Neue Juristische Wochenschrift* 1431

Schwamberger S, 'Zusammenspiel und Friktionen mit anderen Rechtsakten' in Steinrötter B (ed), *Europäische Platformregulierung* (Nomos 2023) 255–288

Sein K, 'The Growing Interplay of Consumer and Data Protection Law' in Micklitz H-W and Twigg-Flesner C (eds), *The Transformation of Consumer Law and Policy in Europe* (Bloomsbury 2023) 139

Shabani M and Yilmaz S, 'Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS' (2022) *Technology and Regulation* 128

Slokenberga S, 'Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject That the Proposed EHDS Regulation Promises to Bring Along' (2022) *Technology and Regulation* 135

Smuha NA and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991> accessed 5 January 2024

Solove DJ, 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law' (2024) 104 *Boston University Law Review* 593

Solove DJ and Hartzog W, 'Kafka in the Age of AI and the Futility of Privacy as Control' (2024) 104 *Boston University Law Review* forthcoming

Specht-Riemenschneider L, 'Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO' (2023) *Zeitschrift für Europäisches Privatrecht* 638

Steinrötter B, 'Datenschutzrechtliche Probleme beim Einsatz der Blockchain' (2021) *Zeitschrift für Bankrecht und Bankwirtschaft* 373

Steinrötter B, 'Verhältnis von Data Act und DS-GVO' (2023) *GRUR International* 216

Tolks D, 'Die finale Fassung des Data Governance Act' (2022) *Multimedia und Recht* 444

Tzanou M, 'Addressing Big Data and AI Challenges: A Taxonomy and Why the GDPR Cannot Provide a One-Size-Fits-All Solution' in M Tzanou (ed), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Routledge 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654119> accessed 5 January 2024

Vilaza GN and Bækgaard P, 'Teaching User Experience Design Ethics to Engineering Students: Lessons Learned' (2022) 4 *Frontiers in Computer Science* 793879

Vincent J, 'Automatic Gender Recognition Tech Is Dangerous, Say Campaigners: It's Time to Ban It' (*The Verge*, 14 April 2021) <www.theverge.com/2021/4/14/22381370/automatic-gender-recognition-sexual-orientation-facial-ai-analysis-ban-campaign> accessed 5 January 2024

Von Lewinski K, *Die Matrix des Datenschutzrechts* (Mohr Siebeck 2014) <www.mohrsiebeck.com/buch/die-matrix-des-datenschutzes-9783161533730?no_cache=1> accessed 5 January 2024

Voss A, 'Position Paper on Fixing the GDPR: Towards Version 2.0' (2021) <www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf> accessed 5 January 2024

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review* 1

Wendehorst C, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Lohsse S, Schulze R and Staudenmayer D (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos/Hart Publishing 2017) 327

Wendehorst C and Duller Y, 'Biometric Recognition and Behavioural Detection' (Study Requested by the JURI and PETI Committees of the European Parliament, PE 696.968, August 2021) <www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf> accessed 5 January 2024

Wittner FN, *Verantwortlichkeit in Komplexen Ökosystemen: Attempt to Further Develop Data Protection in the Context of Distributed Processing Reality* (Mohr Siebeck 2022)

Zahn M, 'Controversy Illuminates Rise of Facial Recognition in Private Sector' (*ABC News*, 8 January 2023) <https://abcnews.go.com/Business/controversy-illuminates-rise-facial-recognition-private-sector/story?id=96116545> accessed 5 January 2024