jipitec

2| 2025

Volume 16 (2025)
Issue 2 ISSN 2190-3387

Editorial
by Miquel Peguera Poch

Articles

Common European Data Space for Cultural Heritage: Is the EU Taking the 'High Road' from 'A Single Access Point' to 'A Single Market for Data' for Digital Cultural Content?
by Pelin Turan and Caterina Sganga

Clouds Connecting Europe: Interoperability in the EU Data Act
by Leonie Ott and Yifeng Dong

Synthetic Data, Data Protection and Copyright in an Era of Generative AI
by Kalpana Tyagi

From Curators to Creators: Navigating Regulatory Challenges for General-Purpose Generative AI in Europe
by Gabriel Ernesto Melian Pérez

Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?
by Nicolaj Feltes

Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation
by Agustina Del Campo, Nicolas Zara, and Ramiro Álvarez Ugarte

The duty of care of online platforms in defamation cases
by Laura Herrerías Castro

The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry
by Stephanie Rossello

The European Union's Pursuit of Digital Sovereignty through Legislation
by Lukas v. Ditfurth

Opinion

Opinión of the European Copyright Society: An EU Copyright Framework for Research
by Caterina Sganga, Christophe Geiger, Thomas Margoni, Martin Senftleben, Mireille van Eechoud

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

2025

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 16 Issue 2 September 2025
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J. (NYU)
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M. (Harvard)
Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin

Prof. Dr. Gerald Spindler (†)
Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

by Miquel Peguera Poch 130

Articles

Common European Data Space for Cultural Heritage: Is the EU Taking the 'High Road' from 'A Single Access Point' to 'A Single Market for Data' for Digital Cultural Content? 133
by Pelin Turan and Caterina Sganga

Clouds Connecting Europe: Interoperability in the EU Data Act 154
by Leonie Ott and Yifeng Dong

Synthetic Data, Data Protection and Copyright in an Era of Generative AI 176
by Kalpana Tyagi

From Curators to Creators: Navigating Regulatory Challenges for General-Purpose Generative AI in Europe 201
by Gabriel Ernesto Melian Pérez

Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft? 222
by Nicolaj Feltes

Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation 238
by Agustina Del Campo, Nicolas Zara, and Ramiro Álvarez Ugarte

The duty of care of online platforms in defamation cases 252
by Laura Herrerías Castro

The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry 270
by Stephanie Rossello

The European Union's Pursuit of Digital Sovereignty through Legislation 286
by Lukas v. Ditfurth

Opinion

Opinión of the European Copyright Society: An EU Copyright Framework for Research 312
by Caterina Sganga, Christophe Geiger, Thomas Margoni, Martin Senftleben, Mireille van Eechoud

Editorial

by **Miquel Peguera Poch**

Recommended citation: Miquel Peguera Poch, Editorial, 16 (2025) JIPITEC 130 para 1.

1 In the midst of rapid evolution in the field of law and technology, the contributions to this new issue of JIPITEC address a range of sensitive topics in the areas of data governance, AI regulation, online speech, data protection, digital sovereignty, and copyright.

2 The first two articles refer to different aspects of **data governance**. The contribution by **Pelin Turan** and **Caterina Sganga**, "**Common European Data Space for Cultural Heritage: Is the EU Taking the 'High Road' from 'A Single Access Point' to 'A Single Market for Data' for Digital Cultural Content?**", explores the legal challenges for the successful deployment of the Common European Data Space for Cultural Heritage (CHDS), launched in 2021 as one of the fourteen sector-specific data spaces within the European Strategy for Data. The authors argue that the CHDS risks becoming a mere 'single access point' rather than a true single market for data. This results, on the one hand, from the lack of adjustment of the legal framework supporting the CHDS, which lies at the intersection of cultural heritage law, data law, and copyright law; and, on the other hand, from the significant influence of the *Europeana* project, which was in fact conceived as a single access point for cultural content. The authors put forward normative proposals to remove the obstacles to a proper deployment and operationalisation of the CHDS as an interoperable and federated infrastructure for the free flow and reuse of cultural heritage data. Also in the field of data governance, **Leonie Ott** and **Yifeng Dong** contribute an article titled "**Clouds Connecting Europe: Interoperability in the EU Data Act**", which focuses on the interpretative challenges arising from ambiguities in the Data Act, for instance in relation to the meaning of "data space" or "data processing service." The authors propose an effects-oriented method to address these challenges and offer an interpretation of the Act's interoperability provisions aligned with the Data Act's goal of enhancing data interoperability in the EU, thus fostering access to and use of data.

3 A second group of articles addresses **legal aspects of AI**, namely, copyright and data protection issues related to the use of synthetic content to train AI models; the status of General-Purpose Generative AI and its role in the production of users' creative content; and the reach of the transparency obligations for some AI systems set forth in Art. 50 of the AI Act.

4 The first of those articles, by **Kalpana Tyagi**, "**Synthetic Data, Data Protection and Copyright in an Era of Generative AI**", considers the increasing use of synthetic data – data generated by AI systems – to continue training AI models. She notes that while such use can help satisfy the need for data for AI training, relying on synthetic data may eventually deteriorate the quality of the models, and that, therefore, human-generated data will also be necessary to guarantee the quality of the training. The author explores legal aspects related to the use of synthetic data in AI training, in particular how it may affect data protection as well as copyright, including the *sui generis* database right. She underscores how the use of synthetic data favours compliance with the GDPR when data are fully anonymised. The author notes, however, the risk of infringing copyright when using AI-generated data based on original copyright-protected data. She calls for 'an innovation-driven synthetic data paradigm' that facilitates a proper balancing of the

rights and interests involved.

5 The next article in this group is authored by **Gabriel Ernesto Melian Pérez**, under the title of **"From Curators to Creators: Navigating Regulatory Challenges for General-Purpose Generative AI in Europe"**. The author examines relevant issues regarding the legal framework for General-Purpose Generative AI (GPGAI). He first explores the use of AI tools in social network platforms, distinguishing between the AI tools used by the platform to curate and recommend content to its users, and the General-Purpose Generative AI (GPGAI) tools made available to users to produce and share creative content. With respect to the latter, the author raises the question of whether a platform that provides a GPGAI tool may rely on the hosting safe harbour – currently set forth in the Digital Services Act (originally in the E-Commerce Directive) – to avoid liability for content that users create using the GPGAI tool. The author concludes that, generally speaking, the social network operator cannot benefit from the hosting safe harbour in this case, since the GPGAI tool is so involved in the creation of the content that the result can no longer be regarded as purely third-party content. In addition, the author delves into the rules applicable to General-Purpose Generative AI, both in the AI Act and in the revised Product Liability Directive, offering insights and proposals to improve its legal treatment.

6 Also regarding AI, **Nicolaj Feltes** contributes an article titled "**Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?**" In his article, the author examines the transparency provisions laid down in Article 50 of the AI Act, designed to strengthen user awareness of, among other things, the use of chatbots, emotion recognition systems, biometric categorisation, deep fakes, and other AI-generated content. The final wording of these obligations departs from the European Commission's 2021 proposal, reflecting both amendments introduced during the legislative process to address identified shortcomings, and the need to respond to the rapid rise of generative AI tools available to the public. The author offers a critical assessment of whether the final text successfully overcomes the flaws of the initial draft. He also analyses the enacted measures, drawing attention to their potential challenges of interpretation and practical implementation. He also considers the interplay of some of these measures with the Digital Services Act, particularly regarding the removal of unlabelled deep fake content.

7 A third group of articles considers different issues related to **online speech**. First, **Agustina Del Campo, Nicolas Zara**, and **Ramiro Álvarez Ugarte** examine the Digital Services Act approach to speech regulation in their article titled "**Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation**". The authors critically analyse the DSA risk approach from the perspective of the human rights standards of freedom of expression, and argue that it generates problematic incentives in relation to content moderation. Furthermore, they contend that the risk approach causes rights to fade in the background, and underscore the risk of symbolic compliance. The other article in this group, by **Laura Herrerías Castro**, "**The duty of care of online platforms in defamation cases**", also considers platforms' duties with regard to online speech. She explores in particular defamatory speech on online platforms, analyses the application of DSA hosting safe harbour for third-party defamatory content and how this regime has been impacted by the development of AI. The article deals with the standards of care for platforms regarding defamatory content, paying attention not only to the DSA but also to soft law instruments such as the Principles of European Tort Law and the Draft Common Frame of Reference, and analyses platforms' practices of content moderation. It also explores the remedies in cases of lack of fulfilment of the required duties of diligence, and particularly the right to compensation provided for in **Art.** 54 DSA.

8 Also regarding speech, now specifically from the lenses of **data protection**, we include an article by **Stephanie Rossello**, "**The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry**". The author considers the right of rectification under EU data protection law and its application to opinions rather than facts. She examines particularly how the issue is dealt with by the Dutch data protection law, tracing the origins of the facts/opinions dichotomy in the drafting of the first Dutch data protection act and showing how it shaped subsequent interpretations by courts and the Dutch DPA. The author notes that this distinction reflects deeper uncertainties: first, around the meaning of accuracy and the standard of proof needed to establish inaccuracy, and second, around how data protection law interacts with other national legal regimes, such as administrative and tort law.

9 Last but not least, this issue includes an article reflecting on the EU's role and purpose in digital regulation, by **Lukas v. Ditfurth**: "**The European Union's Pursuit of Digital Sovereignty through Legislation**". The article examines how digital sovereignty has become the overarching goal of the EU's digital legislation, from the AI Act to the Services Act and Digital Markets Act. He notes that while digital sovereignty enables the EU to chart a course distinct from the US and China by safeguarding rights, democracy, and competition, it also carries risks of regulatory overreach and international conflict. The author concludes that the

EU should pursue digital sovereignty with caution, combining multilateral cooperation with defensive measures to protect its core interests and values.

10 Finally, the issue includes a recent **Opinion** issued by the **European Copyright Society**: "**An EU Copyright Framework for Research**". The Opinion argues that the current EU copyright framework undermines the EU's research ambitions and calls for urgent reform to better balance intellectual property rights with the freedom of art and science as well as with the 'right to research'. It identifies shortcomings in key exceptions, such as the InfoSoc Directive general research exception and the CDSM Directive text and data mining exception, as well as in national secondary publication rights. To address these gaps, it proposes concrete policy measures, including a mandatory EU-wide secondary publication right and the creation of a general mandatory research exception.

11 I would not like to conclude this editorial without announcing that a new editor has joined the journal: Professor Dr. Thomas Margoni, who is Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven, where he is also a member of the Board of Directors of the Centre for IT & IP Law (CiTiP) and the director of the IP & IT Law programme. We warmly welcome him to the Editorial Board.

We hope you enjoy the reading.

Miquel Peguera

Common European Data Space for Cultural Heritage: Is the EU Taking the "High Road" from "A Single Access Point" to "A Single Market for Data" for Digital Cultural Content?

by **Pelin Turan and Caterina Sganga** *

Abstract: The Common European Data Space (CEDS), currently comprising fourteen sector- and domain-specific data spaces, was launched by the European Commission (EC) in 2018 in the context of the European Strategy for Data. The CEDS is devised to catalyse the European Union's transformation into a competitive and digitally sovereign market power informed and governed by a robust legislative framework that would facilitate the cross-border and cross-sectoral flow and reuse of multiple types of data, which are collected and held by public-sector entities, within a "single market for data". Despite their alignment with the overarching aims and objectives of the CEDS project, the Open Data Directive (ODD) and Data Governance Act (DGA) have limited impact on the deployment of the Common European Data Space for Cultural Heritage (CHDS), which constitutes one of the data spaces within the CEDS. This paper investigates the legal obstacles to the successful deployment of the CHDS, including the interplay of the ODD and DGA with other legislative frameworks essential to the realisation of the CHDS (i.e. cultural heritage law and copyright law). The paper suggests that this conundrum stems from the fact that the CHDS leans toward another landmark initiative of the EC: the Europeana platform, which established a "single access point" to cultural heritage assets. Considering that an implementing act for the deployment of the CHDS is yet to be adopted by the EC, the paper provides normative solutions to tackle the legal and policy problems hampering the operationalisation of the CHDS.

Keywords: Common European Data Space, Cultural Heritage, Digitisation, Digital Single Market, European Strategy for Data, Online Accessibility

Recommended citation: Pelin Turan and Caterina Sganga, Common European Data Space for Cultural Heritage: Is the EU Taking the "High Road" from "A Single Access Point" to "A Single Market for Data" for Digital Cultural Content?, 16 (2025) JIPITEC 133 para 1.

A. Introduction

1 Prompted by the Lisbon Strategy of 2000,[1] the European Union (EU) has undergone a major transformation in tandem with the global digitisation movements and ever-evolving technological trends. The Digital Agenda for Europe,[2] the Digital Single

* Pelin Turan is a postdoctoral research fellow at Sant'Anna School of Advanced Studies, DIRPOLIS & LIDER-Lab (Pisa, Italy). Caterina Sganga is a full professor of comparative private law at Sant'Anna School of Advanced Studies, DIRPOLIS & LIDER-Lab (Pisa, Italy).

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, eEurope 2005: An information society for all – An Action Plan to be presented in view of the Sevilla European Council (21/22 June 2022), COM(2022) 263 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52002DC0263> accessed 29 December 2024.

2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245

Market Strategy for Europe,[3] the European Strategy for Data,[4] and the 2030 Digital Compass[5] are only a few milestones in the EU digital strategy underpinning the Union's gradual transition into a thriving information society and data-agile economy. Amidst this plethora of public policy documents, which guide the EU's evolution into a digitally sovereign market power, is the flagship initiative aimed at accelerating the untapped potential of data corpora generated and stored in the EU: the Common European Data Space (CEDS).

2 The CEDS is a novel concept encapsulating the EU blueprint to create a "single market for data".[6] Developed under the aegis of the European Strategy for Data,[7] the CEDS initiative dwells upon three main pillars: (1) accelerating EU competitiveness in the global data economy, and (2) reinforcing the EU digital sovereignty, while (3) upholding and promoting European values and norms across the globe.[8] The first pillar recognises the value of data as a resource for economic growth and innovation, and it promotes the use of public- and private-sector data to foster the development of data-driven goods and services.[9] The second and third pillars not only complement the former but also harness it, as several incidents, including the COVID-19 pandemic,[10] revealed that the vast amount of data collected and pooled in the EU had been processed by non-European market actors – and without having to comply with the EU economic and public policy priorities or the EU legislative framework.[11]

3 To mitigate the negative implications of these social and economic phenomena, the European Commission (EC) established the CEDS in 2018 to enable and facilitate the free and secure flow and cross-border and cross-sectoral reuse of multiple types of data through a trustworthy and secure infrastructure governed by the EU legal framework, hence endorsing the security and economic prosperity of European citizens and businesses.[12] Building upon the decades-long experiences (and frustrations) of the EU and European market actors, the CEDS stands as an articulate project with a robust plan informed by well-formulated objectives. On the one hand, it aims to make the data collected and stored in the EU available for access and reuse by various market actors, including but not limited to citizens and businesses.[13] On the other hand, it encourages the generation of new corpora of data while guaranteeing the data subjects' control over the data they generate.[14]

4 Driven by these goals, the CEDS is designed as a seamless digital area encapsulating several domain- and sector-specific data spaces representing the "strategic economic sectors and domains of public interest."[15] As of December 2024, the CEDS comprises fourteen data spaces dedicated to areas ranking at the top of the EU agenda, ranging from health to agriculture, public administration, energy, finance, tourism, media – and cultural heritage (CH).[16]

5 Given the diversity of sectoral/domain-specific data spaces within the CEDS, "there is no one-size-fits-all structure (...) [applicable to all] data

final <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex%3A52010DC0245> accessed 29 December 2024.

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192> accessed 29 December 2024.

4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0066> accessed 29 December 2024.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2030 Digital Compass: The European Way for the Digital Decade, COM(2021) 118 final <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118> accessed 29 December 2024.

6 'Common European Data Spaces | Shaping Europe's Digital Future' (*European Commission*, 13 March 2024).

7 COM(2020) 66 final (n 4).

8 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a common European data space, COM(2018) 232 final <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018DC0232> accessed 29 December 2024.

9 Ibid.

10 COM(2021) 118 final (n 5).

11 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Shaping Europe's digital future*, COM(2020) 67 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0067> accessed 29 December 2024; COM(2020) 66 (n 4); COM(2021) 118 final (n 5).

12 COM(2018) 232 final (n 8).

13 Ibid.

14 Ibid.

15 "Staff Working Document on Data Spaces | Shaping Europe's Digital Future" (*European Commission*, 14 February 2022).

16 Ibid.

spaces."[17] Whereas each data space shall be deployed considering the specificities of the relevant sector/domain, two defining elements are shared by all: First, data infrastructures and data governance frameworks to operationalise each data space, and second, the aspiration to facilitate pooling, access and sharing data through the data space with the aid of these structures.[18] To rest the foundations for and realise these key objectives, the EU pursues a plan comprising four building blocks: (1) Adopting legislative measures on data governance, access and reuse; (2) making high-value publicly held datasets available to the public; (3) developing data processing infrastructures, data-sharing tools and architectures, and data governance mechanisms; and finally, (4) building up a secure and trustworthy digital area for data flows, also by adopting secure, fair and competitive cloud services.[19]

6 The ongoing efforts that fall under the first agenda item – especially the adoption of the Open Data Directive[20] (ODD) and, more recently, the Data Governance Act[21] (DGA) – are well-tuned with the overarching aims and objectives of the CEDS. Nevertheless, a closer look at the single sectoral/domain-specific data spaces and the particularities of each data space flag misalignments with the main pillars of the CEDS. This puts the efficacy of the EU legislative framework into question and raises doubts on whether and how the CEDS can be successfully deployed as initially anticipated by the EC.

7 In this context, the Common European Data Space for Cultural Heritage (CHDS), which was launched in 2021,[22] represents an interesting example. The CHDS – while waiting for the proposal for an implementing act that would contextualise and detail the roadmap for its deployment, its public policy rationale and blueprint – leans toward previous projects with similar yet relatively limited objectives, such as the *Europeana* platform – or in other words, the renowned digital library of the EU.[23] However, the resemblance of the ambitions of the CEDS and the *Europeana* platform diverts the attention from the ways in which a *data space* differs from an *online platform,* and it blurs the lines between *a single market for data* and *a single access point*[24] for digital CH content. This conundrum is exacerbated by the fact that the CHDS' main stakeholders and key players are yet to be identified, and the data transfers among these players, for both primary and secondary uses, are yet to be systematised via an implementing act. Until then, any future legislative endeavour in this sector requires a meticulous assessment of the capacity of existing legal tools to operationalise the CHDS project.

8 This paper argues that the legislative framework supporting the CEDS, once combined with the EC's path dependence on the *Europeana* project, hampers the successful deployment of the CHDS for several interrelated reasons. The CHDS initiative places its subject matter (namely, CH assets and their trajectories in the digital domain) at the intersection of cultural heritage law, data law and copyright law – three different legal disciplines that originated in response to different needs, evolved through different timelines, and have been shaped per disparate public policy goals. The co-existence of these regimes, which are not adjusted to – let alone tailored for – the specificities of any sector/domain-specific data space, complicates rather than helps the realisation of the CHDS. Besides, the *data space* discourse adds a new dimension to the legal debates sparked by the digitisation of CH and the amendment of the EU copyright *acquis* to accommodate the *Europeana* project. The deployment of the CHDS requires legal tools enabling not only the digital reproduction of CH assets, which was sufficient to realise the *Europeana* project but also tools that would facilitate data transfers and the reuse of transferred data in a federated digital environment. Nevertheless, the EC's reliance on the *Europeana* experience signals that the CHDS might be (mis) guided by a *single access point* vision underpinning the *Europeana* platform rather than a *single market* vision corresponding to a data space for CH.

9 Building upon this policy and legal background, this paper strongly advocates for the urgent enactment of an implementing act designed and devised to inform and assist the deployment of the CHDS. It aims to contribute to such a future legislative endeavour by highlighting the pitfalls in the EC's current approach

17 COM(2018) 232 final (n 8), 3.

18 Ibid, 3-4.

19 Ibid, 4.

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56.

21 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 L 152/1.

22 The enactment of an implementing act for the CHDS is beaconed by the EC in its Decision of 29.06.2021. See: Commission Decision of 29.06.2021 setting up the Commission Expert Group on the common European Data Space for Cultural Heritage and repealing Decision C(2017) 1444 <https://digital-strategy.ec.europa.eu/en/policies/europeana-digital-heritage-expert-group> accessed 29 December 2024, Article 2(e).

23 Council conclusions of 20 November 2008 on the European digital library EUROPEANA (2008/C 319/07) [2008] OJ C 319/18.

24 Commission Recommendation of 24 August 2006 on the digitisation and online accessibility of cultural material and digital preservation (2006/585/EC) [2006] OJ L 2006/28.

to the matter. It suggests realigning the CHDS with the overarching aims of the CEDS while proposing minor readjustments of the existing legal tools to the features of the CHDS.

10 To explain and justify the statements above, Section B offers an insight into the genesis, evolution and particularities of the CHDS, linking it to previous EU efforts with similar ambitions, particularly the *i2010: Digital Libraries initiative* and *Europeana,* to underline the differences between a data space and an online platform, while also explaining the market-related and legal implications underlying this difference. Considering the departure of the CHDS from the overarching aims and objectives of the CEDS and its inclination to be path-dependent on the *Europeana* project, Section C realigns the CHDS' ambitions with the overarching aims and objectives of the CEDS by offering a critical analysis of the EU competences to regulate or harmonise cultural heritage law across Europe and evaluating the compatibility of the EU data and copyright legislation *vis-à-vis* the operationalisation of the CHDS. Finally, Section D concludes with a set of proposals for a legislative act necessary to ensure the proper and effective implementation of the CHDS.

B. "The Road Not Taken"[25]: Cultural Heritage Data Space – or Online Platform?

11 The EC launched the CHDS in 2021,[26] shortly after CH became the lynchpin of the New European Agenda for Culture[27] during the 2018 European Year of Cultural Heritage.[28] The EC's decision to dedicate a data space to CH stems from the duality of CH in European public policies. On the one hand, the Union policies acknowledge CH as a building block of a common European identity, encapsulating the values and communal memory that unites Europe "in all its diversity."[29] On the other hand, these policies often consider CH a catalyser of sustainable innovation and creativity, hence an important contributor to the European economy.[30] Mirroring these attributes and also the goals identified by the CEDS initiative, the CHDS aspires "to accelerate the digital transformation of Europe's cultural sector and foster the creation and reuse of digital [CH] content."[31]

12 Considering the pivotal importance of CH for the European social and economic *milieu*, the CHDS is devised as an instrument to embed multi-stakeholder perspectives and satisfy the diverse and interdependent needs and expectations of each stakeholder group.[32] For instance, from the perspective of cultural heritage institutions (CHIs), which are not only the gatekeepers of public access to CH but also the key market players to digitise CH assets, the CHDS offers the opportunity to digitise various tangible and intangible cultural assets and sites, including those at risk of extinction, inaccessible or temporally closed,[33] with the aid of advanced digital technologies such as 3D, artificial intelligence (AI), machine learning, cloud computing, virtual and augmented reality technologies.[34] As per the viewpoint of cultural and creative industries and sectors (CCISs), the aforementioned advanced technological tools would allow innovative forms of artistic creation while also making CH assets available for the development of new cultural products and services "in various sectors, such as (...) tourism [and research]."[35] Last, from the public's perspective, the CHDS would enhance access to digital CH whilst spurring new ways to digitally

25 By reference to Robert Frost's poem "The Road Not Taken". Frost R, *The Road Not Taken* (Henry Holt ed, Mountain Interval 1916) <https://www.gutenberg.org/files/29345/29345-h/29345-h.htm> accessed 29 August 2024.

26 See: Commission Recommendation (EU) 2021/1970 of 10 November 2021 on a common European data space for cultural heritage, OJ L 401/5.

27 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A New European Agenda for Culture, COM(2018) 267 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A267%3AFIN> accessed 29 December 2024.

28 Commission Recommendation (EU) 2021/1970 (n 26).

29 Ibid; also see: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Empty, Strengthening European Identity through Education and Culture, COM(2017) 673 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0673> accessed 29 December 2024; Council Resolution of 25 June 2002 on preserving tomorrow's memory – preserving digital content for future generations (2002/C 162/02) [2002] OJ C 162/4.

30 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, i2010: Digital Libraries, COM(2005) 465 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0465> accessed 29 December 2024; Commission Recommendation 2011/711/EU of 27 October 2011 on the digitisation and online accessibility of cultural material and digital preservation [2011] OJ L 283/39.

31 Ibid.

32 Commission Recommendation (EU) 2021/1970 (n 26).

33 Ibid, 7.

34 Ibid.

35 Ibid, 5-6.

engage with CH, including its reuse for various purposes.[36] Whereas this public policy rationale is well-aligned with the pillars of the CEDS initiative, and particularly with those aiming to enhance the EU global competitiveness in the digital market and the European digital sovereignty, several aspects prevent the transformation of this vision into reality, most of which stem from the role attributed to the *Europeana* Consortium and platform.

13 The EC entrusts the *Europeana* Consortium to lead a cohort of public and private institutions active in CH or technology sectors to deploy the CHDS.[37] Recognising the Consortium's experience and success in establishing standardised frameworks for the online transfer of digital cultural content and metadata,[38] the EC requires CHIs to comply with "the relevant standards and frameworks, such as (...) the *Europeana* Data Model, RightsStatement.org, and the European Publishing Framework"[39] developed by the *Europeana* initiative, and to "make their digital assets available through [the] *Europeana* [platform]."[40] In so doing, the EC reduces the CHIs' role in the CHDS to the mere transfer of their digital collections to *Europeana* while overlooking CCISs and any other stakeholders' potential contributions to this new data space. In fact, by muddling the distinction between *Europeana* and the CHDS, the EC's action plan diverts from operationalising a *data space* and serves to expand the *Europeana* platform's collections and market power.

14 One of the main reasons underlying this phenomenon is the lack of clarity on to what extent *Europeana*'s IT structure and principles of operation align with those of a *data space*. In broad terms, "data space" is defined as "[a] federated, open infrastructure for sovereign data sharing based on common policies, rules and standards."[41] In line with this generic definition, the Regulatory Scrutiny Board's Opinion of 2020 defines the common *European* data space as "arrangements comprising an IT environment and a set of legislative, administrative and contractual rules on the use of data"[42] to "ensure secure *processing and access* to data by *an unlimited number of organisations.*"[43] The key elements of these definitions have been eventually consolidated into a binding definition within Article 33(1) of the Data Act (DA). This provision – which is dedicated to the interoperability of data, data sharing services and the CEDS – outlines common European data spaces as "purpose- or sector-specific or cross-sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives."[44]

15 Compared to these overarching definitions, the placement of the *Europeana* Consortium at the pinnacle of the CHDS' organisational structure and the path-dependence on *Europeana*'s ongoing practices risk reducing the CHDS to a *minimally decentralised* digital space, if not merely an *online platform.* That said, a glance at *Europeana*'s origins, development and features suffices to understand the differences between this initiative and the CHDS.

16 *Europeana* was devised by the *i2010: Digital Libraries* initiative[45] as a "common multilingual access point"[46] for digital CH assets held by CHIs across Europe.[47] Dedicated to democratising access to culture, *Europeana* aims to enable the online availability of cultural content for wider audiences, enhance the digitisation of analogue cultural content, and, finally, preserve and store born-digital and digitized cultural content for the sustainability of European CH.[48] In line with these goals, *Europeana* was constructed as a "multi-sided digital platform for digital [CH],"[49]

36 Ibid.

37 Commission Decision of 29.06.2021 (n 18); "The Deployment of a Common European Data Space for Cultural Heritage | Shaping Europe's Digital Future" (19 October 2022) <https://digital-strategy.ec.europa.eu/en/news/deployment-common-european-data-space-cultural-heritage> accessed 22 July 2024.

38 Commission Recommendation (EU) 2021/1970 (n 26), 8.

39 Ibid, 11.

40 Ibid

41 Ibid, 1.

42 Regulatory Scrutiny Board Opinion, Proposal for a Regulation of the Parliament and of the Council on European data governance (Data Governance Act), SEC(2020) 405 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC(2020)405> accessed 20 December 2024, 1.

43 Ibid. [Emphasis added.]

44 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) (Text with EEA relevance) [2023] OJ L 2023/2854, Article 33(1).

45 COM(2005) 465 final (n 30).

46 Commission Recommendation (2006/585/EC) (n 24).

47 Council communication (2008/C 319/07) (n 23), 18; Commission Staff Working Document accompanying the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Europe's cultural heritage at the click of a mouse: Progress on the digitisation and online accessibility of cultural material and digital preservation across the EU, SEC(2008) 2372, 513 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008SC2372> accessed 29 December 2024, 5-7.

48 Communication from the Commission, COM(2005) 465 final (n 30), 3-5.

49 Nadine Klass, Hajo Rupp and Julia Wildgans, "Bringing

which facilitates research across the collections of various national CHIs located in the EU and "acts as an interface to resources from all over Europe."[50] *Europeana*, by making available the digital content provided by data aggregators through *a single access point*, serves as an online platform[51] to facilitate the public's access to and engagement with digital CH.

17 Despite the harmony of *Europeana* and CHDS' ambitions, the *Europeana* platform's operation relies on the Consortium's collaboration with a network of data aggregators comprising "national, regional, domain and thematic aggregators"[52] acting as intermediaries between individual CHIs – or data providers – and the *Europeana* platform.[53] In this organisational structure, the platform neither provides content nor stores digital CH assets or data but redirects users to the web pages of national CHIs hosting digital collections.[54]

18 This infrastructure and the *Europeana* platform's functions are far from meeting the criteria to support the *single market for data* vision of the CEDS initiative. Therefore, placing *Europeana* at the centre of the CHDS project, if not equating the CHDS with the *Europeana* platform,[55] promotes the idea of an online infrastructure that is governed by a single entity as the main gatekeeper of data access practices – but not for data-sharing practices – rather than a federated and interoperable IT structure with the active involvement of multiple data-sovereign players. This conceptualisation runs counter to the main pillars of the CEDS initiative, especially those concerning competitiveness and digital sovereignty. The enhancement of the competitiveness of the EU data market via value creation is hard to achieve with the concentration of market power in the hands of *Europeana,* as this is likely to hamper the independent exchange of large sets of data among businesses or the boost of open competition in the data market and the entry of new players (e.g. small- and medium-sized enterprises) in the market.[56] By the same token, it is hard to speak of sovereign control by public institutions or businesses over the data they are expected to generate by digitising cultural assets, let alone the processing of such data for several purposes by freely concluding agreements with other market players and deciding on the conditions of data exchange.[57]

19 The technical incompatibility of *Europeana* with the CHDS also carries several legal implications. The complexity of the CHDS requires the harmonious co-existence of a bundle of legal frameworks to support a single market for CH-related data, such as cultural heritage law to identify cultural assets and their legal status; copyright law for the digitisation of cultural content, making born-digital and digitised content available to market actors and the public in a digital environment, digital preservation and storage; data governance law to regulate data sharing and processing for a fully functioning data space, where born-digital and digitised CH assets can freely flow and be processed by multiple market actors for commercial and non-commercial purposes.

20 Therefore, the enactment of an implementing act for the CHDS requires analysis and understanding of the interplay between the current EU regulatory framework for cultural heritage, data governance, and copyright laws to identify the enablers and disablers of the move from *a single access point* to *a single market* for CH data.

C. At the Crossroad – or Roundabout: Cultural Heritage Data Space and the Cacophony of Cultural Heritage, Data and Copyright Regimes

21 The legal framework informing and governing the EU single market has radically changed in the last few decades. Not only has the Union's data regime (re)shaped the collection, processing, and sharing of personal and non-personal data, but the EU copyright *acquis* has also been modernised and updated in response to global technological advancements and

Europe's Cultural Heritage Online: Initiatives and Challenges" in Irini Stamatoudi and Paul Torremans (eds), *EU Copyright Law: A Commentary* (2nd edition, Edward Elgar Publishing 2021), 945.

50 Ibid, 946.

51 Council conclusions on the role of Europeana for the digital access, visibility and use of European cultural heritage [2016] OJ C 212/9, Annex, 9643/16, 4.

52 "Europeana Aggregators Forum" (*Europeana PRO*) <https://pro.europeana.eu/page/aggregators> accessed 24 July 2024.

53 "About" (*Europeana*) <https://www.europeana.eu/en/about-us> accessed 24 July 2024.

54 Klass and others (n 49), 946.

55 For a similar interpretation of the current efforts of the EC and the public policy documents on Europeana's role in the deployment of the CHDS, please see: Paul Keller, "Five Things I Know about Data Spaces" (*Open Future*) <https://openfuture.eu/blog/five-things-i-know-about-data-spaces> accessed 26 July 2024.

56 For the promises of a data space, as a decentralised and federative structure, on market competitiveness, please see: Peter Kraemer, Crispin Niebel and Abel Reiberg, "What Is a Data Space?" (Gaia-X Hub Germany 2022) White Paper <https://gaia-x-hub.de/wp-content/uploads/2022/10/White_Paper_Definition_Dataspace_EN.pdf> accessed 5 March 2024, 5.

57 For the ways in which a data space supports the self-determination and sovereignty of the market players, please see: Ibid, 5-6.

market trends. These legislative interventions seem to provide a fertile ground for the realisation of the CEDS initiative; nevertheless, they raise several challenges to the operationalisation of the CHDS.

22 As already mentioned above, the CHDS requires harmony between the legal provisions enabling CH data-sharing and reuse in EU and national cultural heritage, copyright and data governance laws. This is already hampered by the limited competence of the EU to regulate CH-related matters, which prevents the Union from identifying CH assets to be digitised and made open to reuse via the CHDS. This problem is exacerbated by legal fragmentation across the national CH regimes of the EU Member States and the interaction of such legal disparities with EU law in general. Yet, it shall be admitted that the situation is not brighter in areas falling under the EU's competences. The disparate and independent public policy justifications and legislative histories of the EU data governance and copyright frameworks resulted in the independent development of these two bodies of law, with minimum or no coordination, hence causing inevitable clashes and overlaps of concepts and regulatory regimes. The implications of this phenomenon are further accelerated by the complex data regime applicable to CH assets, triggered by the public or private nature of the CHIs holding the collection and their eventual cooperation with third parties in the digitisation of the latter. Also, the EU copyright regime falls short in laying a clear regulatory framework for the reuse of digitised CH assets, especially if directed to the launch of data-based products and services. This is mainly because EU copyright law has prioritised the preservation, safeguarding and cataloguing needs of CHIs, all of which require legal tools enabling the reproduction of institutional collections but not necessarily the availability of such content to the public, let alone the transfer of digitised CH assets.

23 Based on these, the investigation of the interplay of cultural heritage with the EU data and copyright regimes becomes essential, especially to better perceive the gaps and enablers featuring the current legislative framework vis-à-vis the operationalisation of the CHDS.

I. On the brink of the Common European Data Space for... Cultural Heritage

24 The democratisation of access to and public engagement with culture through digitisation and online availability of CH have been the lynchpin of European cultural policies since the *i2010: Digital Libraries* initiative.[58] Yet, neither "culture" nor "cultural heritage" has a clear-cut definition in the EU legal and policy documents.[59] *Per contra*, the EU digital agenda dwells upon a common understanding of CH, rather than a legally binding definition, which developed through the negotiations at international norm-setting forums in the aftermath of World War II.

25 Since the 1950s, policymakers and scholars have attempted to find the optimum ways to protect, preserve and enhance the accessibility of CH assets in the public interest, with policy and legislative interventions informed by the socio-economic and political realities and priorities at the time.[60] The first

58 For a selection of the milestones in the field, see: Council Resolution of 25 June 2002 (2002/C 162/02) (n 29), Communication COM(2005) (n 30), Commission Recommendation (2006/585/C) (n 24), Commission Recommendation of 27 October 2011 (2011/711/EU) (n 30); COM(2008) 267 final (n 27); COM(2015) 192 final (n 3); Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Promoting a fair, efficient and competitive European copyright-based economy in the Digital Single Market COM(2016) 592 final <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2016:592:FIN> accessed 29 December 2024; Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the cultural dimension of sustainable development in the EU actions COM(2022) 709 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0709> accessed 29 December 2024. Also see: Klass and others (n 49), 943-944.

59 The EU bodies and institutions do not refrain from admitting the hardship in defining culture and CH. See: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European agenda for culture in a globalizing world, COM(2007) 242 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007DC0242> accessed 20 December 2024, 3.

60 The first international legal instrument to refer to CH was the Hague Regulations concerning the Law and Customs of War on Land. Adopted in 1907, these Regulations aspired to protect "historical monuments" against sieges and bombardments. Likewise, the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflicts, adopted in 1954 under the aegis of UNESCO, was a response to the implications of World War II on tangible, including both tangible and intangible, CH assets (e.g. destruction, deterioration, looting). The other UN instruments that followed the Hague Regulations also concentrated on certain fragments of tangible CH assets. For instance, the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, adopted in 1970, aimed at

international instruments adopted by the United Nations (UN) and Council of Europe (CoE) to preserve CH initially focused on the in-situ protection and accessibility of certain categories of assets, mainly in response to the devastating consequences of armed conflicts.[61] Eventually, this approach resulted in a piecemeal rather than holistic regulation of the matter, while contextualising CH as a static concept within several disparate legal instruments, without a unified and universally accepted definition which grasps CH's dynamic nature.[62] However, more recent international legal instruments, also ratified by the EU, mark a positive shift in the understanding of CH. The CoE Convention on the Value of Cultural Heritage for Society (Faro Convention), adopted in 2005, provides an all-encompassing definition of CH, which acknowledges not only tangible, movable and immovable assets but also intangible, cultural and natural ones.[63]

26 The Faro Convention's resolutions and vision are echoed by the current EU cultural policy agenda, including the CHDS. The EC Recommendation of 10 November 2021 states that the CHDS strategy set therein "covers all types of [CH] (tangible, intangible, natural, born-digital)."[64] It promotes and prioritises the digitisation of CH assets at risk, popular monuments, buildings and sites, and the categories of under-digitised CH assets,[65] such as audiovisual content.[66] Nevertheless, a broadly formulated description of the CH as such complicates the operationalisation of the CHDS for three major reasons. First, the division of competences between the EU and its Member States regarding CH signals that the extent to which the digitisation of European CH assets can be achieved largely depends on the impact of the obstacles created by and the exclusive competence of Member States to regulate the laws concerning CH. Whereas Article 3(3) of the Treaty of the European Union (TEU) and Article 167(1) of the Treaty on the Functioning of the European Union (TFEU) refer to the common European CH and its preservation by the EU, Article 167(5) of the TFEU clarifies that cultural heritage law remains at the exclusive discretion of Member States.[67] The Union's role, as crystallised by Article 167(2) of the TFEU, is restricted to the encouragement and support of Member States' efforts to improve cultural exchange and the preservation of CH. This leaves the Union without a consensus on what CH is, despite the references to CH in the EU primary law.

27 Second, the EC Recommendation of 10 November 2021 does not differentiate between CH assets protected by copyright and those that have fallen into the public domain.[68] In this context, the interaction of cultural heritage and copyright law shall not be overlooked, especially given that these disciplines originated from different public policy rationales and respond to different and possibly conflicting interests whilst being shaped in line with the national policies and priorities of the Member States rather than the EU. As a result, they often feature heterogeneous rules, which may create further barriers to the sharing of digitised CH assets and CH data, particularly when cultural assets, which are allocated to the public domain, are digitally reproduced for non-commercial purposes or used for commercial purposes. The recent precedents of Italian jurisprudence exemplify this conundrum, as the Italian judiciary upheld, in several cases, the fees

preventing the trafficking of tangible and movable elements of CH, whereas, the Convention Concerning the Protection of the World Cultural and Natural Heritage, adopted in 1972, was not only concerned with selected elements of tangible and movable CH (i.e. monuments, groups of buildings, and sites) but also of tangible yet immovable assets (i.e. natural features, geological and physiographic formations, natural sites). As the last link in the chain, the Convention for the Safeguarding of the Intangible Cultural Heritage, adopted only in 2003, recognised the intangible aspects of CH and extended legal protection to, for instance, oral traditions, social practices, rituals, festivals, knowledge and practices, and traditional craftsmanship. Along the same lines, the Convention for the Protection of the Architectural Heritage of Europe, adopted in 1985 by the Council of Europe, is concerned with the in-situ protection and preservation of tangible CH assets in the form of monuments, buildings, and sites.

61 Janet Blake, "On Defining the Cultural Heritage" (2000) 49 International and Comparative Law Quarterly 61 <https://www.cambridge.org/core/product/identifier/S002058930006396X/type/journal_Article > accessed 29 May 2024, 62.

62 Giulia Dore and Pelin Turan, "When Copyright Meets Digital Cultural Heritage: Picturing an EU Right to Culture in Freedom of Panorama and Reproduction of Public Domain Art" (2024) 55 IIC - International Review of Intellectual Property and Competition Law 668 <https://link.springer.com/10.1007/s40319-023-01408-6> accessed 10 February 2024, 670.

63 Council of Europe Framework Convention on the Value of Cultural Heritage for Society (adopted 27 October 2005, entered into force 1 January 2011), CETS no. 199 <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=199> accessed 24 December 2024, Art. 2.

64 Commission Recommendation (EU) 2021/1097 (n 26), 9, also by referring to the UNESCO Conventions of 1972 and 2003.

65 Ibid.

66 Ibid, 8.

67 Consolidated Versions of the Treaty of the European Union and the Treaty on the Functioning of the European Union [2016] OJ C 202/1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT> accessed 20 September 2024.

68 Commission Recommendation (EU) 2021/1970 (n 26), paragraphs 2 and 3.

and tariffs imposed by the Italian Code of Cultural Heritage upon the reproduction of Italian CH assets in the public domain by Italian CHIs.[69] These clashes are difficult to tackle with a harmonised EU-wide solution, given the limited EU competence in the field. In addition, the EC Recommendation of 2021 has limited cogency and thus a reduced impact on Member States' legislative framework.

28 Third, the integration of CH into the CEDS initiative shifts the focus from *in-situ* protection, preservation and accessibility to *digital* reproduction, *online* availability and accessibility, and seamless *transfer* of digital CH assets. Considering that CH is a generic term encompassing an abundance of cultural assets, the digitisation, let alone the transfer, of different types of CH assets requires different legal procedures or rights-clearance mechanisms, disparate techniques and expertise, hence different budget constraints or solutions such as public-private partnerships. The governance of these matters, however, extends the scope of cultural heritage law and interacts (or clashes) with the EU data governance and copyright regimes. Treating born-digital and digitized CH assets as *data* to be transferred and reused across the EU, the European data framework, adopts a variety of approaches to CH assets, depending on whether they are publicly or privately held, whether they contain personal data or whether they are in the public domain or subject to intellectual property rights (IPRs) of public entities, custodial organisations or private third-parties.

69 See: Giulia Dore and Giulia Priora, "The EU Imperative to a Free Public Domain: The Case of Italian Cultural Heritage" (COMMUNIA Association 2024) <https://communia-association.org/publication/the-eu-imperative-to-a-free-public-domain-the-case-of-italian-cultural-heritage/> accessed 29 April 2024, 19-20. Also see: Giulia Dore, "The Puzzled Tie of Copyright, Cultural Heritage and Public Domain in Italian Law: Is the Vitruvian Man Taking on Unbalanced Proportions?" (Kluwer Copyright Blog, 6 April 2023) <https://copyrightblog.kluweriplaw.com/2023/04/06/the-puzzled-tie-of-copyright-cultural-heritage-and-public-domain-in-italian-law-is-the-vitruvian-man-taking-on-unbalanced-proportions/> accessed 29 April 2024; Roberto Caso, "Michelangelo's David and Cultural Heritage Images. The Italian Pseudo-Intellectual Property and the End of Public Domain" (Kluwer Copyright Blog, 15 June 2023) <https://copyrightblog.kluweriplaw.com/2023/06/15/michelangelos-david-and-cultural-heritage-images-the-italian-pseudo-intellectual-property-and-the-end-of-public-domain/> accessed 29 April 2024; Deborah De Angelis and Guiditta Giardini, "Tales of Public Domain Protection in Italy" (COMMUNIA Association, 10 July 2023) <https://communia-association.org/2023/07/10/tales-of-public-domain-protection-in-italy/> accessed 29 April 2024.

II. An EU data regime – or a regime complex[70] – to operationalise the CHDS?

29 To establish a single market for data, the European Data Strategy not only launched the CEDS initiative but also revamped the EU data framework by introducing new pieces of legislation. The EU Data Package, comprising the DGA and the DA, aims to lay the framework to facilitate data-sharing practices across the EU in order to unleash the potential of the European data market and to enable the cross-border and cross-sectoral reuse of underutilised data corpora.[71] Whereas these acts hold several provisions addressing the CEDS, the operationalisation of this initiative is also supported by other instruments such as the General Data Protection Regulation (GDPR), the Regulation on the free flow of non-personal data (FFD) and the ODD. The most relevant acts for the CHDS are the ODD and the DGA, which have introduced, respectively, mandatory and voluntary mechanisms for the reuse of certain categories of publicly held data and public-sector data.

1. Open Data Directive

30 The ODD, which entered into force in 2019, repeals the Public-Sector Information (PSI) Directive[72] to modernise the Union's legislative framework to foster digital innovation.[73] It aims to optimise the reuse of PSI held by public-sector bodies and undertakings, as well as publicly-funded research data, for both commercial and non-commercial purposes, to promote and facilitate the launch of new digital products and services.[74] To this end, the Directive targets the availability of a wide spectrum of PSI including "social, (...), geographical, environmental, (...) touristic"[75] data, by introducing a *mandatory* data-sharing regime for public-sector entities to eliminate the remaining barriers to the

70 Coined by Kal Raustiala and David Victor, the term "regime complex" refers to "a collective of partially overlapping and non-hierarchical regimes". See: Raustiala K and Victor DG, "The Regime Complex for Plant Genetic Resources" (2004) 58 International Organization 277 <https://www.cambridge.org/core/journals/international-organization/Article /abs/regime-complex-for-plant-genetic-resources/5C6B7B9E45268249D2893621CC64A7E5> accessed 13 December 2024.

71 COM(2020) 66 final (n 4).

72 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90. (No longer in force.)

73 Directive (EU) 2019/1024 (n 20), Recitals 3 and 9.

74 Ibid, Article 1(1) and Article 3(1).

75 Ibid, Recital 8.

reuse such information.

31 In this framework, the digitisation and online availability of cultural assets held by cultural establishments and their private partners[76] is acknowledged as a means to achieve the open data goals of the ODD. Therefore, the ODD encourages "the wide availability and reuse of [PSI] (...)"[77] – including public-sector CHI's assets – with minimal or no legal, technical or financial constraints."[78] However, the way the ODD identifies its beneficiaries and sets its scope, as well as the terminology it adopts, raises several questions, particularly concerning its interplay with the EU copyright *acquis* and its efficacy for the population of the CHDS with digital CH assets.

32 The ODD, while giving the impression of opening a vast array of PSI held by cultural establishments to (re)use, carves out multiple CHIs from its mandatory data-sharing regime. Indeed, the Directive does not apply to public-sector broadcasters and their subsidiaries, certain cultural and educational establishments as well as research-performing institutions.[79] Furthermore, if read together with the Copyright in the Digital Single Market Directive[80] (CDSMD) and its definition of CHIs,[81] the ODD causes asymmetries, as it circumscribes the scope of "cultural establishments" to public libraries, museums and archives while leaving, for instance, film and audio heritage institutions and research organisations (including their libraries) out of the scope.[82]

33 The ODD also limits the scope of its subject matter, which has spillover effects on the range of beneficiary institutions. The Directive distinguishes publicly held CH assets based on whether they are protected by third-party IPRs or by IPRs held by public-sector bodies and undertakings. While the former category is excluded from the scope of the ODD, Recital 65 also eliminates certain cultural establishments – orchestras, operas, ballets, theatres, and their archives – from the list of beneficiaries to which the ODD applies. This legislative decision is based on the presumption that cultural assets held by these entities are often subject to third-party IPRs.[83] Additionally, Recital 55 of the ODD exempts CH assets protected by IPRs held by public-sector bodies if such IPRs were acquired from third parties. This specification introduces considerable uncertainty, which risks halting the processes of sharing and reusing whenever previous rightsholders are unknown,[84] as in the case of orphan works.

34 Last but not least, the legal concepts adopted by the ODD generate conceptual turmoil instead of providing clarity for the data-sharing practices involving born-digital or digitized CH assets. The open data strategies and the mandatory data-sharing framework envisioned by the ODD are centred around the term "document", which Article 2(6) ODD defines as "any content whatever its medium (paper or electronic form or as sound, visual or audiovisual recording); or any part of such content."[85] The definition is complemented by Recital 30 of the ODD, suggesting that the document is an umbrella concept encompassing data (in the sense of the EU data legislation)[86] as a sub-category while refraining from any references to works and other subject matter, which are crucial to the EU copyright *acquis*. Concurrently, concerning CH assets, which are fundamental for the CHDS, the term "document" enshrined in the ODD covers only digitized or two-dimensional analogue or digital literary works, databases enlisting cultural establishments' inventories and their associated metadata, whereas three-dimensional artistic works and other artefacts, as well as software,[87] falls outside the term's scope. In addition, it is hard to understand where digitised cinematographic works – comprising born-digital or digitized representations of acts, facts and information combined with musical works (or, audio recordings) that can be displayed via software – stand in this interplay of documents, data and works.

35 Against this background, it becomes evident that, in achieving the CHDS' ambitions, the ODD is of practical use only for the digitisation and sharing of CH assets whose initial IPRs-owners (hence authors/creators/makers) are public libraries, museums or archives, and of CH assets in the public domain that are held in the collections of these public institutions.[88] As to the former cluster, it should be noted that the ODD's beneficiary institutions are custodial/memory institutions rather than generators of CH assets.

76 Ibid, Recitals 33, 49, 65.

77 Ibid, Recital 16.

78 Ibid.

79 Ibid, Article 1(2) sub-paragraphs (i), (k), and (l).

80 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92.

81 Ibid, Article 2(3).

82 Directive (EU) 2019/1024 (n 20), Article 1(2)(j).

83 Ibid, Recital 65.

84 Paul Keller and others, "Re-Use of Public Sector Information in Cultural Heritage Institutions" (2014) 6 Journal of Open Law, Technology & Society 1 <https://www.jolts.world/index.php/jolts/Article /view/104> accessed 9 May 2024, 5.

85 Directive (EU) 2019/1024 (n 20), Article 2(6).

86 Intended as "the digital representation of acts, facts or information, or the compilations of such acts, facts and information", as in Regulation (EU) 2022/868 (n 21), Article 2(1).

87 Directive (EU) 2019/1024 (n 20), Recital 30.

88 Also see: ibid, Recital 54.

In this sense, the types of CH assets that might have been authored/created/made by them and their relevance to the CHDS are matters yet to be clarified. As to the second cluster, empirical evidence reveals that national approaches to the interplay of publicly held data, PSI and the CH assets allocated to the public domain vary from one EU Member State to another, hence blurring the lines that contour the scope of national CH assets to which the ODD might apply.[89] Finally, the possible consequences of the interplay between ODD and analogue public domain CH assets is an unchartered terrain, especially if such CH assets have been digitised using techniques that might exhibit originality (e.g. restoration, translation, reconstitutions in the digitised material). It is yet to be understood whether CH assets will remain in the public domain once digitised via advanced technologies or after being digitally restored and reconstituted. Whereas public-private partnerships might be the optimal solution to reduce digitisation costs and overcome the public entities' lack of expertise in mass digitisation, the current EU regulatory framework does not provide any incentives or mechanisms to balance public-private interests over digitised content.[90]

89 The study conducted by Sganga *et al.* showcases the national legislatures' take on the public domain. Mapping the legal tools available in the national copyright laws of the EU Member States, the study confirms the previous endeavours in the field that the European legal landscape lacks a common understanding of the public domain and the subject matters allocated to the public domain. Furthermore, there are Member States whose copyright laws do not contain any references to the public domain (e.g. France), while some other States allocate certain content (e.g. legislation, official documents, court decisions) to the public domain. Yet, such content is often not essential for the operationalisation of the CHDS. See: Caterina Sganga and others, "D2.3- Copyright Flexibilities: Mapping and Comparative Assessment of EU and National Sources" <https://zenodo.org/record/7540510> accessed 13 February 2024; Kristofer Erickson and others, "Copyright and The Value Of The Public Domain" <https://zenodo.org/record/14975> accessed 29 April 2024. Focusing on the interplay of PSI, copyright and the public domain in the context of the CH sector, the study penned by Sappa *et al.* exposes that while the CHIs in certain Member States have difficulty in assigning "public domain" status to certain content, given the legal ambiguity; there is hardly any norms or incentives for CHIs to open their metadata for the reuse of the public at large. See: C Cristiana Sappa, "Legal Aspects of Public Sector Information: Best Practices in Intellectual Property" (2014) 8 Masaryk University Journal of Law and Technology 233; Cristiana Sappa, "Selected Intellectual Property Issues and PSI Re-Use" (2012) 6 Masaryk University Journal of Law and Technology 444 <https://heinonline.org/HOL/Page?handle=hein.journals/mujlt6&id=451&collection=journals&index=>.

90 Ibid, 6, Recital 12.

36 In sum, the ODD, instead of bringing along "revolutionary changes"[91], merely systematises CHIs' usual practices,[92] which until the PSI Directive were left to the discretion of individual institutions.[93]

2. Data Governance Act

37 The DGA was the first legislative text adopted under the aegis of the European Strategy for Data.[94] Among other goals, its provisions are conceived to support the fulfilment of the aims and objectives of the CEDS by fostering the availability, interoperability and reuse of publicly held data pooled in the Union, especially those "that are expected to be used in different data spaces."[95] To this end, the DGA harmonises cross-border and cross-sectoral data-sharing practices, in order to remove obstacles to the smooth functioning of the internal market for *voluntary* data exchanges with the participation of multiple intermediaries and stakeholders.[96]

38 Devised to complement the ODD,[97] the DGA covers most of the categories of publicly held data to which the ODD does not apply, such as data subject to different legal regimes of protection, including IPRs.[98] In line with the Data Package, the DGA defines data as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording."[99] The Regulation applies to data held by public-sector bodies, including their associations or any other not-for-profit legal entities formed by them if such entities are governed by public law.[100] It enables the reuse of such publicly held data by both natural or

91 Keller and others (n 84), 3.

92 Ibid, 5.

93 Ibid, 3-5.

94 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25.11.2020, COM(2020) 767 final, Explanatory Memorandum, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767> accessed 29 December 2024, 1.

95 SWD(2020) 295 final (n 96), 5.

96 See: Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), SWD(2020) 295 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0295> accessed 29 December 2024, 3-4.

97 COM(2020) 767 final (n 94), Explanatory Memorandum, 1.

98 SWD(2020) 295 final (n 93), 5.

99 Ibid, Article 2(1).

100 Ibid, Article 2 paragraphs (17) and (18).

legal persons,[101] without necessarily differentiating commercial from non-commercial uses.[102] Within this framework, the categories of publicly held data opened to reuse comprise personal data and data that are protected by commercial confidentiality, statistical confidentiality measures, or third-party IPRs.[103]

39 The DGA devises a legal framework based upon three regulatory pillars. The first pillar provides a normative framework for the reuse of certain categories of data without necessarily imposing any obligations on the public-sector bodies holding them.[104] The second pillar sets out the rules applicable to data intermediation services, including the market-driven activities of public-sector bodies, to facilitate the reuse of personal and non-personal data for commercial purposes via online intermediaries.[105] The last pillar introduces a legal framework for data altruism to incentivise and regulate the sharing of personal data by data subjects.[106]

40 The broad formulation of data and the inclusion of IPRs-protected data in the context of the DGA seems promising for the CEDS in general, also given that the DGA was designed to "leave a significant amount of flexibility for application at sector-specific level, including for the future development of European data spaces."[107] However, just like the ODD, the DGA features limitations in its subject matter and a *regime complex*[108] for data-sharing practices which, together with the interplay with other legal regimes applicable to such data, raise several questions on to what extent the Regulation can support the operationalisation of the CHDS.

41 Similar to the ODD, the DGA also omits certain categories of data in a way that endangers the successful operationalisation of several sector/domain-specific data spaces, especially the CHDS. Article 3(2) of the DGA eliminates, *inter alia*, data held by public service broadcasters and their subsidiaries, and cultural establishments and educational establishments, which Recital 12 of the DGA details as "libraries, archives and museums, as well as orchestras, operas, ballets and theatres"[109], from its scope. This policy choice was initially justified by the fact that the data-sharing regime introduced by the DGA is, in principle, addressed to the publicly held data protected by IPRs.[110] However, in the case of cultural and educational establishments, it is not the data held by such organisations, but the *works* and other *documents* in which such data is ingrained, which are usually protected by IPRs.[111] Slightly amending this statement, the final compromise text clarified that the DGA intended to exclude "data included in works or other subject matter over which third parties have [IPRs],"[112] adding that the works and other documents held by these institutions are predominantly subject to third-party IPRs.[113]

42 Regardless of the cryptic justification, the way in which the DGA sets its scope has two major implications for the CHDS. First, the DGA, let alone complementing the ODD, further exacerbates the gap left by the ODD by pushing the CH assets essential to the CHDS to its periphery. In this sense, it is hard to identify the categories of data that the DGA might help reuse to achieve the goals of the CHDS. Second, the terminology used in the different phases of the drafting process has also triggered an unresolved debate on whether and to what extent the subject matters of copyright can be deemed as "data" under the definition offered by the DGA and the DA.[114]

43 The interplay of data and IPRs also comes into play when framing the meaning of "data-sharing" under the DGA, which is necessary for the successful deployment of the CHDS. According to Article 2(10) of the DGA, data-sharing is an umbrella term referring to "the provision of data by a data subject or data holder to a data user, based on voluntary agreement or Union or national law, directly or through an intermediary."[115] Data-sharing practices "cover many transactions, ranging from the mere provision of access to the aggregation and joint exploitation

101 Ibid, Article 2(2).
102 Ibid.
103 Ibid, Article 3(1).
104 Regulation (EU) 2022/868 (n 21), Ch. II, Article s 3-9.
105 Ibid, Ch. III, Article s 10-15.
106 Ibid, Ch. IV, Article s16-25.
107 COM(2020) 767 final (n 94), 3.
108 See footnote 70.
109 Ibid, 6, Recital 12.
110 COM(2020) 767 final (n 94), Recital 8.
111 Ibid.
112 Proposal for a Regulation of the European Parliament and of the Council on the European data governance (Data Governance Act) – Outcome of the European Parliament's first reading (Strasbourg, 4-7 April 2022), P9_ TA(2022)0111, Annex, 19, Recital 10.
113 Regulation (EU) 2022/868 (n 21), Recital 12.
114 See: European Commission. Directorate General for Research and Innovation. and Martin Senftleben, *Study on EU Copyright and Related Rights and Access to and Reuse of Data* (Publications Office of the European Union 2022) <https://data.europa.eu/doi/10.2777/78973> accessed 10 May 2024, 9-10; Julie Baloup and others, "White Paper on the Data Governance Act" (KU Leuven, Centre for IT & IP Law (CiTiP) 2021) Technical Report <https://www.researchgate.net/publication/352690055_White_Paper_on_the_Data_Governance_Act?enrichId=rgreq-3d44a0853c5573556800ac3f5dc16c62-XXX&enrichSource=Y292ZXJQYWdlOzM1MjY5MDA1NTtBUzoxMDM5OTQzODcwNzI2MTQ0QDE2MjQ5NTMzNDgwMDg%3D&el=1_x_2>, 9-10.
115 Regulation (EU) 2022/868 (n 21), Article 2(10).

of data among contracting parties."[116] In this context, *access* to data, according to the DGA, refers to the use of data "without necessarily implying the transmission or downloading of data."[117] The concept of "reuse", on the other hand, stands for the commercial or non-commercial use of data out of the context of the initial purpose for which data has been produced.[118] Based on these definitions, the achievement of a functioning access system, as envisioned by the DGA, also depends on the adoption of voluntary and compulsory licensing schemes under the framework of EU copyright law, given that the reuse of data entails a combination of acts of reproduction, making available/communication to the public and distribution, which are subject to EU copyright law. However, the tools provided by the EU copyright system, particularly the narrow scope and rigid nature of mandatory and optional exceptions and limitations (E&L) and compulsory licensing schemes, can hardly facilitate the commercial and non-commercial reuse of such CH assets.

44 To further complicate the framework, the performance of data-sharing, access and reuse activities through the CEDS infrastructure requires the exercise of economic rights protected under copyright law by various market players. For instance, the intermediation service providers and their data-sharing practices, as regulated by the DGA, add yet another layer of intricacies. The Act introduces a notification system for such services, which tackles the regulatory uncertainty related to the liability of intermediary services concerning legally protected data.[119] It enlists the conditions for providing data intermediation services, including tools to ensure the interoperability of data to be shared or to facilitate data-sharing practices (e.g. temporary storage, anonymisation or pseudonymisation of data).[120] Last, it establishes a monitoring system to ensure compliance with these conditions.[121] While data intermediation services covered by the DGA include the commercial activities of public-sector bodies, Article 2(11)(b) of the DGA carves out "services that focus on the intermediation of copyright-protected content."[122]

45 Along the same lines, Article 2(11) of the DGA requires the separation of copyright-protected content from the public domain content to be shared via data intermediation services; while the services involving the former automatically fall out of the scope of the DGA, services concerning the latter are, in principle, subject to the DGA regime. At this point, however, the DGA introduces another filtering system. Intermediation services concerning the exchange of public domain content are covered by the Regulation only if they take place in the context of commercial relationships. Therefore, data intermediation services involving copyright-protected CH assets, as well as those that deal with the exchange of public domain content in a non-commercial setting, are subject to the piecemeal regulation outlined in the CDSMD,[123] the Digital Markets Act (DMA) and Digital Services Act (DSA).[124] This choice might cause significant uncertainties and hamper the development of the CHDS, especially since the use of advanced technologies to digitise analogue cultural content may save CH assets from the public domain, given that certain techniques used to restore, translate or regenerate them may trigger the granting of copyright to their producers, should their contributions to the digitisation process be deemed original enough to meet the benchmark required for copyright protection. All in all, the regulation of data intermediation services creates, in fact, a web of disparate legal regimes to inform and govern the sharing of different fragments of CH assets essential to the CHDS, with a negative rather than positive contribution to its operationalisation.

46 Based on these explanations, it is clear that the DGA has introduced a multi-layered system that makes data-sharing activities concerning cultural heritage subject to a plethora of different legal regimes. This creates a *regime complex* for those key market players – *Europeana*, national data aggregators, and national CHIs and educational establishments – whose activities are pivotal to the realisation of the CHDS.

III. The Way Forward or the Dead-End? The EU Copyright *Acquis* and the Common European Data Space for Cultural Heritage

47 The EU copyright *acquis* has also undergone a major transformation since the early 2000s in

116 Giovanni Comandé and Giulia Schneider, "It's Time: Leveraging the GDPR to Shift the Balance towards Research-Friendly EU Data Spaces" (2022) 59 Common Market Law Review 739 <https://kluwerlawonline.com/journalArticle/Common+Market+Law+Review/59.3/COLA2022051> accessed 3 May 2024, 741.

117 Regulation (EU) 2022/868 (n 21), Article 2(13).

118 Ibid, Article 2(2).

119 Regulation (EU) 2022/868 (n 21), Article 2(11).

120 Ibid, Article 12.

121 Ibid, Article 14.

122 Ibid, Article 2(11)(b).

123 See: Ibid, Recital 29.

124 Also see: Quintais JP and others, "Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis" (2022) <Zenodo. https://doi.org/10.5281/zenodo.7081626> accessed 29 December 2024.

response to technological advancements and the development of the EU digital and data strategies. Especially the Union's ambitions regarding mass digitisation projects were frustrated by the lack of harmonization of national copyright laws, which the EC underestimated in its Green Paper on Copyright and Challenge of Technology, where it stated that "[m]any issues of copyright law [did] not need to be subject of action at the Community level"[125] given the accession of the vast majority of Member States to the Berne Convention. These international instruments were considered sufficient to harmonise the Member States' laws to the extent needed for the smooth functioning of the internal market, whilst "[m]any of the differences that remained [were deemed to] have no significant impact on the functioning of the internal market of the Community's economic competitiveness."[126]

48 Yet, the Google Books project, inaugurated in 2004, marked a turning point in the history of global copyright law, given that it highlighted the problems raised by the digitisation of copyright-protected works, works in the public domain and other subject matters, including the so-called orphan and out-of-commerce works, showing how an outdated copyright regime might hamper the public's access to and engagement with born-digital and digitized culture and CH.[127] Since then, the modernisation of the EU copyright *acquis* has gone hand in hand with the implementation of the EU Digital Single Market strategy, which included devising large-scale digitisation projects, such as *Europeana*, to ease the digitisation and dissemination of European CH assets, such as printed materials (books, journals, magazines), photographs, museum objects, archival documents and audiovisual materials.[128]

49 Despite these attempts, the EU's efforts to digitise CH assets and *Europeana*'s success were not enough to build a single access point to CH. As admitted by the EC, not even half of the digitised CH assets in *Europeana* collections can be reused for commercial or non-commercial purposes.[129] Now that the EU is committed to establishing a data space to enhance the online access to, availability and reuse of CH assets, it is of pivotal importance to assess the EU copyright *acquis vis-à-vis* its fitness to foster the digitisation of analogue cultural content and enable its reuse by multiple stakeholders for different purposes, in order to understand whether and what reforms are needed to facilitate the implementation of the CHDS. To this end, the following pages will focus on the Information Society Directive[130] (InfoSoc Directive), Copyright in the Digital Single Market Directive[131] (CDSMD), and the Orphan Works Directive[132] (OWD), read through the prism of the CHDS.

1. Information Society Directive

50 Entered into force in June 2001,[133] the InfoSoc Directive represents the first major horizontal intervention of the EU legislator to harmonise national copyright regimes and adjust them to technological advancements and the widespread use of the Internet. The Directive took the opportunity offered by the implementation of the WIPO Internet Treaties[134] to standardise exclusive economic rights enshrined in copyright, regulate digital rights management and technological protection measures, and harmonise national approaches to the democratisation of access and use of protected works by introducing a list of twenty optional and one mandatory E&Ls to copyright and related

125 Communication from the Commission, Green Paper of Copyright and the Challenge of Technology – Copyright Issues Requiring Immediate Action, Brussels, 07.06.1988, COM(88) 172 final <https://op.europa.eu/en/publication-detail/-/publication/f075fcc5-0c3d-11e4-a7d0-01aa75ed71a1> accessed 29 December 2024, 8, paragraph 1.4.9.

126 Ibid.

127 Simone Schroff, Marcella Favale and Aura Bertoni, "The Impossible Quest – Problems with Diligent Search for Orphan Works" (2017) 48 IIC - International Review of Intellectual Property and Competition Law 286 <https://doi.org/10.1007/s40319-017-0568-z> accessed 30 April 2024; Katharina de la Durantaye, "Orphan Works: A Comparative and International Perspective" in Daniel J Gervais (ed), *International Intellectual Property: A Handbook of Contemporary Research* (Edward Elgar Publishing), 193.

128 Commission Staff Working Document, SEC(2008) 2372 (n 48); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Towards a modern, more European copyright framework, COM(2015) 626 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A626%3AFIN> accessed 29 December 2024, 2; Council conclusion on the role of Europeana for the digital access, visibility and use of European cultural heritage (2016/C 212/06) [2016] OJ C 212/6 9.

129 Commission Recommendation (EU) 2021/1970 (n 26), 8.

130 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10.

131 Directive (EU) 2019/790 (n 78).

132 Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works (Text with EEA relevance) [2012] OJ L 299/5.

133 Directive 2001/29/EC (n 127), Article 14.

134 Ibid, Rec. 15; Christophe Geiger and Franciska Schönherr, "The Information Society Directive" in Irini Stamatoudi and Paul Torremans (eds), *EU Copyright Law: A Commentary* (Second Edition, Edward Elgar Publishing 2021), 280, para. 11.01.

rights.[135] Among these E&Ls, only one is relevant to the population of the CHDS with digitized CH assets in general, whereas another one comes into mind with regard to the born-digital and analogue artistic and architectural works.

51 To begin with, Article 5(2)(c) of the InfoSoc Directive introduces an *optional* E&L to the exclusive right of reproduction, directed to facilitate certain acts of reproduction "made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage."[136] The provision applies to authorial works, fixations of performances, phonograms, original and copies of films, and fixations of broadcasts.[137] Computer programs and databases[138] are excluded from the scope of Article 5(2)(c) of the InfoSoc Directive, but the provision finds correspondence in the Database Directive[139] and Software Directive.[140]

52 In line with Recital 21 of the InfoSoc Directive, the act of reproduction referred to in Article 5(2)(c) of the Directive shall be interpreted broadly to ensure legal certainty across the EU, and encompass "direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part."[141] This formulation covers both digital and analogue reproductions of a work or other subject matter, regardless of the original format of the reproduced content, whilst enabling their fixation on a material carrier or via immaterial means.[142]

53 The positive impact of this E&L on the digitisation, digital restoration, digital cataloguing and preservation activities of CHIs is beyond doubt, and so is its contribution to achieving the online accessibility, availability and reuse of born-digital and digitized cultural content. However, once considered in tandem with the multi-stakeholder perspectives underpinning the CHDS initiative, Article 5(2)(c) of the InfoSoc Directive responds to the needs and expectations of only one of the three main players identified by the CHDS initiative – CHIs. The restriction of permitted uses to mere non-commercial purposes is not enough to allow the exploitation of CH assets by creative industries to develop data-based goods and services. Similarly, the limitation of the scope of the provision to reproduction only makes it beneficial for the internal operation of CHIs, and just limitedly to boost the engagement of the public with digitised CH assets.

54 Aside from Article 5(2)(c) of the InfoSoc Directive, the so-called freedom of panorama enshrined in Article 5(3)(h) of the Directive might be considered to assist the cross-border and cross-sectoral data flows within the CHDS. This provision, formulated as yet another *optional* E&L to copyright, allows the Member States to provide an exception or limitation to the reproduction right and the rights for communication and making available to the public in the context of the "use of works, such as works of architecture or sculpture, made to be located permanently in public spaces."[143]

55 Regardless of its broad articulation, several other indicators condemn the freedom of panorama exception to facilitate the operationalisation of the CHDS. First and foremost, the material scope of the provision is quite limited as this provision is devised to legitimise the reproduction of works of fine art available in publicly accessible spaces in various ways, including analogue and digital means, such as sketching, drawing, painting, and photography. Given the ways in which the InfoSoc Directive described the acts that fall under "reproduction", there is no ground to refrain from extending the modes of reproduction in this context also to AI-aided duplication methods or 3D printing. Nevertheless, the public policy rationale and the formulation of this provision leave a significant portion of CH assets – which are clustered under other categories of works, exhibited in CHIs or other closed spaces, or preserved in the archives or repositories of custodial/memorial institutions – outside its scope.

56 Second, a comparative and cross-national analysis of the national copyright regimes of the EU Member States exposes the remarkably fragmented implementation of the freedom of panorama exception across Europe. Indeed, not only the optional nature of the provision but also the simplicity of the letter of the law bestowed the national legislators with the margin of discretion to readjust the scope of the freedom of panorama in accordance with the national cultural policies and priorities. Indeed, there have been legislative attempts to recognise this freedom to certain selected beneficiaries, redefine the scope of the provision by elaborating on the concept of "public spaces", and introduce certain purposes or methods of reproduction.[144] That said, the variations in the

135 Sganga and other (n 89).

136 Directive 2001/29/EC (n 127), Article 5(2)(c).

137 See: Ibid, Article 2(1).

138 Ibid, Article 1.

139 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20, Article s 6(1) and 8.

140 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance) [2009] OJ L 111/16, Article s 5 and 6.

141 Directive 2001/29/EC (n 127), Article 2.

142 Geiger and Schönherr (n 131), 285, paragraph 11.07.

143 Directive 2001/29/EC (n 127), Article 5(3)(h).

144 Dore and Turan (n 62), 48-56. Also see: Sganga and others (n

national freedom of panorama provisions put the efficacy of this legal tool under scrutiny with respect to the smooth and free flow of data in a federated data space.

57 Last but not least, the so-called three-step test, which was introduced into the EU copyright *acquis* through Article 5(5) of the InfoSoc Directive, has become a tool at the hands of the national courts to further limit the efficacy of Article 5(3)(h) of the Directive. In fact, after the notorious *Wikimedia* case[145] – in which the Swedish Supreme Court ruled that the exploitation of images of works of visual art in outdoor spaces through online content-sharing platforms is incompliant with the three-step test, hence the provision in question – the freedom of panorama can be hardly taken into account among the legal tools that might support the operationalising of the CHDS.[146]

58 As a matter of fact, the conservative approach of the InfoSoc Directive, reflected in the identification of the beneficiaries of E&Ls and the national courts' interpretation of the three-step test – also characterises more recent interventions on copyright law, namely the OWD and the CDSMD.

2. Orphan Works Directive

59 Copyright-protected works whose rightsholders can be identified and located constitute merely a fragment of CHIs' collections. While securing digital access to such content via E&Ls or various licensing mechanisms is already a difficult endeavour, the Google Books experiment showcased the hardship entailed in digitising the so-called orphan works and making them available online and revealed that a significant portion of European CHIs' archives and collections comprise orphan works.[147]

60 To give impetus to the "i2010: Digital Libraries" initiative by closing the so-called "20th-century blackhole"[148], the EU adopted the OWD[149] in 2012. The OWD aimed at facilitating the digitisation and wider dissemination of orphan works and other subject matter by setting EU-wide standards for the recognition and termination of the orphan status to works across the EU and by regulating their permitted uses.[150]

61 The OWD is addressed to publicly accessible libraries, educational establishments and museums, archives, film or audio heritage institutions and public-service broadcasting organisations.[151] It covers literary, cinematographic and audiovisual works, phonograms as well as the works and other subject matter incorporated therein.[152] To be granted the status of "orphan work", CHIs should perform a diligent search[153] to ensure that rightsholders cannot be identified or located for rights clearance to reproduce and make such content available to the public.[154] Rightsholders can always terminate this status and have the right to be compensated for the use of their intellectual creations by CHIs.[155]

62 The OWD is the outcome of a comprehensive cross-border mapping of different legislative approaches and a comparative assessment of the strengths and weaknesses of several alternative routes taken by various States to enhance the exploitation of orphan works.[156] In this regard, an E&L to copyright and related rights, complemented by a diligent research requirement, has been considered the most convenient tool to facilitate mass digitisation projects that could empower European digital libraries. Despite its good intentions, the Directive has not achieved the level of success initially anticipated by EU policymakers, primarily because

87).

145 *Bildupphovsra¨tt i Sverige (BUS) ek. fo¨r. v Wikimedia Sverige*, O¨ 849-15.

146 Dore and Turan (n 62), 48-56. Also see: Sganga and others (n 89)

147 Simone Schroff and others (n 124), 287; Katharina de la Durantaye (n 124), 190.

148 Boyle J, "Google Books and the Escape from the Black Hole" (*The Public Domain: Enclosing the Commons of the Mind*, 9 June 2009) <https://www.thepublicdomain.org/2009/09/06/google-books-and-the-escape-from-the-black-hole/>. Also see: "The Missing Decades: The 20th Century Black Hole in Europeana" (*Europeana Pro*) <https://pro.europeana.eu/post/the-missing-decades-the-20th-century-black-hole-in-europeana>.

149 Directive 2012/28/EU (n 129).

150 See: Ibid, Article s 3-6.

151 Ibid, Article 1(1).

152 Ibid, Article 1 paragraphs (2) and (4).

153 Ibid, Article 3 and Article 6.

154 Ibid, Article 3.

155 Ibid, Article 5 and Article 6(4).

156 See: Commission Decision of 27 February 2006 on setting up a High Level Expert Group on Digital Libraries (2006/178/EC) [2006] OJ L 63/25; European Commission, Proposal for a Directive of the European Parliament and of the Council on certain permitted uses of orphan works, COM(2011) 289 final <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0289:FIN:EN:PDF> accessed 29 December 2024.

of the intricacies of the diligent search requirements and the redress mechanism provided in favour of rightsholders.[157] The Study on the application of the Orphan Work Directive,[158] published in 2020, showed that less than a quarter of the beneficiary CHIs had found the OWD a useful contribution to the field, whilst half of them expressed their scepticism on the positive impacts of the Directive on digitisation and dissemination of orphan works.[159] As a consequence, the aforementioned Study proved how the mechanism introduced by the OWD is better suited for small-scale digitisation projects rather than for the larger, massive endeavours envisioned by the EC.[160]

63 Aside from these concerns, two other features weaken the potential of this Directive to assist in the operationalisation of the CHDS. First, the OWD leaves stand-alone graphic works (e.g. photographs, posters, illustrations or postcards) out of its scope,[161] unless they are "embedded or incorporated in, or constitute an integral part of, [orphan] works and phonograms."[162] Second, permitted acts do not cover commercial uses or communication to the public.[163] While these elements constitute shortcomings of the OWD mechanisms already for the *Europeana* project,[164] there is no doubt that their impact on the CEDS and CHDS will be even stronger.

3. Copyright in the Digital Single Market Directive

64 The CDSMD, which entered into force in 2019,[165] constitutes the second horizontal EU intervention in the field of copyright and the most recent attempt to streamline the EU copyright system with the goals of the EU digital agenda. The Directive covers fields that have not (or only cursorily) been touched upon in the past by the EU copyright *acquis*, such as E&Ls for research, innovation, education, and preservation of CH.[166] The latter aims at facilitating large-scale digitisation activities and cross-border and online access to and use of copyright-protected content in the context of these four major fields.[167]

65 Article 6 of the CDSMD is devised to foster the preservation of CH, especially for future generations.[168] It provides a mandatory exception to copyright and related rights in favour of a non-exhaustive list of CHIs such as, *inter alia,* publicly accessible libraries or museums, archives, film or audio heritage institutions.[169] Recital 13 of the CDSMD specifies the range of beneficiaries by listing national libraries and national archives, educational establishments' archives and publicly accessible libraries, research organisations, and public sector broadcasting organisations. Taking into account the financial and technical hurdles faced by CHIs when managing large-scale digitisation activities,[170] the Directive also allows them to benefit from the exception in case of public-private partnerships, by holding that CHIs "should be allowed to rely on third parties acting on their behalf and under their responsibility, including those that are based in other Member States, for the making of copies."[171]

66 Article 6 of the CDSMD permits the reproduction of any works or other subject matter in the CHI's permanent collections, regardless of their nature.[172] The definition covers authorial works, computer programs, databases, fixations of performances, phonograms, fixations of broadcasts, and press publications held in the permanent collections of the beneficiary institutions. Recital 29 of the CDSMD clarifies the notion of "permanent" by specifying that the provision applies only to copies that are "owned or permanently held by that institution, for example as a result of the transfer of ownership or a license agreement, legal deposit obligations or permanent custody agreements."[173] Reproductions can be performed in any format or medium, and "by the appropriate preservation tool, means or technology, (...) in the required number, at any point in the life of a work or other subject matter and to the extend required for preservation purposes"[174], as long as these acts are "for purposes of preservation of such works or other subject matter and to the extent necessary for such preservation."[175]

157 European Commission, Directorate-General for Communications Networks, Content and Technology, McGuinn J, Sproģe, J, Omersa, E, Borrett C and others, *Study on the application of the Orphan Works Directive (2012/28/EU) – Final report*, Publications Office of the European Union, 2021 <https://data.europa.eu/doi/10.2759/32123> accessed 29 December 2024, 87-89.

158 Ibid.

159 Ibid, 83.

160 Ibid.

161 Ibid, 87.

162 Directive 2012/28/EU (n 129), Article 1(4).

163 McGuinn and others (n 150), 88.

164 Ibid.

165 Directive (EU) 2019/790 (n 78), Article 31.

166 Ibid, Recital 5.

167 Ibid, Recital 3.

168 Ibid, Recitals 25 and 26.

169 Ibid, Article 2(3).

170 Ibid, Rec. 28. Also see: "Cultural Heritage: Digitisation, Online Accessibility and Digital Preservation: Consolidated Progress Report on the Implementation of Commission Recommendation (2011/711/EU) 2015-2017", 15-16.

171 Directive (EU) 2019/790 (n 78), Recital 28.

172 Ibid, Recital 13.

173 Ibid, Recital 29.

174 Ibid.

175 Ibid, Article 6.

67 The exception fills in the gaps left by the national transposition of Article 5(2)(c) of the InfoSoc Directive, which in several Member States do not include digitisation and digital preservation,[176] by introducing a harmonized rule that allows the reproduction of copyright-protected CH assets by digital means. Nevertheless, just like its predecessor, Article 6 of the CDSMD is limited to the internal activities of CHIs, since it covers the right to reproduction but not the right to communication and making available to the public. In this sense, the provision falls short of addressing the needs of businesses and citizens as envisioned by the CHDS initiative.

68 In fact, only a handful of the E&Ls and licensing schemes belonging to the EU copyright *acquis* feature an external dimensional. One of these instances can be found in Article 8 of the CDSMD, which introduces measures to ease the accessibility of works and other subject matter that are no longer "available to the public through customary channels of commerce"[177], also known as out-of-commerce works. The provision entrusts collective management organisations (CMOs) with the power to conclude non-exclusive extended collective licensing schemes, covering also works of non-CMO members, with CHIs, which allow them to reproduce, distribute, communicate or make available to the public out-commerce-works or other subject-matter that are in their permanent collections. CMOs should meet specific representativeness and operational requirements. Should this not be possible in a Member State, or for works and other subject matter which cannot be licensed by any CMOs,[178] Article 8(2) of the CDSMD prescribes the implementation of an exception having the same purpose and content of the extended license. Accordingly, CHIs are permitted to reproduce, by any means, in whole or in part, original databases; translate, adapt, arrange or perform any other alteration of copyright-protected databases and communicate, display or perform them to the public; and extract or re-utilize the contents of databases protected by sui generis right. They can also reproduce, translate, adapt, arrange, or perform any other alteration of computer programs, as well as reproduce, communicate and make available to the public works and other subject matter, including works protected by press publisher's rights. Such acts shall be performed for non-commercial purposes and be accompanied by "the name of the author or any other identifiable rightsholder (...) unless this turns out to be impossible"[179] and only if such works and other subject matter are made available on non-commercial websites.[180]

69 Whereas Article 8 of the CDSMD revitalizes the European cultural space by facilitating the flow of cultural and CH content to the European cultural marketplace, it still misses setting common criteria or a standardised procedure to determine the out-of-commerce status of cultural content. By simply requiring that "a reasonable effort has been made to determine whether [the work] is available to the public"[181], the provision leaves any further specification to Member States. This carries obvious risks of fragmentation of national solutions, scarce harmonization and related negative impact on cross-border exchanges, which weaken the potential of Article 8 of the CDSMD to contribute to the realization of the CHDS. The same can be said for the absence of any extended licensing scheme for end users' commercial and non-commercial reuse of out-of-commerce works. This critique, in fact, circles back to the discussions on the EU copyright regime's approach in tackling the digitisation of orphan works, which was another major obstacle to large-scale digitisation projects.

4. Public Domain and the Copyright in the Digital Single Market Directive

70 The public domain has remained at the periphery of the EU legal harmonisation endeavours.[182] Not only does the Union lack a common binding definition of the boundaries of the notion, but the provisions that directly or indirectly refer to it are scattered and vary from one Member State to another.[183]

71 Except for Article 1(2) of the Software Directive,[184] the only other EU copyright provision that explicitly intervenes in the public domain is enshrined in Article 14 of the CDSMD. This provision requires

176 COM(2015) 626 final (n 125), 3; Rosati E, *Copyright in the Digital Single Market: Article -by-Article Commentary to the Provisions of Directive 2019/790* (Oxford University Press 2021), 131, 133.

177 Directive (EU) 2019/790 (n 78), Article 8(5).

178 Ibid, Article 8(3).

179 Ibid, Article 8(2)(a).

180 Ibid, Article 8(2) sub-paragraphs (a) and (b).

181 Ibid, Article 5.

182 Séverine Dusollier, *Scoping Study on Copyright and Related Rights and the Public Domain* (World Intellectual Property Organization (WIPO)) <https://tind.wipo.int/record/28967> accessed 19 August 2024.

183 Ibid, Sganga and others (n 89).

184 Article 1(2) of the Software Directive transposes Article 9(2) of the Agreement on the Trade-related Aspects of Intellectual Property Rights (TRIPs Agreement) by crystallising that "copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such." Accordingly, this provision carves the "ideas and principles which underlie any element of a computer program, including those which underlie its interfaces" out of the scope of copyright protection. See: Directive 2009/24/EC (n 137), Article 1(2).

Member States to ensure that "when the term of protection of a work of visual art has expired, any material resulting from an act of reproduction of that work is not subject to copyright or related rights."[185] This rule, however, does not apply if the material resulting from the reproduction represents an original work, "in the sense that it is the author's own intellectual creation."[186]

72 This provision is crucial for large-scale digitisation activities of CHIs, mainly because public domain materials are prioritised over copyright-protected CH assets for mass digitisation initiatives, including the *Europeana* project.[187] Yet, Article 14 of the CDSMD is not immune to critique, especially if considered through the lens of the CHDS initiative. The letter of the law consists of several vague phrases, which are prone to trigger adverse effects for its beneficiaries, thus discouraging rather than incentivising the digital reproduction of public domain materials, for at least three interdependent reasons. First, the provision employs a new term, namely "works of visual art", which has neither been used before in the EU copyright legislation nor is it defined in the CDSMD.[188] Therefore, the concept carries different meanings, with varying scopes, in different Member States.

73 Second, despite the vague legal formulation within Article 14 of the CDSMD, Recital 53 of the Directive clarifies that the act of reproduction covered by the provision encompasses both analogue and digital copies. Furthermore, the notion of "reproduction" used in EU copyright directives includes direct and indirect, temporary and permanent, and two- and three-dimensional reproductions as well.[189] However, Article 14 of the CDSMD gives the possibility to exclude *original* reproductions that may be protected as new works for they represent an *author's own intellectual creation*. While a limited number of court decisions offer guidance on how to determine the originality of analogue reproductions,[190] there is much less clarity on the relevance of acts accessorial to digitisation practices, such as restoration (e.g. removing blemishes and damages, refining resolution) and editorial interventions on the original work (e.g. transliteration and transcription of ancient texts, annotation, emendation and conjectures in the text). This circumstance creates a remarkable uncertainty on the applicability of Article 14 of the CDSMD on a wide range of digital reproductions, with an inevitable negative impact on the usefulness of the provision *vis-à-vis* the implementation of the CHDS.[191]

74 Third, Article 14 of the CDSMD prevents only the restoration of copyright protection for faithful reproductions of public domain materials, while it remains silent on the reproductions of materials subject to related rights that have fallen into the public domain.[192] Along the same lines, Article 6 of the Term Directive[193], which introduces a sui generis protection for non-original photographs, raises additional uncertainties as to the applicability of Article 14 of the CDSDM to digital reproductions of original photographs in the public domain, in case the latter satisfies the requirements for sui generis protection.[194] The same can be said for unpublished works and works of critical or scientific nature that are in the public domain, which Member States are free to protect through a related right in case of new publication or communication to the public, lasting for 25 or 30 years after the date of first publication or communication, respectively.[195]

185 Directive (EU) 2019/790 (n 78), Article 14.

186 Ibid.

187 COM(2005) 465 final (n 30).

188 Andrea Wallace and Ellen Euler, "Revisiting Access to Cultural Heritage in the Public Domain: EU and International Developments" (2020) 51 IIC - International Review of Intellectual Property and Competition Law 823 <https://link.springer.com/10.1007/s40319-020-00961-8> accessed 30 April 2024, 839.

189 Rosati (n 173), 243.

190 Wallace and Euler (n 185), 826.

191 See: Cristiana Sappa and Bohdan Widła, "Framing Texts and Images: Critical and Posthumous Editions in the Digital Single Market" (2023) 54 IIC - International Review of Intellectual Property and Competition Law 1359 <https://link.springer.com/10.1007/s40319-023-01394-9> accessed 29 April 2024, 1361, 1373, Cristiana Sappa, "Hosting the Public Domain into a Minefield: The Resistance to Article 14 of the DSM Directive and to the Related Rules That Transpose It into National Law" (2022) 17 Journal of Intellectual Property Law & Practice 924 <https://academic.oup.com/jiplp/Article/17/11/924/6693374> accessed 30 April 2024, 936.

192 Rosati (n 173), 248; Valérie-Laure Benabou and others, "Comment of the European Copyright Society on the Implementation of Art.14 of the Directive (EU) 2019/790 on Copyright in the Digital Single Market' (European Copyright Society (ECS), 2020).

193 Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version) [2006] OJ L 372/12, Article 6.

194 Rosati (n 173), 248; Séverine Dusollier, "The 2019 Directive on Copyright in the Digital Single Market: Some Progress, A Few Bad Choices, and An Overall Failed Ambition" (2020) 57 Common Market Law Review 979, 997-998; Cristiana Sappa and Bohdan Widła, (n 188), 1369; Marta Arisi, "Digital Single Market Copyright Directive: Making (Digital) Room for Works of Visual Art in the Public Domain" (2020) 1 Opinio Juris in Comparatione 119 <https://www.opiniojurisincomparatione.org/Article s/digital-single-market-copyright-directive-making-digital-room-for-works-of-visual-art-in-the-public-domain/> accessed 30 April 2024, 128-131, 141-144; Wallace and Euler (n 185), 838.

195 See: Directive 2006/116/EC (n 190), Article 4 and Article 5.

75 The *verbatim* implementation of Article 14 of the CDSMD by most Member States offers no additional guidance on the interplay between this provision and the optional sui generis rights introduced by the Term Directive.[196] Besides, given that Article 14 of the CDSMD mentions only copyright-protected works, it is reasonable to argue that Articles 4 to 6 of the Term Directive will not only shrink the public domain but prevent CHIs from populating the CHDS with digitised public domain works of these kinds.[197]

76 It is also important to assess the possible adverse impacts of the interplay of Article 14 of the CDSMD and the ODD on the operationalisation of the CHDS. On the one hand, Article 14 of the CDSMD curtails the capacity of public-sector bodies to exploit the digital copies of public domain works held in their collections or archives.[198] On the other hand, Article 12(3) of the ODD comes into play when public-sector bodies opt for public-private partnerships to cope with the financial and technical aspects of digitisation (e.g. automated digitisation, AI-aided digitisation and post-production editing techniques),[199] allowing the conclusion of exclusive agreements with private partners, which grant them the exclusive right to exploit the outcome of this digitisation venture for up to ten years. Copyright ownership, combined with such exclusivity, would not only hamper the free flow and reuse of data but also create the need for natural and legal persons to stipulate *ad hoc* license agreements to use such data for commercial or non-commercial purposes.

Also see: Wallace and Euler (n 185), 838-839; Benabou and others. (n 189). For an analysis of Article 4 of the Term Directive and its justification vis-à-vis the technological advancement and the ease in post-humous publication, please see: Sappa and Widła (n 188), 1370-1371; Sappa (n 188), 935.

196 For a comparative analysis of the implementation of Article 14 of the CDSM Directive in the national laws of the selected EU Member States, please see: Dore and Turan (n 62).

197 Ibid.

198 Also see: Wallace and Euler (n 185), 843.

199 Also see: Sappa (n 191), 937.

D. Conclusion

77 A brief analysis of the interplay of the cultural heritage, data and copyright regimes at the EU and national levels reveals that an EU legislative intervention is inevitable should the CHDS be operationalised as an interoperable and federated IT infrastructure dedicated to the free flow and reuse of CH-related data. This, however, will not be an easy task, as the EC inherited several unresolved issues and unmet needs of a wide array of stakeholders interested in born-digital and digitized CH assets.

78 Given its limited competence to regulate European CH,[200] the EU legislator's margin of manoeuvre does not reach beyond encouraging Member States to adopt measures for "higher quality digitisation, reuse and digital preservation"[201] of CH assets in their territories, and leaving the EU with merely the authority to set indicative targets to be reached in digitisation activities by 2030.[202] This partially explains why the Commission has entrusted the *Europeana* Consortium to monitor and govern the operationalisation of the CHDS,[203] which in return assimilated this brand-new *single market for data* project into the EU's previous initiative, the *Europeana* platform – or the initiative to create a *single digital access point* for cultural content. In addition, the key legislations adopted in the last two decades to facilitate the digitisation, online availability and reuse of CH assets feature several shortcomings in supporting a data space dedicated to CH.

79 First and foremost, the genesis and evolution of international instruments concerning CH and the distribution of powers among the EU and Member States have led to conceptual overlaps and conflicts stemming from the lack of a harmonised definition of CH and the norms that govern the born-digital or digitized CH assets critical for the CHDS.

80 Second, the legislative frameworks supporting the CEDS – mainly the ODD and DGA – leave CH assets that are critical to the CHDS outside the scope, while the EU copyright *acquis* – even after the InfoSoc Directive, the OWD and the CDSMD – does not feature effective tools tailored for or adapted to the overarching aims and objectives of the CHDS. Indeed, despite being promoted by the EC as the

200 See: Treaty on the Functioning of the European Union (n 34), Article 6.

201 Commission Recommendation (EU) 2021/1970 (n 26), 6.

202 Ibid, Annex.

203 Commission Decision of 29.06.2021 setting up the Commission Expert Group on the common European Data Space for Cultural Heritage and repealing Decision C(2017) 1444, C(2021) 4647 final <https://digital-strategy.ec.europa.eu/en/news/expert-group-common-european-data-space-cultural-heritage> accessed 29 December 2024.

key legislation for the CEDS,[204] the ODD and the DGA do not apply, respectively, to IPRs-protected data and to "data held by cultural establishments and educational establishments."[205] As a result, the EU data governance framework is of help to populate the CHDS only with public domain material held by public libraries, museums and archives, and copyright-protected works and other materials on which the aforementioned public institutions hold exclusive rights.

81 Third, because the modernisation of the EU copyright framework happened in parallel to the Union's *i2010* initiative,[206] the vast majority of the E&Ls and licensing schemes target only CHIs due to their intermediary role in giving access to CH.[207] Therefore, the existing copyright regime does not allow the reproduction and making available or communication of works to the public – neither by citizens and businesses nor by CHIs for commercial purposes. These features of the existing legal tools drastically reduce the possibility of increasing access to, free flow and reuse of copyright-protected CH assets.

82 Finally, the only legal provision preserving the public domain against further privatisations, namely Article 14 of the CDSMD, is also of limited use for the CHDS project, since its scope is limited to works of visual art only, and there is still no clarity on the implications of the use of advanced technology on the public domain status of digitised works.[208]

83 On top of the points raised above, the interaction of the cultural heritage, data and copyright regimes raises several unresolved issues. It is yet to be clarified whether the concepts of "document", "data", and "work" can be better linked and reconciled. Likewise, the compatibility of the ODD and the DGA with national CH law regimes, and the post-digitisation legal status of public domain materials, especially if realised in public-private partnerships, are among the matters pending resolution.

84 Regardless of the prevalence of such matters, EU policymakers have the tools to mitigate these shortcomings and make the CHDS a successful endeavour. As the first step, it is essential to break the patterns of path-dependency towards *Europeana* and re-focus on the "federated data space", which also encompasses online platforms, to enable access to or reuse of born-digital and digitized CH assets in different forms and formats, such as digital twins, derivative works, user-generated content. Down this pathway, a Memorandum of Understanding, to be concluded under the auspices of the EU, might be a useful option to effectively standardise the selection of CH assets to be digitised, without prejudice to the distribution of competencies among the EU and Member States.

85 Building upon this common ground, an implementing act would help identify, consolidate and systematise the various stakeholders' views and needs as well as the data transfers expected to occur through the CHDS. The implementing act could intervene in the EU data and copyright regimes to successfully operationalise the CHDS, adapting, for instance, existing copyright tools to the features of the CHDS, along with what the proposed Regulation for the European Health Data Space (EHDS) is doing to adjust data portability to the EHDS, by extending the scope originally envisioned by the GDPR.[209] This solution would save the EU legislator from another wave of copyright interventions, but still stretch the scope of the acts permitted by the E&Ls and licensing schemes provided by the EU copyright *acquis*. The implementing act would also be the right venue for the EU legislature to finally reflect on and introduce solutions for the interpretation of Article 14 CDSMD and its interplay with a broader spectrum of public domain works, including CH assets.

86 Whereas the highway currently taken to establish the CHDS is jammed with several bumps and obstacles along the way, the roadmap designed by the overarching aims and objectives of the CEDS initiative could serve as a reliable guide and source of inspiration. In this sense, the prospective implementing Act for the CHDS will need to move from *a single access point* to *a single market for data* model for digital cultural content. This is essential to avoid taking the wrong exit at the roundabout, which might lead the EC to abandon the CEDS path for CHDS for once and forever – an outcome which would be fully detrimental not only from the perspective of the fulfilment of the European Strategy for Data but also for the cultural and economic prosperity of European citizens and businesses.

204 See: Commission Staff Working Document on Common European Data Spaces (n 17).

205 Regulation (EU) 2022/868 (n 21), Article 3(2).

206 See: COM(2008) 513 final (n 47); COM(2015) 626 final (n 125).

207 See: Directive 2001/29/EC (n 127), Directive 2012/28/EU (n 129); Directive (EU) 2019/790 (n 78). Also see: Dore and Turan (n 62).

208 Benabou and others. (n 189); Dusollier (n 191); Sappa and Widła (n 188).

209 Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197> accessed 29 December 2024.

Clouds Connecting Europe: Interoperability in the EU Data Act

by **Leonie Ott and Yifeng Dong ***

Abstract: Interoperability, describing the ability of systems to work together, is a cornerstone of Europe's vision for a connected digital economy, and the Data Act takes a bold step in this direction. Articles 33-35 of said Act contain far-reaching interoperability mandates for data spaces and data processing services, including cloud services. However, the provisions' unclear language and structural complexities present interpretative challenges. For instance, the meaning of central terms like "data space" and "data processing service" remain ambiguous. To address these challenges, we propose an effects-oriented method emphasising an interdisciplinary analysis of the regulated industry and alignment of various legislative objectives with the effects of interoperability as a policy tool.

Applying this method, we find that the term "data space" must be interpreted restrictively in light of the public interest objectives of the relevant provision, namely as a platform that enables broad data sharing. Similarly, we argue that understanding the term "data processing service" is predicated on the insight that the technical terms used in the statutory definition are reflections of specific economic effects which characterize cloud markets (e.g. lock-in effects and the importance of amortisation). In order to reliably apply the definition, the technical terms must be evaluated in light of these economic effects as a set of interdependent factors in a global assessment, whereby a stronger degree in one dimension can offset weaker degrees in other dimensions.

We argue that this stringent effects-oriented approach is necessary for the Data Act to achieve its goals of strengthening Europe's digital economy by enabling seamless cloud environments and shaping a more open and innovative digital landscape.

Keywords: Interoperability, Data Act, Cloud, Switching, Digital

Recommended citation: Leonie Ott and Yifeng Dong, Clouds Connecting Europe: Interoperability in the EU Data Act, 16 (2025) JIPITEC 154 para 1.

A. Introduction

1 Interoperability is omnipresent - in our daily lives and in European law. We encounter interoperability when our phones work seamlessly with smart watches, cloud services, speakers and different apps. We can find interoperability provisions, for example, in the Data Act[1] (DA), the Digital Markets Act[2] (DMA) and the Data Governance Act[3] (DGA). This paper takes a look at the little-known, highly controversial and far-reaching interoperability obligations in the DA, where interoperability is described as the "ability of two or more data spaces

* Leonie Ott: LL.M. (Cambridge), doctoral researcher at the Chair of Prof. Dr. Thomas Ackermann, Ludwig-Maximilians-University Munich, leonie.ott@jura.uni-muenchen.de, Ludwigstraße 29, Raum 318, 80539 München. Yifeng Dong: M.Sc. (Computer Science), law student and student research assistant at the Chair of Prof. Dr. Thomas Ackermann, Ludwig-Maximilians-University Munich. This research project is funded by the Bavarian Research Institute for Digital Transformation (bidt), an institute of the Bavarian Academy of Sciences and Humanities.

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L 2023/2854, hereinafter "Data Act", see: Arts 33-36.

2 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L 265/1, hereinafter "Digital Markets Act", see: Arts 6(4), 6(7) and 7.

3 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 [2022] OJ L 152/1, see: Art 12.

or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions."[4] Simply put, products or services are interoperable if they "can work together".[5]

2 The legislative expansion of interoperability as a policy tool started when the European Commission (Commission) labelled the lack of interoperability as an obstacle to utilizing the full potential of information and communications technologies.[6] This trend is accompanied by high expectations. For instance, the so-called Draghi report on competitiveness recommends incentivising interoperability[7] and mandated interoperability was even called a "supertool".[8] *Prima facie*, promoting interoperability increases interconnectedness as well as competition and resonates with the values underlying the Single Market.[9]

3 However, the technical and economic realities ask for a more differentiated analysis. To begin with, compelled interoperability always includes trade-offs.[10] For instance, standardisation, which is one way to reach interoperability, can stifle innovation because it "freezes" technical progress.[11] Mandated interoperability has the potential to significantly affect product design, business strategies, economic power and market structures. It is a common misconception that interoperability provisions generally are "light touch"[12] regulation. Moreover, the effectiveness of an interoperability provision is contingent on the details, *inter alia*, the distribution of market power and product specifics. Since interoperability is not an end in itself[13] — it is employed to reach other goals — the rule hinges on intricate market mechanisms. Compelled interoperability can even backfire and achieve the opposite of the intended effects.[14] In sum, one can say that interoperability provisions have complex modes of action. A slight change in the details can have counterproductive repercussions.

4 Against this background, it is all the more surprising that the interoperability rules in the DA leave the reader clueless at many points, even regarding the most prominent questions.

5 The DA, which is part of the European strategy for data,[15] aims at fostering data access and use.[16] The cross-sectoral regulation will be applicable from 12 September 2025.[17] It contains substantive provisions, such as access rights, rules "targeted at tech regulation"[18] and enforcement provisions. The broadly discussed first part of the Act focuses on connected products and related services (frequently

4 Data Act, Art 2 No. 40.

5 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 13 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 6 December 2024.

6 Commission, 'A European strategy for data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2020) 66 final, 3.

7 Mario Draghi, *The future of European competitiveness* (Part B: In depth analysis and recommendations 2024) 302 <https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en> accessed 13 December 2024; similarly, the so-called Letta report suggests sector-specific interoperability measures that could foster the European Single Market: Enrico Letta, *Much More Than a Market* (2024) <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf> accessed 13 June 2025.

8 Fiona Scott Morton and others, 'Equitable Interoperability: The "Supertool" of Digital Platform Governance' (2023) 40 (3) Yale J. on Regul. 1013.

9 In addition to the economic perspective taken in this paper, there is also a political dimension of interoperability, for example, when EU databases are merged through interoperability, see: Didier Bigo, 'Interoperability: A political technology for the datafication of the field of EU internal security?' in Didier Bigo and others (eds), The Routledge Handbook of Critical European Studies (Routledge 2021).

10 Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' [2017] 8 JIPITEC 39, 41.

11 Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, 'Competition policy for the digital era' (Working Paper No. 6 2019) 59 <https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en> accessed 9 December 2024; Ilsa Godlovitch, Peter Kroon, 'Interoperability, switchability and portability – Implications for the Cloud' (WIK-Consult, Study for Microsoft 2022) 25 <https://www.wik.org/en/publications/publication/interoperability-switchability-and-portability-implications-for-the-cloud> accessed 6 December 2024.

12 Fiona Scott Morton and others, 'Equitable Interoperability: The "Supertool" of Digital Platform Governance' (2023) 40(3) Yale J on Regul 1013, 1017.

13 Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' [2017] 8 JIPITEC 39, 41.

14 Marc Bourreau, Jan Krämer, 'Interoperability in Digital Markets: Boon or Bane for Market Contestability?' (2022) <https://ssrn.com/abstract=4172255> accessed 6 December 2024.

15 Commission, 'A European strategy for data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2020) 66 final.

16 Data Act, recital 2.

17 Data Act, recital 117.

18 Moritz Hennemann and others, 'Data Act, An Introduction' (2024) 19.

referred to as "smart" products).[19] However, the DA additionally considers other areas of the data economy, for example *data processing services* (e.g. cloud services) and *data spaces*.

6 Focusing on interoperability mandates, two chapters of the DA are important. First, Chapter VI of the Act addresses switching between data processing services. Its contractual and technical rules are designed to make switching easier, and aim at creating a pro-competitive effect by decreasing the risk that customers are locked in because of switching costs.[20] Second, the DA has a frequently overlooked[21] Chapter VIII, entitled "Interoperability", which contains four, quite different rules (Arts 33-36)[22].

7 Article 33 targets participants of *data spaces* and lays down certain requirements on the data offerings shared within them. Surprisingly, there is no legal definition of a "data space" in the DA and the term can be understood in many different ways. Elucidating this term will be one of the problems this paper tries to solve.

8 Articles 34-35 DA then concern *data processing services*, with Article 34 declaring that many of the switching provisions from Chapter VI shall apply *mutatis mutandis* if multiple services are used in-parallel.[23] Again, this begs the question: What are data processing services? The term appears to mainly target cloud services, but does it go as far as encompassing, for example, everyday applications such as "Microsoft Word" if used in the cloud version? Considering that the DA provisions on interoperability concern, *inter alia*, the entire cloud computing industry in Europe, a cornerstone of innovative businesses and future growth, it becomes clear how relevant the provisions are. The way these obligations are interpreted will decide on whether the cloud industry faces burdensome innovation-stifling rules or customers benefit from a connected European cloud infrastructure.

9 Lastly, Article 36 sets out requirements for *smart contracts* that arrange data sharing. However, the requirements laid down in the provision relate to security and cyber-resilience. Although the provision belongs to the Interoperability Chapter, the supposed connection with interoperability is obscure.[24] Hence, we will not further cover this provision.

10 In sum, the conundrum of the interoperability obligations in the DA is that the legislator has left crucial parts blank, while much else is regulated in great detail. Its addressees – data spaces and data processing services – are not clearly defined, even as these terms are central to their application in practice.

11 In the following, we will suggest a systematic method based on an effects-oriented interdisciplinary perspective to answer these questions (part B) and apply our method to the interoperability provisions in the DA (part C-D).

B. Filling the "Gaps" with an Effects-Oriented Interpretation

12 Digital regulation is confronted with the problem that the subject matter is undergoing constant change, which can hinder legislative specificity. Yet, the uncertainty about vital concepts of the interoperability rules (e.g. the meaning of "data space" and "data processing service") poses a problem for the addressees of the frameworks, who have to identify what their precise duties are and if they are even captured by the legislation. Since the regulated issues are complex and technical, an "intuitive" legal understanding is not constructive. Furthermore, the abstract subject matter, consisting of terms like "data" and "data processing services", creates a myriad of interpretative options. Since the framework is cross-sectoral, the rules will also be applied to a wide range of contexts and situations, which further complicates their interpretation. Moreover, the DA pursues a multitude of goals, since it is part of an overarching policy strategy regarding data;[25] this too increases the complexity of interpretation.

13 In order to solve this challenge, we suggest a method based on a combination of the characteristics of

19 See for example: Federico Casolari, Carlotta Buttaboni, Luciano Floridi, 'The EU Data Act in context: a legal assessment ' [2023] International Journal of Law and Information Technology 399.

20 Antonio Manganelli, Daniel Schnurr, 'Competition and Regulation of Cloud Computing Services' (2024), Centre on Regulation in Europe, 79 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

21 Philippe Heinzke, 'Data Act: Neue Regeln für Cloud-Service-Provider' [2024] Betriebs-Berater 1291.

22 In the following, provisions cited without the name of the framework belong to the Data Act.

23 The omitted Article 35 allows for standardisation to foster the interoperability of data processing services (see part D).

24 Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 115.

25 Commission, 'A European strategy for data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2020) 66 final.

regulatory law and digital markets, which may lend itself to being used for the interpretation of digital regulation in general.

14 Due to the instrumental nature of regulatory law[26], which tries to steer behaviour in order to reach a certain outcome in the future, a special method of interpretation is required: The law should be applied by focusing on the practical implementation of the regulatory intention.[27] Put differently, the actual effects provoked by a rule are decisive for its interpretation. This approach goes further than a purposive interpretation, but is still in line with the interpretative approach of the Court of Justice of the European Union (CJEU), which states that "[...] in interpreting a provision of EU law, it is necessary to consider not only its wording, [...] but also the context in which the provision occurs and the objectives pursued by the rules of which it is part".[28]

15 The characteristics of regulatory law require that the aim underlying a provision is not just considered in its theoretical dimension. Instead, one examines whether the provision will actually fulfil the pursued goal. The key question is what the actual effects would be if the provision had a certain content.[29] Based on this, one decides if the rule should have that content or an alternative one.[30] Hence, it is important to identify the typical situation the rule applies to and the factual context of the provision.[31]

16 This *modus operandi* has two implications: first, we must clearly establish the legislative goals of the provisions, and second, we must understand the mechanism by which the legislator intends to reach its goals – in this case, interoperability. Those two aspects are set forth in the following as a preface because they pervade all of the specific interpretation questions.

I. The Goals of the Data Act in Light of the Digital Single Market

17 The prerequisite for any effects-based interpretation is a careful analysis of the legislative goals, because they are the yardstick for assessing the practical effectiveness of interpretative options. Here, we differentiate between the goals on the macro-level and the micro-level.[32] The macro-level goals are the objectives of the legal framework as a whole and its context within EU primary law, in particular the aims set out in Article 3 TEU. Then, zooming in to the micro-level, the goals of each specific provision must also be extracted. This differentiation intends to ensure that the technicalities of data-related provisions neither eclipse the broader constitutional background nor create incoherence within a framework. Furthermore, the separate analysis of the goals pursued by each provision is necessary, since the specific objective of rules, even within a chapter, can vary widely, as we will see in the following. We will start with the general objectives of the DA, which can be identified with a high degree of certainty, because they are spelled out in Article 1 of the Act, the initial recitals and the proposal for the Act. In contrast, the micro-level goals of each provision are much less clear.

18 Generally, the intention behind the DA is to foster access to and the use of data and thereby spur data-related innovation.[33] According to recital 1, "high-quality and interoperable data from different domains increase[s] competitiveness and innovation and ensure[s] sustainable economic growth." Referring to the non-rival nature of data, the recital goes on to highlight that "[t]he same data may be used and reused for a variety of purposes and to an unlimited degree, without any loss of quality or quantity."

19 Although more and more data is being produced,[34] the DA states that data is not sufficiently shared to reach an "optimal allocation of data for the benefit of society."[35] The proposal for the DA identified two root causes why the increasing volume of data does not unfold its full economic potential: The data is either unused, because of trust problems, diverging incentives or technological barriers,[36] or

26 As opposed to, say, private law in its function to organise private relationships.

27 Alexander Hellgardt, *Regulierung und Privatrecht* (Mohr Siebeck 2016) 648.

28 Case C-160/20 *Stichting Rookpreventie Jeugd and Others* [2022] ECLI:EU:C:2022:101, para 29; also: C-373/20 *Dyrektor Z. Oddziału Regionalnego Agencji Restrukturyzacji i Modernizacji Rolnictwa* [2021] EU:C:2021:850, para 36.

29 Alexander Hellgardt, *Regulierung und Privatrecht* (Mohr Siebeck 2016) 653.

30 Ibid 653.

31 Ibid 653.

32 Introducing the differentiation of goals on the macro-and micro-level: ibid 657.

33 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, 2.

34 Data Act, recital 1.

35 Data Act, recital 2.

36 In relation to these challenges, it has been argued that establishing a cross-sectoral data sharing infrastructure as well as a fifth European economic freedom (for data) would be beneficial to fulfil the Digital Single market, see: Andrés Chomczyk Penedo, 'The Regulation of Data Spaces under the EU Data Strategy: Towards the "Act-ification" of the Fifth European Freedom for Data?' (2024) 15 (1) EJLT <https://ejlt.org/index.php/ejlt/article/view/995/1088> accessed 13 June 2025. Yet, the DA is not that far-reaching.

is accumulated by a small number of large firms.[37] Hence, one could argue that the framework has two, closely interrelated, lines of attack: One is focused on creating the conditions to establish a market for currently unused data, and the other one is tackling competition-related phenomena, in order to promote competition on data-related markets.

20 The explicitly mentioned goals of the DA are in line with this two-pronged approach. The Regulation aims at overcoming the technical barriers to the development of the European data economy.[38] Additionally, the DA tries to foster a fairer distribution of value stemming from data.[39] It aims at re-balancing the benefits flowing from data usage by targeting "anomalous concentrations" with view to the rights of the affected parties.[40] Thus, the DA should not only be viewed as part of the European strategy for data, which envisions "a single European data space - a genuine single market for data, open to data from across the world - [...] boosting growth and creating value [...]"[41], but also in light of the competition policy efforts of the Commission, which frequently entail interoperability obligations.[42]

21 In the big picture of the Union's primary law, the DA provisions belong into the context of the single market goal. The DA is built on the legal basis of Article 114 TFEU, which empowers the Union to adopt harmonising laws aiming at the establishment and functioning of the single market. According to Article 26 TFEU, this describes "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured".

22 The proposal for the DA mentions that the completion of the internal market for data is the main intention.[43] It argues that the DA "will allow the Union to benefit from the scale of the internal market".[44] Its Recital 4 elaborates in this regard that, "in order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonised framework specifying who is entitled to use product data or related service data, under which conditions and on what basis." Regarding the need for EU-wide rules, the Commission has stated that that due to the "growing digitalisation of the economy and society, there is also a risk of Member States legislating data-related issues in an uncoordinated manner, which will lead to fragmentation in the internal market."[45]

23 One could question if legal fragmentation is the main problem in digital markets, since in practice, the most significant barriers to, say, a seamless multi-cloud environment are not national borders, but the borders between technical ecosystems.[46] The characteristics of cloud services foster the formation of integrated cloud ecosystems[47] and technical configurations as well as contractual conditions can enclose the costumers inside these so-called "walled gardens".[48] Arguably, the free flow of data and data-related services within the EU is mainly constrained by the borders of ecosystems run by global cloud computing companies, such as Amazon and Google, not by differing regulation.

24 Still, there is a strong nexus between the interoperability obligations in the DA and the single market goal. For example, the method that is chosen to foster interoperability regarding data spaces and data processing services is principally standardisation. Both main provisions, Article 33 and Article 34 (via Article 35), employ standard-setting to facilitate interoperability. This is neither self-evident nor the only option. For instance, in the interoperability provision regarding messaging services in the DMA (cf. Article 7 DMA) the disclosure of interfaces, a technical alternative to standardisation, is the default option for compliance.

37 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, 2.

38 Ibid 1; Data Act, recital 119.

39 Ibid 1; Data Act, recitals 2, 4.

40 Maria Luisa Chiarella and Manuela Borgese, 'Data Act: New Rules about Fair Access to and use of Data' (2024) 10 Athens Journal of Law 47, 53.

41 Commission, 'A European strategy for data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2020) 66 final, 4.

42 Juliane Mendelsohn, Philipp Richter in Björn Steinrötter (ed), *Europäische Plattformregulierung* (Nomos 2023) 547.

43 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, 7.

44 Ibid 7.

45 Commission, 'Impact Assessment Report Accompanying the document "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)"' (Commission Staff Working Document) SWD (2022) 34 final, 24.

46 Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 82 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024.

47 Antonio Manganelli and Daniel Schnurr, *Competition and Regulation of Cloud Computing Services* (Centre on Regulation in Europe 2024) 83 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

48 Primavera de Filippi, 'Cloud computing: analysing the trade-off between user comfort and autonomy' (2013) 2(2) Internet Policy Review, 4.

25 The establishment of EU-wide standards in the DA is a typical example of harmonisation. The standardisation stipulated in the DA is, on the one hand, the technical route to interoperability and, on the other hand, an approximation of national rules to create a single market for data. This shows how interrelated the concept of interoperability and the European single market are. Standardisation enables products to work together and markets to integrate.

26 In summary, the DA as a whole aims at creating a European market for data and data-related services and tries to promote competition on that market.[49] However, we will see later on that on the micro-level, each provision pursues distinct goals that strongly differ from each other. Reconciling these differences will be a key strategy in gleaning a workable interpretation of the provisions.

II. The Effects of Interoperability

27 The second implication of our suggested interpretative method is that the mechanism between a certain rule and its effects becomes particularly important. To that end, understanding policy tools such as interoperability becomes a prerequisite. The focus on effects means that extra-legal considerations play a significant role.

28 In theory, the concept of interoperability is simple. From a customer perspective, interoperability creates more choice and autonomy.[50] If different services or products can work together, they can be combined. Hence, interoperability facilitates the modularisation and product differentiation of products and services.[51] In general, companies have an incentive to offer interoperability and the level of interoperability demanded by the customers is fulfilled via the workings of the market.

29 Yet, the interoperability provisions in the DA demonstrate that the legislator considered the level of interoperability to be insufficient.[52] Since interoperability is an abstract property of systems and not an end in itself, this raises the question of why interoperability should be mandated at all – which effects can mandated interoperability have in general that are desirable? To begin with, one can differentiate between *public interest* effects of interoperability and *economic* effects of interoperability. In the former case, interoperability furthers general public interest purposes such as improved connectivity for communication purposes[53] or digital resilience through the usage of several services in concert.

30 More importantly though, compelled interoperability can have positive economic effects, which are dependent on the type of interoperability and the market setting. For example, mandated interoperability can foster competition and innovation, especially in platform ecosystems.[54] If customers can "mix-and-match" services from different providers and they still work together, then competition does not merely happen between large ecosystems, but smaller providers also have a chance of gaining customers with their specific product. Thus, interoperability can create efficiencies through competition and innovation by complementors.[55]

31 Within the wide range of possible economic effects, *market-power related* effects can be further distinguished from other economic effects. Interoperability provisions are considered a tool to *counteract market concentration*,[56] especially in markets with strong network effects, where products or services gain attractivity through the number of users.[57] Interoperability can reduce the market power conferred by network effects.[57a] For example, the number of users is highly important for a messenger service and compelled interoperability allows the users of smaller services to connect to the large user basis of other providers. Additionally, mandated interoperability can ameliorate lock-in effects, reduce entry barriers and limit the cost advantages of economies of scope and scale. If competition related issues of that kind are prevalent in the market, interoperability can be mandated to counteract concentration tendencies.

49 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, 7.

50 John Palfrey, Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books 2012) 57.

51 Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' [2017] 8 JIPITEC 39, 42.

52 See also Data Act, recital 3.

53 Ibid 48.

54 Raegan MacDonald, Owen Benett and Udbhav Tiwari, 'Digital Markets Act (DMA): July 2021 position paper on the European Commission's legislative proposal for an EU Digital Markets Act' 9–11 <https://blog.mozilla.org/netpolicy/files/2021/07/FINAL_DMA-Position-Paper.docx_.pdf> accessed 1 April 2025.

55 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 26 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 1 April 2025.

56 Fiona Scott Morton and others, 'Equitable Interoperability: The "Supertool" of Digital Platform Governance' (2023) 40 (3) Yale J. on Regul. 1013, 1015.

57 Ibid 1016-1019.

57a Ibid 1019.

32 However, compelled interoperability can also create adverse economic effects. For instance, requesting interoperability can reduce the incentive to multi-home (i.e., use several services for the same purpose), which has the potential to strengthen large players. For instance, if WhatsApp were interoperable with every other messenger, users might lose the incentive to use other apps. Another example of negative effects would be inefficiencies due to vertical separation.[58]

33 These trade-offs raise the question of when it is justified – from a policy perspective – to increase the level of interoperability above the one defined by the market mechanism. In case public interest consequences are the rationale, this is a purely political question. Regarding economic effects, one could argue that interoperability should only be mandated in case a *market failure*[59] can be identified.

34 For instance, a market failure is present if a dominant firm unilaterally decides about standards and the level of interoperability.[60] An example of a market failure situation was seen in the competition law case of Microsoft, decided by the General Court in 2007, in which a workgroup server producer complained that Microsoft did not disclose the interfaces of its operating system, although Microsoft was dominant in this market and without being interoperable with the de facto standard one did not have a realistic chance on the market.[61] In cases like this, interoperability mandates can be used as a tool to correct market failures.

35 As we will see later on, the interoperability provisions in the DA are less stringent regarding their economic justification. Although there is the possibility of market failure in the cloud service market,[62] the obligations target all providers, regardless of market power. In the case of data spaces, it is not even clear which specific economic problem the obligation is trying to tackle through interoperability. This is in line with a characteristic of the DA to "no longer [limit] itself to addressing well-defined market failures (like market power). Rather, it follows a market-shaping approach: it [...] redefines the legal infrastructure based on which markets evolve."[63] Since increasing the level of interoperability is not necessarily economically advantageous, however, this approach is questionable.

36 This categorization of interoperability effects can reveal tenuous economic justifications and allows for a systematic discussion and interpretation of the specific interoperability rules.[64]

C. Article 33: Interoperability in Data Spaces

37 Having developed the required interpretation method and analysis of the DA and interoperability in general, we can now apply these insights to solve the specific open questions in each provision that could hinder their effective application in practice.

38 To begin with, Article 33 addresses *participants of data spaces*. They are subject to a long catalogue of obligations in Article 33(1), which mainly boils down to adequately documenting the data or data services they offer. For instance, participants in data spaces must specify the dataset content, the data quality and the technical means to access the data. In addition, the means to enable interoperability with automated data sharing agreements, such as smart contracts, must be provided "where applicable".

39 The provision refers to this long catalogue of obligations as "essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces". The term "common European data spaces", which refers to a particular Commission initiative, is not to be confused with *data spaces* in general.[65] In

58 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 26 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 1 April 2025.

59 We understand market failure in the economic sense. Recognized instances of market failure are: externalities, imperfect information, market power and adjustment deficiencies, see: Michael Fritsch, 'Marktversagen und Wirtschaftspolitik' (2011 Vahlen) 72-73.

60 Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' [2017] 8 JIPITEC 39, 43.

61 Case T-201/04 *Microsoft v Comission* [2007] ECR II-3619.

62 Antonio Manganelli, Daniel Schnurr, 'Competition and Regulation of Cloud Computing Services' (2024), Centre on Regulation in Europe, 57, 80, 85 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

63 Heike Schweitzer and Axel Metzger, 'Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?' [2023] GRUR International 337, 338.

64 See: part C and D.

65 Common European data spaces, defined in Article 33 DA as "purpose- or sector-specific or cross-sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives", are specific projects coordinated by the Commission itself, such as the "Common European health data space" and the "Common European agriculture data space", see Commission, 'Commission Staff Working Document on Common European Data Spaces', SWD(2024)

sum, Article 33 (1) stipulates that the participants of data spaces are obliged to fulfil certain essential requirements, which are mainly obligations to describe data, in order to enable interoperability (of data, common European data spaces etc.).

40 Since these "essential requirements" are only described in broad terms, the provision provides for the development of standards to concretise the obligations and facilitate compliance. Article 33[66] lays down the procedure for arriving at standards. The Commission must request a European standardisation organisation to develop a *harmonised standard*. A harmonised standard is "a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation" (Article 2(1)(c) Regulation 1025/2012 on standardisation). If this fails, the Commission itself can take action and adopt *common specifications* instead. Article 2(42) of the DA defines common specifications as "a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation". In summary, the provision gives preference to standards developed by the standardisation organisations, but it includes a fall-back option fulfilling the same purpose.[67]

41 If participants of data spaces meet the harmonised standards or the common specifications (depending on what has been established), then conformity with the requirements of paragraph 1 is presumed.[68] As is typical in European standard-setting, the standards are not directly binding, but since they create legal certainty for the addressees through the presumption of conformity, they are expected to be very influential nonetheless.

42 As we have noted in the introduction, a crucial piece of the puzzle is missing here: Who is affected by these obligations? The summary of the provision has shown that it all boils down to the meaning of the term "data space", because the addressees of the rule are the participants of data spaces. The DA gives no statutory definition of this term. Other laws, such as Regulation (EU) 2021/694 establishing the Digital Europe Programme, which also use the term "data space", do not define it either. Since the DA is a Regulation - meaning that it is directly applicable according to Article 288 TFEU - this is surprising. One can only speculate as to why the legislator decided to omit such a central definition. Regardless of whether the term was left deliberately open to anticipate future developments, or because it was seen as sufficiently clear on its own, the legislator has, in any case, left it to the courts to define the term. Despite the lack of an internal definition, it is clear that the term must be given an autonomous and uniform interpretation in EU law.[69] In consequence, national courts will need to refer the question to the CJEU.

43 Since the wording is abstract, various interpretative options are possible. Hence, it is not surprising that what has been written about data spaces varies widely, from only encompassing common European data spaces[70], which again is just a particular Commission initiative[71], to describing "every open offering of data or data-based services on the market".[72]

I. Objectives of the Provision

44 Here, the importance of understanding the provisions' goals and intended effects becomes acutely relevant. This is true both for the question of what the goals are, but also what they cannot be. In contrast with many other interoperability mandates, the point of this specific provision cannot be to *remedy market concentration*. This is clear from the fact that it addresses persons who have *already* decided to share data. Contrast this with the countless provisions in the DA and beyond aiming to encourage or force the sharing of data in the first place. It is clear that Article 33 does not deal

21 final, 3. The term "Common European data *space*" (singular form) is also an unrelated term, and used by the Commission to describe its vision of a common market for data in general, see Commission, 'Towards a common European data space' (Communication) COM(2018) 232 final; Commission, 'A European strategy for data' (Communication) COM(2020) 66 final, 6.

66 Data Act, Art 33 (4-7), (9).

67 Data Act, recital 103.

68 Data Act, Art 33 (4) and (8).

69 The *Infopaq* case-law (Case-5/08 *Infopaq* [2009] ECLI:EU:C:2009:495, para 27) makes it clear that terms in EU law are generally to be interpreted autonomously and uniformly. There Is also no indication to suggest otherwise in this case, since the DA does not point to any national laws and the term "data space" does not seem to be based on the legal traditions of any Member State. See also Karl Riesenhuber in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2021) 252-253.

70 Although ambiguous, the example given indicates this understanding: Kristina Schreiber, Patrick Pommerening, Philipp Schoel, Der neue Data Act (2nd edn, Nomos 2024) 112. The narrow understanding might be interrelated with their assumption that the operators of data spaces are the addressees of the provision, as it was in the proposal.

71 Commission, 'Commission Staff Working Document on Common European Data Spaces', SWD(2024) 21 final, 3.

72 Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 113.

primarily with "reluctant parties" – the quality of forcibly shared data is already regulated specifically in Article 13 DA, and the quality of contractually shared data falls under the scope of the Digital Products Directive.[73] In contrast, Article 33 deals with the quality of a voluntary data *offering* itself.

45 We have seen that the overarching goal of the DA is to promote data sharing and to build a well-functioning single market for data.[74] What motive then, could justify placing obligations on the "good guys" who have already decided to share data by their own volition? The objective can only be the anticipated benefit of the circulation of "more interoperable" (i.e., better documented) data as such. For one, better documented data offerings increase market transparency. Potential users of the data can better compare offerings and make the right choice about which one to use. The text of the provision in Article 33(1)(a) speaks explicitly about letting recipients "find, access, and use the data". Here, the legislator is aiming to achieve an *economic* objective by aiming to make the market work more efficiently. In the same vein, the requirement to ensure compatibility with automated data sharing agreements is also meant to increase efficiency by decreasing transaction costs.

46 Apart from economic justifications, another objective may be the limitation of risks from bad data – Article 33(1)(a) also mandates the disclosure of "data collection methodology, data quality and uncertainty". The proliferation of poorly documented data has been cited as a source of safety concerns regarding the automated systems trained on that data.[75] Conversely, increasing documentation can also increase trust (cf rec. 102 DA), promoting data sharing. In this respect, the provisions are pursuing *public interest objectives* such as product safety.[76]

47 Whether these objectives are sufficient to justify the obligation, is a serious question. When contrasting this provision with other interoperability mandates, it is apparent that the justification for its existence is much more tenuous. With respect to the economic objectives, it is neither justified by a specific market failure nor by the perceived need to pre-emptively counteract evolving market concentration. Moreover, overly burdensome obligations risk discouraging data sharing, perhaps the most undesirable outcome considering the overarching goals of the DA.[77]

48 Thus, the principle of practical effectiveness requires a restrictive interpretation whilst allowing the salient public interest justifications to adequately manifest themselves.

II. The Term "Data Space"

49 It has been suggested in the literature that the term "data space" should cover "every open offering of data or data-based services on the market".[78] In our view, this interpretation is too wide. For one, the Commission's proposal originally only targeted "operators" of data spaces.[79] This strongly suggests that a data space, by virtue of having an operator, needs to have a certain infrastructural element and is not just a stand-in for the market for data in general. During the committee stage in Parliament, the provision was widened to address any "participant" in a data spaces, but this in no way suggests that the original conception of the data space as such has changed.

50 Therefore, a data space within the meaning of Article 33 should be a *platform* whose purpose is to allow users to share data with a large number of other users. These platforms already exist today; an example would be *huggingface.co*, currently the most popular platform for the AI and machine learning industry. It is likely that the Commission intended to dedicate Article 33 to this emerging phenomenon.

51 This is also in line with the effects-oriented approach outlined above. Keeping in mind the public interest objectives of the provision, data sharing on a platform differs from other forms of public offerings in three major ways. First, data offerings on a platform can quickly reach a wider audience. In addition, due to the ease of use, users are more likely to incorporate a data offering into their own project without much afterthought. In other words, the threshold for widespread sharing is reduced. This both increases the risk that badly documented data poses and makes the added value of any single documentation higher. Second, data spaces imply a certain degree of automation of data sharing. This is highlighted by the explicit reference to automated

73 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136.

74 cf. part B.I.

75 Dario Amodei and others, 'Concrete problems in AI safety' (2016) <https://arxiv.org/abs/1606.06565>.

76 Cf. Article 169(1) TFEU.

77 cf. part B.I.

78 Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 113, our translation.

79 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) [2022] COM/2022/68 final, Art 28.

data sharing agreements in Article 33(1)(d), which are also a means of automation. Whereas even public offerings of data outside of a platform usually involve some kind of dedicated customer contact, where a prospective customer could ask questions about the product, this is not (always) the case in data spaces. Lastly, the restrictive interpretation of data spaces as platform related ensures that the provision only targets dedicated data sharing, and not data shared as part of some other product. This reading therefore helps to reduce unintended burdens on market participants, whilst focusing on an area where a mandate may have the biggest cumulative benefit.

D. Article 34 and 35: Interoperability of Data Processing Services

52 By far the most far-reaching provisions of the interoperability chapter in the DA are Articles 34 and 35. They deal with the interoperability of "data processing services", which – inter alia – include *cloud services*.[80] As already mentioned, the definition of the term "data processing services" is cryptic. After setting out the specific goals of Articles 34 and 35 in the following paragraphs (see part D.I), we will decipher the term "data processing service" (see part D.II) along with other ambiguities in the provisions (D.III-IV).

53 It has long been known that the cloud market tends to suffer from lock-in effects, a propensity that the EU legislator also referenced in the context of the Data Act.[81] In general, customers are locked in when they decide to pursue a course of action, but they cannot change the course towards a preferable alternative later on, because the switching costs tie them to the inferior original choice.[82] In the cloud service market, lock-in effects result mainly from financial and technical barriers to switching.[83] Since a customer of a cloud service loses physical control over the data, customers can enter into a situation in which they generate data without being able to easily transfer it to other providers, which leads to data-induced switching costs.[84] This, along with other characteristics of cloud services such as high customizability, creates a dependency of businesses on the cloud service. For instance, in 2020, 59% of the businesses using cloud computing services said that they were "highly dependent".[85] In this context, interoperability can ameliorate lock-in effects by reducing technical barriers between services. Mandated interoperability gives customers the option to build a cloud system comprised of cloud services from different providers (multi-cloud approach).[86] Customers can migrate one cloud service to a different provider whilst keeping the rest of the services where they are. Due to interoperability, the whole cloud ensemble then still works together. This decreases the dependence of customers from specific cloud providers and increases competition.

54 To this end, the DA first includes a series of rules aiming to facilitate *switching* between providers in Chapter VI. Chapter VIII then complements this regime by also targeting the in-parallel use of multiple services, i.e. interoperability.

55 Article 34(1) lays down that certain provisions from Chapter VI about *switching* between data processing services "also apply *mutatis mutandis* to providers of data processing services to facilitate interoperability for the purposes of in-parallel use of data processing services." In layman's terms, the Data Act, on the one

80 Admittedly, the understanding presented above that Article 33 on data spaces and Articles 34 and 35 on data processing services are discrete obligations with diverging application scopes is contested due to the nebulous systematic structure of the chapter. It has been proposed to consider Article 33 the general rule that is then specified by Articles 34 and 35. It was argued that Article 33 mentions the term "data service", which could theoretically be an umbrella term encompassing data processing services, see Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 113. Yet, this reasoning is not convincing. In Article 1 (3) the Data Act clearly distinguishes between the providers of data processing services and the participants of data spaces when describing who the Regulation applies to. Moreover, no indication of such a structure can be found in the legislative material. Above all, the consequences of the suggested hierarchy of provisions militate against it. An obligation for cloud service providers or users to describe shared data could not be justified.

81 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, 14.

82 Edward F Sherry, 'Lock-In Effects' in Mie Augier and David J Teece (eds), *The Palgrave Encyclopedia of Strategic Management* (Palgrave Macmillan UK 2016).

83 Antonio Manganelli, Daniel Schnurr, 'Competition and Regulation of Cloud Computing Services' (2024), Centre on Regulation in Europe, 79 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

84 Ibid 70.

85 Commission, 'Impact Assessment Report Accompanying the document "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)"' (Commission Staff Working Document) SWD (2022) 34 final, 14ff.

86 Antonio Manganelli, Daniel Schnurr, 'Competition and Regulation of Cloud Computing Services' (2024), Centre on Regulation in Europe, 97 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

hand, aims at facilitating the transfer of your photos in the cloud storage to a different cloud storage (switching through portability). By declaring these rules on switching applicable to the in-parallel use of data processing services, the DA aims at making your photo storage and another photo storage or a different cloud service, for example for editing your photos, work together (interoperability for parallel use). The underlying idea behind Article 34 is that different data processing services, such as cloud services, could be used together — if interoperability is enabled— to create a multifaceted but seamless cloud environment.[87]

56 The most important cross reference in Article 34 to the Chapter on switching is the one to Article 30 (2-5), because this leads to the *obligation to offer open interfaces* and *comply with open interoperability specifications or harmonised standards*, once they are established. Due to this cross reference, the scope of which is ambiguous (see part D.III), it is necessary to look at Article 30 first.

57 The referenced provision is captioned with "Technical aspects of switching". According to Article 30, data processing services must offer open interfaces (Art 30 (2)) and comply with certain technical specifications or standards (Art 30 (3)). Whether these obligations shall only effectuate interoperability between services of the same service type or also between complementary cloud services is contested (see part D.IV).

58 More specifically, Article 30 (2) requires data processing services to make open interfaces available for their customers, as well as the destination provider a customer wants to switch to. Open interfaces act as bridges for data flow. They include Application Programming Interfaces (APIs), which are "sets of protocols defining "how software components communicate with one another."[88] Theoretically, this would be a sufficient technical route to interoperability, but the following paragraph goes further.

59 Article 30 (3) states that the data processing services "shall ensure compatibility with *common specifications* based on open interoperability specifications or harmonised standards for interoperability". Interestingly, the wording of the provision requires only "compatibility" and not "conformity" [89] or "compliance"[90] suggesting that there might be some flexibility in applying the standard. Yet, the purpose of the obligation and the legislative material suggest otherwise. In practice, it is difficult to imagine any case in which a service is fully compatible without conforming with the standard.[91] Moreover, recital 100 mentions that the Commission can mandate the usage of those specifications and standards through a reference to them. Therefore, Article 30(3) is considered to make the aforementioned specifications and standards binding.[92]

60 Systematically confusingly, the requirements for these standards and specifications are laid down in Article 35. These are relatively broad. For example, it is stipulated that "open interoperability specifications and harmonised standards for the interoperability of data processing services shall achieve, where technically feasible, interoperability between different data processing services that cover the same service type."

61 In sum, the short provision of Article 34 prescribing interoperability for the purpose of in-parallel use of data processing services might seem mild as a dove at first glance and the term "standards" has connotations of voluntariness. However, the cross reference to the rules on switching creates hard and far-reaching obligations for cloud providers to enable interoperability. Article 34 obligates data processing services to, on the one hand, make open interfaces available (via Art 30 (2)), and on the other hand, fulfil technical specifications or standards (via Art 30 (3)). The requirements for the latter and the procedure to draft them are set out in Article 35. Evidently, the precise content of the obligation hinges upon these technical norms that are still to be produced. Until then, the providers of data processing services must at least "export all exportable data in a structured, commonly used and machine-readable format"[93] upon request, which however only leads to data portability.

62 Finally, it should be mentioned that Article

87 Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 83 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024.

88 Oscar Borgogno, Giuseppe Colangelo, 'Data sharing and interoperability: Fostering innovation and competition through APIs' (2019) 35(5) Computer Law & Security Review 1, 3.

89 cf. Art 33 (3): "conformity with essential requirements".

90 This wording is often used in the context of standards: Regulation 1025/2012 on standardisation, recital 1.

91 This can be illustrated with an analogy to the USB-C-standard for chargers: How should a product be compatible with USB-C without adhering to the standard? Partial compatibility at the most can be reached if the standard is not implemented fully. For example, a charger cable that is not implementing the full standard may only work with certain devices or have restricted functionalities.

92 cf. Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 219.

93 Data Act, Art 30 (3).

30 contains a restricting paragraph, whereby "Providers of data processing services shall not be required to develop new technologies or services, or disclose or transfer digital assets that are protected by intellectual property rights or that constitute a trade secret, to a customer or to a different provider of data processing services or compromise the customer's or provider's security and integrity of service."[94] This defence will have a strong bearing on the effectiveness of the rules[95] considering, for example, that APIs that have been kept secret so far will often qualify as a trade secret, pursuant to the broad definition of Article 2 (1) of the Trade Secrets Directive.[96] Yet, it has been argued that at least one interface must be provided to accord the provision some practical effectiveness.[97] In general, the relationship between the DA and IP law is an intricate issue[98] that, however, goes beyond the scope of this Article.

I. Objectives of the Provision

63 Against the backdrop of the overall goals of the DA, the Commission argues in its Impact Assessment that data processing infrastructure is a prerequisite for data sharing.[99] The Commission further elaborates: "Not having a competitive market for cloud and edge services in place is an additional obstacle in the value creation on the basis of data for many actors. Therefore, access to competitive cloud and edge services needs to be ensured for stakeholders in the data economy."[100] This already indicates that, in contrast to Article 33, Articles 34-35 are provisions whose primary purpose is to foster competition, with a view to the risk of market concentration.

64 As mentioned above, the cloud interoperability provisions are intended to tackle the problem of lock-in effects, which was referenced by the Commission in its proposal as well as in the recitals.[101] According to recital 90, reducing lock-in effects is intended to increase innovation and promote competition.

65 Alongside lock-in effects, the second major competition-related characteristic of the cloud computing market are economies of scope and scale.[102] These scope and scale advantages drive concentration and reduce the intensity of competition, because it means that integrated and large firms have a cost advantage in producing their service.[103] Whilst the offering of a whole ecosystem of connected cloud services can thereby create efficiencies, the tendency towards product bundles could also erect entry barriers to specific service markets,[104] because firms without the ability to offer a wide range of service could be unable to compete. Interoperability as mandated by Article 34 can counteract these tendencies by allowing specialised firms to offer a single cloud service without the need to provide a whole ecosystem encompassing less efficient services.

66 In this vein, recital 78 states that the provisions on switching and interoperability of cloud services are "a key condition for a more competitive market with lower entry barriers for new providers of data processing services, and for ensuring further resilience for the users of this service". Interestingly, the last clause of this recital also demonstrates that promoting competition is not the only goal. The proposal for the Data Act by the Commission states that Chapter VIII is designed to foster a "seamless multi-vendor cloud environment"[105]. These multi-cloud environments of complementary services do

94 Data Act, Art 30 (6). Although Art 34 DA does not reference Art 30 (6) DA, the wording suggests that only the "requirements" are explicitly referenced, and the limitations implicitly apply. Since mandated interoperability is generally even more intrusive for the addressed service providers it would be inconsistent to only have limitations for the switching obligation.

95 Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 219.

96 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157.

97 Ibid 219.

98 cf. Matthias Leistner, Lucie Antoine, 'IP Law and Policy for the Data Economy in the EU' (2023) 17 (1) Economics E-Journal.

99 Commission, 'Impact Assessment Report Accompanying the document "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)"' (Commission Staff Working Document) SWD (2022) 34 final, 13-15.

100 Commission, 'Impact Assessment Report Accompanying the document "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)"' (Commission Staff Working Document) SWD (2022) 34 final, 14.

101 Data Act, recitals 78 and 90.

102 Antonio Manganelli, Daniel Schnurr, 'Competition and Regulation of Cloud Computing Services' (2024), Centre on Regulation in Europe, 80 <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> accessed 1 April 2025.

103 Ibid.

104 Ibid.

105 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, 16. In a similar vein, recital 99 stresses the importance of multi-cloud strategies, which require interoperability.

not only have the potential to increase competition, but also to improve cyber-resilience, because the customer can deploy several cloud services in parallel.[106]

67 In summary, the objectives of these provisions are mainly focused on economic effects and try to prevent a potential market failure resulting from lock-in effects and economies of scale and scope, aiming to prevent further market concentration. Secondarily, they pursue public interest goals like higher cyber-resilience.

II. The Term "Data Processing Services"

68 The terminological fulcrum in Articles 34 and 35 is the term "data processing services" itself. These are defined in Article 2(8) as "a digital service that is provided to a customer and that enables *ubiquitous* and on-demand network access to a shared pool of *configurable, scalable* and *elastic* computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction".

69 Recital 80 gives definitions for each of the technical terms used in this definition. Computing resources include "networks, servers or other virtual or physical infrastructure", but also "software, [...], applications and services". Computing resources are "scalable" if they are flexibly allocated by the provider of the data processing service to handle fluctuations in demand; they are "elastic" if they are provisioned and released in order to rapidly increase or decrease resources available depending on workload. Finally, resources are "ubiquitous" if they can be accessed through the network using a wide range of end devices.

70 Despite these descriptions, it remains extremely unclear what types of services actually qualify as "data processing services".[107] It is apparent from the recitals, the legislative documents, and the literature that the intended targets of this definition are "cloud services".[108] Indeed, the language of the definition is extremely similar to the definition of a "cloud computing service" in Article 6(30) of the NIS-2-Directive[109], which is also used by the Digital Markets Act (see Art 2(13) DMA). However, this does not do anything to alleviate the uncertainty.

71 From a practical perspective, it might seem obvious that services which are part of the cloud *infrastructure* such as those typically provided by Amazon Web Services, Google Cloud, or Microsoft Azure should generally be covered.[110] But do products that are merely *hosted* on the cloud, like consumer products such as Microsoft Office 365[111] or Google Docs, or

106 Data Act, recital 99.

107 Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022) paras 169ff.; Philippe Heinzke, 'Data Act: Neue Regeln für Cloud-Service-Provider' [2024] Betriebs-Berater 1291, 1292.

108 Patrick Pommerening and Michèle Nickel, 'Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act' (2024) Recht Digital 289, paras 8-9; Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 114; Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023), 79 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024; Sean F Ennis and Ben Evans, 'Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence' (2024) <https://ssrn.com/abstract=4395183> accessed 6 December 2024; David Bomhard, 'Auswirkungen des Data Act auf die Geschäftsmodelle von Cloud-Anbietern' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 109; Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022) paras 164ff.; Hans Hermann Schild in Stefan Brink, Heinrich Amadeus Wolff, and Antje von Ungern-Sternberg (eds) BeckOK Datenschutzrecht (49th edn, CH Beck 2024), Data Act Art 2 para 58.

109 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80; Sean F Ennis and Ben Evans, 'Cloud Portability and Interoperability under the EU Data Act: Dynamism Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136 versus Equivalence' (2024), 2 <https://ssrn.com/abstract=4395183> accessed 6 December 2024; Patrick Pommerening and Michèle Nickel, 'Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act' (2024) Recht Digital 289, 291.

110 Patrick Pommerening and Michèle Nickel, 'Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act' (2024) Recht Digital 289 para 7.

111 As suggested by Martin Schallbruch, 'Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste' [2016] Computer und Recht 663, 666 for the NIS-2-Directive.

even simple websites, also qualify, and if not, how does one reliably differentiate between services which *are* the cloud and those which are merely hosted on it?

72 This question is more difficult than it appears, and indeed there is no consensus on it in the literature. In fact, most of the literature on the equivalent definition in the DMA and NIS-2-Directive seem to suggest that any service hosted on the cloud should be covered.[112] And constructively, the definition in the Data Act appears to only widen the DMA cloud computing term in that it also includes edge computing (which refers to when computing resources are highly geographically distributed across many devices).[113] However, unlike the DMA, which contains further stringent requirements before mandates apply, the DA contains far-reaching mandates for *all*[114] data processing services. This means that an overly wide definition could have a much larger negative impact. Therefore, in he context of the Data Act, other authors have questioned whether a contractual view should be taken instead of the technical view[115], or whether "configurability"[116] could be a tool to narrow down he definition.

73 Equipped with the methodological tools described above, we can now approach this conundrum in a more coherent way.

1. Phenomenological Background of the Provisions

74 As discussed above[117], an effects-oriented approach requires us to closely understand the mechanism of action of the policy tool on a particular market. Thus, the properties of the actual cloud market on which effects are expected must be considered. In the context of understanding the term "data processing services", it is therefore crucial to understand the current landscape of services being offered on the market. From this, we can then draw conclusions on the abstract interpretation of the provisions.

75 The original birth of the modern cloud computing market was the 2006 launch of Amazon's Simple Storage Service (S3), which allowed customers to store large objects on Amazon's infrastructure.[118] Users did not need to provision a fixed amount of storage in advance, rather, they simply uploaded and downloaded their stored files as needed and were charged based on the resources actually used – originally $0.15 per GB of storage per month and $0.20 per GB of data transferred.[119]

76 A few months later in August 2006, AWS released their second bombshell service, the Elastic Compute Cloud (EC2).[120] With EC2, customers could provision virtual computers that were hosted on Amazon's infrastructure.[121] These virtual machines could be provisioned and released at any time, and users were charged $0.10 for every hour the machine was "on".[122] In the blog post[123] announcing the product, Amazon "Evangelist" Jeff Barr listed a few use cases for the new service: instead of purchasing enough computer hardware to accommodate a customer's peak usage, they would only need to pay for the computational resources actually used. For example, a customer might want to "experiment with some radical new parallel processing algorithm for a week or two"[124], or do their "end-of-month accounting"[125]. With EC2, they could flexibly provision the computational resources they needed, only when they needed it. Crucially, he addressed another group of users – developers of web applications who needed to scale up processing power based on demand.[126] With traditional on-premises hosting, he wrote, "your

112 Philipp Bongartz and Alexander Kirk in Rupprecht Podszun (ed), *Digital Markets Act* (Nomos 2023), Art 2 para 72; Martin Schallbruch, 'Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste' [2016] Computer und Recht 663, 666; Christian Heinze and Tom Kettler in Björn Steinrötter (ed), *Europäische Plattformregulierung* (Nomos 2023) 325 with further references; Carsten König in Björn Steinrötter (ed), *Europäische Plattformregulierung* (Nomos 2023) 382.

113 Gregor Lienemann in Moritz Hennemann and others (eds), Data Act, An Introduction (Nomos 2024) 181.

114 Except for minor exceptions in Art 31.

115 Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 114.

116 Robert Weinhold and Christian Schröder, 'Data Act – (R) Evolution oder vergebene Chance?' [2024] Zeitschrift für Datenschutz 306, 307.

117 Supra, part B.

118 Amazon.com Inc, 'Amazon Web Services Launches' (14 March 2006) <https://press.aboutamazon.com/2006/3/amazon-web-services-launches> accessed 6 December 2024.

119 Ibid.

120 Jeff Barr, 'Amazon EC2 Beta' (25 August 2006) <https://aws.amazon.com/blogs/aws/amazon_ec2_beta/> accessed 6 December 2024.

121 Ibid.

122 Nik Cubrilovic, 'Almost Exclusive: Amazon Readies Utility Computing Service' TechCrunch (24 August 2006) <https://techcrunch.com/2006/08/24/exclusive-amazon-readies-utility-computing-service/> accessed 6 December 2024.

123 Jeff Barr, 'Amazon EC2 Beta' (25 August 2006) <https://aws.amazon.com/blogs/aws/amazon_ec2_beta/> accessed 6 December 2024.

124 Ibid.

125 Ibid.

126 Ibid.

chance at fame and fortune may very well pass, as thousands of would-be users are greeted with a 'site too busy' message."[127]

77 This message resonated with developers – today, countless websites, platforms, and web apps are hosted on an external cloud infrastructure. For example, AWS' website lists Salesforce as a "case study".[128] The firm collects and processes large amounts of marketing data on behalf of its customers in order to provide them with strategic insights on how their business is performing, and this is done using a variety of AWS products, including EC2. Other listed customers include Netflix, Snapchat, and Expedia.[129] In theory (and in practice), any service ranging from simple websites, games, social networks, and video sharing platforms, to search engines could be (and already are) hosted "in the cloud".

78 At the same time, AWS itself also began to diversify its portfolio of services, developing more and more dedicated services that not only provided general-purpose infrastructure, but concrete applications. For example, AWS Relational Database Service and AWS DynamoDB are so-called "database-as-a-service" products, which do not only provide storage, but also database software that manages and maintains a certain database structure and allows efficient filtering and retrieval of datapoints.[130] The user only sees and interacts with a single database software instance, but this is managed across a distributed infrastructure behind the scenes.[131] Recently, AWS products have become more and more application-specific, even including marketing tools[132] and software development tools.[133]

79 It is against this phenomenological backdrop that the European legislators created the Data Act's switching and interoperability provisions based on the term "data processing services". Armed with this knowledge, we can now better elucidate what "data processing services" should mean in general, by comparing the practical effectiveness of different interpretive options on this industry (cf. B.II).

2. Even Application-Specific Services Are Covered

80 To begin with, it is quite evident that the intention of the European legislators was to capture a large majority of the AWS services we mentioned, even those which are not infrastructural, but consumer- or application-oriented. Recital 81 clearly states that data processing services can be both "Infrastructure-as-Service", "Platform-as-a-Service", and "Software-as-a-Service" products, and should cover "a very broad range of different purposes, functionalities and technical set-ups". Article 30 also differentiates between services "limited to infrastructural elements" and those which also provide access to "the operating services, *software and applications* that are stored, otherwise processed, or *deployed on* those infrastructural elements". The principle of practical effectiveness implies that both of these categories must have some reasonable scope of application. For the latter category, legislators were clearly envisioning the applicability to at least some of the more application-specific AWS services. Therefore, whether a service is general-purpose or application-specific is clearly not a valid criterion. Even a consumer-oriented service that only has one function is not precluded from being a data processing service.

3. Shared Pool of Computing Resources

81 This is made further clear by the fact that the term "computing resources" as defined in Recital 80 also already encompasses "software, including software development tools, [...] applications and services" and not just physical hardware.

82 In the case of S3 and EC2-like services, the shared pool of computing resources is simply the physical infrastructure in Amazon's datacentres, as well as the software needed to allow customer access to them. For database-as-a-service products, the database software itself is also a shared computing resource. For the inclusion of software as a possible shared computing resource to make sense, one must imagine that software and applications are already "shared" when any software running on the provider's infrastructure handles inputs from multiple users. Source code itself is a non-rivalrous

127 Ibid.

128 Amazon Web Services, 'AWS Partner Story: Salesforce DMP' <https://aws.amazon.com/partners/success/salesforce-case-study/> accessed 6 December 2024.

129 Amazon Web Services, 'Amazon EC2 customers' <https://aws.amazon.com/ec2/customers/> accessed 6 December 2024.

130 Manar Abourezq and Abdellah Idrissi, 'Database-as-a-Service for Big Data: An Overview' [2016] 7 International Journal of Advanced Computer Science and Applications 157; <https://aws.amazon.com/dynamodb/>; <https://aws.amazon.com/rds/>.

131 Ibid.

132 E.g. Amazon Simple Notification Service, which is a framework that allows businesses to send communications to their customers using Email or SMS.

133 E.g. Amazon Sagemaker, which is a framework for developing machine learning models.

resource[134] that cannot form a "shared pool" in any meaningful sense, but instances of running software can be thought of as a rivalrous resource that can be, in some sense, shared.

83 Here, it is important to note that many forms of computing resources listed, including software and storage, are not separable into discrete packets, but are continuous quantities. It is therefore not a requirement that a shared pool must contain a numerical plurality of resources (as in "two or more computers"), since this requirement would make no sense for continuous computing resources (it makes no sense to say "two or more storage").

84 The conclusion from this wide definition is that essentially any online service that serves multiple customers involves a "shared pool of computing resources" in some form. Even a simple web server contains software and hardware that is used to serve requests from multiple clients. Hence, this criterion from the legal definition does not do much to narrow down the overly wide term.

4. Access to the Shared Pool

85 A tempting approach to narrow down the definition may be to consider what it means to provide "access" to the shared pool of computing resources within the meaning of Article 2 (8). One approach would be to require that the user gain some degree of control over a subset of the pool. However, this would lead to an overly narrow interpretation, which clashes with defining features of cloud computing. Even in the basic case of hosting services like EC2, the user only gains control over a virtual machine – a resource that is *not* shared. When it comes to the shared computing resources, such as the physical central processing units (CPUs) and hard drives, the customer has no meaningful control. For more specific services like databases, this becomes even clearer. Here, the user does not even need to be aware of the physical computing resources they are using, and their only means of controlling them is by controlling their own amount of usage.

86 One of the core innovations of cloud computing has been to abstract computing services away from the management of resources, and specifically to remove the necessity of "ownership" of resources. Therefore, it would be incoherent to require any degree of control over the resources that goes further than simply the possibility of using them.

5. Scalable and Elastic Computing Resources

87 However, the computing resources in the shared pool must also be "scalable" and "elastic" within the meaning of Article 2(8). Although the literal text of the definition suggests that these are properties of the computing resources, they are in reality properties of the method in which they are used – scalable resources are flexibly allocated based on demand, and elastic resources are provisioned and released quickly according to workload.[135]

88 The difference between "scalability" and "elasticity" is not immediately clear from the definition. However, the fact that the definition of elasticity involves the "provision and release" of resources to "increase or decrease" them suggest that whilst scalability describes the flexible allocation of resources on a global level, elasticity means the increase and decrease of resources available to *specific users* based on *their workload*. "Provisioning" usually describes the self-allocation of resources by the customer, and an "increase or decrease" of resources available only makes sense at the user level, since the totality of resources available is usually fixed.

89 Whilst scalability is also an extremely broad term – every web server flexibly allocates computing resources to incoming requests – our reading of elasticity may provide the first real opportunity to give "data processing services" a somewhat hard edge. Since elasticity requires that the distribution of computing resources must change in response to a *single user's workload*, we can successfully eliminate services like simple websites where a single user's workload is essentially constant. Rather, the service provided to the user must at least theoretically be open to scaling, such that a single user could (within a certain range) self-provision a flexible amount of computing resources depending on their needs.[136] As we have seen above, this provisioning may occur fully automatically and without the need for user supervision or even awareness. At the same time, a manual provisioning and release can also suffice, provided that the process is sufficiently flexible. Therefore, both the possibility of rapid but manual provisioning of additional EC2 virtual machines and the automatic allocation of more computational resources to cloud databases during a spike in traffic, are examples of elasticity.

90 The term "elasticity" thus provides a logical nexus between the service provided to the customer and the

134 James Bessen, 'Open source software: Free provision of complex public goods.' in Jürgen Bitzer and Philipp JH Schröder (eds), *The economics of open source software development* (Elsevier 2006) 57-81.

135 Data Act, recital 80.

136 See similarly Patrick Pommerening and Michèle Nickel, 'Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act' (2024) Recht Digital 289 para 12.

flexibility of the underlying technical infrastructure. In view of this finding, it becomes easier to deal with SaaS services as well. A simple website *hosted* on a cloud service like EC2 would not be a data processing service. Although users gain access to a shared pool of computing resources (the website provider's software as well as the EC2 infrastructure), these resources are not elastic *to them* – every user always roughly uses the same amount and there is no way for a user to self-provision more resources.

91 However, the scope of elastic services is still extremely wide. Not only would a service like those provided by Salesforce fall under the term, where arbitrary amounts of user data can be processed, but even remote-hosted cloud applications like Microsoft Office 365 could still qualify. On its own, a text editor like Microsoft Word in the cloud might not present enough potential for elasticity, since every user's computational usage would be roughly the same, but when combined with the possibility of storing and editing large documents, and the possibility of collaboration with a large number of other users, the service could be considered elastic. The same could be said for project management software. Even social media platforms like video-sharing platforms could be considered data processing services, at least from the perspective of content creators, since these platforms provide them with a shared and highly resource-intensive infrastructure to store and distribute their content, and the computational resources "allotted" to each content creator can vary widely based on their number of viewers.

6. Economic Criteria and Global Assessment

92 Although elasticity provides us with a way to somewhat trace the outline of "data processing services" as a term, it is not fully unambiguous on its own. Since every user of an online service can at least choose *whether* or not to use it and *how long* to use it for, some degree of elasticity is present even in our simple website's case. Put simply, the degree of elasticity needed is a *quantitative* question that cannot be answered with technological definitions alone. In fact, this is not just the case for elasticity, but also for the other technical features mentioned in the definition – scalability, ubiquity, and configurability. None of these features are strictly binary but rather exist on a spectrum.

93 Thus, these technical features cannot be read simply as a set of individually necessary and jointly sufficient conditions. Rather, a specific economic and effects-oriented evaluation in every case, taking into account the degree and effect of the elasticity, as well as scalability, ubiquity, and configurability present in a particular service, is needed. Similar to the approach taken in other fields of EU law such as trademark law [137], these features should be understood as a set of interdependent factors forming part of a global assessment, such that a higher degree in one feature can compensate for a lower degree in another feature.

94 Moreover, the key to this evaluation is that the technical features mentioned in the definition – elasticity, scalability, ubiquity, and configurability – have corresponding economic effects, and it is these effects, not the technical features themselves, which should be decisive.

95 To understand this, one must again turn back to the analysis of the goals of the Data Act's switching and interoperability provisions given above. The defining economic feature of cloud services is the efficiency gained by amortising the usage of computing resources across many customers. This fact is also at the centre of the definition in Article 2(8). As described in the original AWS blog post,[138] this eliminates fixed costs and reduces the risk of investment. In turn, the uptake of cloud services becomes cheap, easy, and attractive, particularly for smaller players. The flip-side of this equation is the risk of severe technological lock-in effects.[139] Since cloud services are easily combinable into ecosystems, large cloud providers also benefit from the positive scaling effect of offering a large number of services, whereas their customers may find it difficult to switch single services to other providers.[140] Here, it is worth noting that these effects are not necessarily confined to "classical" cloud providers like AWS. Even business or consumer cloud applications can benefit from amortisation and ecosystem effects in the same way, even if the customer is never aware of it.

96 These economic effects are the reflections of the technical features of scalability, elasticity, ubiquity, and configurability given in the definition in Article 2(8). Scalability allows amortisation across the many users of a data processing service, and elasticity

137 Case C-39/97 *Canon Kabushiki Kaisha v Metro-Goldwyn-Mayer Inc.* [1998] ECR I-5525 para 17.

138 Jeff Barr, 'Amazon EC2 Beta' (25 August 2006) <https://aws.amazon.com/blogs/aws/amazon_ec2_beta/> accessed 6 December 2024.

139 Justice Opara-Martins, Reza Sahandi, and Feng Tian, 'Critical Analysis of Vendor Lock-in and its Impact on Cloud Computing Migration: A Business Perspective' (2016) 5(4) Journal of Cloud Computing: Advances, Systems and Applications 1, 14.

140 Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 178-17; Netherlands Authority for Consumers and Markets, Market Study Cloud Services (2022) ACM/INT/440323, 62.

negates the need of each customer to accurately predict the resources they need in advance, reducing investment risk. Similarly, ubiquity also decreases risk by increasing technological flexibility. And finally, increased configurability and customizability of a service means that during configuration, customers make more investments specific to a particular service (e.g. the time and energy needed to customize the service to their needs and uploading data).[141] The resulting product differentiation also increases lock-in effects.[142] Therefore, the degree to which these technical features are present must in fact be evaluated based on their economic effects.

97 Against this background, several criteria for evaluating typical cases can be developed. For one, the magnitude of amortisation benefits can be considered. These will tend to be higher the more computationally intensive a service is. Service models like cloud gaming, where a consumer essentially runs a conventional video game in the cloud in real time, rely heavily on amortisation – the main promised benefit to the consumer is that they can forego purchasing expensive gaming hardware, and instead efficiently share a computing infrastructure with a large number of other users over a large area.[143] Since gaming is so computationally intensive, even the elasticity in the user merely being able to choose when and how long to use the infrastructure, when coupled with the scalability of the infrastructure, is sufficient to justify the service model.[144] In this case, it may be justified to mandate interoperability for the service.

98 Second, the concrete risk of lock-in effects in the context of the ecosystem must be considered. An auxiliary service which itself may not be very computationally intensive, but plays a significant role in mediating different services inside an ecosystem (such as a security-relevant service[145]), might provide more reason for its classification as a data processing service.

99 Lastly, cloud services differ from other types of digital services in their infrastructural role as providers of computational power. A service which has a high importance for downstream markets (similar to the DMA's gatekeeper status) could deserve more intense regulation.

7. Summary

100 In summary, a correct understanding of the term "data processing services" is predicated on the insight that elasticity, scalability, and ubiquity are reflections of economic effects, and that they can exist on a continuous sliding scale. In order to make the final assessment, a technical understanding is necessary but not sufficient. Rather, a case-by-case evaluation focusing on the economic effects and the objectives of the provisions is needed. First, the elasticity, scalability, and ubiquity of the service should be quantified. Then, their corresponding economic effects – the degree of amortisation and risk minimization – must be evaluated. Finally, an effects-oriented case-by-case global assessment is unavoidable. This will, of course, come at the cost of reduced legal certainty, but given the cross-sectoral nature of the provisions, no other approach can guarantee a cogent application across their entire scope. Here, the criteria we have derived in the section above – high computational power, concrete danger of lock-in effects, and broader infrastructural role in the data economy – can serve as guideposts for the evaluation in typical constellations.

III. Scope of the Reference in Article 34 to Article 30 in Particular

101 Apart from the general definition of data processing services used in many provisions of the DA, it is unclear if the obligations to make open interfaces available and follow technical norms (cf. Art 30 (2) and (3)) apply to *all* data processing services when referenced by Article 34.

102 Article 30 itself differentiates between services "limited to infrasructural elements" (known as Infrastructure as a Service, IaaS), which are targeted

141 Jasper Sluijs and Pierre Larouche and Wolf Sauter, 'Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market' (2012) 3 JIPITEC 12, 15.

142 Ibid.

143 cf. *Microsoft/Activision Blizzard* (Case M.10646) Commission Decision C/2023/3199 final [2023] OJ C285/8, para 563; Competition and Markets Authority, 'Mobile Browsers and Cloud Gaming: Provisional Decision Report' (22 November 2024) para 12.85.

144 cf. on the role of computational intensity Compl. *United States v Apple Inc*, No. 2:24-cv-04055 (D.N.J. 21 March 2024), paras 71ff.; cf. on scalability Iryanto Jaya, 'Resource allocation in cloud gaming' (Doctoral thesis, Nanyang Technological University, Singapore 2023); additionally, ubiquity also plays a large role in cloud gaming, since a main selling point to consumers is that they are no longer tied to specific hardware, but can rather enjoy games regardless of geographical location, cf. Competition and Markets Authority, 'Mobile Browsers and Cloud Gaming: Provisional Decision Report' (22 November 2024) para 12.10; *Microsoft/Activision Blizzard* (Case M.10646) Commission Decision C/2023/3199 final [2023] OJ C285/8, para 563.

145 Daniel G Arce, 'Security-Induced Lock-In in the Cloud' (2024) 64 Business & Information Systems Engineering 505.

in Article 30(1), from services which also provide access to "the operating services, software and applications", which are targeted in the subsequent paragraphs (2)-(5) with the phrase "data processing services other than those referred to in paragraph 1". Interestingly, Article 34 only references "Article 30(2) to (5)", leaving out paragraph 1. One interpretation would therefore be that the legislator intends for only non-IaaS services to be subject to the *mutatis mutandis* application.

103 A different interpretation, however, would be that Article 34 (which itself specifies that it should apply for "data processing services") intends to extend the switching obligations placed on non-IaaS services in Article 30(2)-(5) to *all* data processing services when in the context of in-parallel use.

104 In other words, the question is whether the reference in Article 34 to Article 30 includes Article 30's specific scopes of application in terms of its addressees or is only targeted at its consequences.[146]

105 This question can be answered knowing the difference between the policy tools of interoperability and data portability. In contrast to interoperability, data portability is only about the export of data from one system to another system.[147] Whereas switching services primarily requires data portability, interoperability is necessary to allow parallel use. Put differently, interoperability constitutes a different, generally higher degree of connectedness. The DA recognizes this distinction,[148] but creates ambiguities due to the systematically unavailing cross reference from the interoperability provisions back to the rules for switching.

106 When understanding the difference between interoperability and portability, it becomes clear that Article 30 (2-5) – when referenced by Article 34 – must concern all data processing services. Regarding switching, the Data Act puts *stricter obligations on IaaS*, requiring "functional equivalence in the use of the destination data processing service", according to Article 30 (1).[149] In comparison, services that also provide access to "the operating services, software and applications" merely have to make open interfaces available[150] and follow technical norms.[151] Thus, the obligations for IaaS providers to facilitate switching are *more burdensome*, because they are outcome-oriented. Since the service delivery model of IaaS is treated more strictly than other services in the portability provisions, it would be inconsistent to completely exempt them regarding the higher form of interconnectedness, namely interoperability. Therefore, it is more plausible to interpret Article 30 (2ff.) in the context of Article 34 as a provision addressing all data processing services.

IV. Interoperability Across Service Types

107 A similar question is whether Article 34 DA only pursues interoperability between services of the same service type. For instance, does a storage service only need to be interoperable with other storage services, or also complementary services like web hosting? The answer to this question significantly changes the application scope of the provision.

108 Article 34 (1) itself simply states that "interoperability for the purpose of in-parallel use of data processing services" shall be facilitated. The provision does not specify whether it only covers the horizontal in-parallel use of services belonging to the same service type or also vertical interoperability between complementary services.

109 Yet, a controversy[152] about the application scope of Article 34 arose due to the fact that many of the switching provisions in Chapter VI that are referenced by Article 34(1) only apply to horizontal constellations. For example, Article 34(1) refers inter alia to the blanket clause on removing obstacles to effective switching (Art 23), which mandates providers to "enable customers to switch to a data processing service, *covering the same service type.*"

146 In German, "Rechtsfolgenverweisung" or "Rechtsgrundverweisung"

147 Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 85-86 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024.

148 Recital 99 distinguishes between the one-off egress of data required for the switching process and interoperability for in-parallel use.

149 Data Act, Art 30 (1).

150 Data Act, Art 30 (2).

151 Data Act, Art 30 (3).

152 Arguing that interoperability between data processing services mandated by Art 34 is limited to the same service type: Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft: Erste Einordnung von Begrifflichkeiten, Systematik und praktischen Herausforderungen' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)) 112, 115. His opinion is predicated on the understanding that Art 35 is the general provision on interoperabiltiy of data processing services and Art 34 regulates a specific case. However, the wording of Art 35 is unambiguous insofar that it sets out the requirements and the procedure for standardisation without mapping out a discrete obligation. Therefore, Art 34 is the main interoperabiltiy provision.

The fact that here, switching is constrained to "the same service type", may lead us to conclude that "in-parallel use of data processing services" within the meaning of Article 34(1) is similarly constrained to the same service type. Moreover, the fact that the subsequent Article 35 explicitly constrains itself to standards covering interoperability within a service type might also lead one to consider that Article 34(1) likewise only covers interoperability within a service type.[153]

110 In contrast, the aforementioned important references to Article 30 (2-5) do not contain such a restriction, whereas the not-referenced Article 30 (1) is limited to services covering the same service type. This argumentative standoff requires a deeper look into the policy tool of interoperability and its effects as suggested above (see part B.II). In general, two types of interoperability can be differentiated. Horizontal interoperability refers to interoperability between products and systems on the same level of the value chain,[154] for example between messaging services, as stipulated by the Digital Markets Act. In this case, mandated interoperability allows every user to reach users from all other interoperable services, thereby reducing network effects. Network effects arise when the attractivity of a product or system increases with the number of users.[155] If strong network effects are present in a market, horizontal interoperability can lower entry barriers and resolve lock-in effects.[156] Entrants do not have to reach a critical mass to compete and switching is less problematic because the same network can still be reached.[157] However, in situations without network effects, horizontal interoperability may not be pro-competitive in an effective way. In contrast, vertical interoperability pertains to different levels of the value chain.[158] It is associated with increased innovation, because customers can "mix and match" components.[159]

111 The question of whether the interoperability provisions for data processing services in the DA only apply to services of the same "service type" is an expression of this distinction. The question can therefore be rephrased as asking whether Article 34 can only mandate horizontal interoperability, or if it also mandates vertical interoperability.

112 Based on the goals of the provisions and the technical background of the market, we argue that Article 34(1) should not be constrained to horizontal interoperability.

113 First, the Data Act itself suggests at many points that both vertical and horizontal interoperability are intended. In Recital 99, the Data Act describes "in-parallel use of multiple data processing services with *complementary* functionalities" when referring to Article 34, a strong indication that vertical interoperability should be covered. And in Article 2(34), the definition of "switching" explicitly covers switching to "using another data processing service of the *same service type, or other service, ...*". Thus, even the notion of switching in the Data Act is not purely horizontal.

114 Second, recital 90 indicates that the legislator also pursued the *effects* of vertical interoperability. The recital states that "an ambitious and *innovation-inspiring* regulatory approach to interoperability is needed to overcome vendor lock-in, which undermines competition and the *development of new services*.[160] Whereas horizontal interoperability has no clear nexus with dynamic efficiencies, vertical interoperability enables product differentiation and increases the chances of specialised services to gain customers. Therefore, interoperability regulation aiming at innovation requires vertical interoperability.

115 Third, the actual need for horizontal interoperability in the industry is low.[161] The practice of using multiple equivalent cloud services, called "multi-homing",

153 Jonas Siglmüller, 'Standardisierungsbestrebungen für das Rückgrat der europäischen Digitalwirtschaft' [2024] Zeitschrift für IT-Recht und Recht der Digitalisierung 112, 115.

154 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 7 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 6 December 2024.

155 Justus Haucap, Ulrich Heimeshoff, 'Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?' (2014) 11 Int Econ Econ Policy (2014) 49, 51.

156 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 19 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 6 December 2024.

157 Ibid.

158 Marc Bourreau, Jan Krämer, Miriam Buiten, 'Interoperability in Digital Markets' (Report, Centre on Regulation in Europe 2022) 7 <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf> accessed 6 December 2024.

159 Ibid 26.

160 Data Act, recital 90.

161 Gregor Lienemann in Moritz Hennemann and others (eds), Data Act, An Introduction (Nomos 2024) 189-190; Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 86, 93 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024.

may be a valid tool to insure oneself against outages and increase resilience.[162] However, when it comes to combating lock-in effects, it does not confer a significant added benefit compared to being able to switch completely.[163] The practice of "multi-homing" alone would not be sufficient to justify the added burden of mandating interoperability, instead of just portability alone, at least on the cloud market. This is related to the fact that there are no significant, direct network effects arising in the cloud service market. Rather, as we have seen, the market is characterized by economies of *scope*, which foster the emergence of larger ecosystems with more *types* of services[164]

116 This brings us to our final argument: even if one were to interpret the *switching* provisions as solely horizontal, across the same service type, the interoperability provisions must be understood vertically to achieve effective horizontal switching. In an ecosystem setting, if a customer wants to horizontally switch from one service to another service of the same type, away from their current ecosystem to a new provider, they can only do so if the switched service can still interoperate with the other services left in the old ecosystem.[165] Otherwise, the ability to switch a single service is effectively useless. Simply put, horizontal portability implies some degree of vertical interoperability to achieve practical effectiveness. The presence of large ecosystems amplifies lock-in effects in a way that can only be effectively counteracted by vertical interoperability. To truly complement the rules on switching that it references, Article 34 must therefore also cover vertical interoperability. In fact, a policy mandating *only* horizontal and not vertical interoperability would in some sense be "the worst of both worlds" – not only would it not effectively achieve its policy goals, it would likely not even be meaningfully less burdensome on service providers, at least on a technical level, since the interfaces needed for interoperability still need to be developed.

117 Considering this analysis, one must conclude that the points where the DA constrains itself to the "same service type" are isolated occurrences that are justified by the specific nature of the provision in question, and should not be generalized to other provisions, at least in the realm of interoperability. For example, Article 35 only allows standard-setting for data processing services of the same service type, but this is owed to the nature of standard setting: a technical standard can usually by nature only address a particular service type. Moreover, standard-setting has a higher potential to overly restrict innovation, which justifies the higher requirements for its use.[166]

118 In sum, "interoperability for the purpose of in-parallel use of data processing services" within Article 34 is not limited to services of the same service type. In combination with the referenced obligations to make open interfaces available and follow interoperability standards (see Art 30 (2 and 3)), this means that far-reaching interoperability obligations will soon apply to cloud and edge services.

E. Conclusion

119 Clouds connecting Europe — the Data Act aims towards this ideal by reducing technical and economic barriers to an internal market for data and data related services. The Regulation aims to tap the full potential of data by laying down a harmonised framework for the use of and the access to data as well as engaging in tech regulation for cloud services to tackle competition-related problems.

120 The interoperability provisions in the Data Act are frequently overlooked, but highly important, because they are far-reaching and concern industries relevant for innovation and competitiveness. Yet, understanding these provisions is complicated. It is not even clear who the addressees are. Similar challenges arise in other data-related frameworks as well, because the subject matter is technical, abstract and dynamic. We suggest an interpretative method based on the characteristics of regulatory law to identify the understanding which increases the practical effectiveness of the provision. First, this approach requires a particularly careful analysis of the pursued goals — of the provision itself, but equally important of the entire framework and the background of primary EU law. Second, the focus on

162 Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 189-190.

163 cf. Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 93 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024.

164 Daniel Schnurr, 'Switching and Interoperability between Data Processing Services in the Proposed Data Act' in Jan Krämer and others (eds), *Data Act: Towards a Balanced EU Data Regulation* (Centre on Regulation in Europe 2023) 82-83, 93-94 <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf> accessed 6 December 2024; Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 178-17; Netherlands Authority for Consumers and Markets, Market Study Cloud Services (2022) ACM/INT/440323, 62.

165 Netherlands Authority for Consumers and Markets, Market Study Cloud Services (2022) ACM/INT/440323, 5.

166 Gregor Lienemann in Moritz Hennemann and others (eds), *Data Act, An Introduction* (Nomos 2024) 219.

the actual effects of a rule implies an interdisciplinary perspective on the regulated industry and the need for understanding a policy tool like interoperability as a whole.

121 We have shown that using this method, we can gain valuable insights into specific problems of interpretation in the Data Act. An effects-oriented approach makes it clear that Article 33 must be interpreted narrowly in accordance with its limited objectives, such that its application is only justified for data spaces with a certain degree of infrastructural sophistication. Crucially, it must not hamper the overarching goals of the rest of the Data Act by inadvertently discouraging data sharing.

122 Furthermore, we have seen that the confusing but central term "data processing services" can be elucidated by considering that the technical terms scalability and elasticity are reflections of economic effects – the amortisation of fixed costs and the reduction of investment risks – that play a key role in the legislative intention behind the provisions. It thus follows that the most appropriate approach to this definition is to consider the degree of elasticity and scalability in each case against economic criteria in a global assessment as a set of interdependent factors. Lastly, we have shown that an effects-oriented analysis of horizontal and vertical interoperability, when applied to the specificities of the cloud market, can lead us to a more reasonable answer on whether the restrictions to the "same service type" have a broad or narrow applicability. Unlike in other markets, the structure of the cloud market, with its economies of scope, tend to justify vertical interoperability mandates, even when only considering horizontal switching scenarios.

123 In sum, a stringent method focused on practical effectiveness is crucial for interpreting the interoperability provisions in the Data Act such that they manifest their desired goals whilst avoiding pitfalls. It might be a distressing insight that data-related regulation is of such technical complexity. At the same time, one cannot lose sight of the fact that, at the end of the day, the policy goals of the Act lie in the economic and public interest *effects* of that technology. If interpreted skilfully, the promising rules on interoperability could benefit end consumers, software developers, European companies and the EU's competitiveness and make it worthwhile that the EU legislator has ventured into this complicated field.

Synthetic Data, Data Protection and Copyright in an Era of Generative AI

by **Kalpana Tyagi** *

Abstract: Data protection, privacy and copyright may be closely aligned, yet distinctly respond to the common element called data – that comprises personal as well as non-personal elements. Data can be of many different types, and when extracted from human-authored works, the expressive form of the work is subject to copyright protection. When personal data are included in a given dataset, it may trigger the application of the EU General Data Protection Regulation. Together, all the different sources form training data, which forms a key input for the training of generative AI models. These models have substantially devoured data to reach their current level of sophistication and capabilities. However, generative AI models are advancing at a rapid pace, such that they are no longer a mere consumer of data; they are also a key producer of new data – one that mimics the original data. This data is known as 'synthetic data'. Once the currently available models go a step further than their present level of development, follow-on synthetic data may look like independent works, with remote resemblance, if any, to the original data. While on the one hand, this may be a big promise to meet compliance with the 2016 EU General Data Protection Regulation, it heralds notable challenges for the current IPR (particularly copyright and database rights) framework and the accompanying balancing of authors' and users' rights. This interplay – considering its inter- and intra-disciplinary complexity – remains under-explored in the literature. This contribution, accordingly, explores the interaction between copyright (and other IPRs), database rights and data protection and privacy in the context of synthetic data and generative AI.

Keywords: Synthetic Data, Generative AI (GenAI), Internet of Things (IoT), Copyright, Database Rights, Personal Data, Data Protection, Privacy, Innovation, 2024 EU AI Act, Text and Data Mining, Robert Kneschke v. LAION, Charter of Fundamental Rights (CFR)

Recommended citation: Kalpana Tyagi, Synthetic Data, Data Protection and Copyright in an era of Generative AI , 16 (2025) JIPITEC 176 para 1.

A. Introduction

1 The complexity of the generative AI value chain means that a range of inputs are required to create a high quality general purpose AI model (GPAI), such as Chat GPT. These inputs, together referred to as the AI infrastructure layer, include the following four key elements – 'computing power', 'skilled workforce', large investments for research and development (R&D) and 'data'.[2] Among these elements, this research article concentrates on 'data', a key input that is used to train generative AI models. The OECD defines data as the 'physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means'.[3] Data used for training a GPAI is

Dr. Kalpana Tyagi. Maastricht University, The Netherlands. Email: k.tyagi@maastrichtuniversity.nl

* The work is author's research output. The author would like to extend her gratitude to Prof. Henning Gross-Ruse Khan, Prof. David Erdos and all the attendees for their inputs at the CIPIL Seminar at the Faculty of Law, University of Cambridge on 24th October 2024. The author would also like to extend her special thanks to Prof. Miquel Peguera Poch, the editorial team at JIPITEC and the anonymous peer reviewers at JIPITEC for their very insightful inputs. This work covers the legal and technical development in the fast-moving field of generative AI until 24 July 2025.

2 Autorité de la concurrence 'Intelligence artificielle générative: l'Autorité s'autosaisit pour avis et lance une consultation publique jusquáu vendredi 22 mars' (8 February 2024) <https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/intelligence-artificielle-generative-lautorite-sautosaisit-pour-avis-et-lance> accessed 27 July 2025.

3 OECD, 'Glossary of Statistical Terms' (2008) p. 119.

referred to as 'training data' in the 2024 EU AI Act. Article 3(29) of the Act defines this training data as 'data' that is used to train the 'AI system [by] fitting its learnable parameters'. Data can be proprietary or non-proprietary, and can include personal, factual, real-time flow of information, creative expression of works (subject to copyright protection), organised as a database (subject to copyright and database rights), technical information (such as in the case of patents) or a business secret (protected as a trade secret[4]). In addition, when in large quantities, data must also be organised to enable structured access to its contents. This structured organisation is particularly central to information systems and machine learning wherein terabytes of data are used to train the AI models. This 'data about data' is known as 'metadata'.[5] Structural, descriptive, administrative and markup languages are some of the common ways of organizing metadata, and depending on their type and structure, may facilitate various use cases.[6] Structural metadata helps establish the correlation between different databases and their contents. Descriptive metadata helps identify the source of information. Administrative metadata helps file management and identify various rightholders (such as authors of copyright-protected works). Markup languages facilitate easy navigation and interoperability. This metadata can also be IP-protected. In *Bart v. Anthropic*, for example, the US District Court for the Northern District of California opined that '[accessing] over seven million copies [of works ... by downloading] a separate catalog of bibliographic metadata for each collection, with fields like title, author, and ISBN' was unauthorized use and constituted piracy of works.[7]

2 Thus, 'data', the oil that lubricates the digital economy, is not one homogenous element. Instead, it comprises many elements, and depending on the source, nature and form, may be subject to different disciplines of law. This diversification can also be classified on the basis of an access-driven framework, grounded in economic rationales, and a rights-driven framework, grounded in the safeguard for the protection of fundamental rights. In addition, it may also be important to clarify at the outset the difference between 'data' and 'information', which in legal literature has been distinguished on the basis of 'differentiation between the form [the 'digital form' that contains the information] and the meaning contained in that form [that is the information]'.[8] Information at a 'semantic' level may be conceived of as the 'meaning' or 'information *per se*', which is different from the syntactic level, which is the 'form' in which this information is 'expressed'.[9]

3 To regulate the digital economy, in 2020, the Commission proposed a 'European Data Strategy'.[10] To build a European single market for data, or Common European Data Spaces (CEDS), data is the key. The European Commission's vision on developing a data economy envisioned a range of measures to achieve this policy objective and facilitate access to data.[11] The EU Digital Markets Act (DMA) seeks to promote contestability and fairness in the digital markets mandates data portability (under Article 6(9)), and data access obligations (under Article 6(10) and 6(11)) on gatekeepers as regards core platform services.[12] In the Internet of Things (IoT), wherein smart devices must effortlessly communicate with one another for effective functioning, access to data from different service providers and device manufacturers is

x<https://www.oecd.org/en/publications/oecd-glossary-of-statistical-terms_9789264055087-en.html> accessed 27 July 2025.

4 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, Article 2; Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), Article 39(1) & (2).

5 Jenn Riley, 'Understanding Metadata: What is metadata, and what is it for?' (2017) NISO p.5 <https://www.niso.org/publications/understanding-metadata-2017> accessed 27 July 2025.

6 I*bid.*, pp. 6-7.

7 Andrea Bartz, Charles Graeber and Kirk Wallace Johnson v. Anthropic PBC, No. C24-05417 WHA p. 3,5 *United States District Court Northern District of California* (23 June 2025) <https://storage.courtlistener.com/recap/gov.uscourts.cand.434709/gov.uscourts.cand.434709.231.0_2.pdf>

8 Václav Janeček, 'Ownership of personal data in the Internet of Things' (2018) *Computer Law and Security Review* 34(5) p. 1042 <https://doi.org/10.1016/j.clsr.2018.04.007> accessed 27 July 2025.

9 Herbert Zech 'Information as Property' (2015) *JIPITEC* 6(3) pp. 193-194 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731076> accessed 27 July 2025.

10 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data (the European Data Strategy) COM/2020/66 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066> accessed 27 July 2025.

11 *Ibid.*

12 John Burden, Maurice Chiodo, Henning Grosse Ruse-Khan, Lisa Markschies, Dennis Müller, Seán Ó hÉigeartaigh, Rupprecht Podszun and Herbert Zach, 'Legal Aspects of Access to Human-Generated Data and Other Essential Inputs for AI Training' (December 2024) *University of Cambridge Faculty of Law Research Paper No. 35/2024* p. 30 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5045155> accessed 27 July 2025.

essential to facilitate competition in the sector.[13] This access-driven framework, targeted at the 'Internet of Things', is triggered when data is generated by connected devices. The governing principle here is that users and other firms (particularly start-ups and small and medium enterprises) can have easier, real-time access to the IoT data, which is otherwise within the *de facto* control of the device manufacturers.[14] Together, the legislative measures flowing from the Commission's digital strategy, namely the Data Act, the Data Governance Act, the Open Data Directive and the Regulation on the Free Flow of Non-Personal Data (FFNDPR), collectively form the 'European data laws'.[15] These EU data laws, as well as the Payment Services Directive 2 (PSD2) for the payment sector, the DMA and the general EU competition law framework are driven by principles of contestability, access, competition, economic and market-based rationales.[16] Even in these market-driven data access frameworks, if personal data is included, additional conditions, such as 'valid lawful ground under the GDPR', must be met.[17]

4 Thus, the nature of the data - whether personal or non-personal, even though a somewhat fluid dividing line[18] – influences 'the rhetoric used and the priorities set' and impacts the 'extent of data access'.[19] Even though a simple binary distinction of data as personal/ non-personal may soon become superficial, it is nonetheless a good starting point, as it helps modulate data, and as discussed below, the technological innovation called synthetic data is to be understood within a fundamental rights framework.[20] Data, when derived from works in an expressive form, may be subject to copyright protection.[21] When a given dataset comprises personal elements, it may trigger the application of the 2016 EU General Data Protection Regulation (GDPR), that acts as a safeguard to protect the fundamental right to data protection and privacy of the data subject. Article 8 of the Charter of Fundamental Rights (CFR) and Article 16 of the Treaty on the Functioning of the European Union (TFEU) offer a constitutional safeguard to personal data as a basic fundamental right. While privacy is a long

13 European Commission, 'Final report – Sector inquiry into consumer Internet of Things' (Brussels, 20.01.2022) *SWD* (2022) 10 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0010> accessed 27 July 2025.

14 Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives' (2023) *GRUR International* 72(2) p. 120, 124 <https://doi.org/10.1093/grurint/ikac107> accessed 27 July 2025; Oscar Borgogno and Gieuseppe Colangelo, 'Shaping interoperability for the IoT: the case for ecosystem-tailored standardisation' (March 2024) *European Journal of Risk Regulation* 15(1) p. 150 <https://doi.org/10.1017/err.2023.8> accessed 27 July 2025.

15 Thomas Margoni, Charlottee Ducuing and Luca Shirru, 'Data Property, Data Governance and Common European Data Spaces' (2023) *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht* p.2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4428364> accessed 27 July 2025, Thoms Streinz 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds) *The Evolution of EU Law* (Oxford University Press, 3rd edn 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971> accessed 27 July 2025.

16 Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition' (March 2023) *JECLAP* 14(2) <https://doi.org/10.1093/jeclap/lpac059> accessed 27 July 2025; Wolfgang Kerber, 'Data Act and Competition: An Ambivalent Relationship' (2023) *Concurrences* 1/2023 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4342488> accessed 27 July 2025; Inge Graef (2021) 'Why End-User Consent Cannot Keep Markets Contestable: A suggestion for strengthening the limits on personal data combination in the proposed Digital Markets Act' (2 September 2021) *Verfassungsblog* <https://verfassungsblog.de/power-dsa-dma-08/> accessed 27 July 2025; John Burden, Maurice Chiodo, Henning Grosse Ruse-Khan, Lisa Markschies, Dennis Müller, Seán Ó hÉigeartaigh, Rupprecht Podszun and Herbert Zach, 'Legal Aspects of Access to Human-Generated Data and Other Essential Inputs for AI Training' (December 2024) *University of Cambridge Faculty of Law Research Paper No. 35/2024* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5045155> accessed 27 July 2025.

17 Thomas Tombal and Inge Graef 'The Regulation of Access to Personal and Non-Personal Data in the EU: From Bits and Pieces to a System?' in Van der Sloot & van Schendel (eds): *The Boundaries of Data* (Amsterdam University Press, 2024) p. 196.

18 Josef Drexl (2019) 'Data Access and Control in the Era of Connected Devices' p. 124 <https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 27 July 2025.

19 Tombal and Graef (2024), *supra* note 17, pp.195-196.

20 Bárbara da Rosa Lazarotto and Gianclaudio Malgieri, 'The Data Act: a (slippery) third way beyond personal/non-personal data dualism?' (4 May 2023) *European Law Blog* <https://www.europeanlawblog.eu/pub/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/release/1> accessed 27 July 2025; Ana Beduschi 'Synthetic data protection: Towards a paradigm change in data regulation?' (2024) *Big Data & Society* p. 3 <https://journals.sagepub.com/doi/10.1177/20539517241231277> accessed 27 July 2025.

21 Cf Recital 9, Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019 CDSM). The recital states that text and data mining can also be carried out in relation to mere facts that are not protected by copyright, and in such instances no authorization is required under copyright law.

established 'venerable right', with firm foundations in national constitutions and international treaties, data protection has been identified as a more '"third generation fundamental right" or innovation for traditional human rights, one that is now included in the EU Charter of fundamental rights'.[22] Likewise, the need to remunerate the human author and balancing the authors' rights and users' rights is becoming increasingly central to the discussion on copyright and related rights in the digital economy. This has drawn the attention of the policy makers and courts alike, and has given way to a 'new doctrinal stream called "digital constitutionalism" [or constitutionalisation of intellectual property rights]'.[23] A fundamental rights-driven rhetoric is thereby more central to the EU GDPR and copyright and related rights framework.

5 Data generated from this original data is called 'synthetic data'. Synthetic data is artificially generated data that can be generated using techniques such as statistical sampling or more advanced AI learning techniques.[24] The '[synthetic] data generation revolution' is anticipated to significantly influence the 'current balance between utility and competing considerations' as over 60% of training data may be synthetically generated and it carries the 'potential to do to data what synthetic threads did to cotton'.[25] GenAI models are experiencing rapid technological advances and are a key generator of synthetic data. Once the currently available technology goes a step further than its current level of development, synthetic data generated from these GenAI models may not even be closely reminiscent of the original training data. While, on the one hand, this may be a big promise to comply with the GDPR as it may safeguard the identity of the data subject, the rise of synthetic (big) data presents notable challenges for the current IPR framework (particularly copyright), as well as for the balancing of authors' and users' rights – the two key legal frameworks central to this contribution.

6 Different possibilities emerge with the rise of synthetic data. Will synthetically generated data replace all the original human-generated data? Or will original human-generated and machine-generated synthetic data co-exist? These potential future scenarios will also impact (and be impacted by) copyright and data protection laws. They will also influence different fundamental rights, such as the right to property, the right to freedom of expression, the right to data protection and the right to privacy. The interplay thus, involves many composite elements, each of which must be decoded to solve the innovation complex. To follow this discourse, this contribution follows an inter- and intra-disciplinary research methodology and is organised as follows. Section 2, with inputs from the technical literature, offers a working definition of synthetic data alongside a non-technical insight in the technical aspects of synthetic data generation. Considering the innovation potential of synthetic data, section 3 assesses the interplay between synthetic data and IP (especially copyright and database rights). Section 4 develops the discourse from the lens of personal data, the EU General Data Protection Regulation (GDPR) and evaluates its pedigree in the fundamental rights, constitutional and doctrinal legal framework. Section 5 concludes with policy recommendations and directions for further research. It also returns to the central hypothesis of this paper, that is whether synthetic data will emerge as a complete substitute or whether will it remain a partial substitute, in other words, a complement to the human generated data, and whether distinct legal, technical and normative trade-offs may limit substitution of human generated data by synthetically generated data.

22 David Erdos, 'Comparing Consitutional Privacy and Data Protection Rights within the EU'(2021) *University of Cambridge Faculty of Law Research Paper No. 21/2021* pp. 1-2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843653> accessed 27 July 2025; *See also* Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (July 2014) *ICLQ* 63 (3) <https://doi.org/10.1017/S0020589314000244> accessed 27 July 2025.

23 Elena Izyumenko and Christophe Geiger 'Intellectual Property and Human Rights in the Jurisprudence of the CJEU and the ECtHR – An Introduction' (*pre-print*, 2025) in Elena Izyumenko and Christophe Geiger (eds.), *Human Rights and Intellectual Property before the European Courts: A Case Commentary on the Court of Justice of the European Union and the European Court of Human Rights* (Edward Elgar Publishing Forthcoming) p. 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5283506> accessed 27 July 2025; Edoardo Celeste, 'Digital constitutionalism: A new systematic theorisation' (2019) *International Review of Law, Computers & Technology* 33(1): British and Irish Law Education and Technology (BILETA Special Edition) p. 88 <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1562604> accessed 27 July 2025.

24 J Hradec, M Craglia, M Di Leo, S De Nigris, N Ostlaender and N Nicholson 'Multipurpose synthetic population for policy applications' (2022) *Joint Research Center, Digital Economy Unit: Technical Report: Publications Office of the European Union* p.12 <https://publications.jrc.ec.europa.eu/repository/handle/JRC128595> accessed 27 July 2025.

25 Michal S Gal and Orla Lynskey, 'Synthetic Data: Legal Implications of the Data-Generation Revolution' (2024) *Iowa Law Review* 109 p. 1091 <https://ilr.law.uiowa.edu/volume-109-issue-3/2024/03/synthetic-data-legal-implications-data-generation-revolution> accessed 27 July 2025. See also the references therein.

B. Synthetic Data

7 In traditional programming, best suited for constrained and structured environments, pre-defined rules called algorithms instruct machines to perform certain tasks.[26] These are simple decision trees, structured into a pre-defined 'IF-THEN-ELSE' format. Distinct from these are AI systems, that instead of following a structured pre-defined path, 'learn how to solve a problem by examining [the] training data'.[27] There are two key methods for training an AI system, namely, 'machine learning' (ML) and 'deep learning' (DL). In ML, systems are trained on large amount of data, and the quantity and the quality of the training data determines the quality of the AI system. ML is a good technique to train AI systems for weather forecasting and image and speech recognition.[28] DL, a subset of ML, mimics the 'complex processes [known as Artificial Neural Networks] inspired by the human brain' and is deployed in complex, creative and research and development-driven tasks, such as for creating 'new works of art and [for] medical drug discovery'.[29]

8 While AI has been around for a long time, it is the disruption by GenAI applications, such as Open AI's ChatGPT, Google's Bard (since Gemini) and Microsoft's Copilot, that has since 2022, gathered the attention of businesses and policy makers alike. This disruptive rise of GenAI was facilitated by a key innovation from Google's team that introduced 'transformers', a novel form of AI architecture, that relied 'entirely on self-attention to compute representation of its input and output without using sequence aligned RNNs [recurrent neural networks] or convolution'.[30] This technical innovation was disruptive at the time, as it was the first time that an 'encoder-decoder architecture with multi-headed self-attention' was used in place of the traditional recurrent layer architecture.[31] This process was significantly faster, more accurate and more data efficient than the, at the time popular, recurrent and convolutional frameworks used for language translation.[32] It also contributed to substantial improvements in the Google translate feature. The framework offered in the said paper, however, was limited to text-based inputs. Following the introduction of transformers, rapid developments took place in the field of deep learning. Follow-on works led to newer innovations and efficiency in image, audio and video generation using deep learning techniques.

9 Common to all these models is the need for the input 'data'. GenAI and large language models (LLMs) follow the 'neural scaling laws', wherein data is a key input. Neural scaling means that the efficient performance of the model enjoys a positive correlation with the size of the training datasets.[33] The larger the number of datasets used to train a GenAI model, the higher the quality and throughput of the model. Quantity alone is insufficient to ensure a high quality GenAI model; the quality of the datasets matters as well. Data is qualified by its five characteristics – volume, velocity, variety, veracity and value, also known as the 'Vs of Big Data'.[34] Higher quality datasets contribute to robust and well-functioning models. This hunger for data is endemic to large-scale deep learning models, and not to the traditional machine learning methods, such as decision trees, SVM, KNN models and discriminant analysis.[35] Large scale deep learning models that are trained on vast amounts of datasets, are referred to as foundation models (FM), and offer potentially diverse capabilities across a range of applications such as text generation, creative applications and even coding.[36]

26 Microsoft, 'Introduction to Artificial Intelligence (AI) Technology' (2024) pp. 8-9 <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-wttc-introduction-to-ai.pdf> accessed 27 July 2025.

27 *Ibid.*, p. 9.

28 *bid.*, p. 10.

29 *Ibid.*, p. 10.

30 Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkorelt, Llion Jonesm, Aidan N. Gomez, Łukasz Kalser, Illia Polosukhin, 'Attention Is All You Need'(2017) p. 2 <https://arxiv.org/abs/1706.03762> accessed 27 July 2025.

31 *bid.*, pp. 9-10.

32 *Ibid.*, p. 10.

33 *See* reference to J Kaplan, S McCandlish, T. Henighan, TB Brown, B Chess, R Child, S Gray, A Radford, J Wu and D Amodei (2020) 'Scaling laws for neural language models' and to J Hoffmann, S Borgeud, A Mensch, E Buchatskaya. T Cai, E Rutherford, D. d.L. Casas, LA Hendricks, J Welbl, A Clark, T Henngan, E Noland, K Millican, G. v.d. Drissche, B Damic, A Guy, S Osindero, K Simonyan, E Elsen, JW Rae, O Vinyals and L Sifre 'Training compute-optimal large language models' (2022), in Pablo Villalobos, Anson Ho, Jaime Sevilla, Tamay Besiroglu, Lennart Heim and Marius Hobbhahn, 'Will we run out of data? Limits of LLM scaling based on human-generated data' (4 June 2024) p. 1 <https://arxiv.org/abs/2211.04325> accessed 27 July 2025.

34 Annie Badman and Matthew Kosinski, 'What is big data?' (18 November 2024) *IBM* https://www.ibm.com/think/topics/big-data#:~:text=Subscribe%20today-,The%20V's%20of%20big%20data,needed%20to%20manage%20it%20effectively.

35 Zehui Zhao, Laith Alzubaidi, Jinglan Zhang, Ye Duan and Yuantong Gu, 'A comparison review of transfer learning and self-supervised learning: Definitions, applications, advantages and limitations' (15 May 2024) *Expert Systems with Applications* 242 p. 23 <https://www.sciencedirect.com/science/article/pii/S0957417423033092> accessed 27 July 2025.

36 Rishi Bommasani, Drew A. Hudson, Ehsan Adeli, Russ Altman, Simran Arora, Syndeny von Arx, Michael S. Bernstein, Jeannette Bohg, Antoine Bosselut, and Emma Brunskill and other 'On the Opportunities and Risks of

10 Thus, a digital firm that aspires to develop a competitive large-deep scale learning model needs data, which is a key input required to train the GenAI model. Between digital incumbents and start-up firms, the latter more frequently confront barriers to accessing quality datasets.[37] The real-world data must also be cleaned and labeled before it can be used for training purposes.[38] Digital gatekeepers, such as Google, Apple, Meta, Microsoft and Amazon (GAMMA) control large volumes of data that serve as training inputs to the LLMs. To add to the complexity, human-generated data has limited availability. Can it be that one may soon confront a paucity of quality data available to train these models? In other words, in addition to the barriers to accessing currently available human-generated data (both personal as well as non-personal), which by default is under the *de facto* control of the digital gatekeepers, will one soon confront another additional challenge – for instance, that this human-generated data becomes scarce and is eventually exhausted? Considering the current rate of data consumption used for training the models, this seems like a reasonable possibility. Villalobos *et al.* predict that if the pace of LLM training continues at the current rate, we may run out of 'public human text data between 2026 and 2032'.[39] Villalobos *et al.* make this observation in the context of LLMs, even though they also estimate the available text and non-text data in their empirical analysis. In addition, it also seems that the terms GenAI, LLMs, and Foundation Models (FMs), even though distinct, are sometimes used interchangeably.[40] Thus, before going further, it may be useful to offer a working definition of GenAI models, LLMs and Foundation Models (FMs), and organize their classification in the AI landscape, including the EU AI Act 2024/1689 (2024 EU AIA).

11 GenAI are AI models trained on large datasets, to generate new content – such as audiovisual, text, code, music or any other content that can be perceived by the senses – upon a mere prompt.[41] LLMs are a sub-category of GenAI as they are used to generate text-based data.[42] Thus, GenAI is a broader term that also covers the LLMs. The general purpose GenAI models, such as Bidirectional Encoder Representations from Transformers (BERT), the first-ever GenAI model, the Generative Pre-trained Transformer (GPT) by OpenAI, Stable Diffusion by Stability AI and Titan FM by Amazon are all widely-trained foundation models (FMs).[43] They are, in the language of the EU AI Act, known as the GPAI models, and require large amounts of training data. These models can then be fine-tuned to perform certain niche and personalized tasks.[44] Broadly speaking, AI models may be trained using one of the following three techniques: supervised learning (wherein models are trained on correctly labeled data), unsupervised learning (wherein data has not been labelled), and reinforcement learning (which involves learning by doing or the trial and error method).[45]

12 The 2024 EU AIA is a lengthy product-safety regulation comprising 108 recitals, 113 articles, and 13 annexes, and is divided into 13 chapters.[46] Even though principally a product-safety regulation, the Act has notable implications for copyright and data protection laws as well. The AI Act, in recitals 104-

Foundation Models' (16 August 2021) < https://arxiv.org/abs/2108.07258> accessed 27 July 2025.

37 Competition and Markets Authority (18 September 2023) 'AI Foundation Models: Initial Report' pp. 28-32

38 Peter Lee, 'Synthetic Data and the Future of AI' (*Cornell Law Review 110 forthcoming, pre-print 2024*) pp. 9-10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4722162> accessed 27 July 2025.

39 Pablo Villalobos, Anson Ho, Jaime Sevilla, Tamay Besiroglu, Lennart Heim and Marius Hobbhahn, 'Will we run out of data? Limits of LLM scaling based on human-generated data' (4 June 2024) p. 6 <https:// arxiv.org/abs/2211.04325> accessed 27 July 2025.

40 This article will use the term GenAI to offer consistency to the discussion. As synthetic data remains central to the discussion, use of the term GenAI is also more representative of the technical field.

41 TechMobius, 'Generative AI vs. LLM, What is the difference?' <https://www.techmobius.com/blogs/generative-ai-vs-llm-what-is-the-big-difference/> accessed 27 July 2025.

42 *Ibid.*

43 Amazon Web Services, 'What are foundational models?' <https://aws.amazon.com/what-is/foundation-models/> accessed 27 July 2025.

44 Kalpana Tyagi, 'Mapping competition concerns along the generative AI value chain' (Forthcoming 2025) *SSRN* p. 18 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5282596> accessed 27 July 2025. See also the references, and various examples of targeted, niche FM models therein. Astro LLaMa for example is a niche, vertical FM model trained on limited data vis-à-vis, its parent FM model Llama by Meta.

45 Alec Radford, Karthik Narasimhan, Tim Salimans and Ilya Sutskever, 'Improving language understanding by generative pre-training' (2018) <https://www.mikecaptain.com/resources/pdf/GPT-1.pdf> accessed 27 July 2025; Microsoft, 'Introduction to Artificial Intelligence (AI) Technology' (2024) pp. 11-12 <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-wttc-introduction-to-ai.pdf> accessed 27 July 2025; DeepSeek-AI 'DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning'(2025) <https://arxiv.org/pdf/2501.12948> accessed 27 July 2025.

46 João Pedro Quintais 'Generative AI, Copyright and the AI Act' (April 2025) *Computer Law & Security Review* 56 p. 6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4912701> accessed 27 July 2025.

109 and Chapter V, dealing with 'General-purpose AI Models', provide copyright-related obligations for GPAI model providers. Notably, Article 53(1)(d) requires the GPAI model providers to offer a 'publicly available' and 'sufficiently detailed summary' of the datasets used for training the model. This summary must be provided in accordance with the explanatory notice and annex template contained in the 'Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models'.[47]

13 The GPAI models are a part of the larger subset comprising GP(AI) systems.[48] As an example, whereas GPT (Generative Pre-trained Transformer) is a model, ChatGPT and Midjourney are systems.[49] The copyright-related (and the data protection-related) obligations under the AI Act principally concern GPAI model providers with regard to the GPAI models, and not GPAI system providers with regard to the AI system.[50] This distinction becomes relevant to determine the application of the AI Act, as also noted by the Hamburg Regional Court in its recent *Kneschke v. LAION* decision, the EU's first GenAI and text and data mining (TDM) decision discussed in section 3, *infra*.

14 As available and clean human-generated data is limited in quantity, how do digital firms resolve the challenge of limited access to superior quality datasets? There are three inter-related technical possibilities that may help overcome this data bottleneck: enhancing the efficiency of data consumption by the GenAI models (1), developing new techniques such as transfer learning (2), and synthetic data generation (3).[51] The current training of GenAI, including BERT, Stable Diffusion and ChatGPT, is inefficient and resource-intensive, and optimizing the efficiency of the training process is a key research agenda in the field.[52] Transfer learning (TL) and self-supervised learning (SSL) can help overcome the data bottleneck associated with the incumbent inefficient learning methods.[53]

15 Transfer learning (TL) is a popular learning method in computer vision and natural language processing (NLP) tasks such as sentiment analysis.[54] TL or knowledge transfer uses pre-trained parameters from earlier trained models to develop a robust foundation model.[55] For example, if a model has been trained to identify deep-faked political news, this pre-trained model can be used to train a new model that can identify political satire. In TL, the relevant parameters from the earlier trained models are pre-selected to further fine-tune and adapt to develop a new FM that is suitable for the task under consideration. Simply put, TL may be suitable when the developer uses 'pre-trained parameters from earlier trained models' to develop vertically-specialised applications in certain domains.

16 Self-supervised learning (SSL), like transfer learning, is another commonly used learning approach to overcome limited data availability. SSL, an unsupervised learning technique, extracts 'reusable features from source data' and recycles them to make new models.[56] In other words, this recycling of the data helps develop personalized models that can leverage the capabilities of earlier trained models.

17 Interestingly, these different approaches are also interconnected. To train the GenAI models, data is an input as well as an output. Though not always, human-generated data may serve as a good and robust input to generate synthetic data. Synthetic data, especially when real datasets are unavailable, may serve as a good input for TL and SSL models and thereby, help optimize the overall learning process. Interestingly, synthetic data is also the output from the GenAI models, which in turn also serves as an input for further training and fine-tuning these models. There is thus a circular element in the GenAI value chain – the input generates an output which is further recycled to generate more output. These efficiency-enhancing steps also save the expert resources required for the creation of large, labeled datasets and considerable time that is otherwise required to train deep neural networks for complex tasks.[57] Interlinkages between different steps – such as how synthetic data is the output and may also

47 European Commission, 'Annex to the Communication to the Commission – Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models required by Article 53(1)(d) of Regulation (EU) 2024/1689 (AI Act)' (24 July 2025) <https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models> accessed 27 July 2025.

48 Quintais (2025), *supra* note 46, p. 6.

49 *Ibid.*

50 *Ibid.*, p. 7.

51 Villalobos et al (2024), *supra* note 39, p. 9.

52 Sashank J. Reddi, Sobhan Miryoosefi, Stefani Karp, Shankar Krishnan, Satyen Kale, Seungyeon Kim and Sanjiv Kumar, 'Efficient Training of Language Models using Few-Shot Learning' (2023) *Proceedings of the 40th International Conference on Machine Learning* p. 1, 7 <https://proceedings.mlr.press/v202/j-reddi23a/j-reddi23a.pdf> accessed 27 July 2025.

53 Zhao et al (15 May 2024), *supra* note 35, pp. 2,22.

54 Niklas Donges, Matthew Urwin and Parul Pandey, 'What Is transfer Learning? Explore the Popular Deep Learning Approach' *Builtin* (15 August 2024) <https://builtin.com/data-science/transfer-learning#:~:text=Transfer%20learning%20is%20a%20machine,model%20despite%20having%20limited%20data> accessed 27 July 2025.

55 *Supra* note 53, p. 2.

56 *Ibid.*

57 *Supra* note 54.

serve as an input in the training process – create economies of scale and scope across the GenAI value creation process.

I. Synthetic Data: Use Cases and Methods of Generation

18 Synthetic data is artificially generated data. Synthetically generated data can be visual, written, tabular, audiovisual, graphic or, as technological advances may permit, data that can be perceived by the senses. An important feature of synthetic data is that it shares the same statistical properties as the original data.[58] Synthetic data are superior to traditional anonymization techniques. Traditional anonymization techniques cover only certain aspects of the data, and are therefore unsuitable in the case of big data, in which there are 'no non-sensitive attributes'.[59] In other words, big data and advanced algorithms makes it possible to deanonymize datasets that may also include non-sensitive attributes. Synthetically generated data that can be reverse-engineered to reconstruct the original dataset cannot qualify as synthetic data.[60] Synthetically generated data, thus, retain the statistical properties of the original dataset without revealing any personal attributes of the original dataset, and in this respect, are a viable option to facilitate compliance with data protection laws, as compared to traditional anonymization techniques. There are, however, certain subtle legal aspects that qualify the conditions under which synthetic datasets may indeed be exempt from the scope of data protection laws – these different use cases are further discussed in section 4 *infra*, which deals with the interface between synthetic data and data protection laws.

19 There are various methods of synthetic data generation. Data synthesis, using statistical techniques such as 'Synthetic Reconstruction' (SR) and 'Combinatorial Optimization' (CO), dates back to the 1980s, and has been regularly used by statisticians to fill-in the missing data and construct artificial populations.[61]. The rise of big data and computing power, along with the use of probabilistic models such as Deep Generative Models (DGM), created 'a new generation of models that exploit deep learning for creating synthetic data'.[62] Herein, Ian Goodfellow's work on deep learning and Generative Adversarial Networks (GANs), contributed significantly to the uptake of synthetic data.[63] Synthetic data can be generated in a fully autonomous environment, such as through a large language model, whereby output from the model is re-fed and used as input to train the model. Alternatively, the training cycle can be mixed with initial training by human-generated data, followed by the next round of training with a mix of synthetic and human-generated data.

20 Synthetic data have a range of applications. They can be used to enhance privacy (1); to de-bias datasets to homogeneously represent under-represented populations in datasets (2); to test products, such as IoT-enabled products for safety and accuracy prior to a formal product launch (3); to train GenAI models (4); and to create safe data spaces for data-driven innovation in digital markets (5). The following paragraphs illustrate some practical use cases of synthetic data to establish its value and policy significance.

1. De-Biasing Datasets for Homogeneous Population Representation

21 A key limitation of current GenAI models is that they tend to exhibit bias.[64] This bias is attributed to the limitations of input data, which itself may exhibit a range of biases, such as bias against certain gender or socio-economic backgrounds. Synthetic data generation techniques are a sustainable approach to de-biasing the datasets. One such approach, Synthetic Minority Over-sampling Technique (SMOTE) involves deliberately adding more artificially generated data about under-represented populations.[65] In large data sets, the majority or over-represented population groups are represented as the normal class, whereas the interesting or under-represented examples are the abnormal class.[66] SMOTE involves over-sampling the minority and under-sampling the majority class for a more uniform and egalitarian representation of the population.[67] This technique, dating back to decades-old statistical sampling techniques, has a wide range of applications to de-bias datasets. Consider, for

58 *Supra* note 24, pp. 14-15.

59 *Ibid.,* p. 44.

60 *Ibid.*

61 *Ibid.,* p.12.

62 *Ibid.,* p.14.

63 Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep learning* (2016) The MIT Press <http://alvarestech.com/temp/deep/Deep%20Learning%20by%20Ian%20Goodfellow,%20Yoshua%20Bengio,%20Aaron%20Courville%20(z-lib.org).pdf>

64 *Supra* note 24, p. 18, 45

65 N.V. Chawla, K.W. Bowyer, L.O. Hall and W.P. Kegelmeyer 'SMOTE: Synthetic Minority Over-sampling Technique' (2002) *Journal of Artificial Intelligence Research* 16 pp. 321-357 <https://www.jair.org/index.php/jair/article/view/10302> accessed 27 July 2025.

66 *Ibid.*, pp. 329-330.

67 *Ibid.*, p. 331, 352.

example, the datasets of scientists working in the STEM field. An original dataset may over-represent those with a certain gender and socio-cultural and ethnic background. With SMOTE, one can de-bias such a dataset and create a more homogenous output that can then be used for better policy decisions. However, this oversampling method needs to be fine-tuned for deep learning architecture, wherein traditional SMOTE techniques may have limited effectiveness. Herein, computer scientists have proposed over-sampling approaches, such as 'Deep SMOTE', that deploys a modified SMOTE architecture in a deep neural network and 'Deep Adversarial SMOTE', that is a further fine-tuned Deep SMOTE model for unsupervised networks.[68]

2. Testing IoT-Enabled Products for Safety prior to Formal Product Launch

22 Internet of Things (IoT) is a world of inter-connected devices, whereby there is smooth machine-to-machine, and human-to-machine communication. As different devices talk to each other to offer novel goods and services, quality data may oftentimes be unavailable to train these IoT models prior to a product launch. Amazon, the world's largest online retailer, with rich data on the products and services sold on its e-commerce platform, too suffered from this data limitation. Even though Amazon has a rich database about user behaviour on its platform, it had limited insight about how users might respond to its yet-to-be-launched voice assistant, Alexa, at the time. To address the challenge of limited access to quality data to 'bootstrap the machine learning models that interpret customer requests', Amazon used large volumes of synthetic data to train Alexa.[69] Amazon required training data to anticipate what its potential customers might want Alexa to do while using it. This challenge is not unique to Amazon alone. Other large digital firms, such as Microsoft, Apple, and Google, confronted similar issues in the early stage of developing their respective virtual personal assistants, that could interact with human users 'via spoken interactions' and 'gesture recognition'.[70] To train Alexa's *Natural Language Understanding* (NLU) systems, the Alexa AI team used the available customer data as a basic template and used it to identify general syntactic and semantic patterns. These patterns were then used as a basis to construct a large number of 'new, similar sentences'.[71] NLU models trained on such data sets could more easily identify complex patterns and deliver higher performance.[72] Following Alexa's success, Amazon has continued to integrate synthetic data and GenAI techniques to make its product lines more robust. Amazon, as a leading IoT player, has detailed user profiles, including personal data, about user interaction with Alexa, an aspect that is subject to data protection laws.[73] This factual information, including elements of personal data, can be simulated and mixed with synthetically-generated data to train the models.[74] Amazon also used this synthetic data generation technique to develop voice recognition systems across different languages, wherein 'it faced a shortage of collected data'.[75] Once developed and successfully launched, these GenAI-enabled, IoT products further leverage on a mix of human generated data to continue optimising their performance. GenAI-enabled IoT, such as Amazon's DialFRED, facilitate 'user-device interaction and foster problem-solving capabilities'.[76] Successive iterations of synthetic and human-generated data, help voice, image and other non-text-based

68 Hadi Mansourifar and Weidong Shi, 'Deep Synthetic Minority Over-Sampling Technique' (2020) <https://arxiv.org/pdf/2003.09788> accessed 27 July 2025.

69 Janet Slifka, 'Tools for generating synthetic data helped bootstrap Alexa's new-language releases' (11 October 2019) *Amazon Science: Conversational AI* <https://www.amazon.science/blog/tools-for-generating-synthetic-data-helped-bootstrap-alexas-new-language-releases> accessed 27 July 2025.

70 Veton Z Këpuska and Gamal Bohouta, 'Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home' (University of Nevada, Las Vegas, 2018) *IEEE 8th Annual Computing and Communication Workshop and Conference* <https://ieeexplore.ieee.org/abstract/document/8301638, open access version available here: https://www.researchgate.net/publication/322418348_Next-Generation_of_Virtual_Personal_Assistants_Microsoft_Cortana_Apple_Siri_Amazon_Alexa_and_Google_Home> accessed 27 July 2025.

71 Slifka (11 October 2019), *supra* note 69.

72 *Ibid.*

73 Guido Noto La Diega and Christiana Sappa, 'The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers' (2020) *Reveue européene de droit de la consummation/ European Journal of Consumer Law*, p. 4,5,11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772700> accessed 27 July 2025. See also the references therein.

74 Amin Fazel, Wei Yang, Yulan Liu, Roberto Barra-Chicote, Yixiong Meng, Roland Maas, Jasha Droppo, 'SynthASR: Unlocking Synthetic Data for Speech Recognition' (2021) <https://arxiv.org/pdf/2106.07803> accessed 27 July 2025.

75 Gal and Lynskey (2024), *supra* note 25, p. 15. See also the references therein.

76 Mazlan Abbas, 'Generative AI Applications for IoT: Exploring the Future of Smart Devices' (3 April 2023) *IoT World* p. 3 <https://iotworld.co/2023/04/3-generative-ai-applications-for-iot-exploring-the-future-of-smart-devices/> accessed 27 July 2025; Maria Kanwal, '3 Generative AI Applications for IoT you must know about' (12 December 2023) *SSRN* p. 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4667577> accessed 27 July 2025.

models continuously strengthen their capabilities, and offer better user experience.[77] Simply put, a mix of human and synthetically generated data is continuously fed into the IoT system to enhance and optimise their performance and capabilities. Co-existence of human and synthetically generated data boosts model performance, and is a particularly appealing approach to training 'end-to-end (E2E) *Automatic Speech Recognition* (ASR) models' for new applications, whereby human-generated data may be sparsely available.[78]

3. Training GenAI Models

23 Synthetic data is a commonly deployed tool for the 'development, test[-ing] and validation' of machine learning systems, where data may either be unavailable or inaccessible.[79] ChatGPT was trained using a large corpus of data – both original human-generated and synthetic data. It was trained using 'unsupervised, Reinforcement Learning coupled with Human Feedback (RLHF) and semi-supervised' learning techniques.[80] The original human-generated data may have elements of personal data, as data can be classified as personal once there is a possibility of identification.[81]

24 Synthetic data can also be generated with sequential modelling, simulated data and decision trees.[82] Another important technique for synthetic data generation is *Fully Visible Belief Networks* (FVBNs) that follow a probability-driven approach to generating synthetic data.[83] FVBN is the basic model that has been further fine-tuned to create and train advanced models such as WaveNet by DeepMind.[84] As FVBN was relatively slow in generating output, it limited the successful commercial application of the technology. DeepMind fine-tuned this technology, and used a neural network driven-approach to accelerate the pace of output generation.[85] This transition to neural network-driven learning and use of 'transformers' by Google, as discussed above, and the addition of 'bidirectionality' to the learning process was disprutive.[86] Bidirectionality meant that GenAI tools, starting with BERT, could read the text in both directions – from the left to right, as well as the right to left. Pre-BERT, GenAI models could read only in one direction, either left to right or right to left. The ability to read bidirectionally offered GenAI to *Contextualize, Iterate and Improvise* (CII) with every iteration.[87] This enabled the GenAI tools to offer meaningful and contextual outputs, such as synthetic data, at a faster pace, and in larger quantities that could be further used as input to train and fine-tune these AI models.

25 General Adversarial Networks (GANs) and Variational Auto Encoders (VAE) are two current and state-of-the-art, commonly deployed deep learning algorithms, that are also the more frequently used models to generate synthetic data.[88]

77 Nishant Prateek, Mateusz Łajszczak, Roberto Barra-Chicote, Thomas Drugman, Jaime Lorenzo-Trueba, Thomas Merritt, Srikanth Ronanki, and Trevor Wood 'In other news: a bi-style text-to-speech model for synthesizing newscaster voice with limited data' in A. Loukina, M. Morales and R. Kumar (eds.) *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies* (2019) pp. 205-213 <https://arxiv.org/abs/1904.02790> accessed 27 July 2025.

78 Fazel et al (2021), *supra* note 74, p. 1, 4.

79 Agencia Española Protección Datos, 'Synthetic data and data protection' (2 November 2023) AEPD Innovation and Technology Division <https://www.aepd.es/en/prensa-y-comunicacion/blog/synthetic-data-and-data-protection> accessed 27 July 2025.

80 Kanwal (12 December 2023), *supra* note 76, p. 3.

81 Michèle Fink and Frank Pallas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR' (2020) *International Data Privacy Law* 10(1) p. 29 <https://academic.oup.com/idpl/article/10/1/11/5802594> accessed 27 July 2025.

82 Agencia Española Protección Datos (2 November 2023), *supra* note 79.

83 Brendan J. Frey, Geoffrey E. Hinton and Peter Dayan, 'Does the wake-sleep algorithm learn good density estimators?' in D. Touretzky, M. Mozer and M. Hasselmo (eds) *Advances in Neural Information Processing Systems 8* (NIPS, 1996) (MIT Press, Cambridge, MA) pp. 661-666 <https://proceedings.neurips.cc/paper_files/paper/1995/file/55b1927fdafef39c48e5b73b5d61ea60-Paper.pdf> accessed 27 July 2025.

84 Aaron van den Oord, Sander Dieleman, Heiga Zen, Karen Simonyan, Oriol Vinyals, Alex Graves, Nal Kalchbrenner, Andrew Senior and Koray Kavukcuoglu 'Wavenet: A generative model for raw audio' (2016) <https://arxiv.org/abs/1609.03499> accessed 27 July 2025.

85 *Ibid*.

86 OECD Digital Economy Papers, 'AI Language Models: Technological, Socio-Economic and Policy Considerations' (2023) pp. 14-22 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/04/ai-language-models_46d9d9b4/13d38f92-en.pdf> accessed 27 July 2025.

87 Kalpana Tyagi, 'Copyright, text & data mining and the innovation dimension of generative AI' (2024) *Journal of Intellectual Property Law & Practice* 19(7) pp. 559-562 <https://academic.oup.com/jiplp/article/19/7/557/7624901> accessed 27 July 2025.

88 Ian J Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherijl Ozair, Aaron Courville and Yoshua Bengio, 'Generative adversarial networks' Advances in neural information processing systems' (2014) <https://arxiv.org/abs/1406.2661> accessed 27 July 2025; For a discussion on the interface between deep fakes, synthetic data and personality rights, see Kalpana Tyagi 'Deepfakes, Copyright and Personality Rights: An Inter-disciplinary Perspective' in Klaus Mathias and Avilasham Tor (eds)

26 GAN as an approach to machine learning offered an important thrust to the GenAI revolution that we are currently witnessing. In GAN, a training dataset is used to train models to generate samples that are varying representations of the original data inputs.[89] GAN was quickly adopted as a standard tool in machine learning, as it substantially multiplied the input and output points, and thus accelerated the rate of output generation.[90] The basic GAN model used supervised learning to approximate actual functions and posited a sustainable technological model for 'image generation and manipulation systems'.[91] Learning may be supervised, unsupervised or reinforced. The resilience of GAN is that it has been updated over time, and there are many variations of GAN that can be adapted and used across all these different approaches to machine learning. Interactive GANs, for instance, are applications used for creating images, whereby input data is used to train models to create similar realistic images.[92] The unsupervised GAN model includes a 'generative' neural network and a 'discriminative' neural network. The generative neural network creates the noise, such as by generating correct and incorrect outputs. The discriminative neural network assesses the factual correctness to ascertain which of the given outputs are factually correct. To visualize how GANs function in practice, consider the generative neural network as the teacher that offers an exam with multiple choice questions to the students, the discriminative neural network. The student has over the course of the year learnt from books, class notes and lectures, which is the equivalent of training data. Based on this learning, the student learns to discriminate amongst correct and incorrect options. The process is iterated until the discriminative neural network learns to correctly distinguish the 'noise' from the data.

27 VAE is another scientifically robust approach for variational learning in deep generative models. Stable Diffusion, a GenAI model, offers realistic images, videos and animations, with a mere text and image prompt. Stable Diffusion uses 'variational autoencoder, forward and reverse diffusion, a noise predictor and text conditioning' to perform its function.[93] VAE translates human expressions into mathematical representations and distribute them over a range of functions. As an example, the human expression of smile may be attached with a higher probability to parodied works and a thoughtful expression be assigned with a higher probability to quotations and news reporting. The mathematical expressions are then coded and decoded to generate images. Stable Diffusion V1 was trained on LAION's datasets using Common Crawl. This process involved scrapping billions of images and text that are protected by copyright and related rights. The following section 3 further develops this discussion in the context of copyright, and other intellectual property rights.

C. Copyright: Synthetic Data, Text and Data Mining and Follow-on Works

28 Intellectual property rights (IPRs) and notably copyright and related rights have an important interplay with GenAI and synthetic data. The key question as regards synthetic data and copyright is whether the process of generation of synthetic data, and the output of GenAI models, namely the synthetic data itself, infringe copyright. To answer this, it is important to look at how GenAI models text and data mine to make inferences, draw correlation and generate new works (Section 3.1). Sub-section 3.1.1 addresses the scope of TDM as discussed by the German regional court in *Robert Kneschke v. LAION*. Subsection 3.1.2 develops the scope and meaning of opt-outs under Article 4(3), 2019 CDSM, and its interpretation thereof by the German court in light of the 2024 EU AI Act (2024 EU AIA). Section 3.2 discusses whether synthetic data infringes copyright, and whether the 2024 EU AIA can safeguard rightholders of the original works from synthetically generated data, that is at some point in the data value chain, based on the original human-generated data.

I. GenAI, Text and Data Mining and Synthetic Data in the EU

29 GenAI involves two key phases – namely, the input/training phase and the output phase.[94] The training

Law and Economics of the Digital Transformation (2023) (Economic Analysis of Law in European Legal Scholarship 15, Springer Switzerland) <https://link.springer.com/chapter/10.1007/978-3-031-25059-0_9> accessed 27 July 2025.

89 Ian Goodfellow (3 April 2017) 'NIPS 2016 Tutorial: General Adversarial Networks' Open AI pp. 2-3 <https://arxiv.org/abs/1701.00160> accessed 27 July 2025.

90 *Ibid.*

91 *Ibid.,* p. 51.

92 J.Y. Zhu, P. Krähenbühl, E. Shechtman and A.A. Efros (2016) 'Generative visual manipulation on the natural image manifold' *European Conference on Computer Vision* pp. 597-613 (Springer) <https://arxiv.org/abs/1609.03552>

93 Amazon Web Services 'What is Stable Diffusion?' <https://aws.amazon.com/what-is/stable-diffusion/> accessed 27 July 2025.

94 Eleonora Rosati, 'Infringing AI: Liability for AI-generated outputs under international, EU, and UK copyright law' (June 2025) *European Journal of Risk Regulation* 16(2) p. 611 <https://doi.org/10.1017/err.2024.72> accessed 27 July

phase involves text and data mining (TDM). TDM may be defined as 'any automated analytical technique aimed at analysing text and data in digital form which includes but is not limited to patterns, trends and correlations'.[95] Data is the input required to train these GenAI (including LLM) models. ChatGPT, one of the fastest adopted and most popular GenAI models, for example, was trained on '300 billion words systematically scraped from the internet'.[96] This included both copyright-protected content, such as books, works, and poems, as well as personal data, such as posts by users on social and professional networking sites, such as Facebook, Instagram, and LinkedIn.[97] Whereas works are subject to copyright, personal data is subject to GDPR. The alleged infringing use of data in the input/training phase is a key complaint in the GenAI-related cases, currently pending before the US courts, and the case of Stability AI, pending before the UK courts. In the EU, text and data mining (TDM) is covered by Articles 3 and 4, 2019 Copyright in the Digital Single Market Directive (2019 CDSM).[98] Article 3 offers an exception for the right of reproduction and extraction made under the Database Directive 96/9/EC, 2001 InfoSoc Directive, and the press publishers right under Article 15 of the 2019 CDSM. Article 4, 2019 CDSM, in addition to these rights, also offers an exemption from the right of reproduction and translation, adaptions and alterations of a computer programme under Article 4(1)(a) and (b) of the 2009 Computer Programmes Directive (CPD). As per Article 4 (1)(a) and (b), 2009 CPD, the rightholder of the computer programme has the right to authorize any permanent or temporary reproduction, translation, adaptation, arrangement, or any other alteration of a computer program. Article 4 of the 2009 CPD is, however, subject to Articles 5 and 6, and offers a set of restricted rights available for computer programmes. Article 5(3) in particular authorizes the user who has a right to use a copy of a computer program, the possibility to 'observe, study or test the functioning of the programme' without seeking an explicit permission from the rightholder. One therefore sees an interplay between Article 4, 2019 CDSM and Article 5 of the 2009, CPD. Article 5(3) of the CPD offers a 'black box exception' to study and evaluate the basic ideas and principles of the program.[99] It must, however, be added, that this research exception under Article 5(3), 2009 CPD is only limited to study the underlying principles, ideas and designs that underlie the programme. In other words, TDM that falls outside the scope of research purposes is not covered under Article 5(3), 2009 CPD. In that respect, Article 4, 2019 CDSM clarifies that TDM beyond those specified purposes are permitted provided that the rightholder has not limited this possibility, such as through the imposition of 'machine-readable means' or any other such reservation[100] an issue further developed in subsection 3.1.2 *infra.*

1. *Robert Kneschke v. LAION*: EU's First Decision on TDM

30 Article 25 of the 2019 CDSM emphasizes the minimum harmonizing nature of exceptions and limitations (E&Ls), meaning that Member States may adopt a broader TDM exception than the one prescribed in the 2019 CDSM. Further, when the matter reaches the CJEU regarding the scope and interpretation of the TDM exception, it may be an opportunity to offer a wider meaning to the exception, as, for example, happened with exceptions under the 2001 Information Society Directive.[101] Meanwhile, the German national implementation of Articles 3 and 4, 2019 CDSM, recently reached the Hamburg regional court for interpretation and the Court's interpretation of Article 3, along with *obiter dicta* regarding Article 4, seem to indicate the direction of one such flexible interpretation. Articles 3 and 4, 2019 CDSM, alongside other provisions of the said directive, were to be transposed by the EU Member States in their national legislation by 7 June 2021. Germany also transposed the said provisions into its Copyright Act, Urheberrechtsgesetz (UrhG). Section 60d UrhG is the German equivalent of Article 3,

2025.

95 Article 2(2), 2019 CDSM.

96 Uri Gal, 'ChatGPT is a data privacy nightmare. If you've posted online, you ought to be concerned' *The Conversation* (Online 10 February 2023) <https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283> accessed 27 July 2025.

97 *Ibid.*

98 See Tyagi (2024), *supra* note 87, pp.9-11; Rosati (2024), *supra* note 94, pp. 2,6-9 on the scope of Articles 3 and 4, 2019 CDSM.

99 Rossana Ducato and Alain Strowel, 'Ensuring Text and Data Mining: Remaining Issues with the EU Copyright Exceptions and Possible Ways Out' (2021) *European Intellectual Property Review* 43 (5) p.11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278901> accessed 27 July 2025.

100 *Ibid.*, at pp. 14-15.

101 Christophe Geiger and Bernd Justin Jütte 'Designing Digital Constitutionalism: Copyright Exceptions and Limitations as a Regulatory Framework for Media Freedom and the Right to Information Online' in Martin Senftleben et al. (eds) *Cambridge Handbook of Media Law and Policy in Europe* (Cambridge University Press, Forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4548510> accessed 27 July 2025. It may be interesting to follow the developments in Like Company v Google, C-250/25, a request for preliminary ruling on the scope and interpretation of Articles 4 and 15 of the 2019, CDSM, currently pending before the CJEU.

2019 CDSM and permits TDM for non-commercial scientific research purposes undertaken by research organizations such as universities and cultural heritage institutions. Section 44b UrhG implements Article 4, 2019 CDSM, which allows commercial TDM by private enterprises.

31 In its decision in *Robert Kneschke v. LAION*, dated 27 September 2024, the German Regional Court of Hamburg (Landgericht) offered an interpretation of the scope of Section 60d UrhG. The case offers clarity on an important issue, namely whether 'AI data scrapping' can qualify as TDM.[102] It may be useful to add that the choice of Section 60d, and not 44b, made a significant impact in determining the outcome of the case. The Court also discussed the scope of Section 44a UrhG, which transposes Article 5(1) of the 2001 Information Society Directive, which covers only temporary and transient acts of reproduction, and is the only mandatory E&L in the 2001 Information Society Directive. However, the said section was found inapplicable in light of the scope of the right covered in the case at hand. Common to all these copyright provisions covering the act of transient copyright (Article 5(1), 2001 InfoSoc Directive) and text and data mining (Articles 3 and 4, 2019 CDSM), is the prerequisite of lawful access, meaning that the user must have lawful access to the copyright-protected works. This is an important fundamental pre-requisite that also impacts whether the process of generating synthetic data, and synthetic data itself, may infringe copyright, an issue developed in Section 5.2 *infra.*

32 The facts in *Robert Kneschke v. LAION* may be briefly described as follows. LAION (Large-scale Artificial Intelligence Open Network), a German-registered not-for-profit firm, created a LAION-5B training dataset, comprising '5.85 billion database-filtered image-text pairs' that it then made available without any access restrictions on its website.[103] The database, available for free on the website, did not contain any images. It only included image descriptions and hyperlinks to the image sources at the time of the creation of the database.

33 Robert Kneschke, the Plaintiff, claimed that LAION had infringed his copyright by scraping his photographs from a stock photo website, bigstock.com. Photographs can be protected as works if they are original, that is, have the 'author's personal touch' [104] or otherwise, under Article 6 of the Term of Protection Directive[105]. The 'image was freely available without a paywall' on the said website.[106] LAION copied only the watermarked versions of Kneschke's photographs that were freely accessible.[107]

34 The Court dismissed Kneschke's cease-and-desist request because, in the Court's opinion, LAION, being a not-for-profit firm, could benefit from the scientific research exception for TDM (Section 60d UrhG, equivalent EU provision Article 4, 2019 CDSM). Kneschke also alleged that LAION received funding from for-profit firms, and that the output of the TDM process, namely the dataset, was used by commercial for-profit firms. The Court, however, was of the opinion that the fact that two LAION members also worked for commercial firms, such as Stability AI, or that Stability AI contributed to financing the LAION-5B dataset, did not automatically translate into 'preferential access [by private enterprises, such as Stability AI] to the findings of LAION's scientific research'.[108] The Court found that non-profit entities such as LAION and Common Crawl contribute to decoding the black box of the data on which GenAI models are trained, how they work, and develop datasets that can then be used by commercial developers.[109] The Court dismissed the profit-driven

102 Ronak Kalhor-Witzel, 'German Court Says Non-Commercial AI Training Data Meets Scientific Research Exception to Copyright Infringement' *IP WatchDog* (Online 10 October 2024) <https://ipwatchdog.com/2024/10/10/german-court-non-commercial-ai-training-data-meets-scientific-research-exception-copyright-infringement/id=182008/#> accessed 27 July 2025.

103 Kristina Ehle and Yeşim Tüzün, 'To Scrape or Not to Scrape? First Court Decision on the EU Copyright Exception for Text and Data Mining in Germany' *Morrison Foerster: Client Alert* (Online 4 October 2024) <https://www.mofo.com/resources/insights/241004-to-scrape-or-not-to-scrape-first-court-decision> accessed 27 July 2025.

104 Case C-145/10 *Eva Maria Painer v. Standard VerlagsGmbH and Others*, paras 87-88.

105 Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006L0116
Article 6, Protection of photographs 'Photographs which are original in the sense that they are the author's own intellectual creation shall be protected in accordance with Article 1. No other criteria shall be applied to determine their eligibility for protection. Member States may provide for the protection of other photographs.'

106 Paul Keller, 'Machine readable or not? – notes on the hearing in LAION e.v. vs Kneschke' *Kluwer Copyright* (Online 22 July 2024) <https://copyrightblog.kluweriplaw.com/2024/07/22/machine-readable-or-not-notes-on-the-hearing-in-laion-e-v-vs-kneschke/> accessed 27 July 2025.

107 Ehle and Tüzün (Online 4 October 2024), *supra* note 103.

108 Mirko Brüß, 'German court finds LAION's copying of images non-infringing' *IPKat* (Online 28 September 2024) <https://ipkitten.blogspot.com/2024/09/guest-post-german-court-finds-laions.html> accessed 27 July 2025.

109 Paul Keller, 'LAION vs Kneschke: Building public datasets is covered by the TDM exception' *COMMUNIA* (Online 11 October 2024) <https://communia-association.org/2024/10/11/laion-vs-kneschke-building-public-

nature of LAION on the grounds that the dataset was made 'freely available to the public' and that subsequent commercialization by another for-profit firm 'is irrelevant for [the] assessment under Section 60d(2) UrhG'.[110] Moreover, the Plaintiff, in the Court's opinion, could not establish that these commercial firms exercised 'a decisive influence' or had 'preferential access to the findings of [LAION's] scientific research'.[111]

35 The decision of the Hamburg court was soon subject to criticism for choosing the wrong legal basis. As the dataset offered only hyperlinks made available following the completion of the TDM activity, Rosati is of the opinion that the issue should have been properly dealt with under Articles 2 and 3, 2001 Information Society Directive.[112] Article 3, 2019 CDSM covers only TDM and not the acts 'following the completion of TDM activities'.[113] In the case at hand, this follow-on act was that LAION made the dataset freely available on its website, without any access or usage restrictions. Prof. Rosati explains how TDM is limited to certain economic rights as described within the scope of Articles 3 and 4, 2019 CDSM; however, the subsequent acts, such as the one in the present case, are not covered by these articles.[114] With the new dataset available on its website, LAION performed an act of communication and making available to the public. In a string of case law, starting with *Svensson*, and later *GS Media* and *VG Bild-Kunst*, the CJEU has stated that the 'link provider's own knowledge… even when the link in question [has been offered] for non-profit purposes' is relevant for a finding of infringement.[115] While Prof. Rosati's remarks merit detailed academic discussion, in light of their insightful awareness of the choice of the correct legal basis, the Hamburg court's decision, at least until the pending appeal is heard[116], remains a good legal precedent on web crawling for access to data to train GenAI models. Once trained using crawled data, these GenAI models also generate synthetic data based on the inputs from human-generated data. If such training from web-scraped data is exempted early on, then follow-on synthetic works may have minimal realistic chances of being caught by copyright infringement rules.

36 Interestingly, the Hamburg Court did not stop there. It went a step further and also elaborated on the scope of the opt-out for machine learning in light of the provisions of the AI Act.

2. Article 53(1)(c), EU AI Act and Article 4(3), 2019 CDSM

37 Article 4(3) of the 2019 CDSM permits rightholders to opt out their copyright-protected works and prevent AI model developers from using their works for training purposes. In *Robert Kneschke v. LAION*, as bigstock.com's terms of service restricted use of automated programs, the Hamburg court found this to be a clear communication of an opt-out for the purposes of Article 4(3), 2019 CDSM. The difference in the opinion of the Plaintiff and the Defendant can be summarized as follows. Kneschke argued that 'digital plain text [being] sufficiently readable' sufficed to express an opt-out, whereas LAION argued that 'to be considered machine readable, an opt-out should be provided in a specific standardized format (in this case, robots.txt) that can be easily understood by crawlers and other bots'.[117] The Hamburg court assessed the facts of the case in light of the provisions of Article 53(1)(c), EU AI Act, which suggests that opt-outs may be exercised in light of the available state-of-the-art technology, and opined that a liberal approach should be taken as regards the machine readability of an opt-out by the rightholder. Furthermore, the Court was of the opinion that as natural language processing tools advance, an opt-out in 'words,' such as the one made by Mr Kneschke may suffice to meet the requirements of Section 44b UrhG. This observation resonates with the discussion in section 2 *supra,* which illustrates how GenAI models, starting with BERT, can bidirectionally read text and therefore contextualise linguistic content. The approach suggested by the Court to the reading of opt-outs during crawling is a rightholder-friendly one. Considering the rapid pace of technological advancements, the question is: what should be the relevant time frame that serves as a benchmark to

datasets-is-covered-by-the-tdm-exception/> accessed 27 July 2025.

110 Simon Hembt, Niels Lutzhöft and Toby Bond, 'Long-awaited German judgment by the District Court of Hamburg (Kneschke v. LAION) on the text and data mining exception(s)' *Bird & Bird* (Online 1 October 2024) <https://www.twobirds.com/en/insights/2024/germany/long-awaited-german-judgment-by-the-district-court-of-hamburg-kneschke-v-laion> accessed 27 July 2025.

111 Ehle and Tüzün (4 October 2024), *supra* note 103.

112 Eleonora Rosati, 'The German LAION decision: A problematic understanding of the scope of the TDM copyright exceptions and the transition from TDM to AI training' *IP Kat* (Online 7 October 2024) <https://ipkitten.blogspot.com/2024/10/the-german-laion-decision-problematic.html> accessed 27 July 2025.

113 *Ibid.*

114 Rosati (June 2025), *supra* note 94, p. 612.

115 Rosati (2024), *supra* note 112.

116 The decision has been appealed before a higher court. CEPIC 'CEPIC supports Robert Kneschke in his copyright lawsuit against LAION and welcomes the appeal' <https://www.cepic.org/post/cepic-supports-robert-kneschke-in-his-copyright-lawsuit-against-laion-and-welcomes-the-appeal> accessed 27 July 2025.

117 Keller (22 July 2024), *supra* note 106.

assess infringement? In *LAION*, the Hamburg Court took into account the state of the technology at the time of the decision (by which point ChatGPT had already been released) and not the technology in use around 2022, when LAION crawled the website to scrape data.[118] However, as the case was decided under Article 3, and not Article 4, the opinion of the Court as regards the format of the opt-out under Article 4 is *obiter dicta,* and the issue remains unresolved. The Hamburg court's *obiter dicta* may serve as a useful reference point for the AI Office to clarify the provisions of Article 53 of the 2024 EU AIA. Another related issue is whether there should be a harmonized and recognized legal standard, such as in the form of 'robots.txt', to standardize web instructions for crawlers.[119] Traditionally, robots.txt has been a *de facto* accepted standard to prevent crawling of a given website. Robots.txt files, usually located at 'websiteaddress.com/robots.txt' are like notices at the door entrance, indicating who is permitted, or restrained, from entering the room. Robots.txt has been a *de facto* web standard for decades, whereby robots (also known as crawlers, worms, or web crawlers) of search engines took it as a signal as to whether they were permitted to crawl a given website.[120] Until the advent of GenAI, there was a *quid pro quo* between websites and Google, whereby Google could crawl and index these websites and display them in the search results.[121] Websites benefitted from appearing in the search results, and crawling was thus seen to bring benefits for both the website and the search engines.[122] With the advent of GenAI, however, it turned against even the interests of formerly robot.txt compliant firms like Google to conform to the instructions on the entrance door, namely the 'robots.txt', of the website. Presently, not only do Google, and GenAI firms, crawl through these webpages, but they also fail to offer any credit to the website owners for content extracted from their pages.[123] In this respect, the Hamburg Court's *obiter dicta* on opt-outs under Article 4(3), 2019 CDSM, in *Robert Kneschke v. LAION* become relevant.[124] Notably, the Court's opinion that advanced GenAI can understand text in plain human language, and therefore, such a communication of an opt-out should suffice for the purposes of Article 4(3) 2019 CDSM and AI Act is a positive development in line with the balancing of authors' rights vis-à-vis users' rights.

II. GenAI, Text and Data Mining and Synthetic Data: Infringing or non-Infringing?

38 Following the completion of text and data mining, GenAI tools generate data. GenAI tools, such as ChatGPT, accelerate the rate and quality of output generation.

39 To generate synthetic data using Deep Generative Models (DGM), data is a key input. This data, in turn, may have different components. Data, as discussed in Section 1 *supra*, can be of many different types, and may include 'unprotected data' such as raw data, or 'protected works of authorship and other protected subject matter'.[125] Copyright only protects expressions of works that are original. Article 2 of the Berne Convention offers an open-ended definition of works, and includes, 'literary and artistic works' in any mode or form of expression. Article 9(2) of the TRIPS agreement clearly brings out this copyright protection for expression in works that are original. This implies that 'unstructured raw data', such as 'mere facts and data "as such"' does not benefit from copyright protection.[126] To qualify for protection, these works must be original, and they must be an expression, and not a mere idea. Copyright 'subsists not in ideas, but in the form in which the ideas are expressed'.[127]

40 While there is no explicit reference to protection

118 Kalhor-Witzel (10 October 2024)), *supra* note 102.

119 Paul Keller and Zuzanna Warso, 'Defining Best Practices for Opting out of ML Training' *Open Future Policy Brief #5* (Online 29 September 2023) <https://openfuture.eu/wp-content/uploads/2023/09/Best-_practices_for_optout_ML_training.pdf> accessed 27 July 2025.

120 David Pierce 'The text file that runs the internet' *The Verge* (Online 14 February 2024) <https://www.theverge.com/24067997/robots-txt-ai-text-file-web-crawlers-spiders> accessed 27 July 2025.

121 *Ibid.*

122 This symbiotic relationship between websites and search engines, such as Google also draws a parallel with the relationship between press publishers and Google. In the press publishing industry as well, the emergence of GenAI seems to have altered the dynamics of the relationship. Cf Kalpana Tyagi, 'Generative AI, EU press publishers' rights & the Australian News Bargaining approach: Copyright & Competition law as enablers of media plurality & diversity of opinion' (Forthcoming, 2024, pre-print) *SSRN* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4933421> accessed 27 July 2025.

123 Pierce (14 February 2024), *supra* note 120.

124 Stepanka Havlikova, 'Technical Challenges of Rightholders' Opt-Out from Gen AI Training after Robert Kneschke v. LAION' (2025) *JIPITEC* 16(1) <https://www.jipitec.eu/jipitec/article/view/422> accessed 27 July 2025.

125 Thomas Margoni 'TDM and Generative AI: Lawful Access and opt-outs' *Auteurs & Media* (forthcoming, pre-print 2024) p. 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5036164> accessed 27 July 2025.

126 *Ibid.* p.7.

127 *Designers Guild Ltd. V. Russell William (Textiles) Ltd.* (2000) UKHL 58, (2011) 1 WLR 2416.

of 'collections of data' in the Berne Convention, however, Article 2(5) affords protection to 'collections of literary or artistic works', which offers the possibility for protection to the extent the collection is an 'intellectual creation'.[128] Different jurisdictions have different thresholds for originality. In the EU, the work is deemed original, if it is the author's own intellectual creation[129], in other words, if it carries the author's personal touch. Databases, when curated or arranged in such a manner that constitute 'the author's own intellectual creation' can also benefit from copyright protection.[130] In addition, Article 10(2) of the TRIPS offers Contracting Parties the possibility to offer protection to compilations of data by virtue of the investment made in the creation of databases or other similar material. It reads thus:

> *Compilations of data or other material, whether in machine readable or other form, which by reason of the selection of arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.*

41 This is the basis on which the EU offers a *sui generis* database right, wherein database are protected for the investment made in the creation and compilation of these database.[131] The Database Directive thus, offers copyright protection for compilations of data, and also offers a 'non-copyright, *sui generis* right in databases to protect the investment of the database maker'.[132] Substantial qualitative or quantitative extraction or reutilization of the database, can therefore, lead to the infringement of the *sui generis* database right.[133]

42 From the lens of copyright and related rights and *sui generis database rights*, unauthorized use of protected works, may mean that both the synthetic data and the system 'training on it' are infringing uses.[134] As the value chain of the data elongates, for example, when synthetic data is generated from human generated data, and further synthetic data is generated using varying proportions of human generated and synthetically-generated data, how does one know whether human-generated data has been used in the GenAI value chain for the generation of this synthetic output? If the synthetically generated data is similar, or bears resemblance to the human generated-data, then it may be possible to assess this through infringement tests, and by showing similarity between the human-generated data that may have been used to train the GenAI model to produce this synthetic output, infringement can be ascertained. This is also a key issue in the ongoing GenAI-related cases. In the Authors Guild/OpenAI case for instance, the Plaintiff, Authors Guild offers examples of how ChatGPT can offer precise summaries and excerpts from copyright-protected works.[135] In the case at hand, ChatGPT could not only accurately summarize the works of authors such as John Grisham, it could also create follow-on works. For example, ChatGPT offered a realistic follow-on novel to the Grisham's famous work, 'The King of Torts' and offered it an equally plausible title, namely 'The Kingdom of Consequences'.[136] While these outputs, in this case, 'The Kingdom of Consequences', may be closer to the original human-generated works, and hence, easier to be identified as infringing, how does one determine infringement, when the GenAI tools offer follow-on works, that are generated based on the synthetically-generated works, and that the human author may have likely created himself? In other words, what happens when synthetic data is used to generate successive generations of synthetic data?

128 Sam Ricketson and Jane C. Ginsburg, *International Copyright and Neighbouring Rights: The Berne Convention and Beyond* (3rd edition, Oxford University Press 2022) pp. 489-490.

129 Case C-5/08 *Infopaq International A/S v Dansk Dagblads Forening*, paras 37, 45, 47.

130 Article 3(1), Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive) OJ 1996 L 77.

131 Case C 203/02 *British Horseracing Board v. William Hill Organisation Ltd*, para 31 usw; Case C-338/02 *Fixtures Marketing Ltd. V. Svenska Spel AB*, paras 24-29.

132 Daniel J. Gervais, 'The Protection of Databases' (2007) 82 *Chicago-Kent Law Review* p. 1120 <https://scholarship.law.vanderbilt.edu/faculty-publications/839/> accessed 27 July 2025; Estelle Derclaye, (2002) 'What is a Database? A Critical Analysis of the Definition of a Database in the European Database Directive and Suggestions for an International Definition' 5 *Journal of World Intellectual Property* p. 981 <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1747-1796.2002.tb00189.x> accessed 27 July 2025.

133 Gervais (2007), *supra* note 132, p.1123.

134 Lee (2024), *supra* note 38, p. 24.

135 For a discussion on the future of work in an age of generative AI in creative industries, see discussion on Authors Guild v. OpenAI (Complaint filed on 19 September 2023) No. 1:23-cv-8292, Kalpana Tyagi 'Redefining a Normative Framework for Meritocracy in the Era of Generative AI: An Inter-Disciplinary Perspective' in Klaus Mathis and Avishalam Tor (eds), *Law and Economics of Justice: Efficiency, Reciprocity and Meritocracy* (Springer 2024) <https://www.springerprofessional.de/en/redefining-a-normative-framework-for-meritocracy-in-the-era-of-g/27041164> accessed 27 July 2025.

136 See discussion on Authors Guild v. OpenAI (Complaint filed on 19 September 2023) No. 1:23-cv-8292 in Kalpana Tyagi 'Redefining a Normative Framework for Meritocracy in the Era of Generative AI: An Inter-Disciplinary Perspective' in Klaus Mathis and Avishalam Tor (eds), *Law and Economics of Justice: Efficiency, Reciprocity and Meritocracy* (Springer 2024) <https://www.springerprofessional.de/en/redefining-a-normative-framework-for-meritocracy-in-the-era-of-g/27041164> accessed 27 July 2025.

This may be particularly true for fiction and art-based works, whereby 'hallucination'[137], abstraction and 'creativity' are closely intertwined. This is distinct from scientific facts and assertions, which may at least, relatively speaking, be easier to identify and are grounded in research. The original human-generated data becomes sequentially distanced from the GenAI value chain, making it increasingly difficult to establish infringement. It may be even more difficult to impose liability in the US, where the GenAI developers are likely to benefit from the 'transformativeness' test, included in the four-factor fair use test.[138] Even if the models simply extend and correlate 'specific memorized examples within the training data, the output will only infringe if enough original expression of any particular example were evident in the final product'.[139] Article 53(1)(d) 2024 EU AI Act offers an important safeguard as it suggests that the providers of general-purpose AI models shall

> *draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.*

43 Article 53(1)(d) of the Act thereby requires transparency regarding the data used to train the General-Purpose AI (GPAI) models. This includes datasets and data sources that are protected not only by copyright, but also by other legal frameworks, such as data protection laws, discussed below. Notably, as regards synthetic data, Warso, Gahntz and Keller offer a valuable proposition for the implementation of Article 53(1)(d). In the AI transparency blueprint, the authors suggest a detailed plan as regards datasets that must be mentioned, and how they can be sufficiently described. The authors also suggest that Article 53(1)(d) can be used to request information on synthetically generated data by the model provider, including the time of generation and methods used to create the synthetic output.[140] In its recent guidance, the EU Commission does seem to follow this approach, as the template also offers a section to include details about the use of synthetic data to train the model.[141]

44 Reference to not only human-generated works and datasets, but also to synthetic datasets, within the possibilities offered by the 2024 EU AIA, will, in the author's opinion, make the Act even more human-centric. Thus, the relationship between the AI Act, GenAI and copyright is a very special one[142], which can be positively leveraged to bring to the surface the human element within the 2024 EU AI Act. This can be attributed to the inherent nature of these two fields of law: whereas the AI Act is public law; copyright, like other IPRs, is private law. While obligations under the AI Act are monitored by the AI Office, a part of the European Commission, breach of copyright is subject to private enforcement by copyright holders.[143] Interestingly, as the above-suggested blueprint indicates, provisions of the 2024 EU AIA can be effectively deployed to remunerate the human author, even when the output is derived from synthetically-generated data. Remuneration of the human author, alongside text and data mining, are, generally speaking, two of the key concerns as regards training of generative AI models.[144] Article 17 of the Charter of Fundamental Rights (CFR) refers to the right to property. Notably, Article 17(2) explicitly refers to protection of intellectual property. The other relevant right, particularly in the context of copyright and related rights, is the right to freedom of expression. The discussion on fundamental rights is gaining prominence in the intellectual property discourse, and has led to the constitutionalisation of intellectual property rights. In *Poland v. Parliament*, Poland challenged the new liability regime against online content sharing service providers under Article 17, 2019 CDSM on the grounds it violated the principles enshrined in the CFR.[145] The Court was of

137 Hallucination is a frequently cited limitation of GenAI. Cf Boxin Wang, Weixin Chen, Hengzhi Pei, Chulin Xie, Mintong Kang, Chenhui Zhang, Chenjian Xu, Zidi Xiong, Ritik Dutta, Rylan Schaeffer, Sang T. Truong, Simran Arora, Mantas Mazeika, Dan Hendrycks, Zinan Lin, Yu Cheng, Sanmi Koyejo, Dawn Song and Bo Li, 'Decoding Trust: A Comprehensive Assessment of Trustworthiness in GPT Models' (20 June 2023) *NeurIPS 2023 Outstanding Paper* pp. 6,11 <https://arxiv.org/abs/2306.11698> accessed 27 July 2025.

138 Cf Andrea Bartz v. Antropic (2025), *supra* note 7.

139 Matthew Sag, 'Copyright Safety for Generative AI' (2023) *Houston Law Review* 61(2) p. 312, 322 <https://houstonlawreview.org/article/92126-copyright-safety-for-generative-ai> accessed 27 July 2025.

140 Zuzanna Warso, Maximilian Gahntz and Paul Keller, 'Blueprint of the template for the summary of content used to train general-purpose AI models (Article 53(1)d AIA) – v.2.0' (2024) *Open Future Foundation* p. 2 <https://openfuture.eu/wp-content/uploads/2024/09/240919AIAtransparency_template_requirements-blueprint_v.2.0.pdf> accessed 27 July 2025.

141 European Commission (24 July 2025), *supra* note 47.

142 Quintais (2025), *supra* note 46, pp. 7-8.

143 *Ibid.*

144 Kalpana Tyagi, 'Generative AI: Remunerating the human author & the limits of a narrow TDM Exception' (13 December 2023) *Kluwer Copyright Blog* <https://copyrightblog.kluweriplaw.com/2023/12/13/generative-ai-remunerating-the-human-author-the-limits-of-a-narrow-tdm-exception/> accessed 27 July 2025.

145 Maria Alexandra Mărginean, *Republic of Poland v. European Parliament and Council of the European Union: Balancing Freedom of Expression with the Filtering Obligations of Article 17 of the DSM Directive* (Bachelor Thesis, Maastricht University 2022); Adrien Dubois, *A comparative analysis of Article 17 CDSM national implementation and Poland v Commission's ECJ Framework* (Master Thesis, Maastricht University 2022).

the opinion that when there are multiple possible interpretations, the one that best complies with fundamental rights should be preferred.[146]

45 Considering the use of human-generated works in the training of GenAI models, copyright scholars have consistently called for a framework to adequately remunerate the human author.[147] Prof. Senftleben, for instance, presents an interesting proposal that a levy, 'an AI levy' can be imposed on GenAI systems that produce literary and artistic outputs.[148] Article 53(1)(d) of the EU AIA 2024, can serve as a useful complement to author remuneration, and to make this effort coherent and effective, Prof. Senftleben's suggestion for an 'AI levy' could provide the required revenues, which may then be equitably and proportionately distributed amongst rightholders.

46 Thus, transparency as regards datasets, under Article 53(1)(d) the EU AIA 2024, will also go a long way in safeguarding the authors' rights. With a requirement that datasets not only refer to human-generated works and other data (including personal data), but also to synthetically-generated data, as mentioned above, identifying the human author, even when high up in the data value chain, can serve as a useful complement for legal enforcement and timely, adequate, and proportionate remuneration of the human author. As a balancing and proportional framework, the rules may prescribe a proportional remuneration for the human author, based on how closely they can be linked in the value chain to the output generated.

47 In addition to copyright and the human author, the 2024 EU AI Act and the EU CFR also connect with personal data protection, that is palpably grounded in the right to privacy and data protection, an issue that we turn to next.

D. Data Protection and Privacy: Promises and Concerns

48 The 2016 GDPR is triggered when the processing of personal data is involved. The EU Data laws clearly specify that unless otherwise specified, the 'provisions are "without prejudice" to … personal data protection and intellectual property rights [except for *sui generis* database rights]'.[149] Sub-section 4.1 highlights the fundamental rights-driven nature of the GDPR. Sub-section 4.2 assesses how and when the GDPR is triggered while developing the GenAI models, and what safeguards in the 2024 EU AI Act are relevant thereto. Sub-section 4.3 assesses whether synthetic data can help effectively comply with the principles of data protection. From an innovation perspective, synthetic data can play a pertinent role as training GenAI models requires deep learning, and once learnt, it may be subsequently difficult (or perhaps even impossible) for data subjects to exercise their individual rights, such as the right of erasure and portability.

I. The Fundamental Rights-Driven Nature of the GDPR

49 The GDPR concerns personal data and is grounded in respect for fundamental rights.[150] This is clear from the

Copy available with the author upon request.

146 Case C-401/19 *Poland v European Parliament and Council*, Judgment of the Court (Grand Chamber) 26 April 2-22, EU:C:2022:297.

147 Cf Christophe Geiger and Vincenzo Iaia, 'Generative AI, Digital Constitutionalism and Copyright: Towards a Statutory Remuneration Right grounded in Fundamental Rights – Part 1' (17 October 2023) *Kluwer Copyright Blog* <https://legalblogs.wolterskluwer.com/copyright-blog/generative-ai-digital-constitutionalism-and-copyright-towards-a-statutory-remuneration-right-grounded-in-fundamental-rights-part-1/> accessed 27 July 2025; Christophe Geiger and Vincenzo Iaia, 'Generative AI, Digital Constitutionalism and Copyright: Towards a Statutory Remuneration Right grounded in Fundamental Rights – Part 2' (19 October 2023) *Kluwer Copyright Blog* <https://legalblogs.wolterskluwer.com/copyright-blog/generative-ai-digital-constitutionalism-and-copyright-towards-a-statutory-remuneration-right-grounded-in-fundamental-rights-part-2/> accessed 27 July 2025 and Martin Senftleben (2023) 'Generative AI and Author Remuneration' *International Review of Intellectual Property and Competition Law* Vol. 54 <https://link.springer.com/article/10.1007/s40319-023-01399-4> accessed 27 July 2025.

148 Senftleben (2023), *supra* note 147; Martin Senftleben (2022) 'A Tax on Machines for the Purpose of Giving Bounty to the Dethroned Human Author – Towards an AI Levy for the Substitution of Literary and Artistic Works' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123309> accessed 27 July 2025.

149 Margoni, Ducuing and Shirru (2023), *supra* note 24, p. 9.

150 David Erdos, 'Comparing Constitutional Privacy and Data Protection Rights within the EU' (2021) *University of Cambridge Faculty of Law Research Paper No. 21/2021* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843653> accessed 27 July 2025; Maximilian von Grafenstein 'Redfining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risk through (Not to) Article 8 ECFR against Other Fundamental Rights' (2021) *European Data Protection Law Review*6(4) p. 516 <https://doi.org/10.21552/edpl/2020/4/7> accessed 27 July 2025; Max van Grafenstein, *The Principle of Purpose Limitation: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation* (Nomos 2018) <https://www.nomos-elibrary.de/de/10.5771/9783845290843/the-principle-of-purpose-

recitals to the GDPR that underline the fundamental rights as the foundation of the Regulation.[151] Personal data concerns any data 'relating to an identified or identifiable' natural person, also referred to as the data subject.[152] The CJEU case law has clearly established the fundamental rights-driven approach of the GDPR on several occasions. The respect for the protection of personal data is referred to in Article 16(1) of the TFEU and Article 8(1) of the EU Charter of Fundamental Rights (CFR).[153] Article 7 of the EU CFR also refers to the right to respect for personal life. Even though neither the European Convention on Human Rights nor the national constitutions of many EU Member States explicitly refer to a right to data protection, they do refer to the freedom of expression (Article 10) and right to respect for private and family life (Article 8) of the European Convention on Human Rights, and that any derogations thereto, must meet the principle of proportionality.[154] The EU courts have on several occasions underlined the need for personal data processing to be compliant with the foundational principles in Article 8 of the EU CFR, as the use of personal data evokes data protection laws.[155] From the lens of 'human rights law', GDPR 'functions as a justificatory regime' to facilitate 'proportionate' data processing, by offering 'safeguards to ensure' that processing does not transgress 'beyond what is necessary'.[156]

50 From a fundamental rights perspective, a distinction is drawn between the right to privacy and the right to data protection.[157] Following an empirical assessment of the evolution of privacy and data protection laws across EU Member States, Prof. Erdos suggests how the parallel emergence of these rights 'confirms the close and even symbiotic relationship' between data protection and privacy rights.[158] It emerges that data protection, while 'a novel and mercurial phenomenon'[159] has 'roots' in privacy, a thread that becomes clearer while looking at 'EU States which have recognised privacy but *not* data protection as a constitutional fundamental' right.[160] This interplay is also evident as one looks at the ePrivacy rules. For example, the rules on the protection of personal data – such as content, traffic and location data – in the ePrivacy Directive are far more granular than in the GDPR.[161] However, the EDPS and the Article 29 Working Party (WP29) have a different opinion, namely that the GDPR concerns personal data, whereas the ePrivacy rule also 'additionally protect[-s] the confidentiality of electronic communications, as well as the integrity of one's device'.[162] What remains clear though is the distinct, but inter-related nature of data protection and privacy. From the lens of synthetic data, the concerns are two-fold – first, whether the training of GenAI models triggers GDPR, as it involves processing of personal data (section 4.2); and second, if so, whether synthetic datasets can help comply with the GDPR, considering that it may be practically infeasible for GenAI models to unlearn following deep learning from the datasets (sub-section 4.3).

II. Does GenAI Trigger GDPR, as it Crawls and Processes Data for Training Purposes?

51 Big data driven processes, such as GenAI, process personal data and are therefore subject to the GDPR. In the digital economy, when every physical aspect of our activity can be mapped on a digital device, scholars, such as Prof. Purtova, have referred to data protection as the 'law of everything'.[163] Consider,

limitation-in-data-protection-laws> accessed 27 July 2025.

151 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), recitals 1, 4, and 51.

152 Article 4(1), GDPR.

153 Charter of Fundamental Rights of the European Union OJ 2010/C83/389.

154 David Erdos, 'European Union Data Protection Law and Media Expression: Fundamentally Off-balance' (January 2016) *International & Comparative Law Quarterly* 65(1) p. 145 <https://doi.org/10.1017/S0020589315000512> accessed 27 July 2025.

155 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd. and Seitlinger and others* EU:C:2014:238, paras 36, 37.

156 Orla Lynskey (2023) 'Complete and Effective Data Protection' *Current Legal Problems* 76 (1) p. 301 <https://doi.org/10.1093/clp/cuad009> accessed 27 July 2025.

157 Erdos (May 2021), *supra* note 150, pp. 1-2.

158 *See ibid* p. 3, pp. 16-19 23 for the National provisions on the general right to privacy (or broad equivalent) across EU Member States and pp. 22-23 for the National provisions on the right to data protection across EU Member States.

159 *Ibid.,* p. 31.

160 *Ibid.*, p. 27, 31.

161 Rosa Barcelo 'The ePrivacy Directive: then and now' in Brendan Van Alsenoy, Julia Hodder, Fenneke Buskermolen, Miriam Čakurdová, Ilektra Makraki and Estelle Burgot (eds) *Two decades of personal data protection. What next? EDPS 20th Anniversary* (European Data Protection Supervisor: Publication Office of the European Union 2024) pp. 49-50 <https://www.edps.europa.eu/data-protection/our-work/publications/book/2024-06-20-two-decades-personal-data-protection-whats-next_en> accessed 27 July 2025.

162 For a discussion on the EDPS and Article 29 Working Party and the European Commission's opinion on the interplay between right to privacy and data protection *see ibid*, pp. 50-51.

163 Nadezhda Purtova 'The Law of Everything. Broad concept

for example, a daily activity, such as shopping for groceries in the supermarket. If one may not be familiar with the local area, the shopper will first look on the internet for nearby markets, followed by the use of a navigation app to go to the nearby supermarket. The physical footprint of the user thus will also be present in the form of a digital map.

52 As GenAI uses publicly available data, from the lens of GDPR, the key concern is whether they have a valid legal basis to undertake such processing activities.[164] The Italian Data Protection Authority (DPA) was amongst the first authorities to initiate an action against ChatGPT for non-compliance with the principles of the GDPR. In 2023, ChatGPT was seen as non-compliant with the requirement for a valid legal basis, required for processing personal data, by the Italian DPA. To be GDPR compliant, the processor must have a valid legal basis to comply with the 'lawfulness principles' prescribed in Article 5(1)(a) GDPR. The Italian DPA initially banned ChatGPT, requiring amongst others 'to change the legal basis of the processing of users' personal data'.[165] To comply with the Italian DPA, OpenAI changed its privacy policy across the EU and the EFTA, and expressed its legitimate interest in 'developing, improving, or promoting' its services, including the training of its models.[166] This change of legal basis only addresses the concern with the users of ChatGPT. The question is much larger – on what legal basis do the GenAI models, and ChatGPT in particular, process the personal data of the internet users at large? The EDPS addressed this aspect in its recent opinion, and its suggestion seems aligned with the Italian DPA's decision. The EDPS opined that GenAI model providers may rely on 'legitimate interest... [especially] with regard to the collection of data', as well as for 'training and validation purposes'.[167]

53 GenAI tools process data to offer meaningful outputs. In an earlier article, I describe how GenAI models contextualize, iterate, and improvise information to generate new works. In addition to the data derived from IP (copyright) protected works, this processing may also involve personal data. Considering that Article 4(2), GDPR offers a very broad meaning to processing, even when GenAI does not copy, store or retain data (whether obtained by web crawling or through other sources) in its database, in the initial training phase at least, GenAI tools do tend to process personal data within the meaning of GDPR. Such an interpretation is aligned with landmark decisions such as *Google Spain*, as also the more recent opinion by the EDPS. In *Google Spain*, the data subject appeared in Google's search results, which offered links to webpages providing data on how the data subject had formerly been involved in a bankruptcy auction. As this step was identified as processing, the CJEU was of the opinion that Google, as the data controller (and also the processor in the case at hand), must ensure compliance with the data subject's rights, including but not limited to the right to removal of the bankruptcy related data from the search results.[168] In the said case, compliance with the data subject's request for erasure was much simpler. However, how does one facilitate compliance with such personal rights under the GDPR in the context of GenAI models that are based on deep learning? To comply with the request, the model may be required to unlearn, a cost that may be disproportionate, and may practically speaking even impossible, particularly in light of the black box nature of these GenAI models.

54 Another important and related question is the duration for which the personal data collected may be stored. In *Schrems*, the Court opined that an unlimited duration may seem intrusive as it may offer an impression of continuous monitoring of the personal life of the data subject.[169]

55 What happens when GenAI systems return incorrect

of personal data and future of EU data protection law' (2018) *Law, Information and Technology* 10 (1) <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 27 July 2025.

164 Taner Kuru (2024) 'Lawfulness of the mass producing of publicly accessible online data to train large language models' *International Data Privacy Law* 14(4) p. 330 <https://academic.oup.com/idpl/article/14/4/326/7816718> accessed 27 July 2025.

165 Garante per la protezione dei dati personali (GDDP), Provvedimento dell'11 aprile 2023 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702> accessed 27 July 2025.

166 Kuru (2024), *supra* note 164, p. 332. See also the references therein.

167 European Data Protection Supervisor, 'Generative AI and the EUGDPR: First EDPS Orientations for ensuring data protection compliance when using Generative AI systems' (3 June 2024) p. 13 <https://www.edps.europa.eu/system/files/2024-05/24-05-29_genai_orientations_en_0.pdf> accessed 27 July 2025.

168 David Erdos, 'Generative AI, Search Engines and GDPR' (15 January 2024) slide 2 <https://www.slideshare.net/slideshow/generative-ai-search-engines-and-gdpr/265438456#1> accessed 27 July 2025. Prof. Erdos maps the search indexing and European Data Protection (EDP) timeline and identifies the following four phases. In phase 1, between mid-1980s and mid-1990s, the EDP identified certain concerns and mildly regulated the news archive searches; phase 2, lasting between late-1990s and 2000s, whereby search engines were seen as 'out of reach' and focus remained on limiting exposure; third phase starting 2007-08, whereby the Spanish DPA identified search engines as ex-post controllers and the fourth phase starting 2014-present, with CJEU's Google Spain as a precedent.

169 C-446/21 *Maximillian Schrems v. Meta Platforms Ireland Ltd.*, ECLI:EU:C:2024:834, paras 58, 60, 62.

results when presented with questions about the data subjects? GenAI output is synthetic. In addition, this synthetic output often gives incorrect information. When this information, correct or incorrect, identifies or can identify a person, it involves personal data and is covered by the GDPR. Can factual incorrectness of information cause prejudice, and can it be covered by the GDPR? As referred to in section 3 *supra,* GenAI models tend to hallucinate which may lead to offering false information, including personal data by these models. In case of inaccurate or false results, GenAI models may be found in breach of the principle of data accuracy as required under Article 4(1)(d), 2016 EU GDPR. To avert such an inaccurate outcome, data accuracy must be assured 'throughout the whole lifecycle of the generative AI systems'.[170] Simply put, accuracy should not be ascertained at the output stage, rather, in light of the black box nature of these deep learning models, the GenAI model developer should be able to ensure accuracy from the input to the output stage of the model.

56 The scope of the term 'personal data' gains significance, as GenAI models, a sub-field of AI, deal with 'multi-layered AI models where each layer performs a specific task of input data analysis or manipulation' and the process goes on in a loop for the GenAI model to improvise itself with each successive iteration.[171] As data goes from one layer to the next in this multi-layered processing, in practice, 'it may be burdensome, or even impossible to trace exactly what behaviour was learned based on' the data subject's personal data.[172] This leads to practical challenges as regards the exercise of individual rights of the data subjects, such as the right of access, rectification, erasure and objection to the processing of personal data prescribed in Chapter III of the EU GDPR.[173] Consider for example, the right to erasure under Article 17 of the GDPR, particularly when the data subject may have initially offered their consent for processing, but withdrew it subsequently. In such a scenario, it may be difficult to exercise the right of erasure, 'as the actual using of that data persists throughout the operation' of the GenAI model.[174] Considering that the exercise of these individual rights may disproportionately 'impact the effectiveness of the model', the CJEU's recent opinion in *Meta v. Bundeskartellamt*, discussed below, may offer a useful benchmark to proportionately balance the distinct fundamental rights (the right of the data controller vis-à-vis that of the data subject). In addition, the 2024 EU AI Act's requirement for detailed information on datasets used to train the GenAI model, may enhance transparency and help decode the GenAI black box.

57 In *Meta v. Bundeskartellamt*, Meta, the processor enjoyed a dominant position, and the question was whether the data subject could, in such a setting, offer free consent under Articles 6(1)(a) and 9(2)(a) GDPR for the processing of personal data.[175] The CJEU was of the opinion that in order to facilitate positive compliance with the requirements therein, three cumulative conditions must be met – first, the pursuit of a legitimate interest; second, the processing of personal data for this legitimate interest; and third, the interests or fundamental freedoms of the data subject do not overshadow the legitimate interests of the controller or a third party.[176]

58 Would the case of processing of sensitive personal data, manifestly made available by the data subject, for training GenAI models be different? To understand the scope and interpretation of Article 9(2)(e) GDPR, the recently decided Schrems case is insightful, whereby the CJEU was of the opinion that

> *'the fact that a person has made a statement about his or her sexual orientation on the occasion of a panel discussion open to the public does not authorize the operator of an online social network platform to process other data relating to that person's sexual orientation, obtained, as the case may be, outside that platform using partner third-party websites and apps, with a view to aggregating and analysing those data, in order to offer that person personalized advertising'.*[177]

59 Processing of personal data that can be deemed 'sensitive' is prohibited by Article 9(1) GDPR, unless the processor can benefit from the exceptions under Article 9(2) GDPR. This could be a better ground to make GenAI firms accountable, as the grounds therein are stricter, and the CJEU has offered 'a broad interpretation of what constitutes sensitive data'.[178]

170 European Data Protection Supervisor (3 June 2024), *supra* note 167, p. 15.

171 Aleksandr Kesa and Tanel Kerikmäe, 'Artificial Intelligence and the GDPR: Inevitable Nemeses?' (2020) *TalTech Journal of European Studies* 10(3) p. 70 <https://sciendo.com/article/10.1515/bjes-2020-0022> accessed 27 July 2025.

172 *Ibid.*

173 European Data Protection Supervisor (3 June 2024), *supra* note 167, p. 22.

174 Kesa and Kerikmäe (2020), *supra* note 171, p. 75.

175 For a discussion of the case from a competition law perspective, see Anne C. Witt (2024) 'Meta v Bundeskartellamt – data-based conduct between antitrust law and regulation' *Journal of Antitrust Enforcement* 12(2) <https://academic.oup.com/antitrust/article/12/2/345/7642048> accessed 27 July 2025.

176 Case C-252/21 *Meta v. Bundeskartellamt*, ECLI:EU:2023:537, para 106; C-597/19 *Microm International Content Management & Consulting (M.I.C.M.) Limited v. Telenet BVBA and others*, ECLI:EU:C:2021:492, para 106.

177 C-446/21 *Maximillian Schrems v. Meta Platforms Ireland Ltd.*, ECLI:EU:C:2024:834, paras 83-84

178 Kuru (2024), *supra* note 164, p. 335.

60 Crawling by GenAI FM developers should be identified as GDPR compliant only after they meaningfully filter sensitive personal data. Making a 'sensitive personal' announcement in a public forum, such as was the case in *Schrems*, does not necessarily mean that the data subject has made the personal data manifestly available under Article 9(2)(e) GDPR.[179]

III. Synthetic Data to Facilitate Compliance with the GDPR

61 The EU GDPR requires that data is processed in a 'lawful, fair and transparent' manner[180] and that the users have given clear consent for the collection and processing of personal data[181]. There are, however, clear gaps between the ideals of data protection and the practice of digital firms. An empirical survey identified how over 92 per cent of the most popular websites tracked users without notification and even when the users clearly opted-out, over 85 per cent of the websites continued to track its users.[182] These limits imposed by the GDPR are breached with even greater impunity by the GenAI model developers as they indiscriminately crawl the web for data. In this regard, can synthetic data, provided it complies with the safeguards of the A29 WP on anonymization techniques – such as singling out, linkability and inferences – facilitate compliance with data protection laws?

62 It may be trite to clarify that privacy is not the same as data protection. However, the fact that synthetic data successfully anonymizes data[183] ensures compliance with the GDPR. GDPR is driven by openness and control over one's data, as distinct from privacy that may require secrecy.[184]

63 With synthetic data as input, datasets may be fully synthetic (1); a part of it may be synthetic and a part human-generated (2) or it may be a combination of human generated, and synthetic data (3).[185] For synthetic data to be exempt from the provisions of Articles 6(1)(b) to 6(1)(f) of the GDPR, it must be sufficiently anonymized. Anonymization is not a shield from the requirement for compliance with the data protection laws. Anonymization is not the same as data protection. Complete anonymization may help evade the requirements under the GDPR, as successful anonymization means that data cannot be linked to a pre-identified individual.[186] In its most recent opinion, the EDPS opines thus[187]:

> *When a developer or a provider of a generative AI system claims that their system does not process personal data (for reasons such as the alleged use of anonymised datasets or synthetic data during its design, development and testing), it is crucial to ask about the specific controls that have been put in place to guarantee this.*

64 The data must be 'evaluated as anonymous, through a process of proven quality [whereby there is] reasonable evidence of impossibility of reidentification'.[188] When a given dataset is fully synthetic, in other words, it consist of fully anonymized data, such a dataset may qualify as pseudonymous or anonymized data under Article 4(5) of the GDPR, which defines pseudonymisation as follows:

> *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

65 Fully synthetic datasets (case 1) can help comply with data privacy and facilitate innovation through more collaborative data sharing.[189] It can help overcome constraints such as trade secrets and privacy regulations while doing an inter or intra-firm data

179 *Ibid.*, p. 345.

180 Article 5, GDPR.

181 Articles 6-7, GDPR.

182 See reference to the study on Europe's 2000 most visited websites by Iskander Sanchez-Rola et al 'Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control' (2019) Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security as discussed in Filippo Lancieri, 'Narrowing Data Protection's Enforcement Gap'(January 2022) *Maine Law Review* 74(1) pp. 17-18, 65 <https://digitalcommons.mainelaw.maine.edu/mlr/vol74/iss1/3/> accessed 27 July 2025.

183 On the techniques of synthetic data generation, and how it successfully anonymizes data, see *supra,* Section 2.

184 La Diega and Sappa (2020), *supra* note 73, pp. 7-8.

185 Nicolas Ruiz, Krishnamurthy Muralidhar and Josep Domingo-Ferrer 'On the privacy guarantee of synthetic data: a reassessment of the maximum-knowledge attacker perspective' in Josep Domingo-Ferrer and Francisco Montes (eds) *Privacy in Statistical Databases* (Cham: Springer Nature 2018) pp. 59-74 <https://link.springer.com/chapter/10.1007/978-3-319-99771-1_5> accessed 27 July 2025.

186 Gal and Lynskey (2024), *supra* note 25.

187 European Data Protection Supervisor (3 June 2024), *supra* note 167, p. 7.

188 Agencia Española Protección Datos, 'Anonymization III: The risk of re-identification' (Online 23 February 2023) *AEPD Innovation and Technology Division* <https://www.aepd.es/en/prensa-y-comunicacion/blog/anonymization-iii-risk-re-identification> accessed 27 July 2025.

189 Lee (2024), *supra* note 38, p. 22.

transfer.[190] Synthetic data can help comply with privacy, but does this also mean compliance with the principles of data protection?[191] The criteria in recital 26 of the GDPR is the appropriate benchmark to ascertain 'whether the final identification [of the data subject] is sufficiently probable to assume a *specific* risk to fundamental rights' and whether the processing must comply with the safeguards under the GDPR.[192]

66 Possibility of re-identification, such as in case of the dataset being partly synthetic, and partly human-generated or alternatively, a combination of synthetic and human-generated data can evoke the applicability of the EU GDPR. Moreover, as many GPAI model providers are based outside the EU, it is important that data transfers must have sufficient safeguards for the protection of personal data, in compliance with the EU GDPR.[193] Even when the datasets can distantly identify a data subject, they may involve processing of personal data, as per Article 4(1), GDPR.[194] In such a scenario, compliance with the following requirements under Article 5 GDPR, namely 'lawfulness, fairness, transparency' (Article 5(1)(a)); 'purpose limitation' (Article 5(1)(b)); 'data minimization'((Article 5(1)(c)), 'storage limitation'(Article 5(1)(e)); 'accountability' (Article 5(2)); accuracy (Article 5(1)(d)), integrity and confidentiality ((Article 5(1)(f))), must be met.

E. Conclusion, Policy Recommendation and Further Research

67 Generative AI models are a key source for synthetic data generation. Synthetic data is in turn used as an input for further training these GenAI models, and thereby 'leverage the diversity and scale of artificial datasets' to make these (generative) models more robust.[195] In an earlier research output, I develop the 'contextualise, iterate and improvise' (CII) model to explain how generative AI models such as ChatGPT 'think and improvise with every successive iteration'.[196] In this paper, I go a step further to add the element of synthetic data. This holistic model (as visually represented in Figure 1) helps understand the situation whereby synthetic data strengthens the capability of Generative AI models, and scenarios wherein human generated data inputs may continue to be a requirement to prevent the 'collapse of [these] models'[197]. This aspect is vital to appreciate why notwithstanding the emergence of synthetic data, high quality human-generated data will continue to be in demand and coexist alongside synthetically-generated data. The additional layer, represented by the blue arrows refers to the additional layer of synthetic data. Synthetic data complements and adds to the quality, variety, and volume of human-generated data available to train the GenAI models.

190 See reference to Steven M. Bellovin, Preetam K. Dutta and Nathan Reitinger, 'Privacy and Synthetic Datasets' (2019) *Stanford Technology Law Review* as discussed in Gal and Lynskey (2024), *supra* note 25, p. 1109.

191 Juliana Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) *International Data Protection Law* 3(4) <https://academic.oup.com/idpl/article/3/4/222/727206> accessed 27 July 2025.

192 Valentin Rupp and Max von Grafenstein, 'Clarifying "personal data" and the role of anonymization in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection' (2024) *Computer Law & Security Review: The International Journal of Technology Law and Practice Vol. 52,* p.18 <https://www.sciencedirect.com/science/article/pii/S0267364923001425> accessed 27 July 2025.

193 The Court did not hesitate to invalidate the then EU-US Safe Harbour and Privacy Shield on the grounds the required legal obligations for transatlantic data transfers, and protection of the European citizens' data was not met. Case C-362/14 *Maximilian Schrems v. Data Protection Commissioner* ('Schrems I', Safe Harbour case) ECLI:EU:2015:650, paras 88-90 and Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd. & Others* ('Schrems II'), ECLI:EU:C:2020:559, paras 184, 185, 191.

194 Beduschi (2024), *supra* note 20, pp. 1, 2.

195 Cem Dilegani 'Synthetic Data Generation: Techniques & Best Practices' (1 October 2024) AI *Multiple Research* <https://research.aimultiple.com/synthetic-data-generation/> accessed 27 July 2025.

196 Tyagi (2024), *supra* note 87.

197 Aatish Bhatia 'When A.I.'s Output Is a Threat to A.I. Itself' (Online 25 August 2024) *New York Times* <https://www.nytimes.com/interactive/2024/08/26/upshot/ai-synthetic-data.html?unlocked_article_code=1.Uk4.lUcJ.NURrC0S1B4oq&smid=em-share> accessed 27 July 2025.

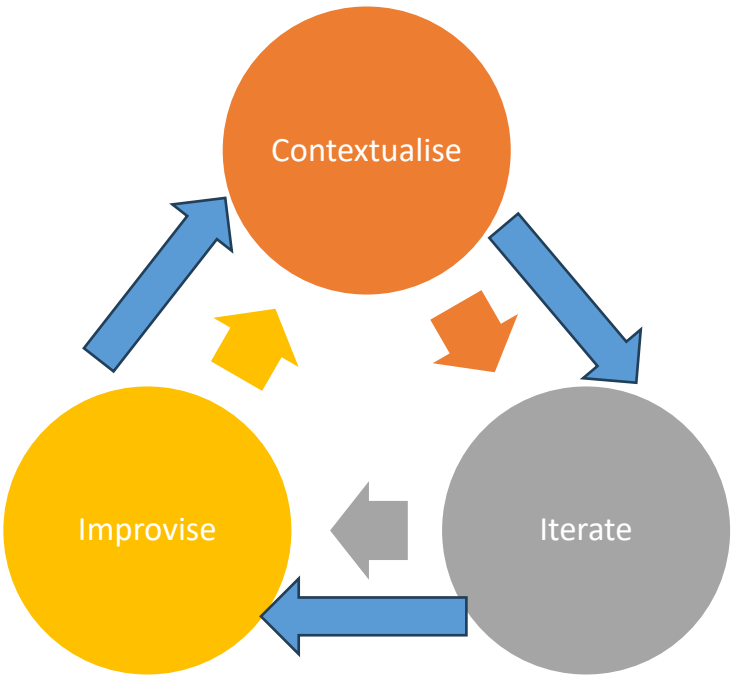

Figure 1: Co-creation by man and machine: Co-existence of human-generated and synthetic data. The outer blue colored arrows indicate a mix of human-generated and synthetically generated data. The inner multi-coloured arrows indicate human-generated data.

68 Synthetic data generation, as section 2 *supra* elaborates, is a complex technical task with substantial sunk costs. The quality of the output is dependent on the complexity of the model used to generate synthetic data.[198] Even though commercial and open-source models for synthetic data generation are currently available in the market, the quality of proprietary commercial models is far superior to the small scale or open-source models.[199] This is not difficult to comprehend. Synthetic data generation requires technical capabilities. There also exist synergies between GenAI and other key technologies, such as the internet of things (IoT), whereby synthetic data is the input as well as the output. Amazon's training of Alexa is a case in point. Another related consideration is that whereas first movers, and early winners in the digital economy and the GenAI race, such as OpenAI and Google, scraped the web to train their GenAI models, they 'have [since] updated their terms of service to prohibit [others from using] their data to train AI models'.[200] This implies that the availability of synthetic data is determined by the degree of competition and contestability in the digital markets. Innovation in high quality synthetic data generation requires substantial sunk costs for research and development, and like the platform economy, and the market for Generative AI, exhibits sectors-specific features such as barriers to entry, and economies of scale and scope. Herein, the scope of the EU Data Laws, EU competition law and the Digital Markets Act becomes relevant to facilitate the continued availability of high quality data.[201] This area of law is driven by economic rationale, and the driving principle is to facilitate access and contestability, a focus area of the follow-on research article. Copyright and data protection, on the other hand are respectively grounded in innovation and respect for fundamental rights, an issue addressed at length in this contribution.

69 Moreover, even when some of the algorithms, such as those provided by Google, IBM and Microsoft, are open source; the datasets used to train these algorithms is a black box.[202] The 2024 EU AI Act calls for transparency and disclosure of the training data. The Commission's Template offers a 'common minimal baseline' for GPAI model providers to publicly share information about the list of data sources, including synthetic data used for training the model.[203]

70 Synthetic data can notably help overcome the limitation of quality datasets – a key input and barrier to entry in the digital markets – and can thereby contribute to the innovation dimension of the economy. As regards copyright, the follow-on works may be deemed infringing if the initially synthetically generated data is derived from copyright-protected works. Synthetic datasets only when fully anonymised can facilitate compliance with data protection rules.[204] Even when a part of dataset may remotely identify personal data of the data subject, the processing of such a dataset must meet the requirements under Article 5, GDPR.

71 While it may be true, provided that the analysis is correct, that over 60 per cent of data currently available on the internet is synthetic, 'recursive training of the GenAI models [with synthetic data] can lead to model collapse'[205]. Training

198 *Supra* note 24, p. 60.

199 *Ibid.*, pp. 59-60, 62.

200 Alistair Barr 'AI Hypocrisy: OpenAI, Google and Anthropic Won't Let Their Data Be Used to Train Other AI Models, But They Use Everyone Else's Content' (Online 2 June 2023) *Business Insider* as referred in Lee (2024), *supra* note 38, p. 8.

201 *See supra* note 12.

202 Amanda Levendowski 'How Copyright Law Can Fix Artifical Intelligence's Implicit Bias Problem' (2018) Washington Law Review 93(2) p. 583 <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=5042&context=wlr> accessed 27 July 2025.

203 European Commission (24 July 2025), *supra* note 47.

204 *See* Gal and Lynskey (2024), *supra* note 25.

205 *See* Illia Shumailov, Zakhar Shumaylov, Yiren Zhao, Yarin Gal, Nicolas Papernot and Ross Anderson, 'The Curse of

GenAI models repetitively on synthetic data can overtime deteriorate the quality and 'negatively affect downstream performance' of the model.[206] To prevent this, there will always be a demand for high quality human-generated works. For a sustainable digital future and growth of GenAI applications, the models will require a mix of synthetic and human-generated data.[207]

72 Simultaneous availability of human-generated and synthetic data can be useful to address the copyright and data protection-related concerns, and the need to balance distinct fundamental rights – such as the rights to author remuneration (safeguarded under Article 17(2), CFR), the right to privacy (Article 7, CFR) and the right to data protection (Article 8, CFR)). Thus, an innovation-driven synthetic data paradigm can also be an enabler of different rights and competing interests at stake. From a technical lens, constraints, such as model collapse, may help avert complete substitution of human-generated data by synthetic data, and a sound fundamental rights-driven legal framework may ensure a balanced sharing of profits among the co-creators of data (human generated as well as synthetic) in the generative AI value chain. To meaningfully facilitate this, effective enforcement should not succumb to corporate lobbying or the US calls for relaxing compliance requirements by the big tech.[208]

Recursion: Training on Generated Data Makes Models Forget' (31 May 2023) <https://www.cl.cam.ac.uk/~is410/Papers/dementia_arxiv.pdfin> accessed 27 July 2025, also discussed in Lee (2024), *supra* note 38, p. 26.

206 Ryuichiro Hataya, Han Bao and Hiromi Arai 'Will Large-scale Generative Models Corrupt Future Datasets?' (15 November 2021) *Cornell University Computer Science: Artificial Intelligence* <https://arxiv.org/abs/2211.08095> accessed 27 July 2025.

207 Gonzalo Martínez, Lauren Watson, Pedro Reviriego, José Alberto Hernández, Marc Juarez and Rik Sarkar, 'Towards Understanding the Interplay of Generative Artificial Intelligence and the Internet' (8 June 2023) *Cornell University Computer Science: Artificial Intelligence* <https://arxiv.org/abs/2306.06130> accessed 27 July 2025.

208 Mathieu Pollet and Pieter Haeck 'EU could postpone flagship AI rules, tech chief says' (Online 6 June 2025) *Politico* <https://www.politico.eu/article/eu-could-postpone-parts-of-ai-rulebook-tech-chief-says/> accessed 27 July 2025.

From Curators to Creators: Navigating Regulatory Challenges for General-Purpose Generative AI in Europe

by **Gabriel Ernesto Melian Pérez ***

Abstract: This study examines the regulation of general-purpose generative AI (GPGAI) in the European Union, dividing the analysis into two parts. First, it explores whether GPGAI, by generating new content, qualifies as a content provider and thus falls outside the scope of 'safe harbour' protections. Drawing on case law from the CJEU and the Digital Services Act (DSA), the paper argues that GPGAI, by actively contributing to content creation, goes beyond the role of a mere intermediary and should therefore not benefit from safe harbour exemptions. Having established GPGAI's active role in content generation, the second part of the study addresses the broader regulatory implications, focusing on the AI Act and the revised Product Liability Directive. It contends that the AI Act's risk-based approach is insufficient to address the dynamic and unpredictable nature of GPGAI, potentially leading to ineffective regulatory obligations. The paper concludes by advocating for more tailored legal frameworks to ensure the responsible development of GPGAI, striking a balance between fostering innovation and safeguarding users.

Keywords: Safe Harbour, Curation AI (CAI), Generative AI (GAI), General-Purpose Generative AI (GPGAI), AI Act.

Recommended citation: Gabriel Ernesto Melian Pérez, IFrom Curators to Creators: Navigating Regulatory Challenges for General-Purpose Generative AI in Europe, 16 (2025) JIPITEC 201 para 1.

A. Introduction

1 Recent years have seen rapid technological advancements, resulting in the deployment of various types of AI with diverse functionalities. Some are designed for specialized applications in fields such as medicine, education, and defense, while others serve more general purposes aimed at non-specialist audiences. Among these AI tools, generative models stand out as particularly remarkable. They can create entirely new and original content based on the data they were trained on (Hacker et al., 2023), pushing the boundaries of creativity and innovation. However, these same capabilities carry the potential for misuse, as the content generated may inadvertently or intentionally be harmful, ranging from misinformation to offensive or defamatory material.

2 One of these AI tools is Meta's Imagine. In broad terms, Imagine is a generative AI that creates images, in the style of the already famous Midjourney, Stable Diffusion or DALL-E. Recently, Meta has announced that Imagine's functions will be incorporated into Facebook, Instagram and Messenger, so that the user can generate images to use them in the Facebook feed, in Stories, as comments, reactions or as profile pictures. This means that Meta would implement two different types of AI on its Facebook and Instagram social network: this generative AI (GAI)[1]

* LL.M. Göttingen, PhD fellow, Civil Law Department, Pompeu Fabra University. I express my deep gratitude to Professors Antoni Rubí Puig and Migle Laukyte for their valuable comments and feedback. I also appreciate the anonymous reviewers for their comments, which contributed significantly to the improvement of this work. This research has been developed within the framework of the research project "Responsabilidad contractual y extracontractual de las plataformas en línea", supported by the Ministry of Science and Innovation, the Agencia Estatal de Investigación and the European Regional Development Fund (PID2021-126354OB-I00).

1 Because of its broad capabilities and general scope of use, this generative AI (GAI) can be classified as a General-

and the AI that organizes and curates content (CAI). This seemingly innocuous distinction could have important legal consequences. Understanding the differences between these two types of AI and their respective levels of control over the content they generate and show is crucial for determining their responsibilities and potential liability.

3 This research compares the levels of control that GAI and CAI have over the content. The hypothesis proposed is that the two AIs have different levels of control over the content, and therefore, the same legal principles cannot be applied. As generative AI performs a substantial intervention in the creation of content, it could be considered that its role is too active to benefit from the safe harbour[2]. On this premise, GAI would then be subject to other EU[3] and national rules that will determine their level of liability for the content they generate. The most relevant norms include the AI ACT and the new defective products directive. However, a general review of them reveals a number of loopholes in the regulation of GPGAIs. The aim of this paper is to address these shortcomings and to propose some *ex ante* regulatory adjustments that would better clarify what the obligations of developers of these technologies would be.

4 The first part of this paper delves into the technical elements that distinguish the two types of AI at the core of this study, so that the reader has a clear understanding of the technological background before entering the more theoretical legal framework. The second section focuses on the classification of social networks within the broader landscape of media players, examining how the concepts of control and knowledge have shaped this model. The third section analyzes the evolution of these variables (knowledge and control) in the jurisprudence of the European Court of Justice, culminating in their consolidation within the recent Digital Services Act (DSA). Building on these theoretical insights, the next section discusses the relevance of technical differences in advocating for the exclusion of GAI from the benefits of the safe harbour provision. The fifth section focuses on the assessment of the current regulation of GPGAI, suggesting regulatory clarifications and changes aimed at reducing the generation of harmful content resulting from such systems. The last section concludes.

B. Technical Framework of GAI and CAI

5 Before discussing more specific issues, it is necessary to provide a general definition of AI. This article rests on the concept developed by the Organization for Economic Co-operation and Development (OECD) and supported also by G'sell (2024) that states: "*An AI system is a machine-based system that, for explicit or implicit objectives,* ***infers****, from the* ***input*** *it receives, how to* ***generate outputs*** *such as predictions,* ***content, recommendations,*** *or decisions that can* ***influence*** *physical or virtual environments. Different AI systems vary in their* ***levels of autonomy*** *and adaptiveness after deployment*" (OECD, 2024). The stressed aspects are the most important ones in the concept[4]. On this basis, let us proceed to analyze the typologies of interest to us: *recommendations* (CAI) and *content*

purpose generative AI (GPGAI).

2 There are arguments for (Henderson et al., 2023; Volokh, 2023) and against (Bambauer and Surdeanu, 2023; Miers, 2023), but they focus on US jurisdiction and Section 230. Therefore, it is necessary to settle this debate within the framework of European legislation, specifically the Digital Services Act, which is the norm that defines the criteria for enjoying Safe Harbour immunity.

3 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024 (Artificial Intelligence Act, hereinafter AI Act). Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final. DIRECTIVE (EU) 2024/2853 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

4 This definition fits perfectly with that of the IA Act in Article 3(1) and Recital 12: "... A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling...". According to de Graaf and Veldt (2022, p. 806) "it better expresses two common features of AI: self-learning and/or autonomous behaviour". For Hacker (2024, p. 9), however, "distinguishing AI from traditional software will be a challenge under this definition and require a good understanding of what it means to 'infer' the AI output from input. Furthermore, a purposive interpretation of the definition will need to posit a 'sufficient degree' of autonomy for models to qualify as AI".

(GAI).

I. CAI

6 Basically, a social network is an online platform that allows users to connect with one another and share content. However, what users can see, share and do on the Platform is not completely free, as it is subject, in principle, to the rules set by the platform (and of course, also to national legislation). These rules are usually set out in the "Terms and Conditions", "Community Standards" or "Content Policies" of each platform. The process by which the platform ensures that these rules are followed is known as "content moderation"[5]. This content moderation has two dimensions:

- platforms decide what content is suitable for publication, which York and Zuckerman (2019) call "*hard control*"[6];
- then, certain parameters determine what users see in their particular feed, which would be the "*soft control*" or curation.

7 Regarding the curatorial functions, social networks don't just give users a chronological set of information provided by everyone in their network[7]. Using specialized algorithms, content is displayed through intricate design parameters programmed into an AI[8] and complemented by the activity of the users themselves: interests shown, geographic location, what their "friends" like, etc.[9]. Therefore, these algorithms determine what content will be shown to users and in what order. According to the OECD definition, we could a priori classify it as a *recommendations* AI.

8 When one first creates an account, the content that is displayed can be quite random. However, as one engages with the content and other users, the algorithm will use this information to provide you with more tailored content. Essentially, the more you interact on the network, the more information the AI will obtain from you and the more personalized the experience will be (Chander and Krishnamurthy, 2018; Sylvain, 2021). Arguably, social network platforms differ from each other mainly by the content moderation they perform. This is why Gillespie (2018, p. 201) rightly argues that content moderation "*is central to what platforms do, not peripheral... is, in many ways, the commodity that platforms offer*"[10]. In fact, users opt for one platform or another mainly based on the choices made by these companies about the content they display.

II. GAI

9 Generative AI has been a revolution in the artificial intelligence landscape. It refers to "*a category of deep-learning models that are "trained" on extensive datasets and that can then be directed to generate content based on the data on which they have been trained*" (G'sell, 2024, p. 31) . Broadly speaking, generative AI usually works in response to an initial 'prompt', either a text

5 To Grimmelmann (2015, p. 47), moderation is "*the governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse*".

6 This would be *ex ante* moderation, whereby the platform uses algorithms to determine whether the content to be uploaded complies with the content policies. For example, in a platform that only allows videos of pets, the system would prevent the uploading of videos about cars. Given today's information flow, it is impossible, or prohibitively costly, for humans to perform this function. To do so, implementation of a sufficiently competent AI to identify between pets and cars is required.

7 Although some platforms are currently implementing this functionality.

8 "Ranking algorithms often factor in machine-cognizable information about content, like whether machine learning models predict that an image includes nudity... Overall, the goal of ranking algorithms is to prioritize material according to content-based attributes like subject matter, relevance, or authoritativeness" (Keller, 2023a). However, they are not perfect and often tend to make mistakes when assessing these attributes (Llansó et al., 2020).

9 The displayed result (recommendation, ranking) is nothing more than the conjunction of design features chosen by the platform plus the behavior of the users (Llansó et al., 2020, p. 15). A recommender system is an algorithm designed to sift through a vast array of items and identify which ones to present to a user. These systems serve as essential tools in managing the overwhelming volume of content generated daily, assisting users in discovering relevant and personalized recommendations. *"Services like photo-sharing and community site Flickr, or Amazon.com's community ratings system, take inputs from millions of users in the form of ratings, tags, and engagement (e.g., via analyzing what and how much users click, comment on, or forward to their friends) to make the online experience better"* (Ziniti, 2008, p. 592). *"Internet platforms and services do not just show us information randomly—they organize, curate, and manage information for us... These platforms generally purport to be showing us information that we want to see based on a complex formula that takes into account our past information consumption habits combined with the habits and preferences of others... Because these formulas are proprietary and central to their business models, platforms do not share many details about how they make these decisions"* (Land, 2019, p. 290). It is difficult to know exactly how these systems work because the algorithms used by each platform are trade secrets. See (Thorburn, 2022).

10 In the same line, see Elkin-Koren, De Gregorio and Perel, 2021 (p. 987).

sentence or an image. This prompt is the guidance that instructs the generative AI system to produce certain content, which can consist of text (such as those provided by OpenAI's ChatGPT or Google's Bard), images (such as those created by Stability AI's Stable Diffusion or Meta's Imagine AI) or even videos and music.

10 The fast-paced development we have been experiencing lately in generative AI is essentially driven by three key factors: the availability of big data, high computational power and the development of new models[11]. The confluence of these three critical factors has driven AI progress: big data provides extensive training information, increased computational power enables faster and more complex processing, and innovative AI models and architectures have led to breakthroughs in various domains, including natural language processing.

11 From a technical point of view, generative AI is based on machine learning and training on huge data sets. This training allows the system to learn patterns and relationships in the data, which it can then use to generate *new* content similar in style and structure to the data it was trained on. To do this, GAI makes use of artificial neural networks (ANNs), which are a key building block of many generative AI systems[12]. ANNs try to imitate human neural networks, a kind of digital brain, with interconnected nodes that process information. Each 'neuron' receives information, performs calculations and transmits the result to other neurons at the next level. Through training, these nodes are adjusted to learn patterns and relationships in the data[13]. These neural networks and deep learning are closely related; in fact, deep learning is a sub-area of machine learning that uses neural networks, especially deep neural networks. These additional layers allow networks to learn more complex representations of data, which is especially useful for tasks such as image recognition, natural language processing and text or audio generation. (Hacker et al., 2023).

12 This whole process benefits from big data, that is, the progressive accumulation of large amounts of data. The specific type of data employed in training a large model determines its functional model:

- **Generative text AI (Language Models):** The text generation process is based on the prediction of the next most likely word or phrase, given the previous sequence of text.
- **Generative image AI (Text-to-Image Models):** Image generation is more complex, as it involves translating a textual description into a visual representation. They can use techniques such as generative antagonistic networks (GANs)[14], diffusion models or transformers to create images that match the textual description (Noto La Diega and Bezerra, 2024).
- **Multimodal generative IA**: It is designed to process and generate multiple types of data, such as text, images, audio and video. For example, OpenAI's GPT-4o accepts combinations of text, audio, images and video as input and generate any of these formats as output. These capabilities make multimodal models highly versatile and useful in applications that require understanding and generating information in a variety of formats (G'sell, 2024).

13 The development of new artificial intelligences and their performance is also benefiting from technical developments, notably the introduction of the Transformer architecture by Google researchers in 2017 (Vaswani et al., 2017) and improvements in Generative Pre-Trained Transformer (GPT) models

11 "In sum, an AI model is a program trained on a large set of data with the ability to identify patterns in that data in order to produce relevant outputs in response to inputs without the need for human intervention" (G'sell, 2024, p. 32). "AI models include, among others, statistical models and various kinds of input-output functions (such as decision trees and neural networks)... AI models can be built manually by human programmers or automatically through, for example, unsupervised, supervised, or reinforcement machine learning techniques" (OECD, 2024, p. 8).

12 Although ANN-based models dominate the market, there are other types of AI that are not based on neural networks.

13 "Determining the model's size mainly involves determining the number of parameters or weights it will include. "Weights" are the numerical values that determine the strength of neural connections within a neural network and, thereby, help determine a model's output. During the training process, these weights are adjusted to optimize the model's performance, helping it produce more accurate and useful outputs. Furthermore, the relationship between the size of the model and its performance is mediated by the model's topology. "Topology" refers to the arrangement of neurons and layers within the neural network and how they are interconnected" (G'sell, 2024, p. 44). Although it is worth clarifying that more parameters do not mean that a model is better, with better performance, as it is currently more of a priority to synthesize those nodules to make it lighter. Models with many parameters tend to require more computational resources, both to train and to use.

14 These networks consist of a generator, which creates images, and a discriminator, which evaluates whether they are real or fake. During training, the two compete: the generator gets better at fooling the discriminator, and the discriminator learns to detect fake images. Over time, the generator produces images that are indistinguishable from the real ones. (Noto La Diega and Bezerra, 2024)

since around 2019 (Belcic and Stryker, 2024; Radford et al., 2019). Several companies have leveraged the use of transformer models[15], which have become popular because of their ability to process data streams and generate images with refined detail and contextual coherence.

14 Although each technology has its specific methods and approaches, the fundamental principles of pattern learning, progressive generation and fine-tuning are applicable to all image generative AI. In this sense, generative AI uses the elements and structures learned from the data to generate new combinations and variations[16].

C. Evolution of Intermediary Liability

15 Before the advent of the Internet, the most well-known media and intermediaries were broadcasters, newspapers, telephone networks and bookstores. These entities were placed into one of three traditional intermediary liability models: publishers/content providers (newspaper), distributors (libraries, bookstores), and conduits (telephone companies) (Patel, 2002, p. 651; Volokh, 2021, p. 454). In the 1990s, following the Internet boom, regulators were faced with the problem of assessing whether the liability of new web entities would be based on those traditional models or whether they were worthy of a new approach.

16 The basic principle underlying the question of whether an agent qualifies as a publisher, distributor or conduit is closely related to the idea of *control* exercised over the content; the more control is exercised, the more responsibility should be attributed to the agent. According to this model:

- Newspapers are subject to publisher liability because they have full editorial control over the content of their columns and articles.
- On the other hand, telephone, mail or courier companies are understood to have a very low share of responsibility. They have no control over what is discussed in a phone call or what is sent in a letter, therefore, it was understood that the fairest solution would be not to hold them liable for third parties' illegalities. Therefore, they fall into the category of common carriers or conduits, which refers to an entity acting as a passive conduit of illicit content (Candeub, 2020, p. 410).
- Meanwhile, libraries are somewhere in between the publisher and the conduit. They have "distributor liability" as they are entities that distribute third-party content, do not exercise editorial control over such content, but have some access to it. It has been understood that requiring distributors to review the content they distribute for illegalities would be an unjustifiably heavy burden[17]. Therefore, they are only liable for the illegal content they distribute if they become aware of such illegality.

17 To differentiate the distributor from the publisher, the latter is sometimes referred to as the primary publisher, since it is the publisher who exercises editorial control over the content, while the distributor is known as the secondary publisher or "re publisher", since its function is not to control the content, but to make it available to others without performing any creative or editorial function (Mirmira, 2000, p. 439; Patel, 2002).

18 With the emergence of the Internet, the rise of blogs first, then discussion forums and now with web 2.0 and social networks, it became clear that these new types of media were not easily categorized into the

15 "The transformer architecture marked a significant turning point for deep learning, particularly in the areas of natural language processing and computer vision. It enabled a huge leap in the amount of data that AI models could leverage and resulted in increased performance... The two most popular types of transformers are generative pre-trained transformers (GPT) and bidirectional encoder representations from transformers (BERT). OpenAI has used GPT to develop GPT-3 and GPT- 4, while Google has refined BERT to develop Bard (now called Gemini)" (G'sell, 2024, p. 34).

16 There is a large body of scholarship debating the impact of this issue on copyright. Due to the involvement of multiple parties in the outcome, it is difficult to establish from a copyright lens who should be considered the creator of the work. For example, Khosrowi et al. (2024) argue that "*GenAI outputs are created by collectives in the first instance. Claims to creatorship come in degrees and depend on the nature and significance of individual contributions made by the various agents and entities involved, including users, GenAI systems, developers, producers of training data and others*". Viewpoints such as these can contribute to reinforcing GAI's involvement in shaping content.

17 *Smith v. Cal.*, 361 U.S. 147, 153 (1959) ("*[I]f the bookseller is criminally liable without knowledge of the contents... he will tend to restrict the books he sells to those he has inspected*"). This conclusion, supported by Justice William Brennan, is reasonable since the distributor would try as much as possible to avoid any liability. This would have an undesirable impact on fundamental rights, specifically the right of access to information. If we were to expect every piece of content to pass through the distributor's filter, the content available to the public would be only that which the distributor has had time to review and approve, leading to the unavailability of legal content and a substantial risk of private censorship and false positives.

three traditional groups mentioned above. While publishers and social media platforms consist, broadly speaking, of making decisions on what content to show to users and in what order, some preliminary distinctions may include the following:

i Traditional media companies perform *ex-ante* moderation, based on editorial guidelines, before content is broadcast or published. Moderation in social networks generally operates *ex ante* and *ex post* and the review of such content is performed by computer tools, which do not understand the content in the same way that a human does (Keller, 2023a). "*... editors (human) and recommendation systems also differ in many regards, including that recommendation systems are automated and process third-party content, and as a result are generally less intentional or deliberate about overall outcomes... The effects of recommended content are highly unpredictable*" (Llansó et al., 2020, p. 16).

ii The moderation that is carried out on platforms is not comparable to an editorial process of those carried out in traditional media. Traditional media focus on keeping people informed on various topics, for which the information goes through several levels of fact-checking. In addition, this information is provided by licensed professionals who are guided by codes of conduct and ethics. This endows the information with a degree of reliability that is not associated with the content uploaded by users to social media. Traditional media "endorse" the content they publish after going through this editorial process. However, Internet platforms have never pretended to "endorse" the contents they host or claim authorship over them, because it is not "their speech", but that of the users (Zurth, 2020, p. 1145). The purpose of social networks is to share content provided by the users themselves, which are not platform employees. That content generally comes without centralized editorial oversight or planning (Elkin-Koren et al., 2021, p. 1033). The mere existence of a recommendation/curation system on the platforms does not necessarily mean that they have knowledge of the content of a particular item[18].

iii Traditional media only support one-way communication. On the contrary, social media lets people communicate in two-way. It means unlike traditional media, social media users can leave reactions, comments, etc. "*Twentieth-century print and broadcast media were not participatory media; the vast majority of people were audiences for the media, rather than creators who had access to and used the media to communicate with others. Twenty-first century model, by contrast, involves crowdsourcing and facilitating end user content. Social media host content made by large numbers of people, who are both creators and audiences for the content they produce.*" (Balkin, 2021, p. 75)

19 These aspects reveal an important element: social media platforms do not *control* content like an editorial desk would. The editor is responsible for knowing the content of any article that will be published and has the power and resources to control and approve the content before it is published. It can be said that content management in the case of newspapers and broadcasters is more *conscientious*, while on the platforms it is more superficial[19]. Platforms have no control over the accuracy or fairness of the content that users produce and upload.

20 So, what are social networks? Participatory networking platforms are, broadly speaking, *online platforms* that allow users to connect with each other to share content and communicate. These platforms also allow companies to connect with their customers and get feedback from them to improve their products and services. From this description,

18 See Keller (2023b, 2023a) and "Brief of Center for Democracy & Technology and 6 technologists as amici curiae in support of respondent", case Gonzalez v. Google LLC, 598 U.S. 617 (2023).

19 As said, the mere existence of a recommendation system on the platforms does not necessarily mean that they have knowledge about the content of an item. The algorithm makes decisions about what to do based on *signals* or elements it identifies in that content and the behavior shown by users (Leerssen, 2020). This process is perhaps sufficient to detect content that the user may like. However, it may not be sufficient to gather the necessary elements to determine the illegality of such content; this process is more complex and requires more information and intellectual capabilities. This curation process is not equivalent to "understanding" or "knowledge", at least not from the perspective of how a human would process a given item of content (Keller, 2023a, 2023b; Llansó et al., 2020). The algorithm can identify, for example, that an image contains nudity, however, it might be unable to differentiate between nudity occurring within the realm of artistic expression and that which signifies abuse. The inherent complexity of these situations underscores the need for human judgment and contextual understanding. This is explained very well by Keller (2023b): "*algorithms don't "know" what message a post conveys in the way a human would. That's why they make mistakes humans might not, like assuming any image with a swastika is pro-Nazi. In that narrower sense, one could perhaps argue that algorithms are not considering "content" but, rather, "data" or "signals" about the content*". That is why it is not the same whether a content is analyzed by a human editor of a magazine or by an algorithm within the framework of a platform.

one can conclude that, in principle, social networks do not create content themselves, but by means of AI, they organize and structure the information that third parties upload to the platform[20]. Based on what has been mentioned so far, we can place them in the broad category of hosting, specifically online platforms. Content hostings are generally associated with the liability of a distributor or secondary publisher, like that of a bookstore, which is triggered upon notification of illegal content[21]. In principle, the basic requirement to avoid liability would then be that the platform does not control or is responsible, in whole or in part, for creating or developing content and has no knowledge of the illegality of that content (Kosseff, 2022; Pagallo, 2011; Patel, 2002).

D. The Safe Harbour Doctrine

I. CJEU Case Law

21 In the 1990s, the European Union found itself in the same conundrum as other jurisdictions: it was unclear what standards of liability to apply to those new intermediaries that were emerging in the context of the Internet. The fact that each member state applied different standards was detrimental to the harmonization of the European internal market. Therefore, the European Union decided to harmonize the field by enacting the "*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*" or eCommerce Directive (ECD)[22]. One of the three pillars on which the ECD was based was the 'Safe Harbour' doctrine. This liability regime shields "online intermediaries" from liability for the content they transmit and host under specific conditions. Hosting firms are obligated to take down illegal content upon notification of their existence, that is, they are not liable for illegal content or activities unless they possess "actual knowledge" of them.

22 Section 4 (Arts. 12 to 15) shields certain online intermediaries (Mere conduit, Caching, Hosting) against claims that may arise from the transmission or storage of information *provided* or requested by their users. Although the goal of unifying the Internet intermediaries' liability rules was relatively achieved with the enactment of the ECD, the implementation and interpretation of this Directive in the different states was not homogeneous, perhaps due to its lack of clarity in some important points. For example: more precision was needed to establish when a platform played an "active role" and when exactly the "actual knowledge" was obtained. Over the years, the CJEU would clarify these issues, although in some cases it would make it even more blurred. The most relevant rulings could be the following:

- **i** C-236/08 to C-238/08 *Google France*: Clarifies the applicability and preconditions for the liability exemptions of the ECD. In this case, the CJEU develops an argument focused on the active/passive role of online service providers, criterion that would permeate subsequent judgments. According to the court's interpretation, based on Article 14 and recital 42, a provider can only be exempt from liability if it has played a neutral and non-active role, meaning that it has no knowledge or control over the data stored. If its action is neutral, i.e. technical, automatic and passive, which indicates a lack of knowledge or control over the data it stores, then it could benefit from immunity.

- **ii** C-324/09 *L'Oréal vs. eBay*: This is another case that involves determining whether the intermediary's actions are sufficiently active

20 This organization and structuring of content has been the most complex dimension of regulating social networks. Today's recommendation algorithms are so complex and advanced that they challenge the traditional distinction between publisher and mere distributor, as it is sometimes difficult to determine whether an intermediary cross the threshold of control, especially because of the intense content moderation work they perform. See Recommendation CM/Rec (2011)7 on a new notion of media which states in paragraph 25 that "*it should be noted that different levels of editorial control go along with different levels of editorial responsibility. Different levels of editorial control or editorial modalities (for example ex ante as compared with ex post moderation) call for differentiated responses and will almost certainly permit best to graduate the response*". The author recognizes the multiple challenges involved in moderating content on social networks. However, a critical assessment of this issue is beyond the scope of this article. The description of the content moderation process made here is meant to provide a framework to highlight the differences between the two types of AI examined in this paper.

21 "*An owner of a bookstore cannot be held responsible for the content of each and every book in her store. She does not read and inspect all the books. Similarly, it can be argued, an Internet provider should not be held accountable for content on its server. But if a bookstore owner is informed that a specific book contains child pornography, some other illegal material, or material that violates copyright, and she does not take the book out of the shelves, then the owner may be held legally responsible for violation of the law*" (Cohen-Almagor, 2010, p. 387)

22 Prior to the enactment of the ECD, there were two European countries that took the lead in regulating liability exemptions. In 1997, Germany adopted the IuKDG with a system based on knowledge. Sweden also did so shortly thereafter. (Husovec, 2023, p. 890)

(which allows him to have knowledge or control of the data stored) to deprive the intermediary of immunity. Accordingly, a platform can be held liable for trademark infringements committed by its users if it plays an active role that allows it to have knowledge of or control over the stored data. This is the case, for example, when the platform provides assistance to optimise the presentation of promotional offers or promotes them (Paragraph 123). In these cases, eBay does not limit itself to technical and automatic data processing but is actively involved in the management and presentation of the information. Another question that the court seeks to clarify is the scope of monitoring measures that can be imposed on intermediaries, a recurring matter in preliminary rulings. According to the CJEU, an active monitoring of all the data of each of its customers in order to prevent any future infringement would be precluded by EU law. Hence, the CJEU sets the boundaries of the notion of specific—and general—monitoring obligations by noting that ISPs can be only ordered to prevent further infringements by the same seller in respect of the same trademarks[23].

iii C-291/13 *Papasavvas*: This judgment further explores the role of the provider regarding the disputed content as the criterion for assessing whether it falls within the scope of Articles 12-14. The ruling draws an important distinction between the categories set out in articles 12-15 of the ECD and the *O Fileleftheros* newspaper, which, as *content provider*, has knowledge of the information it posts and exercises control over it. In this case, a newspaper company had a website that posted an online version of their articles. The Court ruled that the company had *knowledge* and *control* over the information posted on their website, making it ineligible to be considered a neutral intermediary service provider. If the articles on their website included illicit information, they should be held accountable for it. It would be a different matter if the newspaper provided a section on its online page for users to comment. Regarding these comments, the platform would not be considered a content provider but should be subject to the distributor regime. In this way, it clarifies the difference between a third-party content host and a newspaper that publishes and controls its own content, for which it is liable.

iv Joined Cases C-682/18 and C-683/18 *YouTube and Cyando*: In this case the court re-emphasizes that a platform cannot be compelled to introduce a screening system which entails general and permanent monitoring, because this would be contrary to Article 15 of the ECD. It also clarifies that in order for knowledge to materially arise, and immunity to be removed, the provider must be notified of an infringement in a concrete and precise manner, so that it can verify it without an in-depth legal and material examination. Therefore, a superficial notification is not enough to remove the intermediary's immunity.

II. The Digital Services Act (DSA)

23 Concerning liability, there was a certain consensus that hosting service providers should not be liable for illegal content shared through their services until they had actual knowledge. The DSA rightly maintains the principles of the ECD, reproducing in its articles 4, 5 and 6, content almost identical to the previous Articles 12, 13 and 14. While doing so, some adjustments are made considering the jurisprudence of the CJEU discussed in the previous sub-section[24].

24 One of the most relevant clarifications in the recitals are those related to the "active role", as the essential element to assess the liability of intermediaries. The DSA borrows the old formula of neutrality/passivity from recital 42 of the ECD. Recital 18 states that:

> "*The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider*".

25 Therefore, collaboration or authorship implies not acting neutrally, in which case it would not be eligible for the safe harbour[25]. In order to nuance this statement and provide greater clarity, the regulation specifies in recital 22 that "*... the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have 'specific' knowledge of illegal activities carried out on that platform or of illegal*

23 On active content filtering measures, see also C-70/10 *Scarlet Extended vs. SABAM* and C-360/10 *SABAM vs. NetlogNV*.

24 See recital 16.

25 See also recital 20 and article 6(2).

content stored on it"[26]. This clarification is made to eliminate any uncertainty about the immunity that social media companies enjoy for their work in curating and displaying the information uploaded by users of the service.

III. "Active Role" as Threshold and How it Should be Understood.

26 In Europe, the case law discussed concludes that intermediaries could be held liable only if they actively and significantly contribute to the infringement. The fundamental premise is that a provider of services cannot govern the content that is transmitted and, provided it refrains from engaging in any editorial intervention, it should not be held liable for any unlawful content that individuals post via its services.

27 I think we can agree that the implementation of recommendation algorithms in social networks cannot be considered as playing an "active role" or exclude them from the "safe harbour" (Angelopoulos, 2017; Arroyo Amayuelas, 2020; Pagallo, 2011; Sartor, 2017; Valcke et al., 2017; Van Eecke, 2011; Van Hoboken et al., 2018). The factor that makes an intermediary acquire an active role is whether the content is third-party or can be attributed to the platform because it had some involvement in its creation. When the task consists only of optimizing the presentation of the content uploaded by users employing algorithms, it should not be understood that an active role is acquired or that the platform automatically endorses or makes the content its own[27].

28 However, as proposed by Arroyo Amayuelas (2020, p. 817) "*it would be better to abandon this distinction between "active role" and "passive role" when qualifying hosting providers and replace these expressions with other more accurate terms, such as "degree of control", "performance of editorial functions", or "effective knowledge"*". The distinction between active and passive roles in the context of hosting providers' responsibilities may oversimplify this highly complex issue. This binary categorization fails to capture the nuanced spectrum of involvement and liability that service providers navigate in today's interconnected online environment. The suggested alternative terms offer a more granular approach to understanding the varied roles and responsibilities of these entities. By shifting the focus towards aspects such as control and editorial functions, regulators and policymakers can develop more comprehensive and adaptable frameworks.

IV. Comparison

29 As indicated by the legislation and case law analyzed, to assess whether an operator can benefit from the safe harbour, it would be essential to assess two key factors: (i) their level of knowledge and (ii) their degree of control over the content. Therefore, these are the two variables we should consider relevant to assess whether an operator has adopted an active role, enough to lose this benefit. "Knowledge" would refer to an entity's ability to know, be aware of and understand a piece of content. On the other hand, the concept of "control" implies the ability of a system to directly influence or determine such content. It implies that an agent has the ability to modify or adjust the resulting content through instructions, rules or configurations. On this basis, let's analyze how this works in each context.

1. Knowledge and Predictability of the Outcome

30 CAI works after the content is created. It organizes, filters, and selects pre-existing content without altering or modifying its original form or meaning. Here, AI does not have semantic understanding[28] of the content beyond the parameters used to classify and suggest it. In fact, its results depend on metrics of relevance, popularity and personalization. Although the arrangement of content has a certain impact on its visibility[29], this is not considered to constitute modification of the content itself. For instance, rearranging search results or grouping articles by topic affects their visibility but does not change their substantive content. Therefore, an AI that merely curates content qualifies for safe harbour protections.

26 This notion seems to have been borrowed from the CJEU judgment on YouTube and Cyando, para. 114.

27 A good example is described in the Amicus curiae of *Gonzalez v. Google*, presented by some internet law scholars in support of Google: "*The more apt analogy, which supports Respondent in this case, would be the difference between YouTube simply saying "Here are the videos we have picked and chosen for you based on your interests" (or a shortened version of that, such as "You might like . . . .") and one that consisted of the words "John Smith is a Murderer, Watch this Video to Learn More!" The former involves just the statutorily protected filtering, picking, and choosing, with a statement that YouTube has filtered, picked, and chosen. The latter involves the software adding defamatory material of its own, and not just filtering, picking, and choosing.*"

28 See 6.

29 It's important to note that while content organization AI may not modify the content itself, the way it arranges and presents information can significantly impact user perception and interpretation.

31 Meanwhile, GAI interprets and applies patterns learned from training data to create new content. However, it cannot be claimed that as a computational tool, it 'knows' or is aware of what it is generating, as current AI systems lack self-awareness or comprehension. This is due to the essentially stochastic nature of how these tools work, meaning it involves an element of randomness or unpredictability. This stochastic nature is a fundamental characteristic of generative AI models, which allows them to produce diverse and creative outputs. The inherent randomness allows generative models to produce different outputs from the same input. Generative AI can also produce incorrect or nonsensical information, a phenomenon often referred to as "hallucinations" (Noto La Diega and Bezerra, 2024).

32 Since the variable 'knowledge' is not so relevant to the argument, it is argued that the degree of control over the outcome should be considered as a defining factor.

2. Degree of Control and Influence on the Content

33 In CAI, control is limited to technical aspects, such as sorting or prioritizing according to general criteria. Thus, AI does not control the content itself but its visibility or availability. In contrast, GAI represents a significant shift. It plays a substantial role in content creation, depending on the model and its design[30]. Generative AI tools, such as Imagine AI, contribute to the creation of new content by combining, transforming, and synthesizing data.

34 When viewed on a spectrum, this collaboration in content creation positions generative AI closer to a content provider than a mere distributor. Even though this type of AI does not 'understand' what it creates in a conscious sense, its intervention is active: it responds to user input and generates information that did not previously exist[31]. Consequently, GAI exercises greater control over the final outcome compared to CAI.

35 Its influence comes in several ways. Developers shape AI behaviour through model design, training processes and data selection (Henderson et al., 2023). Ultimately, they control the dataset that serves as the core for the model's content generation[32]. This gives them, to some extent, the ability to limit certain outcomes or influence the likelihood of specific results emerging[33]. The influence of developers extends beyond initial model creation and data selection, as they can also implement safeguards and filtering mechanisms to further refine AI outputs[34]. These measures can help mitigate potential biases or undesirable content, though their effectiveness may vary. Additionally, developers and deployers can continuously update, and fine-tune models based on user feedback and emerging ethical considerations. However, their control is limited, as outputs depend heavily on user prompts, and adversarial attacks can bypass filters.

36 To summarize, GAI and CAI operate with different purposes and capabilities. Having analyzed how each works, we can conclude that GAI can produce *new* content based on patterns learned from large volumes of data. However, AI that organizes and curates content in social networks does not create new information; instead, it classifies, filters and recommends existing content using algorithms based on user history, relevance, trends, or similar parameters. In other words, in the case of social network, AI could be responsible for the organization and arrangement of content, but not for the content itself, which is created by the users of the network[35].

30 Here we anticipate that not all generative AIs are the same, so the benefit of the safe harbour will depend on the specific case. This issue will be further elaborated in the next section.

31 "*This task combines forecasting and recognition tasks. However, the output often combines several existing elements such as images, text and audio to produce an object that was never seen before*". (OECD, 2022, p. 52)

32 As recognised by the OECD (2024, p. 6), "*Human intervention can occur at any stage of the AI system lifecycle, such as during AI system design, data collection and processing, development, verification, validation, deployment, or operation and monitoring*". In its 2022 version they explain that "*The lifecycle encompasses the following phases that are not necessarily sequential: planning and design; collecting and processing data; building and using the model; verifying and validating; deployment; and operating and monitoring*" (OECD, 2022, p. 7). As will be explained in Section 5, each of these phases should be subject to specific obligations.

33 "So just as these base models might identify associations that do not exist, they might successfully recover harmful associations present in the training data. Major training datasets have been shown to include websites with harmful hate speech and disinformation". (Henderson et al., 2023, p. 603)

34 See Section 5.2.

35 It should be noted that, despite the conceptual simplification made here to support the argument, also a CAI could exceed the passivity threshold defined by the CJEU. This could arise if: a recommendation algorithm systematically prioritizes illegal or infringing content, especially when the platform knows or should know that such content is problematic, or when the platform already has actual knowledge that certain sources are "of a dubious nature" (i.e. known for breaching rights) and still allows or encourages their visibility. This could be interpreted as an active role. In essence, not all CAI can be considered automatically passive under the current

Whereas in GAI, the model is much more involved in the configuration of the content created. It can be said that it acts as a kind of co-creator or contributor to the outputs and therefore could be considered a content provider.

E. GAI does not Fit into the Safe Harbour

37 Having analyzed all the historical, legal and technical aspects, it only remains to assess whether generative AI can benefit from the 'Safe Harbour'.

38 There are arguments in favor. Since generative AI lacks intention or knowledge in the human sense, some might argue that it could benefit from safe harbour protections, similar to CAIs, on the basis that it is merely a tool responding to user instructions without directly understanding the content. Authors such as Botero Arcila (2023), Stalla-Bourdillon (2023), Miers (2023), Bambauer and Surdeanu (2023), suggest that GAI products like ChatGPT share functional similarities with tools such as search engines and predictive technologies like autocomplete. These similarities stem from the foundational purpose and operation of these systems: to process user input and generate output aligned with their queries or prompts. In essence, they argue that the entire process is grounded in probability calculations, what could be described as "statistical inference". Both CAI and GAI rely on identifying patterns in existing content and producing outputs consistent with user needs, whether it be a social media feed or a generated image[36].

39 However, this argument is open to counterarguments based on the qualitative difference between organizing existing content and creating new content, which increases the likelihood of liability. DSA' Recital 18 states: "*... Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider*". Editorial responsibility implies that the provider makes active decisions about the content, its creation, development or modification[37]. In other words, they will not be able to invoke the safe harbour for information that they themselves have helped to create or develop.

40 As Perault (2023) rightly points out, but on the basis of section 230, that relevant question will be whether GAI 'develop' content, at least 'in part' to the extent that it can control or influence the outcome. Although drafted differently, the DSA and section 230 appear to follow the same line of reasoning[38]. "*The immunity extends to those who merely host or pass on information created by others. That's not necessarily true of generative AI*" (Henderson et al., 2023, p. 622). Content creation can then be considered a more 'proactive' act compared to organizing pre-existing content, which may make it difficult to argue that generative AI operates in a neutral way.

41 This paper does not argue that GAI alone is the author of the content; clearly, the user's prompt plays a significant role. However, a relevant contribution to the creation of content may suffice to disqualify a provider from safe harbour protections (because it has some level of control over the content). This would likely apply to a tool like Meta's Imagine, which transforms text prompts into entirely new images. As Perault (2023) observes, Twitter does not draft tweets for its users and thus qualifies for legal immunity. By contrast, using a *contrario sensu* interpretation, if Twitter were to assist in drafting tweets, it might lose that immunity[39]. This is precisely the scenario with Meta's Imagine function, which actively contributes to the creation of content by generating images based on user input.

42 While this is the general notion, this conclusion should also be nuanced on a case-by-case basis and

legal framework. Depending on the design and operation of the algorithm, a CAI could be held liable if it crosses the thresholds discussed here.

36 Authors from Europe who argue that GAIs are similar to search engines, such as Botero Arcila (2023) or Stalla-Bourdillon (2023), generally seek to have the due diligence obligations of the DSA, namely transparency and systemic risk assessment and mitigation, extended to them.

37 It should be emphasized that we are not referring here to basic system design decisions (e.g., how the interface is structured or how the model responds to prompts). This does not necessarily imply that the provider has editorial control over the generated content. Control neither is merely selecting or organizing third party information (what CAIs do). Editorial implies a certain degree of involvement in the outcome.

38 This analysis would perhaps be easier if the DSA had introduced a definition of 'content provider' as Section 230(f)(3) does: "*The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service*". In the United States, the analysis is facilitated by the availability of the 'material contribution test', developed by the case law to determine what degree of contribution to the content makes you cross the threshold, turning you into a content provider.

39 At this point, X (formerly Twitter) has arguably crossed that threshold by deploying Grok, its AI model that answers user queries. As a GAI, Grok produces new content based on patterns learned from large volumes of data.

not be treated in absolute terms, as there are different types of GAIs. In this respect, the distinction made by Henderson et al. (2023) and G'sell (2024) between *extractive* models, which are based on extracting information from third party sources, and *abstractive* models, is particularly relevant. *Extractive* models directly use and reproduce content from third-party sources without significant alteration. Their output is a direct reflection of the input data, making it easier to trace the origin of the information. *Abstractive* AI models, on the other hand, are designed to generate new content based on a deeper understanding of the input data. Unlike extractive models, abstractive systems create their own summarized representation of information, enabling them to reformulate, restructure, or combine ideas. As a result, extractive models are more likely to qualify for safe harbour protections, whereas abstractive models, due to their transformative nature, are less likely to do so (Volokh 2023, p. 496).

43 Another element to consider would be the use of synthetic data created by the company itself to train its AI. If the company is found to have played a substantial role in shaping the content on which the model is trained, its impact on the outcome of the model could be considered to be even higher. The manner in which data is incorporated into the model's training through the use of proprietary data sources could strengthen the argument that the company is actively shaping the content. In essence, the more a company is involved in the curation, editing, or creation of data, the more difficult it becomes for immunity to be applied (Henderson et al., 2023).

44 In summary, under current EU regulations, GAI would have to be excluded from the safe harbour benefit because of its active role in content creation. It would be a matter of degrees, the more 'expressive' and 'creative' the AI is, the more influence it can be said to have on the final content. An AI that only reproduces third party excerpts might have a stronger argument for immunity.

45 This even seems to have been understood by the companies themselves, which can be inferred from their reaction to some lawsuits in the US[40]. In *Walters v. OpenAI*[41], Mark Walters, a radio talk show host, filed a defamation lawsuit against OpenAI after ChatGPT generated false information about him. The AI system erroneously described Walters as a defendant in a separate lawsuit and falsely accused him of fraud. Walters claims that these fabricated statements caused significant reputational damage, particularly affecting his career and audience. In *Battle v. Microsoft*[42], the plaintiff, Jeffery Battle, a U.S. Air Force veteran, filed a defamation lawsuit against Microsoft after discovering that searching his name on Bing resulted in a false description linking him to the "Portland Seven", a group of U.S. citizens who attempted to join the Taliban after 9/11. This mistake arose from the AI-assisted Bing search, which conflated his biography with that of a similarly named individual. Battle claims the false information caused significant reputational harm and seeks both monetary compensation and permanent removal of the erroneous data from Bing search results. What is interesting about these two cases is that defendants have not relied on the Section 230 defense so common in previous cases where social networks have been sued. It can be inferred that these companies may also have anticipated that immunity does not apply to the type of business they operate[43].

F. How to Limit the Proliferation of Harmful Content from General-Purpose GAI (GPGAI)?

46 The "easier" question has been clarified in the previous sections: GIA does not receive immunity based on European legislation and case law. However, we must still decide how to regulate these tools that have the potential to generate so much harmful content. To this end, the article now focuses on European law's responses to this issue. The goal must be to find solutions that both empower these new technologies and incentivize the implementation of reasonable security measures[44].

47 In the European Union (EU), known for its proactive and comprehensive approach to technology regulation, GPGAI[45] poses unique challenges that

40 To date, I am not aware of similar processes in Europe.

41 L.L.C., 1:23-cv-03122, (N.D. Ga.).

42 No. 1:2023cv01822 - Document 48 (D. Md. 2024)

43 Keep in mind that this is only an author's inference, since other factors may have also influenced this defense.

44 To some extent this may contribute to decreasing the presence of illegal content on social media platforms, i.e. as less illegal content comes out of these IAGs, less illegal content will be published on the platforms. These tools should be designed for legitimate uses, not as tools to achieve harmful outcomes. "*Lawmakers could directly ex ante regulate the AI's risk-creating behaviour. Namely, regulatory agencies could ex ante set detailed standards for the behaviour, employment, operation and functioning of any AI*". (Kovač, 2021, p. 109)

45 The previous sections dealt with generative artificial intelligence from a broader perspective, however, this section 5 focuses specifically on one type of generative artificial intelligence, namely general-purpose generative artificial intelligence (GPGAI), given the unique challenges it poses.

expose some loopholes. Therefore, this section discusses the main legal uncertainties in the European regulation of GPGAI, specifically how due diligence duties and transparency obligations are structured. This critical examination aims to contribute to the debate on the need for a more robust legal framework adapted to the realities of this emerging technology.

I. Loopholes in European Law regarding GPGAIs

1. AI Act

48 The EU AI Regulation (Artificial Intelligence Act), considered a pioneering global framework, seeks to establish risk categories for AI applications and set reasonable standards for their implementation. This represents a significant shift in policy by adopting a risk-based, preventive approach to regulate AI *ex-ante*, focusing on preventing harmful outcomes using safety principles. This "ecosystem of trust" aims to provide legal certainty for innovation while ensuring AI operators fulfill obligations proportionate to the risks their systems pose. The regulation seeks to prevent both material harm (e.g., threats to health, safety, or property) and immaterial harm[46], such as violations of fundamental rights (e.g., privacy, freedom of expression, dignity) and societal concerns like disinformation (de Graaf and Veldt, 2022, p. 804; Kretschmer et al., 2023, p. 3).

49 Four risk categories are distinguished:

- **Unacceptable risk**: implementation of AI in these areas will be forbidden. Examples include social scoring systems, facial recognition in public spaces, and manipulative AI. (Chapter 2, Article 5)
- **High-risk AI**: Most of the regulation focuses on this category. These systems are recognized in Annex III: Remote biometric identification systems, critical infrastructure, education, employment, access to and enjoyment of essential public and private services, law enforcement and Administration of justice[47].
- **Limited risk**: In theory this is the relevant category for General Purpose AI models and systems, requiring transparency in cases of, for example, chatbots or generation that may constitute deepfakes.
- **Minimal risk**: This level includes all other AI systems that do not fall under the above-mentioned categories.

50 The AI Act imposes specific obligations depending on the type of technology; therefore, it is crucial to accurately identify the technology in question to establish the applicable responsibilities. In this regard, to understand the obligations of a GPGAI, such as Meta's Imagine or Midjourney, it is necessary to differentiate between *general-purpose AI models*, *general-purpose AI systems* and *AI systems*. This distinction is essential, as different responsibilities and obligations apply to each of these categories, that in the end represent different stages and actors in the chain of operation of an AI.

51 ***General-purpose AI models*** (Article 3(63) and Recital 97) are characterized by their ability to perform a wide variety of tasks in a competent manner[48]. They can be distributed in various forms, such as libraries, APIs, direct downloads or hard copies, and are commonly modified or tweaked to create new models[49]. It is important to note that while these AI models are essential components of AI systems, they do not constitute systems per se. To become AI systems, they need additional elements, such as a user interface. In general, AI models are often integrated as part of larger AI systems. The EU IA Act classifies general purpose IA models (GPAIM) according to their level of risk: *systemic* or *non-systemic*. A GPAIM is considered systemic risk if it has 'high capabilities', that is, if it has considerable calculation capacity, which implies that it has required more than 10^25 floating point operations per second (FLOPS).

52 According to Article 3(1) an ***IA system*** is "*a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*". This is the most encompassing category for which the AI act is meant from the outset.

53 Meanwhile, a ***general-purpose AI system*** (Article 3(66) and Recital 85) "*means an AI system which is based on a*

46 As will be discussed later, this is an essential difference with the new Defective Products Directive.

47 Although these were the activities initially listed, the plan is for the list to be periodically reviewed and updated.

48 "The term "general purpose" is indicative of the models' abilities to be adapted to a variety of tasks outside of those for which they were specifically trained". (G'sell, 2024, p. 34)

49 In these cases, the question of accountability can be complicated by the fact that another actor is involved in the production chain, which may incorporate functionalities unforeseeable by the creator of the original model.

general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems". Recital 100 is more specific and indicates that "*when a general-purpose AI model is integrated into or forms part of an AI system, this system should be considered to be general-purpose AI system when, due to this integration, this system has the capability to serve a variety of purposes*"[50].

54 Using our case study to better illustrate these differences, the *system* and the *model* can be distinguished as follows:

- **LLama** is the underlying model on top of which Imagine runs (as ChatGPT runs on top of Open AI's GPT model). If we focus on the definition of the AI Act, LLama has the key characteristics of a GPAI model, namely generality. It can be tuned or adapted to specific applications, be it in the field of health, education, etc. On its own, LLama is not a system, as it lacks the necessary components to interact with users directly (such as user interfaces or specific input/output mechanisms). In other words, this is the general purpose model, designed for a wide range of tasks but not linked to a specific use case until it is integrated into a system.

- **Imagine** is the system that uses LLama as its core but incorporates other elements that make it a functional and specific tool: an interface that allows user interaction and additional components designed to handle the outputs (tuning and adjustments) to meet the specific objectives of the system and facilitate its practical use. In other words, it is the complete AI system, which, based on LLama, adds components needed to solve specific problems and provides an interface for users to interact with the underlying model.

55 Considering the above distinction, we shall now consider what obligations the AI Act establishes for such general-purpose GAI tools as Imagine, Midjourney or ChatGPT. In the case of Imagine and some other AIs, a single company concentrates control over both the model and the system. That is, Meta owns both the model (LLama) and the system (Imagine). This means that Meta will have to take into account the obligations that the regulation establishes for both tools[51].

56 As mentioned earlier, as far as the *system* is concerned, this type of AI seems to fit, in principle, in the Limited risk group, which means that the law establishes for them some specific obligations. According to Article 50:

- Providers should ensure that AI systems that interact directly with individuals inform them that they are dealing with an AI, unless this would be obvious to a reasonably informed and observant person in the context.

- Providers must mark the generated synthetic content (audio, image, video or text) in a machine-readable format and detectable as artificial[52]. Technical solutions must be effective, interoperable, robust and reliable, taking into account technical constraints, costs and recognized standards.

- Deployers of AI systems that generate or manipulate content (image, audio or video) as deepfakes must disclose that it is artificial[53]. If text is generated to report on matters of public interest, it must be disclosed as artificial, except if it is authorized by law to combat crime or if the content has been reviewed and is under human editorial responsibility.

57 Regarding the model, its obligations are recognized in Chapter 5. It first sets out the obligations of general-purpose AI models and later those that present systemic risk. Regarding the former, Article 53 states that providers must (a) maintain detailed technical documentation of the model, including its training, testing and results; (b) provide information and documentation to AI system providers that integrate the model, ensuring understanding of the model's capabilities and limitations; (c) implement a policy to comply with copyright laws, using state-of-the-art technologies to identify rights reservations in accordance with Directive (EU) 2019/790; (d) publish a detailed summary of the content used to train the model. As for the latter, article 55 states that they must follow the above obligations and in addition must (a) conduct assessments following standardized protocols and advanced tools, including documented adversarial testing to identify and mitigate systemic risks; (b) assess and mitigate systemic risks in the European Union, including their possible sources during the development, marketing or use of the model; (c) timely record, document and report relevant information on

50 "The majority of generative AI users do not engage directly with a generative AI model. Rather, they interact through an interface with a generative AI system that incorporates the model". (G'sell, 2024, p. 36)

51 Although this is the case in other scenarios such as Open IA with GPT or Google with Gemini, it does not always necessarily be so, as in other cases a company could only be in charge of the model, while another company is developing the system. In these cases, each will have to respect their respective set of obligations.

52 This would make it easier for social networks to detect them.

53 This would facilitate the moderation of AI-generated content in social networks.

serious incidents and corrective actions to the IA Office or to the authorities; (d) ensure an adequate level of cybersecurity protection for the model and its infrastructure.

58 It should be mentioned that these obligations became part of the Regulation very late in the process. This is because the GAI explosion happened at a stage when the general structure of the regulation was already relatively advanced. This situation explains why some aspects of the law may seem insufficient or not fully adapted to the techno-social realities of these systems[54]. One of the most problematic issues is when these general-purpose AIs end up being used in the context of activities that qualify as high risk. If the interface allows Imagine to be used in areas considered high-risk according to Annex III of the regulation, such as education or justice[55], would the whole system be classified as a high-risk AI system and be subject to the corresponding obligations? It is a plausible scenario, one that puts in tension the coherence of the whole norm with techno-social reality.

59 As Helberger and Diakopoulos (2023, p. 2) rightly note, generative AI systems, such as Imagine or Midjourney, have key differences from the traditional AI systems for which the AI Act was originally intended. These differences are their dynamic context and scale of use. It should be stressed that these generative AI systems are not designed for a specific purpose or context, but rather they are adaptable for later use in a wide range of fields, and their accessibility allows for a massive and diverse use, and is not aimed at a specific audience. This broad scope is partly a result of the massive scale of data used for training. These characteristics pose significant challenges to the AI Act's core approach, especially in terms of classifying these systems into high/low risk categories and the inherent unpredictability of future risk. Therefore, this classification criterion may not be the most appropriate for AI of general and widespread use.

60 According to the current logic of the AI Act, the classification of an AI system as unacceptable, high or minimal risk depends on the intended use of the system. Systems intended for areas specified in Annex III are considered high risk, while in other cases they are classified as minimal or no risk. However, in the case of general-purpose AI, it is the deployer who decides how to use the system, meaning that it is the deployer who ultimately determines whether the system falls into the high or low risk category[56] or even whether a use prohibited by Article 5 is made[57]. In most cases, therefore, the risks to society stem from the use of these systems by deployers. However, the personal scope of the regulation must be considered here. In the definition of deployer it states: "'*deployer means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*"; which means that the obligations of this rule do not extend to ordinary users. The problem is that the regulation is ignoring the millions of users who use General-Purpose AI Systems, when these users are the ones who introduce the prompts to generate illegal content and on whom a certain share of responsibility should perhaps fall. It therefore seems that the regulation does not fully capture the particularities of GPGAI that have the capacity to generate a massive and unpredictable impact.

61 The unpredictability of future risks associated with GPGAIs also relates to their widespread use and to the versatility of these systems. According to the AI Act, providers of high-risk AI systems should be able to identify and analyze all potential risks associated with their use in areas such as health, security and fundamental rights. This includes anticipating all high-risk uses that may arise, including those that were not initially foreseen[58]. For each of these possible scenarios, suppliers would have to develop and implement mitigation strategies to reduce risks (Recitals 65, 114, and article 9). However, this is extremely costly and difficult to implement, as risk

54 "*While this scheme has worked relatively well for tangible products, the division of duties seems much more questionable in a world of (a) AI as a service which learns and changes, (b) 'AI as a service' or 'upstream' AI services, (c) general purpose AI and (d) AI as part of the services of a platform (the 'AI lifecycle').*" (Edwards, 2022, p. 5)

55 GPGAI can potentially be used to assess the learning outcomes of individuals (see recital 56) or to assist in the drafting of judicial documents (see recital 61).

56 This is a reality that the regulation seems to recognize in Recital 85: "*General-purpose AI systems may be used as high-risk AI systems by themselves or be components of other high-risk AI systems*" and Recital 84: "*To ensure legal certainty, it is necessary to clarify that, under certain specific conditions, any distributor, importer, deployer or other third-party should be considered to be a provider of a high-risk AI system and therefore assume all the relevant obligations. This would be the case if that party ... modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service, in a way that the AI system becomes a high-risk AI system in accordance with this Regulation*".

57 The use of generative AI to create misleading or manipulative advertising or propaganda.

58 "AI systems can be general purpose, meaning the same system can be applied to different contexts and raise different impacts for different individuals and groups. For example, a developer of a facial recognition system could sell their product to authenticate entry to prisons or to surveil customers for targeted advertising. Holistically evaluating the risk of such a system in the abstract is an impossibility". (Edwards, 2022, p. 6)

assessments would have to be based on hypothetical scenarios and mitigation measures would depend on specific conditions of use, which have not yet occurred at the time of the assessment[59]. This is a shortcoming of the regulation, as *ex ante* risk assessments may not adequately capture all of the multiple real-life scenarios of use of a GPGAI. (Hacker et al., 2023, p. 1114).

2. Defective Products Directive (EU) 2024/2853

62 Product safety is not only achieved with *ex ante* and preventive standards. Ex post liability rules also operate as strong normative elements to moderate certain activities and to prevent damage. It could be said that *ex ante* rules such as the AI Act try to prevent the event of harm from occurring in the first place, but sometimes the harm does occur anyway, and someone has to compensate the victim. This is where tort law and its deterrence function intervene.

63 In the field of AI, it is the new Product Liability Directive (EU) 2024/2853 that regulates compensation for certain damage caused by AI systems[60]. The fundamental goal of this new directive is to harmonize the laws of the Member States of the European Union regarding the producer's liability for damage caused by defective products. This new directive repeals and replaces the previous Directive 85/374/EEC of 1985, thus updating the EU legal framework to adapt it to current technological and legal realities. This harmonization seeks to ensure better consumer protection in the European internal market. The directive addresses the challenges and opportunities posed by recent technological developments, especially in the following areas: Digital products, Artificial intelligence and Software (now explicitly considered as a product). Member States will have to transpose this new directive into national law by 9 December 2026 at the latest.

64 The first issue to highlight here, in the words of de Graaf and Veldt (2022, p. 823), is that "*product liability is, in short, limited to damage to property (other than the product itself) and damage resulting from death or personal injury caused by a defect in the product. In any case, liability for pure economic loss is left to national law*". Therefore, here we already face the first obstacle: the outputs of generative AI could be illegal, but the directive is unlikely to apply given the nature of the harm that such technology can generate (child abuse, defamation, intellectual property breaches, non-consensual sexual deepfakes or hate speech)[61]. This regulation is therefore of little relevance in assessing the damage caused by GPGAI. This has been criticized by Hacker (2024, p. 12) in the following way: "*instances of discrimination or violation of personality rights equally, and in some cases perhaps even more strongly, impact fundamental rights as the typical PLD scenarios of damage to property or health".*

65 In addition to the above, there is a CJEU ruling that may make it difficult to hold GAIs liable for the outputs they produce under the new defective product Directive. In the *Krone*[62] case, the Court determined that a newspaper containing erroneous health advice could not be deemed a defective product because the defect lay in the information, not the newspaper itself. Information, as a service, was considered out of the scope of the Directive. Applying this reasoning to generative AI outputs remains contentious[63]. Van Staalduinen (2024) argues that, unlike the newspaper in *Krone*, an AI system is not merely a carrier of information but its source. The outputs of AI are integral to their design and purpose. Unlike external advice published in a newspaper, the output of a GAI reflects its functionality and adaptability. This perspective hinges on the notion that the AI's design and operation inherently shape its outputs, linking any defects in those outputs to the product itself. Therefore, if a GAI produces erroneous or harmful outputs, it could be classified as defective under the Directive. This distinction highlights that not all information-providing products are the same; while the newspaper in *Krone* served as a medium for external information, GAI directly create the information they provide, warranting potential liability under the DPLD for resulting damages.

59 "... it is simply impossible to predict if, and if so, what the risks are that we can expect from unleashing extremely powerful AI models on society". (Helberger and Diakopoulos, 2023, p. 4)

60 This paper focuses on the Defective Products Directive, as the draft of the AI Liability Directive remains unofficial and lacks a definitive agreement on its provisions.

61 Directive' Recital 24: "*Types of damage other than those provided for in this Directive, such as pure economic loss, privacy infringements or discrimination, should not by themselves trigger liability under this Directive. However, this Directive should not affect the right to compensation for any damage, including non-material, under other liability regimes*".

62 ECJ, Krone, 1 June 2021, C-65/20, ECLI:EU:C:2021:471.

63 For arguments in favor of recognizing these AI tools as defective products see Spindler (2023) and Camacho Clavijo (2024). "*Contrary to what is established in the Case C-65/20 VI v KRONE, there is in our case a fundamental difference that may justify a different qualification in the context of product liability for software and printed information. In our case software does not simply convey information but constitutes an entity that can be used for the specific purpose for which it has been designed. The inaccurate medical assessment or prediction/information issued by the AI system constitutes an intrinsic element of the purpose-built system itself and is therefore implicit in its use and could therefore qualify as a defective product*" (Camacho Clavijo, 2024). For the argument against see (Borges, 2023, p. 39)

66 However, the application of the Directive to GAI remains contentious. While Van Staalduinen's interpretation offers a compelling argument[64], it must be acknowledged that this is still a matter of controversy and as such, some may still consider GAI to be outside the scope of the defective product Directive. Courts may need to address this regulatory gap by clarifying the scope of the DPLD regarding harmful information/outputs provided by GAI systems.

67 Even if GAI outputs are deemed outside the DPLD's scope, this does not mean such activities are exempt from liability. In these cases, national law, often based on principles of negligence, would likely govern. Here, the existence of a duty of care, a breach of that duty, and causation of harm would need to be established. For instance, if a developer fails to adequately train or monitor the AI system, and this negligence results in harm, liability could still arise under national frameworks, either civil, criminal or administrative.

II. Clarifying GPGAI Obligations.

68 While the AI Act and the new Defective Products Directive seek greater regulatory harmonization across the EU, the reality is that the current framework does not fully address the particularities and risks of GPGAI, limiting its effectiveness in both preventing and redressing harm. This legal exposure may have major implications for the future deployment of generative AI products and the public at large.

69 Thus, a more dynamic approach to continuous risk monitoring and mitigation is advocated here. In order to do so, however, amendments to the current AI act would have to be made. For example, the duties under Article 55[65], namely (i) to conduct adversarial testing to identify and mitigate systemic risks and (ii) to assess and mitigate risks during the development, marketing or use of the system, should apply to all GPGAI systems without having to subject them to high/low risk categorization. These duties are best performed not by the model developer[66], but by the system developer, who has a sounder awareness of how the system is being used by the users. It would be something like GPGAI with systemic risks or "general risk GAI".

70 Helberger and Diakopoulos (2023, p. 4) suggest drawing inspiration from Article 34 of the Digital Services Act (DSA)[67], already obliging very large *intermediaries* (online platforms and search engines) to regularly monitor the negative effects of their algorithmic systems on fundamental rights and social processes. This approach could be extended to providers of large-scale generative models, requiring them to assess and mitigate systemic risks on an ongoing basis. Hacker et al. (2023) go a step further and propose to amend the DSA to incorporate a fourth category: GPGAIs as *content providers*[68]. This is due to what has already been discussed: the DSA's scope of application is restricted to intermediaries, it does not apply to content providers *per se*. However, this does not prevent this norm could be expanded in the future with some amendments to regulate also some aspects of the GPGAIs[69]. Certainly, this technology could also benefit from the implementation of some established solutions developed in the DSA, including notice and action, trusted flaggers systems or compulsory dispute resolution[70], as none of these

64 Van Staalduinen (2024) also argues that if software, alarm systems, smart watches or other measurement devices are recognized as products by the DPLD impact assessment, and after all, their function is essentially to provide information, there is no reason to exclude AI which ultimately performs a similar function.

65 Obligations of *providers* of general-purpose AI *models* with systemic risk.

66 The duties of the model developer should actually focus on ensuring the quality and security of the training data and knowing as much as possible about the capabilities and limitations of the model, which should be communicated to the system developer.

67 These generative models are special because they produce content that can support human communication, which raises new challenges and questions about how to regulate the use of AI to ensure that this communication is ethical and responsible. The DSA regulates digital spaces where much of this human communication happens, establishing a framework to make it safer, more transparent and more respectful of fundamental rights. Although the DSA is designed to apply only to intermediaries, as argued at the beginning of this article, its general objectives and purposes are so broad that, in principle, it could cover a wide variety of electronic services.

68 "*For example, to extend the DSA to LGAIMs in specific ways, one would have to update the DSA or include a reference in the AI Act. Both modifications require concurring decisions by the EP and the Council (Art. 289 TFEU)*" (Hacker et al., 2023, p. 1120). As can be noted, these authors only consider it possible to find a solution through the modification of one of the two norms. This seems to be a sound solution compared to writing a completely new standard.

69 This would require a number of modifications to the DSA, in particular to nuance the active/passive division, which is not representative of GPGAIs. A different activity criterion should be introduced for GPGAIs, one that measures rather the degree of involvement, influence or contribution to the content, based on the differences explained between extractive and abstractive models.

70 "*While the notice and action mechanism applies to all hosting services, instruments like trusted flaggers, obligatory dispute resolution, and risk management systems are reserved for the*

are recognized as such in the AI Act. It would seem a good idea to require developers and operators of GPGAIs to adopt notice-and-action mechanisms, prioritizing alerts sent by trusted moderators[71]. They could then adjust systems to block problematic prompts and avoid loopholes exploited by malicious actors. Therefore, this article argues that effective regulation of the GPGAI necessarily requires the amendment of at least one of the two regulations currently in force: the DSA or the IA Act (Hacker et al., 2023, p. 1120). A revision is required to establish a bridge between these two regulations, avoiding a vacuum that would be filled by opaque self-regulatory measures. While it is certainly plausible to adopt expansive interpretive approaches (Botero Arcila, 2023; Stalla-Bourdillon, 2023), such a strategy would provide only partial solutions and does not comprehensively address the existing regulatory gap. Legal certainty for market operators and users must be ensured through the development of clear, tailored, and predictable legal obligations.

71 In summary, to limit the massive generation of illegal content, the norm should at a minimum have the following obligations in place for model providers and system deployers, regardless of the level of risk involved:

- Obligations relating to the developer of the general-purpose GAI *model*: safeguards related to the training of the model, i.e.: curation of data used to train the model (inspired by Article 10), collaboration with potential deployers to create operational synergies that improve the security of the system (Article 11), conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks (Article 55(1)(a)), ensuring an adequate level of protection for cybersecurity and for the physical infrastructure (Article 55(1)(d))

- Obligations relating to the deployers of general purpose GAI *systems*: as this is the system that is implemented around the model and is the one with which the public interact directly, the duties are more focused on fine-tuning, adding security layers and functionalities, for example: collaborating with the model developers to create operational synergies to improve the security of the system, conducting and documenting adversarial testing of the model in order to identify and mitigate systemic risks, implementing external systems that analyze inputs and outputs to identify and block problematic content, implementing a DSA-inspired notice and action system, involving trusted flaggers.

72 Some companies are already incorporating some of these security mechanisms on a voluntary basis. In a recent paper, Chi et al. (2024) present Llama Guard 3 Vision, a model that improves the safety of multimodal AI conversations by addressing harmful content in both inputs (prompts) and outputs (responses) involving images. Unlike previous versions of Llama Guard, which only analyzed text, this version is specifically designed to support image reasoning use cases. Llama Guard 3 Vision can therefore analyse images in conjunction with text to identify harmful content that previous versions of Llama Guard might miss. For example, it can detect an inappropriate request based on the image provided, even if the text itself is not problematic. The model is trained to predict safety labels based on the 13 risk categories of the MLCommons taxonomy. These categories include violent crimes, sexual content, hate speech, election misinformation, and more. While Llama Guard 3 Vision offers an additional layer of protection, it is not immune to adversarial attacks. It is important to be aware of its limitations and to continue to explore ways to improve its robustness against malicious users.

G. Conclusion

73 The technical differences between generative AI (GAI) and content curation AI (CAI) are central to defining their potential liability regarding the content they create or organize. Based on the European law and case law approach, this differences are key to deciding whether they can benefit from the safe harbour doctrine. The European Union (EU), through the Digital Services Regulation (DSA), focuses on the

narrower group of "online platforms"". (Hacker et al., 2023, p. 1118)

71 Developers of generative AI systems usually implement a variety of measures to prevent their product from being used for malicious purposes. These measures consist of stress-testing the system in an attempt to identify potential vulnerabilities in advance. This approach is known as "red-teaming" (Ahmad et al., 2024). This generally consists of asking a network of external human testers to try to bypass security safeguards in an attempt to identify vulnerabilities. This is one way to understand how users could potentially interact with the system. However, no amount of testing can completely rule out unwanted or harmful behavior due to the complexity of language models and the ways in which users interact with them. That is why this article advocates borrowing approaches from the DSA as a way to improve the system on a more continuous basis and with the involvement of more stakeholders beyond "red-team". It suggests the implementation of a "notice and action" system, allowing continuous monitoring based on real-time detection and active response to incidents. This approach overcomes the limitations of relying solely on ad hoc tests such as those carried out by the "red-teams".

concept of active role to determine the liability of online intermediaries. An entity has an active role when it has a direct involvement (control) in the creation of content. As discussed, the *abstractive* GAI has a more active role, since it produces new information, something that goes beyond curation or mere recommendation. Therefore, the *abstractive* GIA loses the benefit of safe harbour in the EU, as its crucial contribution to content creation makes it to some extent responsible for the outcomes.

74 This raises the need for specific rules to define the appropriate scope of accountability expected for these technologies. However, current EU legislation presents loopholes in the regulation of GPGAI. With its massive usage capacity, versatility and unpredictability of potential risks, GPGAI challenges the current risk-based approach of the AI Act. The difficulty of anticipating and mitigating all risks, together with the exclusion of ordinary users from legal obligations, limits the effectiveness of the law in preventing and redressing harm. It could be important to draw inspiration from Article 34 of the Digital Services Act (DSA), which obliges large search engines and platforms to regularly monitor the negative effects of their algorithmic systems on fundamental rights. It is also particularly important to define the responsibilities of the actors involved in the supply chain: essentially those who design and train the models and those who put the system into operation for the public. Specifically, the latter, due to their closer understanding of user actions, should focus on fine-tuning and implementing functionalities like adversarial testing, input/output monitoring, and notice-and-action systems to mitigate risks and ensure safety. The implementation of safeguards in GPGAI should be continuous, based on real-time detection and active response to incidents, rather than depending solely on adversarial *ex-ante* testing. However, in order to materialize these obligations, it is necessary to bridge the gap between the DSA and the IA act, since it seems that neither of them succeed in capturing the real essence of the GPGAIs.

75 To conclude, it is worth remembering that any legislative strategy in the field of AI must acknowledge the global nature of this market and the intense competition for technological development but also restate the commitment to the protection of democratic values and fundamental rights. Any successful European regulatory reform cannot afford to ignore the strategies adopted by other jurisdictions, especially the United States and China. However, neither can it uncritically replicate their approaches, which often prioritize innovation at the expense of safety, transparency and accountability. Instead, Europe must go its own way, it must aspire to become a global benchmark in AI development and deployment, not only for its technological capabilities, but also for its commitment to ethics and security. Ultimately, the European approach must be based on the conviction that technological development and the protection of fundamental rights are not incompatible, but complementary. We are confident that in the long term this is the right way forward for sustainable leadership in the age of artificial intelligence.

H. REFERENCES

Ahmad, L., Agarwal, S., Lampe, M., Mishkin, P., 2024. OpenAI's Approach to External Red Teaming for AI Models and Systems. Technical report, OpenAI, November 2024. URL: https://cdn.openai.com/papers/openais-approach-to-external-red-teaming.pdf

Angelopoulos, C., 2017. "On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market". Available at SSRN 2947800.

Arroyo Amayuelas, E., 2020. "La responsabilidad de los intermediarios en internet: ¿Puertos seguros a prueba de futuro?" Cuadernos de Derecho Transnacional, 2020, num. 1, p. 808-837.

Balkin, J.M., 2021. "How to regulate (and not regulate) social media". J. Free Speech L. 1, 71.

Bambauer, D.E., Surdeanu, M., 2023. "Authorbots." J. Free Speech L. 3, 375.

Belcic, I., Stryker, C., 2024. "What is GPT (generative pre-trained transformer)?" | IBM [WWW Document]. URL https://www.ibm.com/think/topics/gpt (accessed 11.25.24).

Borges, G., 2023. "Liability for AI Systems Under Current and Future Law: An overview of the key changes envisioned by the proposal of an EU-directive on liability for AI". Computer Law Review International 24, 1–8.

Botero Arcila, B., 2023. "Is It a Platform? Is It a Search Engine? It's ChatGPT! The European Liability Regime for Large Language Models Symposium: Artificial Intelligence and Speech." J. Free Speech L. 3, 455–488.

Camacho Clavijo, S., 2024. "AI assessment tools for decision-making on telemedicine: liability in case of mistakes". Discover Artificial Intelligence 4, 24.

Candeub, A., 2020. "Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230". Yale JL & Tech. 22, 391.

Chander, A., Krishnamurthy, V., 2018. "The myth of platform neutrality". Geo. L. Tech. Rev. 2, 400.

Chi, J., Karn, U., Zhan, H., Smith, E., Rando, J., Zhang, Y., Plawiak, K., Coudert, Z.D., Upasani, K., Pasupuleti, M., 2024. "Llama Guard 3 Vision: Safeguarding Human-AI Image Understanding Conversations". arXiv preprint arXiv:2411.10414.

Cohen-Almagor, R., 2010. "Responsibility of and Trust in ISPs". Knowledge, Technology & Policy 23, 381–397.

de Graaf, T., Veldt, G., 2022. "The AI Act and Its Impact on Product Safety, Contracts and Liability". European Review of Private Law 30.

Edwards, L., 2022. "Regulating AI in Europe: four problems and four solutions". Ada Lovelace Institute 15, 2022.

Elkin-Koren, N., De Gregorio, G., Perel, M., 2021. "Social Media as Contractual Networks: A Bottom Up Check on Content Moderation". Iowa L. Rev. 107, 987.

Gillespie, T., 2018. "Platforms are not intermediaries". Geo. L. Tech. Rev. 2, 198.

Grimmelmann, J., 2015. "The virtues of moderation". Yale JL & Tech. 17, 42.

G'sell, F., 2024. "Regulating under Uncertainty: Governance Options for Generative AI". Stanford Cyber Policy Center. Freeman Spogli Institute. Stanford Law School.

Hacker, P., 2024. "Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment". EPRS | European Parliamentary Research Service.

Hacker, P., Engel, A., Mauer, M., 2023. "Regulating ChatGPT and other large generative AI models", in: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. pp. 1112–1123.

Helberger, N., Diakopoulos, N., 2023. "ChatGPT and the AI Act". Internet Policy Review 12.

Henderson, P., Hashimoto, T., Lemley, M., 2023. "Where's the Liability in harmful AI Speech?" J. Free Speech L. 3, 589.

Husovec, M., 2023. "Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules". Berkeley Technology Law Journal 38.

Keller, D., 2023a. "What the Supreme Court Says Platforms Do". Lawfare. URL https://www.lawfaremedia.org/article/what-the-supreme-court-says-platforms-do (accessed 11.30.23).

Keller, D., 2023b. "Carriage and Removal Requirements for Internet Platforms: What Taamneh Tells Us". Journal of Free Speech Law 4, 87–138.

Khosrowi, D., Finn, F., Clark, E., 2024. "Engaging the many-hands problem of generative-AI outputs: a framework for attributing credit". AI and Ethics 1–19.

Kosseff, J., 2022. "A User's Guide to Section 230, and a Legislator's Guide to Amending It (or Not)". Berkeley Technology Law Journal 37.

Kovač, M., 2021. "Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework". European Journal of Risk Regulation 13, 94–113.

Kretschmer, M., Kretschmer, T., Peukert, A., Peukert, C., 2023. "The risks of risk-based AI regulation: taking liability seriously". arXiv preprint arXiv:2311.14684.

Land, M.K., 2019. "Regulating Private Harms Online: Content Regulation under Human Rights Law", in: Human Rights in the Age of Platforms. Cambridge, MA : The MIT Press, p. 285.

Leerssen, P., 2020. "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems". European Journal of Law and Technology 11.

Llansó, E., van Hoboken, J., Leerssen, P., Harambam, J., 2020. "Artificial Intelligence, Content Moderation, and Freedom of Expression". Transatlantic High Level Working Group, Working Group on Content Moderation Online and Freedom of Expression. Annenberg Public Policy Center.

Miers, J., 2023. "Yes, Section 230 Should Protect ChatGPT And Other Generative AI Tools". Techdirt. URL https://www.techdirt.com/2023/03/17/yes-section-230-should-protect-chatgpt-and-others-generative-ai-tools/ (accessed 11.20.24).

Mirmira, S., 2000. "Lunney v. Prodigy Services Co". Berk. Tech. LJ 15, 437.

Noto La Diega, G., Bezerra, L.C., 2024. "Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive". International Journal of Law and Information Technology 32, eaae021.

OECD, 2024. Explanatory memorandum on the updated OECD definition of an AI system (No. 8),

OECD Artificial Intelligence Papers. OECD Publishing, Paris.

OECD, 2022. OECD Framework for the Classification of AI systems (No. 323), OECD Digital Economy Papers. OECD Publishing, Paris.

Pagallo, U., 2011. "ISPs & Rowdy web sites before the law: Should we change today's safe harbour clauses?" Philosophy & Technology 24, 419–436.

Patel, S.K., 2002. "Immunizing Internet Service Providers from third-party Internet defamation claims: How far should courts go". Vand. L. Rev. 55, 647.

Perault, M., 2023. "Section 230 Won't Protect ChatGPT." J. Free Speech L. 3, 363.

Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., Sutskever, I., 2019." Language models are unsupervised multitask learners". OpenAI blog 1, 9.

Sartor, G., 2017. "Providers Liability: From the eCommerce Directive to the future", IP/A/IMCO/2017-07. ed. European Parliament's Committee on the Internal Market and Consumer Protection.

Spindler, G., 2023. "Different approaches for liability of Artificial Intelligence–Pros and Cons", in: Liability for AI. Nomos Verlagsgesellschaft mbH & Co. KG, pp. 41–96.

Stalla-Bourdillon, S., 2023. "What if ChatGPT was much more than a chatbox? What if LLM-as-a-service was a search engine?" Peep Beep! URL https://peepbeep.blog/2023/04/03/what-if-chatgpt-was-much-more-than-a-chatbox-what-if-llm-as-a-service-was-a-search-engine/ (accessed 3.31.25).

Sylvain, O., 2021. "Platform Realism, Informational Inequality, and Section 230 Reform". Yale LJF 131, 475.

Thorburn, L., 2022. "How Platform Recommenders Work. Understanding Recommenders". URL https://medium.com/understanding-recommenders/how-platform-recommenders-work-15e260d9a15a (accessed 12.1.23).

Valcke, P., Kuczerawy, A., Ombelet, P.-J., 2017. "Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien have in common", in: The Responsibilities of Online Service Providers. Springer, pp. 101–116.

Van Eecke, P., 2011. "Online service providers and liability: A plea for a balanced approach". Common Market Law Review 48.

Van Hoboken, J., Pedro Quintais, J., Poort, J., Van Eijk, N., 2018. Hosting Intermediary Services and Illegal Content Online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape, A study prepared for the European Commission DG Communications Networks, Content & Technology. URL: https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf

van Staalduinen, J.H., 2024. "European Product Liability for AI-based Clinical Decision Support Systems", in: Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. Springer, pp. 15–40.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, L., Polosukhin, I., 2017. "Attention Is All You Need". Presented at the 31st Conference on Neural Information Processing Systems, Long Beach, CA, USA. https://doi.org/10.48550/arXiv.1706.03762

Volokh, E., 2023. "Large libel models? liability for AI output". J. Free Speech L. 3, 489.

Volokh, E., 2021. "Treating social media platforms like common carriers?" J. Free Speech L. 1, 377.

York, J.C., Zuckerman, E., 2019. Moderating the public sphere, in: Human Rights in the Age of Platforms. Cambridge, MA: The MIT Press, p. 137.

Ziniti, C., 2008. "Optimal liability system for online service providers: How Zeran v. America online got it right and web 2.0 proves it". Berkeley Tech. LJ 23, 583.

Zurth, P., 2020. "The German NetzDG as role model or cautionary tale? Implications for the debate on social media liability". Fordham Intell. Prop. Media & Ent. LJ 31, 1084.

Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?

by **Nicolaj Feltes** *

Abstract: On April 21, 2021, the European Commission presented the first draft of the EU Artificial Intelligence Act, marking a significant step in Europe's regulatory approach to Artificial Intelligence (AI). The original proposal already included foundational transparency requirements, many of which are now formalised in Art. 50 of the Artificial Intelligence Act (hereinafter: AI Act). However, as AI technologies evolved rapidly – including the emergence of advanced tools like ChatGPT – the transparency obligations in Art. 50 AI Act were expanded to address new concerns around user awareness and content authenticity. Thus, notable additions such as labelling requirements for synthetic content and AI-generated texts were implemented in the final version of the AI Act.

In its finalised version, the AI Act specifies five distinct transparency obligations designed to enhance clarity and user protection across various AI applications. These obligations apply to interactive AI systems such as Chatbots (para. 1), AI systems for the creation of synthetic content (para. 2), systems for emotion recognition or biometric categorisation (para. 3), concerning AI-generated deep fake content (para. 4, subpara. 1), and AI-generated texts (para. 4, subpara. 2).

This article closely examines the transparency obligations, addressing potential issues of interpretation, practical challenges, and discusses whether the final version of the AI Act effectively addresses the problems present in the Commission's draft.

Keywords: AI Act, Transparency, Generative AI, Deep Fakes, DSA

Recommended citation: Nicolaj Feltes, Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?, 16 (2025) JIPITEC 222 para 1.

A. Introduction

1 With its proposal for a Regulation on Artificial Intelligence in April 2021 (hereinafter: AI Act-COM)[1], the European Commission introduced a comprehensive set of transparency provisions aimed at regulating AI systems and addressing concerns related to user awareness, content authenticity, and potential misuse. These obligations included requirements to design and develop AI systems in a way that natural persons are informed when interacting with an AI system (Art. 52(1) AI Act-COM), to notify users exposed to emotion recognition systems or biometric categorisation systems (Art. 52(2) AI Act-COM), and to disclose deep fake content as artificially generated or manipulated (Art. 52(3) AI Act-COM). However, several shortcomings of these transparency provisions have been identified, particularly due to the use of undefined legal terms in the proposal[2] and concerns regarding the effectiveness of the

* The author is a Research Associate at the Digital Law Institute Trier (IRDT) and PhD candidate of JProf. Dr. Lea Katharina Kumkar.

1 Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts' COM(2021) 206 final.

2 See for example C. I., regarding the transparency obligation of Art. 50(1) AI Act (formally Art. 52(1) AI Act-COM), which uses several undefined terms such as "interaction" and "obvious".

obligations, especially those focused on AI system users.[3]

2 More than three years later, on July 12, 2024, the final version of the AI Act was published in the OJEU, incorporating several revisions of these provisions. In addition, as more potent AI tools – such as ChatGPT – have surfaced since the initial draft of the AI Act, new transparency obligations for synthetic content and AI-generated texts have been introduced. This raises the question of whether the revised provisions, together with the newly introduced obligations, effectively address the proposal's deficiencies. This article compares the transparency obligations in the Commission's draft with those in the final Act, critically evaluating whether the modifications effectively address these shortcomings. It also explores potential gaps in the regulatory framework, focusing on the scope of the obligations, their addressees, the associated requirements, legal consequences, and exceptions.

3 Moreover, the interplay between the AI Act and the Digital Services Act (DSA) is examined, highlighting potential synergies and conflicts, as undisclosed AI-content may have significant implications for users on online platforms. This is particularly pertinent in the case of unlabelled deep fakes and AI-generated news, which can facilitate the rapid spread of disinformation. Accordingly, it seems imperative to assess whether platform providers are obligated to remove content not labelled in compliance with the given provisions. Central to this discussion is whether such content qualifies as "illegal content" under the DSA and whether machine-readable markings prescribed by Art. 50(2) AI Act effectively support the implementation of risk mitigation measures under Art. 35(1) DSA. Finally, this article raises critical questions about the adequacy and enforceability of the AI Act's transparency obligations in mitigating the risks associated with rapidly evolving AI technologies.

B. Relevant Actors and Scope of the Obligations

4 Before examining the transparency obligations set out in Art. 50 AI Act, it is necessary to determine whether and to what extent the AI Act applies. This requires an analysis of its scope – including the material scope (which systems are covered by the obligations), the personal scope (who is subject to the obligations), and the territorial scope (in which geographical contexts the AI Act is applicable).

I. Material Scope

5 The AI Act primarily targets providers and deployers of AI systems. Art. 3(1) AI Act defines the term "AI system" comprising five main components. An AI system is "(1.) a machine-based system (2.) designed to operate with varying levels of autonomy and that (3.) may exhibit adaptiveness after deployment, and that, (4.) for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that (5.) can influence physical or virtual environments".[4] A key characteristic of such systems is the capability to infer.[5] According to Recital 12 AI Act, this capability refers to the process of obtaining outputs (e.g. predictions or content) "which can influence physical or virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data".[6]

6 The Commission's draft initially proposed a "technology-specific" concept, which faced significant criticism for diverging too much from the OECD's "technology-neutral" definition.[7] The definition of an AI system as provided in the final version of the AI Act aligns with this definition outlined by the OECD.[8] These adjustments made during the legislative process, however, were of little significance for the transparency obligations now outlined in Art. 50 AI Act. For instance, general adversarial networks (GANs), commonly used to create synthetic content and deep fakes, meet the criteria in both the Commission's draft and the final version of the AI Act.[9]

3 This concern has been mainly raised in the context of deep fake disclosure, as AI systems providers are more likely to implement disclosure solutions within the system itself, see C. IV. 3.

4 See Martina J. Block, 'A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union' (2024) 4 EuCML 184, 185 f.

5 Recital 12, sentence 3 AI Act; for a more detailed analysis of the term "infer", see Alexander Steen, 'Ableitungen als wesentliche Fähigkeit von KI-Systemen nach der KI-VO' (2024) 1 KIR 2024, 7 ff.

6 Recital 12, sentence 4 AI Act.

7 Christiane Wendehorst in Martini/Wendehorst (ed.), KI-VO (2024), C.H. Beck, Art. 3 para 14 ff.

8 ibid para 17.

9 See Block, (n 4) 186; Additionally, as part of the "technology-specific" concept, the Commission's draft enumerates a list of covered technologies in Annex I. Notably, "deep learning" is highlighted in Annex I (a) AI Act-COM, which is primarily used in context of generative AI and deep fakes.

II. Personal Scope and Addressees

7 The personal scope of the AI Act includes both "providers" and "deployers" of AI systems, who are also the relevant actors subject to the respective obligations. The first two transparency obligations set out in Art. 50 AI Act pertain to the provider of the AI system, while the subsequent three fall under the responsibility of the deployer of the AI system.

1. Provider

8 Under Art. 3(3) AI Act, a *"provider"* is a natural or legal person, public authority, agency, or other body that develops an AI system or general-purpose AI model or has one developed. Additionally, the system or model has to be placed on the market[10] or put into service[11] under its own name or trademark, regardless of whether for payment or free of charge. In many cases, the term "provider" is synonymous with the software developer.[12] For instance, in the case of ChatGPT or Dall-E, OpenAI would be considered the "provider" of the AI system.[13]

2. Deployer

9 The three other transparency obligations pertain to the deployer of the AI system. Art. 3(4) AI Act defines the term *"deployer"* as a *"natural or legal person, public authority, agency or other body using an AI system under its authority"*. It is noteworthy that in the event that these subjects use the AI system "*in the course of a personal non-professional activity*" they are not considered to be a "deployer".[14] Thus, users who privately operate AI systems are not subject to the transparency obligations outlined in Art. 50(3) and (4) AI Act, as these obligations apply exclusively to deployers. Strong arguments favour a narrow interpretation of this exclusion, drawing parallels to the restrictive application of the household exemption in the General Data Protection Regulation (hereinafter: GDPR).[15] In this context, only "personal activities" are covered by the exception, suggesting that only natural persons can invoke this exception.[16]

10 Within the scope of Art. 50 AI Act, it is questionable what requirements should be placed on such "personal non-professional activities". In the context of the transparency obligations, this is particularly relevant with regard to the disclosure obligation for deep fakes outlined in Art. 50(4) subpara. 1 AI Act, as such content is typically disseminated via the internet, raising the question of whether such dissemination can still be considered a "personal non-professional activity". The exception under Art. 3(4) AI Act is contingent on whether the "use" of the AI system occurs within the context of a personal activity. Strictly speaking, the system itself is exclusively being operated during the creation of the deep fake – but not during the utilization of the output (such as the dissemination of the deep fake). This raises the question of whether, in cases where the creation of a deep fake occurs within the private sphere of an individual, the intention to subsequently disseminate the content constitutes a decisive criterion for assessing whether the activity falls outside the scope of a purely personal non-professional activity.

11 This would result in substantial evidentiary challenges, as the intention to disseminate content is typically difficult to prove. Accordingly, all essential steps – from the input of the input data to the utilization of the output of the system – must take place within the control of the user.[17] Contrarily, the mere use of an output, without prior operation of the generative AI system is not sufficient to qualify the disseminator as a deployer.[18]

12 Furthermore, the term "deployer" was originally referred to as "user" in the AI Act-COM.[19] The definition itself, however, has remained unchanged in the final version of the AI Act. The term "deployer" was introduced by the Parliament in response to

10 See Art. 3(9) AI Act.

11 See Art. 3(11) AI Act.

12 Mireille M. Caruana and Roxanne Meilak Borg in Sammut, Mifsud (ed.), The EU Internal Market in the Next Decade – Quo Vadis?, (Brill 2025) 108, 124. <https://library.oapen.org/bitstream/handle/20.500.12657/98980/9789004712119_webready_content_text.pdf?sequence=1#page=119> accessed 24 April 2025.

13 OpenAI has also acknowledged this, see <https://openai.com/global-affairs/a-primer-on-the-eu-ai-act/?utm_source=chatgpt.com> accessed 24 April 2025.

14 See Art. 3(4) AI Act; Art. 2(10) AI Act reiterates this in a contradictory manner: it excludes *"deployers"* utilising AI systems in the course of such a private activity from the scope of the AI Act. However, in accordance with Art. 3(4) AI Act, natural persons using such systems for private purposes cannot conceptually be classified as deployers in the first place, see Wendehorst in Martini/Wendehorst (ed.), (n 7) Art. 2 para 93.

15 Viktoria Kraetzig, 'Deliktsschutz gegen KI-Abbilder – Teil 1: Täuschende Deepfakes' (2024) 3 CR 207, 210.

16 LeaKatharinaKumkar/MoritzGriesel,'Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO' (2024) 4 KIR 117, 121; this aligns with the originally intended clarification in Art. 2(10) AI Act, which explicitly states that only natural persons can invoke the exception.

17 Wendehorst in Martini/Wendehorst (ed.), (n 7) Art. 3 para 83.

18 ibid.

19 See Art. 3(4) AI Act-COM.

repeated criticism that the term "user" could be misleadingly interpreted as referring only to the "end user."[20]

III. Territorial Scope

13 Art. 2(1) AI Act establishes the territorial scope of the AI Act. Art. 2(1) (a) AI Act mandates a "market place-principle"[21] for providers of AI systems: The AI Act applies to providers placing their AI systems (or general-purpose AI models) on the (EU-) market or putting such systems into service in the Union. This principle applies irrespective of whether the provider is established or located within the Union or in a third country.

14 Conversely, Art. 2(1) (b) AI Act prescribes a "principle of establishment" for deployers, signifying that the AI Act is applicable only to deployers who are either established or located within the Union.[22] For other provisions, such as the transparency requirement for synthetic and deep fake content, it must be taken into account that the recipient – the viewer of the content – interacts solely with the output generated by the AI system, rather than the AI system itself. The legislator has addressed this by stipulating in Art. 2(1) (c) AI Act that the regulation applies if the output is situated within the Union, regardless of the provider's or deployer's location.

C. Obligations

15 Article 50 AI Act encompasses five distinct transparency obligations. Recital 132 explains that these obligations, set out in paragraphs 1 to 4, are motivated by the fact that certain AI systems pose a particular risk with regard to identity fraud or deception. This is especially true for AI systems that interact with natural persons or generate content, regardless of whether these AI systems are classified as high-risk or not. Accordingly, Art. 50(6) AI Act underscores that the transparency obligations in paragraphs 1 to 4 do not alter or replace requirements and obligations for high-risk AI systems outlined in the AI Act. Additionally, these transparency obligations operate without prejudice to other transparency requirements imposed by Union or national laws for deployers of AI systems.[23]

16 Moreover, under Art. 50(5) AI Act, these transparency obligations must be presented to the affected natural persons "in a clear and distinguishable manner", at the latest by the time of their first interaction or exposure to the AI system. This information must also comply with applicable accessibility requirements, ensuring that it is accessible to all individuals as required by the AI Act.[24]

I. Art. 50(1) AI Act: Transparency for Chatbots and Interactive AI Systems

17 Art. 50(1) AI Act imposes an obligation on providers of AI systems intended to directly interact with natural persons to ensure that these systems are designed and developed in a manner that informs the individuals in question that they are interacting with an AI system.

1. Systems Intended for Direct Interaction

18 This requirement specifically applies to providers of AI systems designed for direct human interaction. The AI Act does not provide a definition of *"interaction"*. Therefore, its common linguistic meaning should be applied, which denotes reciprocal and interrelated actions, specifically through tactile, auditory, or visual influence.[25]

19 Furthermore, the system must be specifically intended for "*direct*" interaction. Notably, the

20 Christiane Wendehorst, 'The Proposal for an Artificial Intelligence Act COM(2021)206 from a Consumer Policy Perspective' (Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, 14.12.2021), 11 <https://www.sozialministerium.at/dam/sozialministeriumat/Anlagen/Themen/Konsumentenschutz/Konsumentenpolitik/The-Proposal-for-an-Artificial-Intelligence-Act-COM2021-206-from-a-Consumer-Policy-Perspective_dec2021__pdfUA.pdf> accessed 24 April 2025; Wendehorst in Martini/Wendehorst (ed.), (n 7) Art. 3 para 81.

21 Similarly, the GDPR stipulates a "market place-principle" in Art. 3(2) GDPR, requiring controllers and processors from third countries to comply with the GDPR if they target individuals in the EU, see Gerrit Hornung in Spiecker gen. Döhmann/Papakonstantinou/Hornung/De Hert (ed.), General Data Protection Regulation (2023), Beck/Hart/Nomos, Art. 3 para 32.

22 This principle also resembles the "establishment principle" found in Art. 3(1) GDPR, which ensures that the GDPR is applicable to controllers or processors established in the EU, ibid, Art. 3 para 13.

23 Art. 50(6) AI Act.

24 Art. 50(5) AI Act.

25 David Bomhard/Marieke Merkle, 'Europäische KI-Verordnung' (2021) 6 RDi 276, para 35; Marieke Merkle, 'Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?' (2024) 9 RDi 414, para 32.

Commission's draft did not differentiate between direct and indirect interactions.[26] This distinction in the final version of the AI Act raises questions about the types of interactions the legislator intended to address. For instance, automated recommendation systems that simply analyse user data to offer personalised suggestions likely fall outside the scope of Art. 50(1) AI Act, as they lack "direct" interaction.[27] In these cases, the provider is therefore not required to disclose that it is an AI system. Conversely, the transparency requirement primarily applies to systems like chatbots, which clearly engage in "direct" interaction.[28]

2. Designed and Developed to Inform Natural Persons about the AI Interaction

20 As a legal consequence, the provider shall ensure that the system is designed and developed to inform the natural persons concerned that they are interacting with an AI system. This indicates that para. 1 does not directly obligate the provider to inform affected individuals. Rather, it requires the provider to ensure the technical provision of this information by design.[29]

21 According to Art. 50(1) AI Act, affected individuals must only be informed "that" they are interacting with an AI system. This suggests that the information provided is limited to the mere question whether they are interacting with an AI system. Additional information – e.g. information concerning the operation of the system – must not be provided upon the persons concerned.[30]

22 Pursuant to Recital 132, providers shall take into account characteristics of natural persons belonging to vulnerable groups – particularly those affected by age or disability – when fulfilling their obligations, given the AI system is intended to interact with those groups. This notice should not be understood to mean that a "greater" amount of information must be provided to these individuals. Instead, it aims to ensure that the respective group can receive and comprehend the information.[31] For a technically savvy audience, an information such as "I am your virtual assistant" would suffice, whereas an older audience is likely to understand the information only if it is explicitly disclosed as, e.g., "You are interacting with an AI system."

3. Exceptions

23 According to Art. 50(1) AI Act, the transparency obligation does not apply when it is *"obvious"* – taking into account the circumstances and context of the use – that the individuals concerned are interacting with an AI system. The AI Act-COM originally lacked clarity on when interactions with AI systems are *"obvious"*.[32] This was regrettable, as the providers of AI systems could interpret this undefined term in very broad ways.[33] An amendment proposed by the Czech Presidency (of the Council of the European Union) introduced the notion of a *"reasonably well-informed, observant, and circumspect"* natural person as a benchmark for this determination – a standard consistent with consumer protection law and used by the European Court of Justice (ECJ) since the 1990s.[34] Further points of reference or illustrative cases are not provided in this context. Likely referenced here are aspects such as predefined response options and the instantaneous appearance of responses.[35] Predefined response options differ significantly from the open-ended, free-form responses typical

26 See Art. 52(1) AI Act-COM.

27 Philipp Roos/Johanna Voget, 'Transparenzpflichten für die Nutzung von KI auf Online-Marktplätzen' (2024) 10 RDi 487, 490 f.; also see Thomas Gils, 'A Detailed Analysis of Article 50 of the EU's Artificial Intelligence Act', 9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4865427> accessed 24 April 2025.

28 The European legislator had already aimed primarily at regulating Chatbots during the drafting of the Commission's proposal, see COM(2021) 206, Explanatory Memorandum, 1.1.

29 Merkle, (n 25) para 31; the focus on the requirement of systems to be "designed and developed" in a certain way likely stems from the increased responsibility imposed upon providers. Similarly, the obligations set out in Arts. 13-15 AI Act for providers of high-risk AI systems also require the system to be "designed and developed" in a certain way. Critical: Gils, (n 27) 9, who argues that the "deployment-phase" is particularly crucial in this context.

30 Lea Katharina Kumkar in Hilgendorf/Roth-Isigkeit (ed.), 'Die neue Verordnung der EU zur künstlichen Intelligenz' (2023), C.H. Beck, § 6 para 38.

31 See Gianclaudio Malgieri and Maria-Lucia Rebrean, 'Vulnerability in the AI Act: Building an interpretation', 23 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5058591> accessed 24 April 2025.

32 Christoph Engelmann/Nico Brunotte/Hanna Lütkens, 'Die Regulierung von Legal Tech durch die KI-Verordnung' (2021) 7 RDi 317 para 22; Frauke Rostalski/Erik Weiss, 'Der KI-Verordnungsentwurf der Europäischen Kommission' (2021) 4 ZfDR, 329, 351.

33 ibid.

34 See <https://artificialintelligenceact.eu/wp-content/uploads/2022/09/AIA-CZ-3rd-Proposal-23-Sept.pdf> accessed 24 April 2025; See for example Case C-210/96 *Gut Springenheide und Tusky v Oberkreisdirektor des Kreises Steinfurt* [1998] ECLI:EU:C:1998:369, para 31.

35 Kilian Georg Wolf, 'Chatbots als KI-Systeme mit besonderen Transparenzpflichten nach Art. 52 KI-Verordnung' (2022) DSRITB, 601, 613.

of conversations with human interlocutors. This difference can manifest itself in different ways: Some AI systems include buttons or clickable options to help the user navigate, for instance, multiple-choice menus. In addition, many chatbots provide almost instantaneous responses to user input. Typical delays that occur in human conversations, such as when the conversation partner is typing or thinking, are absent. This lack of delay is often considered an indicator that an AI system is involved.[36]

24 In many cases, chatbots are already labelled as *"[company name] bot"* by design.[37] In such instances, it would be obvious that one is interacting with an AI system.[38] Here again, it should be noted that this standard changes if, for example, a disadvantaged group is part of the target audience of the chatbots.[39]

25 Lastly, the obligation does not apply to AI systems legally authorised for the detection, prevention, investigation, or prosecution of criminal offenses, if appropriate safeguards for the rights and freedoms of third parties are in place, unless such systems are made available to the public for reporting a crime.[40]

II. Art. 50(2) AI Act: Synthetic Content

26 Art. 50(2) AI Act imposes a transparency obligation for providers of AI systems generating synthetic audio, image, video and text content. Providers shall ensure that system outputs are marked in a machine-readable format, allowing such content to be detectable as artificially generated or manipulated. Paragraph 2 seeks, on the one hand, to ensure transparency regarding the authenticity of the content, specifically addressing whether events depicted in AI-generated photos or videos might mistakenly be perceived as *"real"*.[41] On the other hand, the provision clarifies whether content is human-made or AI-generated (e.g., whether the design of a logo or a music piece is AI-generated).[42]

1. AI Systems Generating Synthetic Content

27 Subject to the marking obligation are AI systems generating synthetic audio, image, video or text content. The AI Act does not provide a definition of the term "synthetic". Rather, this term should be equated with the term(s) "AI-generated" as the content should be distinguished from human-made content.[43] Accordingly, (almost) every output of such an AI system is subject to this marking requirement.

28 Paradoxically, paragraph 2 requires outputs to be marked as "artificially generated" or "manipulated", yet it only applies to systems that generate synthetic content.[44] Neither the term "artificially generated" nor "artificially manipulated" are defined in the AI Act. Linguistically, the phrasing suggests that "artificially generated" refers to content created entirely by AI, whereas "artificially manipulated" pertains to the modification of pre-existing content through AI.[45] The aforementioned stipulation, however, reflects a legislative imprecision. Correctly, paragraph 2 should encompass both artificially generated and artificially manipulated content, as this would align with its intended scope – to ensure that all content shaped by AI, whether through generation or manipulation, can be distinguished from purely human-made material.[46] The further wording of paragraph 2, which explicitly provides an exception for cases where the system does not substantially "alter" input data, does not support a differing interpretation.[47] This indicates that the provision is meant to also address AI manipulated content.

2. Marking in a Machine-Readable Format

29 Firstly, according to Art. 50(2) AI Act, providers are legally required to mark synthetic content in a machine-readable format. This marking obligation is, in a sense, specified in the recitals:

36 ibid.

37 For instance, Pizza Hut utilizes its 'Pizza Hut Chatbot', while H&M employs the 'H&M AI' bot, and Sephora features the 'Sephora Virtual Artist' for personalized customer experiences, see Anuj Kumar, Nimit Gupta, Gautam Bapat, 'Who is making the decisions? How retail managers can use the power of ChatGPT' (2024) 3 Journal of Business Strategy 161, 167 <https://www.emerald.com/insight/content/doi/10.1108/jbs-04-2023-0067/full/html> accessed 24 April 2025.

38 Maximilian Becker, 'Generative KI und Deepfakes in der KI-VO' (2024) 6 CR 2024, 353 para 48.

39 See C. I. 2.

40 Art. 50(1) AI Act.

41 Additionally, many of the affected contents are likely to also fall under the deep fake provision of paragraph 4. In that case, the transparency requirements apply cumulatively.

42 Recital 133, sentence 1 AI Act.

43 Angelica Fernandez, '"Deep fakes": disentangling terms in the proposed EU Artificial Intelligence Act' (2021) 2 UFITA 392, 413; Mario Martini in Martini/Wendehorst (ed.), (n 7) Art. 50 para 62.

44 Block, (n 4) 188.

45 See Lea Katharina Kumkar, 'Deepfakes – Risiken und Regulierung im europäischen Verordnungsentwurf für künstliche Intelligenz' (2023) 10 supplement 1 K&R 32, 35.

46 See Recital 133 sentence 1 AI Act.

47 Gils, (n 27) 17.

Providers must embed technical solutions to enable marking in a machine-readable format. Recital 133 sentence 4 AI Act gives a few examples for available techniques and methods to be used, namely watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods and fingerprints. It is emphasised that multiple labelling methods can also be combined.[48] The use of combined marking methods may even be essential, as for example metadata-based techniques can be easily bypassed by screenshots or automatic metadata removal on online platforms, rendering them ineffective.[49]

30 According to Art. 50(2) AI Act, the providers "shall ensure that their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, implementation costs and generally acknowledged state of the art, as may be reflected in relevant technical standards".

31 The "effectiveness" of the chosen solution extends beyond its technical functionality, as the other requirements (such as "robustness", "reliability" or the "generally acknowledged state of the art") already cover this aspect.[50] Rather, this criterion requires that the technical solutions practically enable a clear distinction between AI-generated and human-created content. For example, effectiveness is particularly not ensured if it is disproportionately difficult to decode the machine-readable marking.

32 The requirement to account for the specifications and limitations of the various content types implies that the watermark must be appropriately aligned with the nature of the respective content. For instance, it would be incongruous to apply an auditory watermark to an AI-generated image.

3. Detectable as Artificially Generated or Manipulated

33 Secondly, according to Art. 50(2) AI Act, providers must ensure that the content is "*detectable as artificially generated or manipulated*". The understanding of cumulative recognisability of the artificial origin ("marked in a machine-readable format *and* detectable as artificially generated or manipulated") suggests that a visible label for humans must be provided in addition to the machine-readable marking.[51] However, the stipulation that the mark must be "*detectable*" implies that the artificial origin of the content does not need to be visible to the human eye without the aid of additional tools.[52] Recital 135 further mentions (the access of) "detection mechanisms" if essential for enabling the public to effectively distinguish AI content. The fact that specific mechanisms are required for detection suggests that the obligation is intended to facilitate detection by technical systems, subsequently enabling recipients to be informed about the artificial origin of the content through these mechanisms.[53] Therefore, the two-tiered marking approach should rather be understood as a duty that distinguishes between the implementation of a machine-readable marking itself and the specific information to be disclosed when tracing the marking.

34 Pursuant to Art. 50(7) AI Act, the Commission is requested to facilitate the drawing up of codes of practice to ensure the effective implementation of the obligation to detect AI-generated content, including the access to detection mechanisms.[54] Additionally, other actors – such as the providers of very large online platforms (hereinafter: VLOPs) or very large online search engines (hereinafter: VLOSEs) in the sense of the Digital Services Act – are taken into account for embedding algorithmic detection mechanisms.[55]

4. Exceptions

35 Three exceptions apply to the marking obligation under Art. 50(2) AI Act. Firstly, according to para. 2, the obligation shall not apply to the extent the AI systems perform an "assistive function for standard editing". This could be the case if the AI system is used "as a tool for an essentially human product".[56] A straightforward example of such a fundamentally human-driven action is the automatic recognition of objects in photos to enable the segmentation of individual objects.[57]

36 Furthermore, the obligation set out in para. 2 shall not apply to the extent the AI system in question does not substantially alter the input data provided by the deployer or the semantics thereof. It is probable that this exception will cover programs

48 Recital 133, sentence 4 AI Act.

49 Becker, (n 38) para 55; Ramak Molavi Vasse'i, 'Watermarking von KI-generierten Inhalten als regulatorisches Instrument' (2024) 9 RDi 406, para 16.

50 Molavi Vasse'i, (n 49) para 31.

51 Kumkar/Griesel, (n 16) 124.

52 Block, (n 4) 188.

53 Molavi Vasse'i, (n 49) para 10.

54 Recital 135 AI Act.

55 European Commission, C/2024/3014, subsection 3.3. (40) (d).

56 Becker, (n 38), para 57.

57 ibid, Becker cites the example of the object isolation function on iPhones.

designed for spelling and grammar verification.[58] In addition, the scope may extend to systems that focus on optimizing image quality, translating text, reducing noise from recordings and converting file formats.

37 Lastly, a similar exemption to para. 1 is provided for instances where the system is legally authorised for crime investigation or prevention purposes.

5. Issues

38 A particular issue is that the provision does not require the deployer to specify which part of the content is AI-generated. Accordingly, it remains unclear whether only an insignificant part of the content was artificially generated or manipulated, or whether the content was predominantly or entirely AI-generated. Since no further information regarding the nature or extent of the generation or manipulation of the content is disclosed, the labelling remains largely uninformative.[59]

39 It is not yet possible to determine whether machine-readable markings effectively contribute to combating disinformation and ensuring transparency regarding whether content is AI-generated or human-made. A key factor will be whether social networks such as Facebook, Instagram, or X implement technical solutions that enable the identification of such content,[60] as users are unlikely to independently verify the origin of every piece of content they encounter.

III. Art. 50(3) AI Act: Emotion Recognition Systems and Biometric Categorisation Systems

40 According to Art. 50(3) AI Act, "deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system". In contrast to the Commission's draft, paragraph 3 now declaratively states that the deployers of these systems must process personal data in accordance with the GDPR and the EU Data Protection Regulation (EU-DPR), as well as the Data Protection Law Enforcement Directive (DP-LED). In this context, Art. 2(7) AI Act already clarifies that the AI Act and the aforementioned regulations and directive apply concurrently.

1. Additional regulations

41 The transparency obligation for emotion recognition systems and biometric categorisation systems is part of a broader set of regulations targeting such AI systems. For example, in certain cases, these systems are prohibited entirely: Art. 5(f) AI Act explicitly prohibits systems used to infer emotions of a natural person in a workplace or educational institution. Pursuant to Art. 5(g) AI Act, the same applies to biometric categorisation systems used to deduce or infer sensitive information such as the race, political opinions or sexual orientation of the affected individuals.

42 Additionally, AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the interference of those attributes or characteristics, are considered high-risk AI systems pursuant to Art. 6(2) AI Act and Annex III, 1(b) AI Act.[61] Likewise, systems intended to be used for emotion recognition are classified as "high-risk" pursuant to Annex III, 1(c) AI Act. If an emotion recognition system or a biometric categorisation system is classified as a high-risk AI system, the transparency requirements set out in Art. 50(3) AI Act must be fulfilled cumulatively.[62]

2. Emotion Recognition Systems and Biometric Categorisation Systems

43 Art. 50(3) AI Act obliges providers of "emotion recognition systems" and "biometric categorisation systems" to "inform the natural persons exposed thereto of the operation of the system". Art. 3(39) AI Act defines the term "emotion recognition system" as an "AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data". Recital 18 further clarifies this notion by distinguishing between recognised emotions and intentions – such as happiness, sadness, anger and surprise – and explicitly excluding physical states like pain or fatigue. In practical terms, however, the threshold between emotions and physical states is likely to be

58 Block, (n 4) 189.

59 Molavi Vasse'i, (n 49) para 56.

60 E.g., "meta" labels content identified by its systems as AI-generated, as well as content that users themselves declare to be AI-generated, cf. <https://www.meta.com/en-gb/help/artificial-intelligence/How-ai-generated-images-in-ads-are-identified-and-labeled-on-Meta/> accessed 24 April 2025.

61 See Annex III, 1. b) and c) AI Act.

62 See Art. 50(6) AI Act.

difficult to determine.[63]

44 Under Art. 3(40) AI Act, a "biometric categorisation systems" is defined as an AI system "for the purpose of assigning natural persons to specific categories on the basis of their biometric data". Recital 16 AI Act specifies that these categories may encompass aspects such as "sex, age, [...] religion, membership of a national minority, sexual or political orientation". However, an AI system is not considered a "biometric categorisation system" if its categorisation function is merely ancillary to another commercial service and is strictly necessary for objective technical reasons. Recital 16 further clarifies that such a feature is deemed purely ancillary only if it cannot, for objective technical reasons, function independently of the principal service and if its integration is not intended to circumvent the requirements outlined in the AI Act.

45 Lastly, Art. 3(34) AI Act specifies the term "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data". Pursuant to Recital 14 AI Act, the notion of "biometric data" should understood in line with its definitions in Art. 4(14) GDPR, Art. 3(18) EU-DPR and Art. 3(13) DP-LED.

46 Despite this intention to align these definitions, the term provided in the AI Act differs from that of the GDPR, as Art. 4(14) GDPR expressly subsumes only those data under the term "biometric data" that allow for the unique identification of a person. The AI Act, however, does not incorporate this requirement.[64] Interestingly, the definition presented in the Commission's draft aligns precisely with the definition provided in the GDPR.[65]

47 The identical wording of the definition found in the Commission's draft – particularly the phrase "allow or confirm the unique identification of that natural person" – has been subject to criticism in literature.[66] This phrasing results in only "strong" biometric features, such as fingerprints, being covered by the definition.[67] For emotion recognition, so-called "weak" biometric features (such as body shape or voice) are crucial; for biometric categorization, "soft" biometric features, such as those associated with a specific age, gender, or skin colour, are relevant.[68] As a result, the final version of the AI Act deliberately omits the phrase "allow or confirm the unique identification of that natural person" as found in the GDPR to tailor the concept of "biometric data" to emotion recognition systems and biometric categorisation systems. This change is to be welcomed.

3. Inform the Person Exposed of the Operation of the System

48 Unlike Art. 50(1) AI Act – which requires the AI system to be designed in a way that informs the individual affected *"that"* they are interacting with an AI system – paragraph 3 requires the deployer to inform the person exposed *"of the operation of the system"*. This comparison implies that the obligation in paragraph 3 goes beyond a mere notification that an individual is exposed to such a system.[69] This alludes to the deployer not only informing the person exposed about "whether" they are using such a system but also about the specific manner of use – the "how" of the system.[70] Accordingly, essential parameters, based on which the system makes a decision – such as which feature (e.g. voice or facial structure) the system evaluates – must be disclosed.[71]

4. Exceptions

49 Art. 50(3) AI Act also includes an exception for systems authorised by law for the detection, prevention and investigation of criminal offences. Unlike other similar exemptions set out in Art. 50 AI Act, the exception in para. 3 sentence 2 does not include systems that are legally authorised to *"prosecute"* criminal offences.[72] This implies that the use of such

63 Mario Martini in Martini/Wendehorst (ed.), (n 7) Art. 3 para 279.

64 ibid, Art. 50 para 84.

65 See Art. 3(33) AI Act-COM.

66 Wendehorst, (n 20) 93 ff.; Wendehorst in Martini/Wendehorst (ed.), (n 7) Art. 3 para 232.

67 Wendehorst in Martini/Wendehorst (ed.), (n 7) Art. 3 para 232.

68 ibid para 240 f.

69 Kumkar in Hilgendorf/Roth-Isigkeit, (n 30) § 6 para 53; critical: Gils (n 27) 20, who notes that the phrasing "of the operation of the system" is ambiguous. It may either refer to the individual being exposed to the system "in operation" – in which case it suffices to inform the person of their exposure to an emotion recognition or biometric categorisation system – or to the person being informed "about the operation", which would require informing the individual about how the system functions.

70 ibid.

71 Martini in Martini/Wendehorst (ed.), (n 7) Art. 50 para 89.

72 The transparency obligations in paras. 1 and 4 (including subparas. 1 and 2) all contain exemptions related to the detection, prevention, investigation, and prosecution of criminal offences. Moreover, the Commission's draft also included an exception for emotion recognition systems and biometric identification systems legally authorised to prosecute criminal offences, see Art. 52(2) sentence 2 AI

AI systems for crime prosecution purposes is not outright prohibited but is in authorised cases always subject to the transparency obligation.[73]

50 Additionally, the exemption declaratively mentions that the AI system also has to be used in accordance with Union law. Likely, this addition was included to highlight the significance of the associated fundamental rights, as some applications of these systems are even prohibited or classified as high-risk.[74]

IV. Art. 50(4) subpara. 1 AI Act: Disclosure Obligation for "Deep Fakes"

51 Art. 50(4) subpara. 1 AI Act establishes a disclosure obligation for deep fake content. Under this provision, deployers of AI systems that generate or manipulate image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated.

1. AI Systems Generating or Manipulating Content Constituting a Deep Fake

52 Art. 50(4) subpara. 1 AI Act pertains to deployers of AI systems that generate or manipulate image, audio or video content constituting a deep fake. As explained regarding the transparency obligation under Art. 50(2) AI Act, the obligation covers both fully AI-generated but also merely modified content.[75] However, in contrast to paragraph 2, Art. 50(4) subpara. 1 AI Act does not extend to text-based content.

53 Furthermore, the content must qualify as a deep fake. Art. 3(60) AI Act defines "deep fakes" as *"AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful"*. Accordingly, Art. 3(60) AI Act provides an extensive list of potential "targets" for deep fakes: In addition to persons, objects, places, entities, or events can also be the subject of a deep fake. This expansive list contradicts the common understanding that primarily humans can be subject of deep fakes, ultimately leading to numerous overlaps with Art. 50(2) AI Act.[76]

54 The deep fake definition no longer explicitly requires an *"appreciable resemblance"* to the mentioned subjects like Art. 52(3) AI Act-COM did.[77] At first glance, it appears that the legislator is broadening the definition of deep fakes to include content that is similar to the given subjects, rather than requiring near-identical resemblance. Recital 134, however, still mentions that the content has to *"appreciably resemble"* these subjects. This raises confusion and appears to be a regulatory imprecision with no practical impact.[78]

55 It is important to note that Art. 3(60) AI Act explicitly refers to "a person" perceiving the content as authentic or truthful.[79] In particular, there is no reference to a specific benchmark such as "a reasonably well-informed, observant, and circumspect natural person".[80] This suggests that a different standard is intended here. Overly stringent standards should not apply here to ensure that the regulatory purpose is not undermined. Since the spectrum of potential recipients includes both technically skilled and unskilled individuals, the question of whether image artefacts alone can disrupt the impression of authenticity should be critically considered.[81] Rather, it should suffice if the content appears authentic or truthful at a cursory glance to an average recipient.[82]

2. Disclosure Obligation

56 Deployers must *"disclose"* that the deep fake content is *"artificially generated or manipulated"*. Recital 134 further mandates that deployers must "clearly and distinguishably disclose"[83] AI-generated content by "labelling the AI output accordingly" and "disclosing its artificial origin".

57 This requirement implies that only the artificial origin needs to be disclosed, without necessarily labelling the content explicitly as a "deep fake". However, the

Act-COM.

73 *Argumentum a contrario* Art. 5(1)(g) AI Act.

74 See C. III. 1.

75 See C. II. 1.

76 However, if both provision are applicable, the obligations must simply be fulfilled cumulatively, see fn 42.

77 Gils, (n 27) 21.

78 Kristof Meding, Christoph Sorge, 'What constitutes a Deep Fake? The blurry line between legitimate processing and manipulation under the EU AI Act', 5 <https://arxiv.org/abs/2412.09961> accessed 24 April 2025; Łabuz, 'Deep fakes and the Artificial Intelligence Act – An important signal or a missed opportunity?' (2024) 4 Policy & Internet 783, 787 <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.406> accessed 24 April 2025; Gils (n 27) 21.

79 Block, (n 4) 189.

80 ibid.

81 Kumkar/Griesel, (n 16), 120.

82 ibid.

83 Also cf. Art.50(5) AI Act.

term "disclosure" remains somewhat ambiguous:[84] Neither Art. 50(4) subpara. 1 AI Act nor Recital 134 provide further details on the specific manner in which the disclosure should be implemented (e.g., whether the labelling must be affixed directly to the medium itself or if a notice in the caption suffices). An *argumentum a contrario* regarding the exception in sentence 3 can be drawn, suggesting that the deep fake must be directly labelled. Within the scope of this exemption, the legislator has aimed to limit the disclosure obligation in a manner that does not impair the presentation or enjoyment of the work. If disclosure in the caption were sufficient to meet the requirements of Art. 50(4) subpara. 1 AI Act, this exemption would be redundant.[85]

3. Does Art. 50(2) AI Act Effectively Complement Deep Fake Disclosure?

58 Unlike Art. 50(2) AI Act, the regulation set out in Art. 50(4) subpara. 1 AI Act is aimed at deployers. This issue was heavily criticized in the Commission's draft, as such disclosure requirements are for one technically much easier for the provider who could, for example, embed the necessary disclosures directly into the software code.[86] Additionally, provider obligations prove ineffective when malicious actors are the users of such systems.[87] Specifically, under Art. 50(4) subpara. 1 AI Act, if the provider harbours malicious intent, they are unlikely to label their deep fakes before dissemination. Imposing the disclosure obligation on the provider would at least require malicious actors to either establish their own generative AI systems or modify existing AI systems to eliminate the labelling applied by the provider. In either case, there would be at least some technical barrier to overcome, necessitating at least a certain level of effort from these actors. While this requirement may not deter professional disinformants, it does present an obstacle for everyday users attempting to disseminate disinformation on social media from their home computers.

59 One reason the obligation under Art. 50(4) subpara. 1 AI Act may not apply to providers is that a substantial share of deep fakes is created using general-purpose generative AI systems such as DALL-E or Midjourney.[88] Imposing a labelling requirement on providers would mean they must track every piece of content their systems create to assess whether it qualifies as a deep fake under Art. 3(60) AI Act and then disclose its artificial origin. This would, in effect, turn the transparency obligation for disclosing deep fakes into a moderation duty for providers.[89]

60 These issues appear to have been addressed, as the disclosure obligation is now supplemented by the aforementioned marking requirement for synthetic content (Art. 50(2) AI Act). As previously discussed, the recognition of these machine-readable markings requires the aid of detection mechanisms.[90] For instance, if a deployer circulates a deep fake without labelling it (as permitted under Art. 50(4) subpara. 1 AI Act), identifying its artificial origin still depends either on the recipient himself verifying its authenticity or the social media platform offering detection solutions.

61 Given the sheer volume of content circulating on social media, expecting every user to consistently verify the authenticity of content is highly unrealistic.[91] Consequently, the effectiveness of the transparency obligation under paragraph 2 relies heavily on social media platform providers independently applying visible labels to such content. However, such a platform provider focused framework seems to align with the legislator's objectives.[92]

84 cf. Lea Katharina Kumkar/Julian Philipp Rapp, 'Deepfakes' (2022) 3 ZfDR 199, 224; Becker, (n 38) para 73.

85 Kumkar/Griesel, (n 16) 122.

86 Mario Martini/Jonas Botta, 'Der Staat und das Metaversum', (2023) 12 Supplement MMR 887, 895; Kumkar/Rapp, (n 84) 224; Tobias Hinderks, 'Die Kennzeichnungspflicht von Deepfakes' (2022) 2 ZUM 110, 112; in a similar vein, Veale and Zuiderveen Borgesius note that, when such obligations are placed on deployers, enforcement becomes particularly challenging, see Michael Veale/Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 CRi, 97, 108.

87 Differently, Georg Borges, 'Die europäische KI-Verordnung (AI Act) Teil 3 – Transparenzpflichten, Durchsetzung, Gesamtbewertung' (2024) 10 CR 663 para 59, who argues that service providers (such as in the case of ChatGPT) should be regarded as the deployers of the AI system rather than the "users".

88 On the capability of such systems to generate highly realistic image, video, and text content, see Zhengyuan Jiang/Jinghuai Zhang/Neil Zhenqjang Gong, 'Evading Watermark based Detection of AI-Generated Content', (2023) ACM Conference on Computer and Communications Security 1168 <https://dl.acm.org/doi/10.1145/3576915.3623189> accessed 24 April 2025.

89 For a proposal on the transfer of content moderation obligations of the DSA to providers of large GenAI models, see Philipp Hacker/Andreas Engel/Marco Mauer, 'Regulating ChatGPT and other Large Generative AI Models' FAccT'23, 1112 , 1120 <https://dl.acm.org/doi/10.1145/3593013.3594067> accessed 24 April 2025.

90 See C. II. 3.

91 See C. II. 5.

92 See for example E. I.; the European legislator foresees that platform providers should take risk mitigation measures based on the labelling of synthetic content in machine-

4. Exceptions

62 Art. 50(4) subpara. 1 sentence 3 AI Act provides limitation: If the content in question forms part of an "evidently artistic, creative, satirical, fictional, or analogous work or programme", the disclosure provision is limited to disclosing "the existence of such generated or manipulated content in a manner that does not impede the display or enjoyment of the work."

63 In this regard, Recital 136 AI Act clarifies that compliance with Art. 50(4) subpara. 1 AI Act should not be interpreted as indicating that the use of the AI system or its output impedes the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights (hereinafter: CFR). This is particularly relevant if the limitation specified in Art. 50(4) subpara. 1 sentence 3 AI Act is applicable.

64 The EU Commission's draft included a similar exception in Art. 52(3) AI Act-COM.[93] Under the AI Act-COM, deep fakes whose use is necessary for the exercise of the rights to freedom of expression and freedom of the arts or science, as guaranteed by the CFR, were entirely exempt from the disclosure requirement. However, it is commendable that the exemption in the final version of the AI Act does not provide such a complete exemption from disclosure. Such exceptions ultimately create uncertainty for the recipient regarding whether the content in question is truly a deep fake, as AI system deployers could simply invoke the exception.[94] Accordingly, it is to be welcomed that a complete exemption from this disclosure obligation is no longer possible in this context.

65 In the final version, the ambiguity of when the work or programme of which the deep fake forms part is "*evidently*" artistic, creative, or satirical (etc.) raises questions about the applicable standard for assessment.[95] In comparison, the transparency obligation set out in Art. 50(1) AI Act uses the linguistically (almost) identical term "*obvious*", which is further defined by the benchmark of a "reasonably well-informed, observant, and circumspect natural person". The fact that Art. 50(4) subpara. 1 AI Act avoids the term "obvious" suggests that a different standard is intended.[96]

66 Lastly, the second sentence of Art. 50(4) subpara. 1 AI Act further provides for an exception in cases where the use is authorized by law to detect, prevent, investigate or prosecute criminal offences. Here, the preceding discussions to the other exceptions apply.

V. Art. 50(4) subpara. 2 AI Act: Disclosure of AI-Texts

67 Art. 50(4) subpara. 2 AI Act introduces a new disclosure requirement for AI-generated text, which was not included in the original Commission's draft. Pursuant to this obligation, deployers of AI systems that generate or manipulate texts published with the purpose of informing the public on matters of public interest shall disclose that the text is AI-generated.

68 A key point to note is that the general requirement for marking synthetic content under Art. 50(2) AI Act also applies to AI-generated texts. Conversely, the term "deep fake" in Art. 3(60) AI Act – and, by extension, the deep fake disclosure obligation stated in Art. 50(4) subpara. 1 AI Act – excludes AI texts.

69 The primary reason lies in the nature of resemblance and its applicability to textual data. Unlike image, audio or video content – which can directly mimic the physical or sensory attributes of a specific entity (e.g. the appearance of a person) – text does not inherently "resemble" any such tangible or sensory reality.[97] However, although AI texts may not offer the same realistic illusion as other types of content, they can still serve as effective tools for disseminating misinformation. This is particularly concerning in the scope of automated journalism, where AI systems generate news articles or reports.

1. Text Published with the Purpose of Informing the Public on Matters of Public Interest

70 The transparency obligation set out in Art. 50(4) subpara. 2 AI Act pertains to deployers of AI systems generating or manipulating text content, provided the text is published with the purpose of informing the public on matters of public interest.

71 Notably, the obligation exclusively applies to texts that are "published". A linguistic understanding of the term "published" implies that the deployer must intentionally make the text accessible to the public. This aligns with the second requirement as

readable format.

93 See Art. 52 para. 3 subpara. 2 AI Act-COM.

94 Kumkar/Rapp, (n 84) 224.

95 Also see Gils (n 27), 25, who argues that the assessment of whether the work is "evidently" creative or satirical is highly subjective.

96 Paradoxically, the German language version of the AI Act uses the term "offensichtlich" for both cases. However, the use of two different terms in other language versions suggests that these terms do not share the same benchmark.

97 See Łabuz, (n 78) 787.

the obligation only concerns texts published with the specific intention of informing the "public". This term presupposes that the text is intended to be addressed to more than a limited number of people. In internet-related scenarios, particularly in the case of automated journalism as mentioned initially, this requirement is generally met.

72 Lastly, the text must address "matters of public interests". Recitals 7 and 8 AI Act give examples of "matters of public interest" as "health, safety and (the protection of) fundamental rights".[98] Beyond the aforementioned enumeration, the term "matters of public interest" may also include political, social, economic and cultural matters, with the key indicator being their relevance to public discourse and their relevance for the public opinion formation.[99]

2. Disclosure Obligation

73 Pursuant to Art. 50(4) subpara. 2 AI Act, where AI-generated or manipulated text is published with the purpose of informing the public on matters of public interest, the deployer "shall disclose that the content has been artificially generated or manipulated". In a similar manner to subpara. 1, subpara. 2 fails to provide any clarification regarding the method of "disclosure". Specifically, it remains unclear whether the text must be highlighted, for instance, through bold lettering, colour emphasis, or specific placement.[100] As with the other transparency obligations, the information must generally be provided to the affected party in a "clear and distinguishable" manner (Art. 50(5) AI Act).

3. Exceptions

74 The transparency obligation laid down in para. 4, subpara. 2, is exempted in the same way as the other obligations when the use is authorised by law for the purpose of detection, prevention, investigation or prosecution of criminal offences.

75 In addition, if the "content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content" the provider must not disclose the artificial origin of the text.

76 The extent to which human review or editorial control must occur is not directly evident from the wording of the Art. 50(4) subpara. 2 AI Act. In this context, it should be noted that the purpose of the transparency obligation is not solely to reveal whether an article was authored by a human or an AI system. Rather, its aim is to prevent the spread of misinformation, which could proliferate on a large scale if the substantial volume of automatically AI-generated news content were left unchecked.[101] The purpose of the subpara. 2 is of paramount importance when determining the extent of editorial control. Therefore, the human reviewer or editorial controller must ensure that no misinformation is disseminated through these AI-generated texts. A mere review of spelling errors and grammar is insufficient in this regard.[102]

D. Penalties

77 In the event of non-compliance with these transparency obligations, Art. 99(4) (g) AI Act provides for administrative fines. These fines may be up to € 15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

78 In addition, according to Art. 99(1) AI Act, the Member States shall lay down rules on penalties and other enforcement measures. These shall include warnings and non-monetary measures, applicable to infringements of the AI Act by operators. Moreover, the Member States shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Art. 96 AI Act.[103] Due to the absence of measures by the Member States, nothing further can be said regarding the sanctions and measures provided here.

E. Interplay with the Digital Services Act

79 Transparency obligations set forth in Art. 50 AI Act have various implications for the Digital Services Act (hereinafter: DSA).

I. Risk Mitigation Measures

80 Both Recital 120 and (the almost identical) Recital 136 AI Act emphasize the risk of actual or foreseeable negative effects on democratic

98 Gils, (n 27) 26.
99 Martini in Martini/Wendehorst (ed.), (n 7) Art. 50 para 113.
100 Gils, (n 27) 26.
101 ibid para 114.
102 Gils (n 27) 27.
103 Art. 99(1) AI Act.

processes, civil discourse, and electoral integrity, including disinformation. Moreover, these Recitals underscore that the obligations established in the AI Act for enabling detection and disclosure of artificial origin (referring to both Art. 50(2) AI Act and Art. 50(4) AI Act) are essential for the effective implementation of the DSA. These obligations hold particular significance for providers of VLOPs and VLOSEs, as they relate to the risk mitigation measures mandated in Art. 35(1) DSA.

81 Online platforms (and online search engines) with over 45 million active users in the EU are designated as VLOPs and VLOSEs pursuant to Art. 33(4) DSA. According to Art. 34(1) DSA, providers of such VLOPs and VLOSEs shall diligently identify, analyse and assess any systemic risk stemming from their platform. These systemic risks may include, for instance, the dissemination of illegal content through their platforms or (actual or foreseeable) negative effects on the exercise of fundamental rights as well as on civic discourse and electoral processes.[104] Consequently, Art. 35 DSA requires such providers to put in place reasonable, proportionate and effective risk mitigation measures. In particular, Art. 35(1) sentence 2 (k) DSA outlines a risk mitigation measure to "prominently label" deep fake content or deep fake-like[105] content. In principle, however, providers of such platforms are not bound to a specific risk mitigation measure, but may freely choose between several measures, provided that these are found to be reasonable, proportionate, and effective.[106]

82 Additionally, the Commission has issued guidelines for providers of VLOPs and VLOSE on the mitigation of systemic risks for electoral processes pursuant to Art. 35(3) DSA.[107] These guidelines include specific risk mitigation measures linked to generative AI.[108] In addition to measures like labelling deep fakes[109], platform providers shall take measures such as adapting their content moderation processes to detect AI content marked in accordance with Art. 50(2) AI Act.[110] This enables VLOP- (and VLOSE-) providers to effectively search for AI-generated content as part of their moderation duties and, where necessary, filter out problematic content.

83 The guidelines were primarily developed in connection with the 2024 European Parliament elections but are intended to remain applicable beyond these elections, particularly concerning threats to electoral processes.[111] Nevertheless, the platform provider is granted a degree of discretion, similar to that of the risk mitigation measures mentioned in Art. 35(1) sentence 2 DSA. As a result, there is, in practice, no obligation to enforce these measures.

II. Unlabelled Content as Illegal Content in the Context of the DSA?

84 Furthermore, the DSA introduces a notice-and-action mechanism for service providers such as Facebook, Instagram or X. Generally, hosting service providers are not liable for illegal content uploaded by their recipients, provided they have no actual knowledge of such content.[112] Contrarily, if service providers become aware of illegal content, they are obligated to "expeditiously" remove it; otherwise, they might be liable for the respective content.[113] As part of the notice-and-action mechanism, users can report content they consider illegal to hosting service providers. According to Art. 16(6) DSA, service providers shall process these notices and take their decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrarily and objective manner.

85 The basis for this decision is a generally broad definition of the term "illegal content". Pursuant to Art. 3(h) DSA, "any information that, in itself or in relation to an activity [...] not in compliance with Union law or the law of any Member State [...] irrespective of the precise subject matter or nature of that law" is considered "illegal content".

86 Recital 136 AI Act, however, emphasises that violations of the transparency obligations established in Art. 50 AI Act should not affect the assessment of the legality of the relevant content. That assessment "should be performed solely with reference to the rules governing the legality of the content".[114] In this context, "rules governing the legality of content" should be interpreted as referring to regulations that pertain to the "expressive content" of the given material.[115] Accordingly, content is classified

104 See Art. 34(1) DSA.

105 Unlike Art. 50(4) subpara. 1 AI Act, Art. 35(1) sentence 2 (k) DSA does not require the content to be artificially generated or manipulated. This initially seems contradictory, as Art. 50(2) AI Act also discloses only the artificial origin of the content. Nevertheless, it simplifies the labeling process for VLOPs in that the vast majority of content covered by Art. 35(1) sentence 2 (k) DSA is likely to be AI-generated as well.

106 This is already implied by the wording of Art. 35(1) sentence 2 DSA: "Such measures may include, [where applicable]".

107 C/2024/3014.

108 ibid subsection 3.3.

109 ibid (40) (b).

110 ibid (40) (d).

111 ibid subsection 1.1. (3).

112 Art. 6(1) (a) DSA.

113 Art. 6(1) (b) DSA.

114 Recital 136, sentence 4 AI Act.

115 Lennart Laude/Andreas Daum, 'KI als neues

as illegal under the DSA depending on whether it infringes personal rights, for example, or is defamatory, insulting or libellous.

87 In the context of deep fake content, this classification presents a notable weakness: A violation of the transparency obligation set out in Art. 50(2) and (4) AI Act does not automatically result in the content being removed.[116] Instead, if such content is not inherently illegal due to the lack of appropriate disclosure or marking, an individual assessment of its legality must be carried out.

88 This process carries significant risks. While this legal assessment is ongoing, the content may continue to circulate and be accessible, potentially causing irreversible damage – especially in cases involving manipulated media, such as deep fakes, where the rapid spread of misinformation or harmful content can have far-reaching consequences.

89 For example, if a deep fake is not disclosed in accordance with Art. 50(4) subpara. 1 AI Act and is simultaneously suspected of being defamatory towards the person depicted, the service provider is not automatically obligated to remove the deep fake due to the lack of proper disclosure. Rather, the content may remain on the platform until an assessment determines whether it defames the person portrayed. For these reasons, the absence of an immediate removal mechanism for unlabelled synthetic (deep fake) content highlights a critical gap in the regulatory framework.

90 Since the Commission's draft did not yet contain a marking obligation for synthetic content – and thus no illegality attached to such content – the final version of the AI Act could have marked a pivotal advancement in moderating disinformative content. Instead, this development represents a marked legislative regression: The AI Act-COM did not have a Recital corresponding to Recital 136 AI Act, thus, unlabelled deep fake content was considered "illegal" in the context of the DSA.[117] As a result, the AI Act's stance inadvertently weakens enforcement against potentially harmful AI-generated content by deprioritizing transparency violations and their consequences.

Wahlkampfinstrument' (Verfassungsblog, 3 May 2024) <https://verfassungsblog.de/ki-als-neues-wahlkampfinstrument/> accessed 24 April 2025.

116 Kumkar/Griesel, (n 16) 125.

117 See Kalbhenn, 'Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung' (2021) 8/9 ZUM 663, 671.

F. Final Evaluation

91 Compared to the Commission's draft, the transparency obligations were revised and refined during the legislative process, albeit mostly just in detail. Many of the adjustments made serve a clarifying purpose, such as the implementation of the term "reasonably well-informed, observant, and circumspect natural person" as standard for assessing obviousness under paragraph 1. In addition, existing transparency obligations have been optimised. For instance, the disclosure obligation for deep fakes no longer includes any exceptions for the exercise of certain fundamental rights. This was necessary, as such selective exceptions in the context of transparency obligations would undermine the intended transparency.

92 The most notable addition, however, is the new marking requirement for synthetic content under Art. 50(2) AI Act, which serves to support the disclosure obligation for deep fakes as well as the (also newly introduced) obligation to disclose AI-generated texts. Furthermore, this marking obligation synergises with the risk mitigation measures for providers of VLOP and VLOSE outlined in the DSA as these providers will be able to easily trace the machine-readable marking, allowing for a straightforward detection of AI content. This ease of AI content detection assists platform providers in specific risk measures such as the labelling of deep fakes in accordance with Art. 35(1) sentence 2 (k) DSA.

93 Nevertheless, the European legislator has missed a crucial step in the fight against disinformation by failing to classify unmarked content as "illegal content" within the meaning of the DSA. Accordingly, platform providers are not required to remove the content in cases of mere non-compliance with the transparency obligations set out in Art. 50(2) and (4) AI Act. This is particularly problematic concerning the spread of false information. In this context, deep fakes pose a significant threat because they can spread globally via the internet within seconds. This risk could have been mitigated – at least in part – by classifying unlabelled deep fakes as "illegal content" under the DSA and thereby holding platform providers accountable.

94 Overall, the adjustments compared to the Commission's draft are to be welcomed. However, the transparency obligations can only partially address the underlying risks. This is partly due to a fundamentally flawed approach, such as the assumption that malicious or uninformed actors will voluntarily disclose deep fakes as AI-generated. A more effective strategy would be to rely on trustworthy actors, such as AI system providers,

and to establish comprehensive regulations, such as mandatory content moderation for such materials, akin to the provisions of the DSA.

Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation*

by **Agustina Del Campo, Nicolas Zara and Ramiro Álvarez Ugarte** **

Abstract: This paper discusses the risk-based approach of the Digital Services Act (DSA) of the European Union. By embracing open-ended standards instead of rules and by imposing broad risk-identification and mitigation obligations on private parties, the DSA pushes forward a form of managerial co-regulation that is a paradigmatic shift in platform regulation that has already influenced other regulatory proposals around the globe. This paper argues that the move is consequential from the perspective of the role of human rights in Internet governance. We posit that the approach poses unique problems when seen from the popular three-prong test used by apex courts around the world to assess restrictions on freedom of expression. Furthermore, we argue that it pushes rights out of the center stage of Internet governance and may create a logic of "symbolic compliance" where the governance role of rights is further diminished. Finally, this paper identifies opportunities to address or mitigate the challenges identified, especially in an enforcement stage that remains quite open to these kinds of efforts.

Keywords: Regulation; Internet Governance; Digital Services Act; Coregulation; Human Rights

Recommended citation: Agustina Del Campo, Nicolas Zara and Ramiro Álvarez Ugarte, Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation, 16 (2025) JIPITEC 238 para 1.

A. Introduction

1 Regulatory proposals for online platforms managing speech online have embraced a risk-based approach that puts the concept of risk at the center stage. The adoption of this approach by important rule-making bodies and organizations in the field of technology is an innovation worthy of study. It happened along two broader paradigmatic shifts in regulatory approaches. First, the tech sector has been slowly but steadily moving from a self-regulatory to a regulatory paradigm;[1] second, trends in regulation have shifted from a "command and control" approach to "new governance" forms of

* This paper is the result of several months of discussion with the team at CELE. We want to thank Matías González for his insights and valuable feedback on earlier drafts of this work. We also greatly benefted from conversations with Rachel Griffin, Joan Barata, and Alexander Hohlfeld and from our participation in the European Rights & Risks Forum organized by the Global Network Initiative and the Digital Trust and Safety Partnership in June 2024, the Summer Course on European Platform Regulation organized by the University of Amsterdam Law School's Institute for Information Law (IViR) in July 2024, and our involvement in the DSA Civil Society Coordination Group led by CDT Europe. The authors extend special thanks to Professors Aleksandra Kuczerawy (KU Leuven) and Joris van Hoboken (UvA), as well as to the participants in the seminar held at CiTiP (KU Leuven) in December 2024, for their critical perspectives on an earlier version of this paper. Any errors that remain are solely our responsibility.

** Agustina Del Campo is a Director at Centro de Estudios en Libertad de Expresión (CELE), Palermo Law School, Buenos Aires, Argentina. Nicolas Zara is a Researcher at Centro de Estudios en Libertad de Expresión (CELE), Palermo Law School, Buenos Aires, Argentina. Ramiro Álvarez Ugarte is a Researcher and deputy director at Centro de Estudios en Libertad de Expresión (CELE), Palermo Law School, Buenos Aires, Argentina.

1 Monroe Price and Stefaan Verhulst, 'The Concept of Self-Regulation and the Internet' in J Waltermann and M Machill (eds), *Protecting our children on the Internet. Towards a new culture of responsibility* (Bertelsmann Foundation Publishers 2000).

regulation[2] that rely heavily on informal processes of rule-making[3] and an ongoing dialogue between regulators and regulatees.

2 The European Digital Services Act (DSA)[4] was the first formal regulation to adopt a risk-based approach to speech governance. The Act defines a set of systemic risks that very large online platforms (VLOPs) and search engines (VLOSEs) should assess, including the dissemination of illegal content and other negative impacts of their services on fundamental rights, democratic processes, public health, minors, any person's physical and mental well-being, and gender-based violence.[5] Platforms are to conduct their own assessments of risks. Upon their findings, they must adopt mitigation strategies, be duly diligent in the measures they adopt, go over yearly external audits that evaluate their compliance,[6] and learn from the process.[7] Furthermore, the DSA empowers regulators to monitor, enforce, and punish these companies for non-compliance or poor compliance through different means.[8] The DSA's approach has since been replicated by UNESCO in their 2023 Platform regulation guidelines,[9] and more recently endorsed by the UN within the Global Digital Compact,[10] the European Union AI Act[11] and, partially, in other pieces of national legislation.[12]

3 The risk-based approach is not new and can be genealogically traced to previous experiences and regulatory trends. It first emerged in the field of environmental law, consumer protection, and financial services, and it eventually became its own legal "regime"—a particular way to connect and manage certain legal rights and obligations to achieve certain goals. What is unique to these iterations of risk-based approaches is that, when applied to content platforms, they ultimately entail classifying content and speech. And there lies the problem.

4 Content classification has been a fundamental tool for the protection of freedom of expression under human rights law. International treaties allow only certain types of speech to be legitimately restricted by the state. Clearly determining what content is legal and which is not is key for freedom of expression theory and practice, for the State can only restrict content that is deemed illegal, whether because it infringes upon the rights of others or because it affects an important social interest, as stated, for example, by article 19 of the International Covenant on Civil and Political Rights (ICCPR), article 10 of the European Convention on Human Rights (ECHR), or article 13 of the American Convention on Human Rights (ACHR). State restrictions to freedom of expression need to pass an analysis of legality, legitimate interest, necessity, and proportionality under the most stringent standards. Risk-based regulations applied to content platforms not only allow for but mandate the creation of new categories of speech that fall somewhat short of the binary distinction between what is legal and what is not. They also mandate platforms and search engines to address them under the risk identification and mitigation paradigm and expand the universe of content categories to be indirectly governed by the State.

5 Section two discusses the history of the current trend towards risk-based regulation by highlighting the use of risk as a concept in different legal institutions and the rise, in the 1970s, of a managerial approach to regulation. The DSA combines both. Section three dwells on the reasons why states have turned to a risk-based approach for the tech sector. Section four argues that regulating speech like the DSA does poses unique challenges and trade-offs for freedom of expression. In particular, we discuss

2 Julile Cohen and Ari Waldman, 'Introduction: Framing Regulatory Managerialism as an Object of Study and Strategic Displacement' (2023) 86 Law and Contemporary Problems i <https://scholarship.law.duke.edu/lcp/vol86/iss3/10>; Christopher T Marsden, *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011); Chris Marsden, Trisha Meyer and Ian Brown, 'Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?' (2020) 36 Computer Law & Security Review 1 <http://www.sciencedirect.com/science/article/pii/S026736491930384X> accessed 17 August 2020.

3 Robert Gorwa, 'The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content' (2019) 8 Internet Policy Review <https://policyreview.info/articles/analysis/platform-governance-triangle-conceptualising-informal-regulation-online-content> accessed 25 August 2020.

4 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

5 Ibid, pars. 80-84.

6 Ibid, art. 37.

7 Ibid.

8 Ibid 2.

9 UNESCO, 'Guidance for Regulating Digital Platforms. Safeguarding Freedom of Expression and Access to Information Through a Multistakeholder Approach' (UNESO 2023) Final version.

10 GDC, 'Global Digital Compact' (United Nations General Assembly 2024) A/79/L.2.

11 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 [2024] OJ L 1689/1

12 Online Safety Act 2023, c 50; Online Harms Act, Bill C-63 (44-1), 1st Sess, House of Commons (Canada), 26 February 2024 (died on the Order Paper 6 January 2025); Kids Online Safety Act, S 1409 (118th Cong, 30 July 2024) (reintroduced May 2025).

the differences between risks under the UNGPs and under the DSA and the tension of the latter approach with the popular three-prong test used by many courts to analyze the legitimacy of restrictions to freedom of expression. We argue that the risk-based approach pushes rights out of the center stage of Internet governance and may create a logic of "symbolic compliance" where their governance role is further diminished. Finally, this paper identifies opportunities to address or mitigate the challenges identified, especially in an enforcement stage that remains quite open to these kinds of efforts.

B. Risk-based Regulation: A Brief History

6 Risk-based regulation is not new. It has been used in the past in environmental and financial regulations,[13] among others. But its adoption by the European Union in the field of technology and Internet governance[14] has influenced other regulatory proposals at the international,[15] regional[16] and even national levels.[17]

7 Indeed, risk is a concept used in the law in many ways, sometimes implicitly as a reason to adopt a rule that regulates conduct to prevent an undesirable event from happening or to determine who should carry its costs. This is what happens when the law distributes general duties, like the duty of care or assessment by those who engage in activities deemed risky, or imposes precise rules, like the ones mandating the use of a seat belt while driving or special requirements to transporting hazardous waste. Risk is also present when the law identifies those responsible if legally redressable harms occur.[18] The legislator makes a balancing exercise between the costs of risk prevention or risk avoidance and the magnitude of harms to be produced to determine which harms will be legally redressable and which risks of harm should be managed, for not all harms are to be remedied by law. For instance, the emotional risks involved in engaging in interpersonal relationships, for example, are not redressable by law, but the financial ones sometimes are. Moreover, not all risks are to be managed legally, so you can be a journalist without proper training but you cannot be a lawyer or a doctor without a degree. From a legal standpoint, risk is deeply imbued with normativity.[19]

8 The law also invokes risks more explicitly as something to be managed and with the purpose of creating value out of things that—without the law—would not have any. As François Ewald put it, from a legal perspective risk is "a specific mode of treatment of certain events capable of happening to a group of individuals—or, more exactly, to values or capitals possessed or represented by a collectivity of individuals: that is to say, a population. Nothing is a risk in itself; there is no risk in reality. But on the other hand, anything can be a risk; it all depends on how one analyzes the danger, considers the event".[20] Identifying a risk is the first step of its operation as a legal mechanism. Once the risk has been named, assessed, and valued, it can be distributed and what previously was a reason not to go somewhere becomes part of the planning process that will take us there. The maritime insurance contract is a good example of this mechanism in action. The possibility of a shipwreck weighs heavily on the mind of a merchant before loading a ship with valuable cargo. What if the ship foundered under an unexpected raging sea? The insurance contract distributes those risks and creates incentives for maritime travel and shipping.[21]

9 Generally speaking, the way the law operates when dealing with risk is as follows: identification of a risk, of the agent responsible for its management, of the behavior that is expected to be followed or avoided, and of the liability for the eventual harm. This is the essence of how risk operates as a legal mechanism to distribute potential costs implied in human activities and creates incentives for activities deemed beneficial.

10 Legal systems can identify, assess, and manage risks differently depending on the topic, the complexity of the issues, or the incentives or disincentives they seek to create. Traditional democratic rule-making models heavily support a command-and-control approach, where rules are made through public deliberation and the conduct prohibited or expected is clearly defined and prescribed. In the

13 Cohen and Waldman (n 2).

14 European Commission Digital Services Act (n 4).

15 GDC (n 10).

16 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689/1.

17 Online Safety Act 2023; David Lametti Online Harms Act (Canada) (n 12); Richard Blumenthal and Marsha Blackburn Kids Online Safety Act (n 12).

18 François Ewald, 'Insurance and Risk' in Graham Burchell, Colin Gordon and Peter Miller (eds), *The Foucault Effect: Studies in Governmentality* (University of Chicago Press 1991) 201 ("Insurance and the law of responsibility are two techniques which bear on the same object").

19 Ortwin Renn and Andreas Klinke, 'Risk Governance: Concept and Application to Technological Risk' in Adam Burgess, Alberto Alemanno and Jens Zinn (eds), *Routledge Handbook of Risk Studies* (Routledge 2019).

20 Ewald (n 18) 199.

21 Ibid 199–200.

1970s, a "new regulatory mood began to emerge",[22] that was skeptical of the power of governments alone to identify and assess redressable risks and regulate accordingly. It posited that the state should adopt certain methods and techniques designed to manage processes of capitalist production in its approach to regulation.[23] It rejected the command-and-control model in favor of "relatively informal modes of policymaking and enforcement … and its emphasis on devolution of regulatory authority to private-sector partners and delegates".[24] Under this approach, which Cohen and Waldman call "regulatory managerialism", general obligations of process are designed by the legislator or administrative body, and the prescribed conduct is replaced with guidances, best practices, compliance certifications, and negotiation.[25]

11 Those being regulated are an essential part of the processes of regulatory managerialism. Some say the approach is especially suitable for rapidly changing environments: it is "flexible, nimble, responsive to stakeholder priorities, and well suited to a fast-changing, complex economy".[26] It is also good to deal with serious information asymmetries. Those who criticize these techniques find that they are easily co-optable by corporations, who will pursue their own interests at the expense of the public's.[27] They argue corporations can develop check-box compliance approaches that pay lip service to the values being pushed and produce no real change in the world whatsoever.[28] We have recently witnessed the development and expansion of this managerial approach in different spheres of governance, including corporate governance. The state sponsors self-regulatory practices within certain fields, but under its guidance and oversight.[29] It creates obligations upon the private sector to disclose information and seeks to leverage this mandated transparency for different public purposes. Self-regulatory and co-regulatory frameworks encourage the active involvement of those being regulated and evolving obligations and interpretations of the expected conduct along the life of the regulation.[30] Risk is an essential piece of the managerial approach, for it is what authorities can clearly identify and signal as relevant for action, even though they may not have the necessary knowledge, information, or incentives to act upon it most efficiently.

C. Technology as a Risk to be Managed

12 The extent to which the flow of information on the Internet should be unrestrained or governed, or individual speech acts should be protected or limited, seem to be questions of vital importance in a democratic society committed to values of self-government.[31] Before the DSA, there was no precedent on the application of the managerial model to the field of platform governance through domestic legislation, where either rule of civil liability or immunity laws for third-party posted content were applied.[32] These rules were meant to promote and protect the internet as a means of distribution of speech in a decentralized manner, under the principles of neutrality and non-censorship.[33] But the early immunity approach, designed to encourage the development of an industry unencumbered by potential litigation costs, took some of those key questions out of legal debates. Instead, it created a quid-pro-quo mechanism of paralegal governance that made corporations receptive to government and civil society demands. The state offered immunity but expected collaboration in return.[34] Public officials and civil society organizations (CSOs) became accustomed to asking corporations for actions on a "voluntary" basis. Sometimes, those requests went beyond what the state could accomplish through formal methods of rule-making.

13 At least since the mid-2010s, immunity rules have come under criticism, and calls to change them have become louder. The growing anxiety regarding the

22 Michael Power, *The Audit Society: Rituals of Verification* (Subsequent edition, OUP Oxford 1999) 52.

23 Cohen and Waldman (n 2).

24 Ibid, i.

25 Ibid, iv-v.

26 Ibid, i.

27 Ibid, vi-vii.

28 Lauren B Edelman, *Working Law: Courts, Corporations, and Symbolic Civil Rights* (Illustrated edition, University of Chicago Press 2016).

29 Marsden (n 2); Marsden, Meyer and Brown (n 2).

30 Benoît Frydman, Ludovic Hennebel and Gregory Lewkowicz, 'Co-regulation and the Rule of Law' in Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds), *Governance, Regulation and Powers on the Internet* (Illustrated edition, Cambridge University Press 2012).

31 Alexander Meiklejohn, *Free Speech and Its Relation to Self-Government* (Harper & Brothers Publishers 1948).

32 Agustina Del Campo, 'Volume, Speed, and Accessibility as Autonomous Harms: Can Modern Legal Systems Deal With Harmful but Legal Content? - New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms - Carnegie Endowment for International Peace' (*Carnegie Endowment for Democracy*, 29 November 2023) <https://carnegieendowment.org/2023/11/29/volume-speed-and-accessibility-as-autonomous-harms-can-modern-legal-systems-deal-with-harmful-but-legal-content-pub-91082> accessed 11 January 2024.

33 Communications Decency Act 1996 (USC); Directive 2000/31/CE 2000.

34 Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019) 2.

effect of the Internet on democracy seems to have caused the shift. The Internet became a risky thing to be governed, especially since 2016, the year of Brexit, Trump and the Colombian Peace referendum that marked the beginning of the disinformation scare and an era of techlash.[35] Regulatory push-back, such as the Netzwerkdurchsetzungsgesetz in Germany in 2017[36] and the Loi Avia in France in 2020[37] were among the first regulatory efforts against the status quo. The DSA is in many ways a product of these developments.

14 Speech online, however, has always generated concerns that exceed the traditional distinction between the legal and the illegal content. The volume of content produced daily on the Internet is unprecedented as is the speed at which it spreads, or the fact that, in principle, the content remains up indefinitely. Concerns over potential new harms arising from some of the Internet's structural affordances have been growing louder and have caught the attention of regulators and civil society alike. For instance, can content that would be perfectly legal in isolation become harmful when aggregated? Can its permanence on the Internet be a source of redeemable grievances?[38] These questions highlight new kinds of potential harms that are not addressed by traditional freedom of expression laws neither locally nor regionally or internationally. Evelyn Douek, for instance, first described the difficulty of assessing a platform's compliance with freedom of expression on a content-by-content basis, as international human rights law traditionally proposes. She posited that, given the volume and scale of content within platforms, content moderation could be assessed in bulk. Compliance with human rights law could be measured based on aggregates where States or companies themselves could determine what percentage of error would be deemed acceptable and the platforms' compliance could be guided by probability and proportionality.[39] She argued that the move was needed to create a content moderation system that was scalable, flexible, adaptable to the ever-changing environment of online speech, and able to treat errors in content moderation decisions as inevitable. More recently, Robert Post has argued that "the scale of the internet produces forms of harm that may best be characterized as stochastic. Previously we asked whether particular speech acts might cause particular harm. The internet has rendered this kind of question almost obsolete. Speech that is simultaneously distributed to billions of persons may produce harm in ways that cannot meaningfully be conceptualized through the lens of discreet causality. We will need instead to think in terms of the statistical probability of harm".[40] He warns, though, that at present "we lack any legal framework capable of assessing stochastic harms in ways that will not drastically over-regulate speech".[41] In many ways, the risk-based approach adopted in the DSA, and other provisions since, have built their legitimacy on the need to address these new harms that technology generates and offer a path forward.

15 The risk-based approach now adopted by formal regulation was previously pushed on corporations through the voluntary and soft law approach of the UN Guiding Principles (UNGPs) on Business and Human Rights. This model was supposed to "internalize" corporate commitments to human rights,[42] that could not be imposed externally through hard law because of the gridlock affecting the UN on the issue of human rights and transnational corporations. Risk played a meaningful role in its design. Under the UNGPs, corporations are committed to identifying risks to human rights, and monitoring and evaluating their actions[43] to take "adequate measures for their prevention, mitigation and, where appropriate, remediation".[44] To this end, corporations resorted to processes of impact assessments, procedural devices designed to help them make better decisions regarding their operations and their impact that were

35 Robert D Atkinson and others, 'A Policymaker's Guide to the "Techlash"—What It Is and Why It's a Threat to Growth and Progress' (Information Technology & Innovation Foundation 2019) <https://itif.org/publications/2019/10/28/policymakers-guide-techlash/> accessed 22 August 2022.

36 Netzwerkdurchsetzungsgesetz 2017 (BGBl).

37 Loi No. 2020-766 visant à lutter contre les contenus haineux sur internet 2020 (JORF).

38 Del Campo (n 32).

39 Evelyn Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3679607> accessed 23 April 2022.

40 Robert Post, 'The Internet, Democracy and Misinformation' 8 <https://papers.ssrn.com/abstract=4545891> accessed 4 November 2024.

41 Ibid.

42 James Harrison, 'Human Rights Measurement: Reflections on the Current Practice and Future Potential of Human Rights Impact Assessment' (2011) 3 Journal of Human Rights Practice 162, 108 <https://academic.oup.com/jhrp/article/3/2/162/2188745> accessed 14 May 2020.

43 John Ruggie, 'Protect, Respect and Remedy: A Framework for Business and Human Rights' (Human Rights Council eport of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises 2008) A/HRC/8/5, par. 25.

44 John Ruggie, 'Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework' (Human Rights Council Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises 2011) HR/PUB/11/04 principle11.

particularly well known in the environmental field of law,[45] and applied it to human rights.[46] A whole industry of consultants, experts, and knowledge emerged as a consequence. The field of Business and Human Rights produced the professional cadre that regulatory managerialism needed to operate in the content platform industry.

16 In sum, the new generation of platform regulation embraces a managerial, co-regulatory model, where risk plays the fundamental role of bridging the gap between state desires to deal with certain harms—some poorly identified and currently not legally redressable—and the much-needed collaboration of those corporations in the position to address them. In this evolution, the identification of the Internet as a risk plays a crucial explanatory role, and the path-dependency of the informal mechanisms of governance allowed by the old rules on intermediary liability and the UNGP framework explain the managerial and procedural turn as something more like an evolution than a clean break with the past.

D. The Risks of the Risk-Based Approach as Applied to Speech

17 Although risk-based approaches are not new and the risk-based model borrows language and processes from existing human rights soft law documents, the risk management system in the DSA poses new challenges. The DSA broadens the scope of the risks it mandates corporations to mitigate as compared to the UNGPs. Under the DSA, the violation of fundamental rights is only one risk to be addressed among many. Furthermore, the DSA adopts a hard law approach that invokes the coercive power of the state. Because it is tailored to content platforms, it deals mainly with third-party posted content and thus must be scrutinized under freedom of expression standards. Finally, the DSA also expands the speech to be governed by imposing obligations on corporations to act on speech that is, according to standard human rights principles, out of State action reach. As a result of these factors combined, human rights lose centrality and fade into the background of the DSA's risk-based approach.

I. Differences in Kind Between UNGPS and the DSA

18 Unlike the UNGPs, which focus exclusively on risks related to human rights, the DSA treats adverse effects on human rights as just one risk among many.[47] This outward expansion is consequential, for human rights are a framework that plays a somewhat constraining function. The UNGPs don't target any harmful conduct that companies may produce, but only those that may infringe upon human rights. Human rights law, for example, mandates that certain harms be tolerated in democratic societies. Therefore, not every infringement upon the right to privacy or the right to honor, for instance, may be legally redressable. Restrictions to freedom of expression are illegitimate unless necessary, proportionate, and well-defined in the law in order to be legitimate, even if the expression in question might have produced harm.[48] This standard test has been established through a shared practice that has produced a corpus of standards, case law, precedents, and rules that defines and distinguishes legally redressable from non legally redressable harms and, therefore, limits the kinds of risks of harm that companies need to address under these norms. The expansion of "risks" that the DSA encourages is less constraining, for the harms to be mitigated are more vague, are not attached to any particular legal framework, and are built on less developed foundations. The law, for example, requires auditors to have expertise in risk management in general;[49] expertise regarding "the systemic societal risks referred to in Article 34" is also expected.[50] Notably, but not surprisingly, no expertise is required in the field of human rights. This is especially telling given the lack of standards or benchmarks provided by the

45 John Glasson, *Introduction to Environmental Impact Assessment* (Taylor & Francis Ltd 1998).

46 Desirée Abrahams and others, 'Guide to Human Rights Impact Assessment and Management' (International Business Leaders Forum, International Finance Corporation & el Global Compact de las Naciones Unidas 2010).

47 Rachel Griffin, 'What Do We Talk about When We Talk about Risk? Risk Politics in the EU's Digital Services Act - DSA Observatory' (*DSA Observatory*, 31 July 2024) <https://dsa-observatory.eu/2024/07/31/what-do-we-talk-about-when-we-talk-about-risk-risk-politics-in-the-eus-digital-services-act/> accessed 5 November 2024; European Commission Digital Services Act (n 4), article 34.1(b).

48 CIDH, 'Marco Jurídico Interamericano Del Derecho a La Libertad de Expresión' (Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos 2009) OEA/Ser.L/V/II CIDH/RELE/INF. 2/09, par. 67.

49 European Commission Digital Services Act (n 4), article 37.3.

50 Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines 2023, recital 9.

delegated act on independent audits,[51] the centrality of auditors in the DSA's oversight infrastructure,[52] and how audit results can inform regulatory supervision.[53]

19 The UNGPs are a soft law instrument that companies may voluntarily choose to abide by and that lack formal enforcement mechanisms. They came to be as a way of dealing with the thorny question of business and human rights inside the United Nations, crossed by a pervasive disagreement between the countries that produced transnational corporations (in the North) and those who received them (in the South). The UNGPs were the way out of that gridlock, and they were meant to deal with resource-intensive industries with profound social and environmental impact on the ground, such as the extractive industries.[54] They assumed that the main risk for human rights came from states, but transnational corporations could on occasion violate them or contribute to their violation. They were meant to close the governance gap "created by globalization—between the scope and impact of economic forces and actors, and the capacity of societies to manage their adverse consequences. These governance gaps provide the permissive environment for wrongful acts by companies of all kinds without adequate sanctioning or reparation".[55] The DSA batters on a similar nail through a much more powerful hammer. Unlike the UNGPs, the DSA is hard law and foresees enforcement mechanisms, penalties, and sanctions against companies that fail to comply with its mandates. The difference becomes significant particularly when dealing with content platforms and an open framework of "risks" as discussed above.

20 Finally, the DSA is tailored to deal with content-facilitating and content-producing companies within the Internet's decentralized architecture. It targets a particular industry and explicitly articulates the new paradigm: that online speech generates risks that need to be managed, mitigated, or else. And while the UNGPs are focused on human rights obligations, the narrative[56] the DSA tells is not that of rights but one centered on risks: in its risks and harms approach, human rights concerns are present, but only as one risk among many. And even when the DSA does have Human Rights safeguards built into its text, if not taken seriously, they could even end up legitimizing state action in violation of Human Rights (for instance, the insufficient safeguards in article 9 against illegitimate state orders).

21 Furthermore, the DSA fails to acknowledge the state as a risk for the protection of human rights. Mandated transparency is among the most celebrated measures adopted by the DSA, as is data access for researchers, but every procedural measure incorporated in the DSA is directly tied to what is considered relevant to address the risks identified in Article 34. There are ongoing discussions about the possibility of State agents engaging with companies as trusted flaggers and no duty to report on the potential correlations this may bring about. The framework is prone to obscure rather than provide transparency to state-led censorship.

22 At the center of the DSA lays a right deemed fundamental for the working of democratic societies: the right to freedom of expression. Unlike the extractive industries contaminating the environment or exercising violence upon local populations, the transnational corporations targeted by the DSA are in the business of facilitating communications between individuals. It is an economic activity, but one closely connected to the exercise of the fundamental rights of their users.

II. Expanding the Speech to be Governed

23 The correlation between the expressions generally frowned upon by society and those considered illegal under the law is not perfect. As a general rule, under either international human rights law, constitutional law, or both, all speech is protected under the right to freedom of expression, with very limited exceptions. This leaves a lot of offensive, unpleasant, shocking expressions still protected by the law. Those expressions are generally referred to as "lawful but awful" or "harmful but legal" speech —new categories that grew out of the anxieties produced by the effects of certain Internet-based speech on democratic societies. The risk-based approach that the DSA embraces allows it to expand its governance over these new categories of speech.

51 Ibid.

52 Giovanni De Gregorio and Oreste Pollicino, 'Auditing Platforms under the Digital Services Act' [2024] Verfassungsblog <https://verfassungsblog.de/dsa-auditors-content-moderation-platform-regulation/> accessed 25 November 2024.

53 Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines, recital 1.

54 Ramiro Álvarez Ugarte and Laura Krauer, 'ICT and Human Rights: Towards a Conceptual Framework of Human Rights Impact Assessments' (Centro de Estudios para la Libertad de Expresión 2020).

55 Ruggie (n 43), par. 3.

56 Robert Cover, 'Foreword: Nomos and Narrative' (1983) 97 Harvard Law Review 4.

24 Under old-school intermediary liability laws, each platform had the discretion and the incentive to address the problem of "harmful but legal" content as they saw fit through enforcement of their terms of service, without concerning themselves with potential liability stemming from under or over-removal of content. This structure enthroned platforms as digital sovereigns, private censors, and new governors of speech.[57] The DSA challenges this model and brings about a system of content governance to tackle the issues posed by lawful but awful expression online.

25 The risk-based approach is presented as useful for this venture because it allows the state to shape content moderation practices by intervening mostly on processes, which, in turn, awards each platform the much-needed flexibility to tailor their interventions to the very specific risks derived from their operations. In the DSA's model, it is not the legislator who identifies the kind of legal but harmful content they want platforms to disallow. Such a law would most probably violate freedom of expression guarantees. Platforms are the ones that must identify, assess, and mitigate the specific risks that their affordances or the use of their services generate. However, the risks that platforms should look for are outlined by the legislator, mostly on Article 34. Additionally, the DSA prescribes some of the measures that could be taken to mitigate those risks.[58] While there are no explicit mandates to remove certain categories of content, the expansion of the risks that companies should mitigate beyond those identified in international human rights law per se expands the categories of speech governed. The list is not exhaustive, so companies are permitted to engage in different, innovative mitigation measures exceeding those included in the law.

26 Rather than imposing hard metrics or targets, the DSA seeks to encourage platforms and search engines to "think" about the risks they potentially generate.[59] It presents itself as a holistic approach that stays away from drawing clear lines or establishing clear-cut rules that mandate the removal of content other than the illegal one. However, although not prescriptively, article 35 suggests the expeditious removal of hate speech and cyber violence as an effective and desirable mitigation measure.[60] The Codes of Conduct on Disinformation and Hate Speech also provide concrete suggestions like demonetization, filtering, blocking or deindexing for harmful but legal content. By maintaining platform immunity for third-party posted content, the DSA keeps companies safe from the liability arising from their own "errors" in content moderation.

27 The DSA has been portrayed as a law mainly dealing with processes. It mandates companies to offer a series of appeals systems and complaint mechanisms designed to make sure that content producers' and their audiences' rights are respected and terms of service are applied to them consistently.[61] A series of information disclosure obligations, such as transparency reports, independent audits, and data access for researchers, are incorporated into the law to make platform accountability possible. The inclusion of these procedural obligations upon companies is a significant and well-received contribution to platform governance debates.

28 However, the DSA does not only regulate processes but also deals with substantive issues. The systemic risks it identifies force corporations to assess the nature of content and act upon legally protected speech. It also mandates companies to assess their own tools and means to distribute and organize legally protected speech. Some may argue that the DSA only generates obligations vis-à-vis the companies' own actions rather than those of content producers, but VLOPs and VLOSEs systems are directly tailored to present, distribute, and curate content. And both the generation and distribution of content are essential parts of well-established freedom of expression laws and standards all over the world. In well-functioning democracies, limiting the reach of a newspaper by fixing its selling price through law or limiting the number of copies that may be printed of a given book or magazine would be as unconstitutional as censoring it.

III. Systemic Risks and Compliance with Freedom of Expression Human Rights Standards

29 Voluntariness matters when non-state actors are involved, especially when it comes to speech. For

57 Kate Klonick, 'The New Governors: The People, Rules, And Processes Governing Online Speech' (2018) 131 Harvard Law Review 73; Jack M Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296 <https://www.jstor.org/stable/23742038> accessed 10 March 2023.

58 European Commission Digital Services Act (n 4), article 35.

59 Evelyn Douek, 'The Siren Call Of Content Moderation Formalism' in Lee Bollinger and Geofrey Stone (eds), *Social Media, Freedom of Speech, and the Future of our Democracy* (Oxford University Press 2022).

60 European Commission Digital Services Act (n 4), article 35.

61 Pietro Ortolani, '"If You Build It, They Will Come". The DSA "Procedure Before Substance" Approach' in Joris van Hoboken and others (eds), *Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications* (1st edn, Verfassungsblog gGmbH 2023); European Commission Digital Services Act (n 4), article 21.

instance, a microblogging platform for and by puppy owners could establish an "only pictures of puppies" rule without triggering human rights concerns. However, if state-mandated, the rule would trigger heightened human rights-based scrutiny as a potential infringement on freedom of expression. The nature of the right affected is also important. Patrimonial rights, for instance, are generally easier to limit than those deemed essential for the good working of democratic institutions. Constitutional courts have generally shown more deference to legislators affecting the former rather than the latter.

30 The DSA seeks to navigate these important distinctions. On the one hand, it grants corporations a lot of leeway to manage their services as they see fit—they just need to be aware of, and manage, a set of very vague risks that the European legislator identified as "systemic". It does not regulate the patrimonial rights of corporations (that's a job for the Digital Markets Act) but it claims not to regulate speech rights either. The DSA, we are told, is about processes rather than substance. But the nature of the companies being regulated pulls speech rights back in, for issues as varied as disinformation and misinformation, the sale of illegal products, online scams, election interference, hate speech and discrimination, and terrorism-promotion content, all include, quite obviously, a freedom of expression dimension that demands that we carefully assess whether restrictions based on the state's interest to combat these harms are necessary in a democratic society.[62] If corporate action upon third-party posted content is directly linked to a state mandate, such restriction should be subjected to the scrutiny called for by the three-prong test. And the distance between the action and what was required—a distance established by design—does not fare well under this light. Article 53(3) of the European Charter, which is directly cited by the DSA, mandates that the rights contained therein be interpreted in light of the European Convention on Human Rights.

1. The Legality Principle

31 Any restriction to freedom of expression must be prescribed by law. Under stable criteria of the ECtHR, any restriction to freedom of expression must be "formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[63] The ICCPR adopts a similar standard.[64] Laws restricting freedom of expression "may not confer unfettered discretion on those charged with their execution".[65]

32 Absolute legal precision is not, however, the standard—"experience shows this to be unattainable", and "whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice".[66] As it stands today, and without proper guidance from the European Commission, it remains unclear which is the risky content that platforms and search engines need to identify and mitigate to fulfill their Article 34 and Article 35 obligations under the DSA.

33 Proponents of the risks-based approach in the DSA distinguish the clarity needed to directly restrict speech from that required to hold companies accountable for speech-generated harms. They argue that vagueness in the categories of risks listed in Article 34 and the lack of concrete definitions of risks might be features, rather than bugs, of the risk-based approach in the DSA.[67] They introduce a degree of flexibility that allows both VLOPs and VLOSEs and the European Commission to initiate an iterative process where they can jointly set goals according to their growing capabilities and build on previous findings. This, they hope, will encourage a kind of regulatory dialogue where progress is made developmentally. They favor, thus, a flexible framework that would be more responsive to the fast-paced and ever-changing activity of the sector, which could render more rigid systems with static rules and bright lines useless.[68]

34 However, the DSA is concerned with harms caused

62 Tarlach McGonagle and Onur Andreotti, *Freedom of Expression and Defamation* (Council of Europe 2016) 12.

63 *The Sunday Times v the United Kingdom (no 1)* [1979] ECtHR 6538/74, par. 49.

64 HRC, 'General Comment No. 34 on Article 19 of the ICCPR' (Human Rights Council 2011) CCPR/C/GC/34, par. 25.

65 Ibid; HRC, 'General Comment No. 27 on Article 12 of the ICCPR' (Human Rights Council 1999) CCPR/C/21/Rev.1/Add.9, part. 13.

66 *The Sunday Times v. the United Kingdom (no. 1)* (n 63), par. 49.

67 Zohar Efroni, 'The Digital Services Act: Risk-Based Regulation of Online Platforms' [2021] *Internet Policy Review* <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606> accessed 24 November 2024.

68 Justin Hurwitz, 'Regulation as Partnership' (2019) 3 Journal of Law and Innovation 1; Tim Wu, 'Agency Threats' (2011) 60 Duke Law Journal 1841 <https://heinonline.org/HOL/Page?handle=hein.journals/duklr60&id=1857&div=&collection=>; Stuart Brotman, 'Communications Policy-Making at the FCC: Past Practices, Future Direction' (1988) 7 Cardozo Arts & Ent LJ 55.

by categories of speech defined in the broadest terms and distributed, organized and curated by companies. As long as there are people expressing themselves, there will be risks to the well-being, health, security, and even the enjoyment of some human rights as conceived in the DSA. Platforms cannot completely mitigate these risks without shutting down their operations entirely. So difficult questions come up. How much of each risk could reasonably remain unmitigated and what are the relevant metrics to be used for each? Are metrics as effective to encapsulate these risks as those used to measure water's fitness for human consumption? Human expression is inherently complex—tensions will appear regarding the proper balancing between freedom of expression vis-à-vis countervailing interests, protection against certain risks, and even frustration of the human rights of third parties, or between different interpretations of freedom of expression, the adoption of either of which would lead to inevitably different outcomes.[69]

35 The "systemic" component of risks as early as we are in the implementation of the DSA poses additional challenges. It is still unclear whether the systemic aspects refer to the systems within a single company, a group of similar companies that together create a system, a larger group of companies encompassing hardware and software providers and their consumers, or an even broader interpretation—as in the system formed by the outlets and the agents whose interaction form a Habermasian public sphere.[70]

36 Looking to the financial services literature, where the idea of "systemic risk" comes from, is not helpful (nor is the inspiration promising, considering the success of financial regulation to prevent abuses and harms). Broughton Micova and Calef, after looking at financial markets, suggested that "the systemic nature of risk is not only about the number of users affected by any harm but also derives from the way very large services function as public spaces and from the potential for effects on public systems due to the scale and role of the services designated as VLOPs and VLOSEs".[71] And yet, this concept remains a "remarkably broad category" in the context of the DSA.[72] Article 34 does not offer a definition and researchers disagree.[73] As Griffin puts it, "there are deep ideological and political conflicts over the nature of these essentially contested concepts".[74] The hard work of defining "risk area-specific understandings of what systemic failure or crisis looks like and what effects contribute to those" remains ahead of us.[75]

37 While there are visible advantages to a flexible approach towards evolving technologies, the vagueness of the existing categories give both companies and the European Commission a great deal of discretion, which is exactly what the principle of legality was meant to prevent. There is, then, a fundamental tension between the risk-based approach as broadly defined in the DSA and the black-lettered stable rules established by the European Court of Human Rights to assess restrictions on freedom of expression. This tension will have to be resolved in the future, either by insisting on the need for clarity and precision or by relaxing the legality principle.

2. The Legitimate Aim

38 This is probably the easier part of the three-prong test for the DSA to pass. International Human Rights Law requires that limitations be justified to pursue a legitimate aim and sets out what those legitimate objectives may be. The ECtHR has consistently held that there is little scope under Article 10.2 for restrictions on political speech or the debate of issues of public interest.[76] However, the Court has also been deferential to the kind of arguments that states usually deploy to justify restrictive measures. The requirement that the state justifies them under a "legitimate objective" has often been easily met.[77]

69 Ramiro Álvarez Ugarte, 'From Soft Law to Hard Law: Human Rights Impact Assessments in the Digital Services Act Era | TechPolicy.Press' (*Tech Policy Press*, 20 June 2024) <https://techpolicy.press/from-soft-law-to-hard-law-human-rights-impact-assessments-in-the-digital-services-act-era> accessed 29 October 2024.

70 Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (The MIT Press 1991).

71 Sally Broughton Micova and Andrea Calef, 'Elements for Effective Systemic Risk Assessment Under the DSA' [2023] SSRN Electronic Journal 49 <https://www.ssrn.com/abstract=4512640> accessed 25 November 2024.

72 Paddy Leerssen, 'Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act' (2024) 4 Weizenbaum Journal of the Digital Society 24 <https://ojs.weizenbaum-institut.de/index.php/wjds/article/view/4_2_3> accessed 3 August 2024.

73 Oliver Marsh, 'Researching Systemic Risks Under the Digital Services Act' (*AlgorithmWatch*, 26 July 2024) <https://algorithmwatch.org/en/researching-systemic-risks-under-the-digital-services-act/> accessed 5 November 2024.

74 Griffin (n 47).

75 Broughton Micova and Calef (n 71) 50.

76 *Castells v España* [1992] Tribunal Europeo de Derechos Humanos 11798/85; *Wingrove v United Kingdom* [1996] European Court of Human Rights 17419/90, HUDOC.

77 Lorna Woods, 'Freedom of Expression in the European Union' (2006) 12 European Public Law 371, 376 <https://kluwerlawonline.com/journalarticle/European+Public+Law/12.3/EURO2006026> accessed 5 No-

39 The harms derived from speech are actual, real, and in many cases serious. The impact of technology on public discourse and society as a whole is undeniably deserving of attention. Tech companies need to be held accountable for the legally redressable harm they produce or contribute to producing. States are allowed to address them and restrict freedom of expression when necessary but, in that venture, they are also obligated to respect this three-prong test. In its own problematic way (as discussed in the previous section), the DSA has invoked a set of aims that are indeed legitimate. So we move on quickly to the next step of the analysis.

3. The Necessity and Proportionality Test

40 To be compatible with the ECHR, restrictions must be "necessary in a democratic society" and proportional, which means that they must correspond to a pressing social need and be proportionate to the legitimate aims being pursued.[78] Under the ECHR, proportionality requires that restrictions are adopted through the least restrictive means to achieve the goals pursued by the regulation.[79] Under the ICCPR, proportionality requires measures not to be overbroad and "the least intrusive instrument amongst those which might achieve their protective function".[80] They must be "proportionate to the interest to be protected".[81] The principle must be respected both in the law establishing the restriction and in the specific instances in which it is enforced.[82]

41 The DSA mandates that risk assessments should be "proportionate to the systemic risks, taking into consideration their severity and probability".[83] And mitigation measures should also be "proportionate".[84] However, when compared to the international standards reviewed, the DSA framework tweaks proportionality in some relevant ways. First, by requiring that the obligations under Articles 34 and 35 are complied with in a way that is proportionate to the risks identified and reported, the DSA is departing from the understanding of proportionality under international human rights and European fundamental rights law. Under international standards, proportionality contains an objective dimension, one that requires using the least restrictive means possible on each occasion. Under Article 35 of the DSA, mitigation measures must be "proportionate" to risks. Hence, the bigger the (self-assessed) risk, the more stringent acceptable mitigation measures can be. Second, the DSA outsources the determination of the proportionality of mitigation measures to VLOPS/VLOSEs with no further guidance than stating—redundantly—that they must fulfill their assessment and mitigation obligations in a way that is proportionate to the risks identified. Third, instead of assessing the proportionality of each decision where expression is affected (each modification in the terms of service, each removal, each demotion, etc), it looks at platforms' conduct on an aggregate basis. This makes the proportionality of platform content moderation decisions very hard to oversee outside of the internal complaint mechanisms and out-of-court dispute settlement entities provided for in Articles 20 and 21.[85] The instructions set out in articles 13 and 14 of the Delegated Act on independent audits are written in broad terms and lack the granularity and nuances necessary to evaluate proportionality. Although the instructions mandate that auditors evaluate proportionality, reasonableness, and effectiveness, the indicators identified only address the latter. There are no proposals for indicators to measure proportionality or reasonableness vis-à-vis other human rights. This lack of concrete indicators allows auditors to work with radically different benchmarks, so the performance evaluations of different VLOPs or VLOSEs might not be comparable, even when some of them could be to some extent similar in their affordances.

42 To be fair, setting a priori benchmarks as a one-size-fits-all solution would not necessarily be a better idea, for it would impair the auditors' ability to contemplate the risks inherent to platforms of different natures. It makes sense to settle for more realistic expectations in connection with the kind of control that auditors can exert over platforms. Perhaps audits are useful in determining only one aspect of proportionality: whether the narrative presented by platforms makes sense, that is, whether the chosen measures are effective against the specific risk they were intended to mitigate and "reflect the severity of the risk to society and platform users identified by the platform".[86] However, the auditing process seems ill-suited to assess whether the measures were among the least restrictive means to pursue the same policy goals. This is aggravated by the fact that compliance with

vember 2024.

78 McGonagle and Andreotti (n 62) 12.

79 *Axel Springer Se And Rtl Television Gmbh V Germany* [2017] European Court of Human Rights 51405/12, HUDOC; *Perinpçek v Switzerland [GC]* [2015] European Court of Human Rights 27510/08, HUDOC.

80 HRC (n 64), par. 34.

81 Ibid, par. 34.

82 Ibid, par. 34.

83 European Commission Digital Services Act (n 4), article 34.

84 Ibid, article 35.

85 Ibid, articles 20 and 21.

86 Jeff Allen and Abagail Lawson, 'On Risk Assessment and Mitigation for Algorithmic Systems' (Integrity Institute 2024) 52–53 <https://integrityinstitute.org/news/institute-news/risk-assessment> accessed 25 November 2024.

the voluntary codes of conduct is also evaluated in the audits, as per Article 37 (1)(b).

IV. The Incentives in the Risk Management System of the DSA

43 Every legislation creates incentives. The immunity laws that characterized the prior generation of platform regulations created incentives for self-regulation and the development of increasingly complex terms of service and content moderation practices and techniques. The DSA creates some problematic incentives vis-à-vis content moderation that we have already developed. But it can potentially have other impacts that may be as problematic and need to be addressed and monitored closely during implementation. The risk-based approach of the DSA is not immune to the critiques towards similar procedural regulation, which in many cases have failed to bring about real change and have instead generated disappointment.[87] We would like to focus on two issues: the decentering of rights produced by the risk-based approach and the risk of "symbolic compliance".

1. Rights Fade into the Background

44 Behind any state decision regarding a legal determination of risk "is the question of what is safe enough, implying a normative or moral judgment about acceptability of risk and the tolerable burden that risk producers can impose on others".[88] How States assess this threshold of tolerance "provide hints over what kind of mental images are present and which moral judgments guide people's perceptions and choices" in that state.[89] Reading articles 34 and 35 of the DSA under this lens allows us to understand the relative importance awarded to fundamental and human rights vis-à-vis other risks brought about by big internet platforms. We believe the outcome to be unsatisfactory.

45 Indeed, the DSA changes the framing of platform regulation. The risk identification, assessment, and mitigation mandates within the DSA seek to strike a balance between competing and often contradicting interests at play in platform governance—innovation, commercial interests, protection of rights, and protection of state interests. It adopts a flexible stand in order to allow for different kinds of platforms to operate, and different approaches and business models to flourish. The premise of regulatory managerialism is that companies have the expertise and the knowledge that regulators lack. It is this information asymmetry that normative flexibility is meant to overcome.

46 This reframing, however, does not exempt the resulting rules from human and fundamental rights scrutiny. De Gregorio holds that the risk-based approach championed by the EU in the DSA (also in the GDPR and the AI Act) not only can coexist but is also intimately connected to a rights-based approach.[90] However, under this interpretation risks would take the place formerly occupied by rights as the objective parameter against which all the other elements of legislation are measured. It pushes rights to a subservient place—they become another risk category as Article 34 shows. Rights assume a new role— they are "embedded" in the risk analysis and can be "managed" or measured using the same analytic categories.

47 This shift entails a realignment in policy priorities. The risk-based approach of the DSA downplays human rights analysis and replaces the proportionality analysis that tests state regulations against strict requirements of justification for a risk assessment process where rights are another interest to be balanced against competing interests and concerns. In this exercise, rights no longer hold a preferred position. With big fines looming on the horizon,[91] companies have incentives under the DSA to err on the side of over-mitigation—they simply cannot afford to leave risks insufficiently mitigated and be found noncompliant. To put it in risk management language, the legal risks of under-mitigation are way higher than the alternative. It seems safer to overstate risks than to overstate rights. Auditors will not be of much help, because it is unlikely they will have the necessary information to second-guess companies in their own risk-assessments. Audits might only show us whether the mitigation measures taken by companies are efficient in tackling the risks stated in their risk reports. We have not seen any investigation or RFIs open on the basis that a company went too far in protecting public health or civic discourse, and we don't envision any either. Ultimately, more restrictive terms and conditions can be attributed to companies' stricter policies, and being private and voluntary, these can be deemed

87 Nikolas Rose and Peter Miller, 'Political Power Beyond the State: Problematics of Government' (1992) 43 The British Journal of Sociology 173 <https://www.jstor.org/stable/591464> accessed 18 March 2024.

88 Renn and Klinke (n 19) 209.

89 Ibid.

90 Giovanni De Gregorio, 'How Does Digital Constitutionalism Reframe the Discourse on Rights and Powers?' (*Ada Lovelace Institute*, 7 December 2022) <https://www.adalovelaceinstitute.org/blog/digital-constitutionalism-rights-powers/> accessed 12 November 2024.

91 European Commission Digital Services Act (n 4), articles 74, 76.

independent from their legal obligations.

48 Regulators hold some power to prevent this from happening. If the DSA does propose a regulatory dialogue moving forward, regulators might push back against companies that overestimate risks. This is not an entirely impossible scenario, but it seems unlikely considering the political and ideological drivers currently in place, including the centrality of risks and the displacement of rights, the absence of the state as a potentially threatening actor in the DSA landscape, and the lack of concern for over-removal. These factors limit potential remedies to this problem to the appeals systems in the platforms, out-of-court settlement dispute mechanisms and private enforcement of the DSA, driven by individual content producers or their audiences.

2. Rights as Checkboxes

49 The trends towards "managerialization" and "proceduralization" of human rights through regulations that establish mandatory due diligence obligations give rise to novel challenges. One of them is linked to the UNGPs as the precedent to the DSA, an approach that has proven limited and that introduces a "distortion" in the very idea of human rights as legal institutions. In many ways, human rights in the UNGPs framework are deprived of some of their essentially legal features such as "enforcement mechanisms, liability, and penalties".[92] While the DSA brings the law back in, the gaps identified previously endure.

50 One of the challenges that remain ahead, and that those in charge of implementing the DSA should carefully consider, is the risk that Laura Edelman called of "symbolic compliance"—when rights acknowledged in laws and other regulations are taken by corporations as opportunities to develop ritualistic but rather ineffective measures, such as assigning resources, creating positions, and developing procedures that ultimately fail to produce meaningful conduct change.[93] In these processes, certain actors within corporations gain power but have a limited impact on corporate decision-making, at best.[94]

51 The fact that risk management approaches are becoming, under the weight of the DSA, a form of hard law creates a number of questions that will remain open as organizations comply and adapt to the regulatory dialogue the act promises. For instance, it is likely that the flexibility of risk assessments under the UNGPs will be lost under the pressure of actual regulations that companies will have to comply with (and it will make no sense for companies to develop different risk assessment procedures). Black-letter law will take over voluntary corporate practices.[95] Many companies that developed APIs to encourage developers services, for example, closed them down under the weight of the GDPR. Would something similar happen under the DSA? It is also likely that corporations will develop positions and adapt their structure to the new laws, and work under a paradigm of compliance,[96] that could be, however, symbolic if previous research is ascribed with a predictive function. This will turn human rights into corporate checkboxes to be filled in a compliance exercise. The fact that they appear somewhat secondary to the primacy of risks in the DSA makes matters worse, and the black-letter nature of the act does not seem to be capable of preventing this dynamic from unfolding.[97]

E. Conclusion

52 The first generation of internet regulations, a model that provided absolute immunity for internet companies as its bedrock, led us to a crisis. A new model, with the DSA as its most salient example, is being developed. The bar is set higher for VLOPs and VLOSEs. While they retain their conditioned immunity, they have a new set of due diligence and transparency obligations that can make them

92 Ramiro Álvarez Ugarte, 'Bad Cover Versions of Law. Inescapable Challenges and Some Opportunities for Measuring Human Rights Impacts of Corporate Conduct in the ICT Sector' (2024) preprint, under review.

93 Edelman (n 28).

94 John W Meyer and Brian Rowan, 'Institutionalized Organizations: Formal Structure as Myth and Ceremony' (1977) 83 American Journal of Sociology 340 <https://www.journals.uchicago.edu/doi/10.1086/226550> accessed 10 September 2024; Tricia Olsen and others, 'Human Rights in the Oil and Gas Industry: When Are Policies and Practices Enough to Prevent Abuse?' (2022) 61 Business & Society 1512 <https://doi.org/10.1177/00076503211017435> accessed 11 September 2024.

95 European Commission Digital Services Act (n 4), article 41.1.

96 Daphne Keller, 'The Rise of the Compliant Speech Platform' (*Lawfare*, 16 October 2024) <https://www.lawfaremedia.org/article/the-rise-of-the-compliant-speech-platform> accessed 5 November 2024.

97 Caroline Omari Lichuma, 'Mandatory Human Rights Due Diligence (mHRDD) Laws Caught Between Rituals and Ritualism: The Forms and Limits of Business Authority in the Global Governance of Business and Human Rights' [2024] Business and Human Rights Journal 1 <https://www.cambridge.org/core/journals/business-and-human-rights-journal/article/mandatory-human-rights-due-diligence-mhrdd-laws-caught-between-rituals-and-ritualism-the-forms-and-limits-of-business-authority-in-the-global-governance-of-business-and-human-rights/E8578EFE441CA76E61E461B0F2045A6D#fn3> accessed 5 November 2024.

responsible for noncompliance. The European Union is leading this new experiment to make businesses accountable for the consequences of their activities. This new regulation brought about the challenging and much-needed debate over what tech company accountability could look like and how it could be enforced. It also brought the platform governance multi-stakeholder community out of gridlock and forced us to unpack and build consensus for the adoption of new terms of art and standards for this industry. The DSA has hence been effective already in many different ways.

53 During the implementation stage, however, the meaning of new terms needs to be interpreted and fleshed out. Best industry practices will be identified, and mandated risk assessment reports will ideally provide more nuanced information about content moderation and curation structures and practices within companies. The eyes of the world will be somewhat set in Europe to see if the model delivers what it promises.

54 This paper has tried to work through a number of open questions and identify inherent tensions in the risk-based approach adopted by the DSA that could hinder its effectiveness and may have broader impacts on the conception of the right to freedom of expression in Europe and beyond. While some of the challenges identified may be addressed during the implementation or through litigation, others probably cannot. The latter may nevertheless be important as the DSA gets – willingly or inadvertently– turned into a model for international soft law documents and comparative legislation.

55 As we analyzed, this approach is neither the logical corollary of applying the UNGPs to the ICT sector nor is it entirely consistent with international Human Rights standards of freedom of expression. It pushes rights out of the center stage and replaces them with risk analysis and the new governance techniques associated with the concept. Human rights become part of risk assessment processes, something that downplays their importance and efficacy while using their language and terminology to legitimize the new paradigm.

56 The enforcement stages of the DSA, however, offer opportunities to bring rights back to the center and make this new paradigm work. First, the European Commission should issue guidelines that demarcate the scope of companies' due diligence obligations under articles 34 and 35 of the DSA. Conversely, and even in the absence of those, when assessing the content-related risks stemming from their operations, VLOPs and VLOSEs should flesh out the open-ended terms and generic obligations by anchoring them to existing legal frameworks. For instance, the interpretation of "gender-based violence" and "the protection of minors", should be tied to the text of the CEDAW and the United Nations Convention on the Rights of the Child, and the full body of hard and soft law arising from the relevant treaties under the International and European systems of Human Rights protection, and the interpretation and application to concrete cases by the pertaining Tribunals and Committees. Furthermore, regardless of its absence in Article 34, companies should identify and assess, if appropriate, any risks stemming from state action, including removal orders and more subtle "jawboning" attempts, in their reports under the DSA.

57 From a freedom of expression perspective, the indirect expansion of the speech to be governed by the state is incompatible with agreed international standards. Under the weight of systemic risks, content that is perfectly legal is subjected to the DSA's indirect speech governance mechanisms. The DSA allows the state to achieve, through the risk-based approach, what it could not legitimately do through a more direct and traditional form of regulation. While the risk-based approach to the regulation of VLOPs and VLOSEs responds to new potential sources of harm, carefully addressing volume, speed and permanence as potentially independent sources of legally redressable harm may be a first step in the right direction.[98] So far, volume, speed and permanence have been only indirectly addressed by States and current legal regimes do not contemplate them as independent sources of harm but rather as elements to determine remedies. Openly discussing these issues will allow for a more sincere and productive conversation within the platform governance community although it will bring about the need to reconsider, as Post suggests, some of the fundamentals of freedom of expression (like causality for instance).

58 Good democratic politics, in every single state of the Union, will have to dwell on the extent to which the DSA delivers its double promise of freedom and safety. Otherwise, we expect a healthy degree of pushback, driven—mainly—by concerned citizens and individuals. While premature, we can nevertheless imagine a future where the DSA incorporates obligations for states as well as companies, especially safeguards to prevent abuses from enforcement mechanisms and the specific identification of state actions that contribute to the "systemic risks" that companies are to address. Furthermore, restricting the DSA risks to those proposed within the human rights framework, thus, making it more like the UNGPs, would likely make the whole endeavor more narrow and viable.

98 Del Campo (n 32).

Liability of Online Platforms in Defamation Cases

by **Laura Herrerías Castro** *

Abstract: Online platforms provide an unprecedented space for exercising freedom of expression while simultaneously facilitating the immediate and potentially global spread of defamatory content. At the same time, AI plays a dual role as a generator of risks to individuals' fundamental rights and as an indispensable tool for detecting and preventing illegal content. This article explores the risks to the right to honor arising from the use of online platforms and their increasing reliance on AI, with a threefold aim: to establish the standard of conduct of online platforms in defamation cases, to assess the impact of AI developments on their liability regime, and to identify the remedies available to victims when platforms fail to comply with their due diligence obligations.

Keywords: Defamation, Digital Services Act, Artificial Intelligence, Online Platforms, Due Diligence Obligations

Recommended citation: Laura Herrerías Castro, Liability of Online Platforms in Defamation Cases, 16 (2025) JIPITEC 252 para 1.

A. Introduction

1 Social networks provide users with an unprecedented space to exercise their right to freedom of expression[2]. The US Supreme Court has referred to social media as "the vast democratic forums of the Internet"[3]. However, factors such as the immediate dissemination of content, its accessibility and interactivity, the lack of editorial control, and the permissibility of anonymity increase the risk of users infringing fundamental rights, especially the right to honor.

2 Article 8 of the European Convention on Human Rights (hereinafter ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union (hereinafter CFEU) protect reputation as part of the right to respect for private life. The ECHR does not define "defamation", but under the European Court of Human Rights (hereinafter ECtHR) case law, it is generally a civil wrong committed by an individual against another or others that harms a person's reputation or good name[4].

* Laura Herrerias Castro is a Postdoctoral Researcher at the Faculty of Law of Pompeu Fabra University (Barcelona). This work was supported by the research project "Contractual and non-contractual liability of online platforms", funded by the Spanish Ministry of Economy, Industry and Competitiveness, the European Fund of Regional Development and the Spanish State Research Agency (PID2021-126354OB-I00). The author would like to thank Prof. Antoni Rubí Puig and Prof. Sonia Ramos González for his valuable comments on earlier versions of this article.

2 *Ahmet Yildirim v Turkey* App no 3111/10 (ECtHR, 18 December 2012) para 54.

3 *Packingham v North Carolina* 137 US 1730, 1735 (2017). As laid down in *Moody v NetChoice LLC* 603 US 707 (2024), 'Social-media platforms … structure how we relate to family and friends, as well as to businesses, civic organizations, and governments. The novel services they offer make our lives better and make them worse – create unparalleled opportunities and unprecedented dangers'.

4 T McGonagle, *Freedom of Expression and Defamation: A Study of the Case Law of the European Court of Human Rights* (Council of Europe 2016) 14 <https://rm.coe.int/16806ac95b> accessed 23 June 2025. Similarly, the US *Restatement (Second) of Torts* § 559 provides that 'A communication is defamatory if

3 The EU has neither harmonized substantive law on defamation[5] nor the conflict-of-law rules in that field[6]. Consequently, each court applies the law designated as applicable under its national conflict rules. In Spain, Article 7.7 of the Organic Act 1/1982, of 5 May, on the civil protection of the right to honor, to privacy and to one's own image, defines defamation as "the imputation of facts or the manifestation of value judgements by acts or expressions that infringe in any way the dignity of another person, damaging his fame or impinging on his self-esteem". In a similar vein, Article 29 of the French Law on the Freedom of the Press, of 29 July 1881, defines defamation as "any allegation or imputation of a fact which is prejudicial to the honor or reputation of the person or entity to which the fact is attributed".

4 In *Delfi v Estonia*, the ECtHR noted that defamatory and other types of clearly unlawful speech "can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online"[7]. Facebook's Transparency Report[8] shows that defamation is the main reason for notices submitted in accordance with Article 16 of 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 (hereinafter DSA)[9]. On Google Maps, 99.3% of reported illegal content is for defamation[10], probably due to user reviews and opinions[11].

5 From a regulatory perspective, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter, ECD)[12] established a safe harbor for hosting service providers[13], which has been maintained in the DSA. While some of the principles that inspired the ECD have remained unchanged, the fight against illegal content has led to the adoption of a myriad of sector-specific and horizontal regulatory solutions, increasing platform responsibility. In turn, AI plays a dual role as a generator of new risks and as a tool for detecting and preventing illegal content. To address some of these risks, the EU legislator adopted Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (hereinafter, AIA)[14].

6 This paper explores the risks to the right to honour posed by online platforms and their increasing reliance on IA. It seeks to answer the following research questions: What is the required standard of conduct that online platforms must observe to avoid incurring liability for hosting defamatory content, what influence do developments in AI have on this liability regime, and what remedies are available to victims for platform's infringement of their due diligence obligations.

7 The paper is structured as follows: Section B examines the platform's liability regime under the DSA. Section C explores online platforms' reactive and proactive duties regarding defamatory user-generated content. Finally, Section D analyses the remedies for non-compliance with the due diligence obligations of the DSA.

it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him'.

5 For a comparative analysis on the protection of the right to honor, see H Koziol, A Warzilek. *The protection of personality rights against invasions by mass media*. New York: Springer, 2005.

6 Art 1.2(g) Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40.

7 *Delfi v Estonia* App no 64569/09 (ECtHR [GC], 16 June 2015) para 110. See also *Editorial Board of Pravoye Delo and Shtekel v Ukraine* App no 33014/05 (ECtHR, 5 May 2011) para 63.

8 Regulation (EU) 2022/2065 *Digital Services Act* Transparency Report for Facebook (25 April 2025) <https://transparency.meta.com/reports/regulatory-transparency-reports/> accessed 23 June 2025.

9 OJ L 277, 27 October 2022, 1–102.

10 *EU Digital Services Act (EU DSA) Biannual VLOSE/VLOP Transparency Report* (28 February 2025) <https://transparencyreport.google.com/report-downloads?hl=en> accessed 23 June 2025.

11 The commercial reputational interests of a company could not be equated with the reputation of an individual concerning his or her social status. Whereas the latter might have repercussions on one's dignity, interests of commercial reputation are devoid of that moral dimension. However, States enjoy a margin of appreciation as to the means they provide under domestic law to enable a company to challenge the truth, and limit the damage, of allegations which risk harming its reputation. See P Hirvelä, S Heikkilä *Right to respect for private and family life, home and correspondence*. Cambridge (UK): Instersentia. 2022, 69.

12 OJ L 178, 17 July 2000, 1–16.

13 This framework was inspired by Section 5 of the German *Teledienstegesetz* of 1997 and, especially, by Section 512 of the US Digital Millennium Copyright Act of 1998. See M Peguera Poch The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. *Columbia Journal of Law & the Arts.* 2009, 32(4), 481.

14 OJ L 1689, 12 July 2024.

B. The Safe Harbor for Online Platforms under the DSA

8 The safe harbors for mere conduit, caching and hosting services regulated in Articles 12-14 ECD rested mainly on three factors[15]: the impossibility or excessive cost of monitoring user-generated content, the inequity of imposing liability on mere passive intermediaries, and the prevention of the chilling effects that the risk of liability could have on freedom of expression[16].

9 Nowadays, content moderation is not an ancillary aspect of what online platforms do; it is rather essential and definitional. As Gillespie claims: "Not only can platforms not survive without moderation, they are not platforms without it"[17]. The current best industry practice is to use automatic tools to narrow down the set of contentious content for vetting by human experts (human-in-command principle)[18]. For example, according to TikTok's Community Guidelines: "Content first goes through an automated review process. If content is identified as a potential violation, it will be automatically removed, or flagged for additional review by our moderators"[19]. Nevertheless, as Gillespie points out: "The overwhelming majority of what is being automatically identified are copies of content that have already been reviewed by a human moderator. Stats like these are deliberately misleading, implying that machine learning (ML) techniques are accurately spotting new instances of abhorrent content, not just variants of old ones"[20].

10 There are no neutral platforms, not only because they all moderate content but also because their main and sometimes only source of funding is advertising. For example, in 2024, Meta Platforms, Inc. obtained 98.9% of its net profit from targeted advertising[21]. Recommender systems aim to maximize platform revenue by displaying content tailored to users' interests[22]. Although illegal content may harm a platform's credibility and reputation[23], it often boosts user engagement, increases ad exposure, and ultimately drives more clicks on advertising links[24].

11 Despite the above, the DSA preserves the knowledge-and-take-down principle (Articles 4-6 DSA) as well as the no general monitoring obligation (Article 8 DSA), as both have allowed many novel services to emerge and scale up across the internal market[25]. Besides, some form of conditional immunity is still necessary to prevent collateral censorship[26]. Otherwise, platform operators would have strong incentives to over-censor, limit access or deny users' speech[27]. As Wilman highlights[28]: "The knowledge-based liability model thus aims to strike a middle-way. It avoids the negative consequences of stricter forms of liability that would impact not only the service providers themselves, but also their users[29]. At the same time, it does not completely preclude the possibility for aggrieved parties to have recourse to the service provider concerned where their rights are at stake"[30].

I. Knowledge-and-Take-Down

12 Pursuant to Article 6.1 DSA, hosting service providers

15 *Pursuant to art. 89(2) DSA*: 'References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 4, 5, 6 and 8 of this Regulation, respectively'.

16 L Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' in L Edwards (ed), *Law, Policy and the Internet* (Hart Publishing 2019) 257.

17 T Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media (Yale University Press 2018) 21.

18 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms* COM (2017) 555 final 14.

19 TikTok Community Guidelines <https://www.tiktok.com/community-guidelines/es> accessed 25 June 2025.

20 T Gillespie, 'Content moderation, AI, and the question of scale' (2020) 7(2) *Big Data & Society* 3.

21 Meta, *Meta Reports Fourth Quarter and Full Year 2024 Results* <https://investor.atmeta.com/investor-news/press-release-details/2025/Meta-Reports-Fourth-Quarter-and-Full-Year-2024-Results/> accessed 25 June 2025.

22 Personalized content leads to echo chambers and filter bubbles, see E Pariser *The filter bubble. What the Internet is hiding from you*. London: The Penguin Press, 2011, 9-10.

23 M C Buiten, A de Streel and M Peitz, 'Rethinking liability rules for online hosting platforms' (2020) 28(2) *International Journal of Law and Information Technology* 150.

24 R Griffin, 'The Sanitised Platform' (2022) 13(1) *JIPITEC* 42.

25 Recital 16 DSA.

26 M Husovec, 'Rising above liability: The Digital Services Act as a blueprint for the second generation of global internet rules' (2023) 38(3) *Berkeley Technology Law Journal* 110. See also J Grimmelmann and P Zhang, 'An economic model of online intermediary liability' (2023) 38(3) *Berkeley Technology Law Journal* 1039.

27 JM Balkin, 'Old-school/new-school speech regulation' (2014) 127 *Harvard Law Review* 2309.

28 F Wilman, 'The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act' (2021) 12 *JIPITEC* 323.

29 Cf art 47 *Cybersecurity Law of the People's Republic of China* <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> accessed 25 June 2025.

30 Cf *s 230(c) US Communication Decency Act 1996.*

are exempt from liability for users' content as long as they lack actual knowledge or awareness of the illegality, and, upon obtaining such knowledge or awareness, act expeditiously to remove or restrict access to it. For an online platform to qualify for safe harbor protection, it must also provide its services neutrally, by a merely technical and automatic processing of the information provided by users.

1. Actual Knowledge v. Red Flag Knowledge

13 Under Section 512 (c)(1) of the US Digital Millennium Copyright Act of 1998 (hereinafter DMCA), the difference between actual and red flag knowledge is not between specific and generalized knowledge[31], but instead, between a subjective and an objective standard. The actual knowledge provision turns on whether the provider actually or "subjectively" knew of a specific infringement, while the red flag provision turns on whether the provider was aware of facts that would have made the specific infringement objectively obvious to a reasonable person[32].

14 Similarly, the European Court of Justice (hereinafter CJEU) interprets red flag knowledge as being aware, in one way or another, of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question[33]. The situations covered include those in which the platform operator finds out illegal content as the result of an own-initiative investigation, as well as situations in which the operator is notified of the existence of such content by public authorities, trusted flaggers[34], or users. Under Article 16.3 DSA notices shall be considered to give rise to actual knowledge or awareness in respect of the specific item of information concerned "where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination"[35].

15 Knowledge must be human, i.e. it is not sufficient that an algorithm detects potentially illegal content[36]. In the case of legal entities, the question arises as to when a content moderator's knowledge of illegality can be attributed to the platform operator. As stated by Hofmann, it can be assumed that the platform operator has knowledge or awareness of the illegality when it entrusts its employees with the autonomous management of content[37].

16 Finally, when platforms host manifestly illegal content, the rights and interests of others and society may entitle States to impose liability on online intermediaries without contravening Article 10 ECHR if they fail to take measures to remove it without delay, even without previous notification[38]. Content is considered manifestly illegal where it is evident to a layperson, without any substantive analysis, that is illegal[39]. This would be the case for war crimes, crimes against humanity, incitement to or apology of violence, certain acts of terrorism or child abuse content[40], but not for defamation[41].

31 Recital 22 DSA also establishes that knowledge must be content-specific: "Such actual knowledge or awareness cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content".

32 *Viacom Intern., Inc. v YouTube* (2nd Cir. 2012) 676 F.3d 19. In *Capitol Records, LLC v Vimeo, LLC* (2016) 826 F.3d 78 the US Court of Appeals 2nd Cir. concluded that a copyright owner's showing that a video posted by a user on the service provider's site includes substantially all of a recording of recognisable copyrighted music, and that an employee of the service provider saw at least some part of the user's material, was insufficient to sustain the copyright owner's burden of proving that the service provider had red flag knowledge of the infringement. The US Copyright Office argues that such a narrow interpretation of red flag knowledge minimizes an online platform's duty to act upon information of infringement and, in doing so, protects activities that Congress did not intend to protect. See US Copyright Office. Section 512 of title 17: a report of the register of copyrights (2020) 123 <https://www.copyright.gov/policy/section512/section-512-full-report.pdf> accessed 23 June 2025.

33 *Case C-324/09 L'Oréal and Others v eBay International AG* [2011] ECR I-6011, paras 120–122. See also P Valcke, A Kuczerawy and P-J Ombelet, 'Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common' in M Taddeo and L Floridi (eds), *The Responsibilities of Online Service Providers* (Springer International Publishing 2017) 101.

34 Art 22 DSA.

35 Article 16.3 establishes an irrebuttable presumption of knowledge. See F Raue Article. 16. Notice and action mechanisms. In B Hofmann/F Raue (dirs.). *Digital Services Act: Article-by-article commentary*. Baden-Baden: Nomos. 2024, 337.

36 P Van Eecke, 'Online service providers and liability: A plea for a balanced approach' (2011) 48 *Common Market Law Review* 1475.

37 B Hofmann, 'Article 6. Hosting' in B Hofmann and F Raue (eds), *Digital Services Act: Article-by-Article Commentary*(Nomos 2024) 170.

38 *Delfi* (n 7) para 159.

39 Recital 63 DSA.

40 G Frosio and C Geiger, 'Taking fundamental rights seriously in the Digital Services Act's platform liability regime' (2023) 29 *European Law Journal* 64.

41 *Magyar Tartalomszolgáltatók Egyesülete* (MTE) *and Index.hu Zrt v Hungary* no 22947/13 (ECtHR, 2 February 2016) para 64.

2. Expeditious Reaction

17 The DSA does not include any time limit for removing or disabling access to illegal content[42]. Regarding the treatment of notifications, Recital 52 DSA merely states that: "Providers of hosting services should act upon notices in a timely manner, in particular by taking into account the type of illegal content being notified and the urgency of taking action"; and Recital 89 DSA that: "Other types of illegal content may require longer or shorter timelines for processing of notices, which will depend on the facts, circumstances and types of illegal content at hand".

18 Facebook's Transparency Report shows that the average time needed to take action on reported content is 13.2 hours, while Instagram's is 18.4 hours[43]. Both reports warn that more complex decisions, such as defamation or harassment, may require more time or additional guidance from specialised staff.

19 In conclusion, the expeditious reaction of platforms should be assessed on a case-by-case basis depending on factors such as[44]: the type of illegality, the volume of hosted content, the number, accuracy and source of notifications, as well as the availability of content moderation mechanisms.

3. Neutrality Test

20 Recital 18 DSA sets forth that: "The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information"[45].

21 As Peguera Poch points out the test consisting of whether the activity gives the provider knowledge of or control over the hosted information seems ill-suited because platforms usually have some basic form of control over the information they host. Furthermore, it is at odds with the fact that under the hosting safe harbor, a provider is only supposed to lose protection when it obtains knowledge regarding the illegal nature of specific content and fails to expeditiously remove or block access to it[46].

22 The neutrality test should be interpreted narrowly so that a platform cannot benefit from the safe harbor if it knowingly participates or collaborates in the dissemination of illegal content or if it has editorial control over it[47]. Nonetheless, when editorial control is fully automated or AI is used to validate content before publication, platforms should be considered "neutral" in terms of Recital 18 DSA, as the activity consists of a "purely technical and automatic processing of information".

II. No General Monitoring Obligation

23 Article 8 DSA, in very similar terms to Article 15.1 ECD, reads as follows: "No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers"[48]. The prohibition of general monitoring does not affect the possibility for judicial or administrative authorities to require the service provider to terminate or prevent specific infringements[49], even where platform operators

42 During the parliamentary debate on the DSA proposal, the Committee on legal affairs (Rapporteur: Geoffrey Didier) proposed to add to Article 6.1 the following paragraph (amendment 111): "1a. Without prejudice to specific deadlines, set out in Union law or within administrative or legal orders, providers of hosting services shall, upon obtaining actual knowledge or awareness, remove or disable access to illegal content as soon as possible and in any event: (a) within 30 minutes where the illegal content pertains to the broadcast of a live sports or entertainment event; (b) within 24 hours where the illegal content can seriously harm public policy, public security or public health or seriously harm consumers' health or safety; (c) within 72 hours in all other cases where the illegal content does not seriously harm public policy, public security, public health or consumers' health or safety" <https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html> accessed 23 June 2025.

43 None of the reports detail the reaction time according to the type of illegal content, nor do they include information on standard deviation.

44 J Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 408.

45 See also *Joined Cases C-236/08, C-237/08 and C-238/08 Google France* (CJEU 23 March 2010) paras 116–119; *Case C-324/09 L'Oréal and others* (n 33) paras 115–116; *Joined Cases C-682/18 and C-683/18 YouTube and Cyando* (CJEU 22 July 2021) paras 107–109.

46 M Peguera Poch, 'The Platform Neutrality Conundrum and the Digital Services Act' (2022) 53 *International Review of Intellectual Property and Competition Law* 683.

47 Art 6(2) and recitals 18 and 20 DSA.

48 For a thorough analysis of the CJEU's interpretation of general monitoring prohibition see T H Oruç, The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it? *JIPITEC*, 2022, 13(3), 179-190.

49 Art 9 DSA.

meet the conditions set out in Article 6.1 DSA[50].

24 The distinction between general and specific obligations has been developed in the case law of the CJEU. In *L'Oréal and others*, the CJEU resolved whether it is possible to issue an injunction requiring a website operator to prevent future infringements of intellectual property rights. The CJEU responded that injunctions cannot consist of active monitoring of all users' data, but accepted injunctions to prevent further infringements by the same user in respect of the same trademarks[51]. In *Tommy Hilfiger Licensing and others,* the CJEU insisted on the idea that: "The intermediary may be forced to take measures which contribute to avoiding new infringements of the same nature by the same market-trader from taking place"[52]. Thus, an injunction that meets this double identity requirement - same subject and same object - does not entail a general monitoring obligation.

25 Subsequently, in *Scarlet Extended* and *SABAM*, the CJEU concluded that an injunction for preventing copyright infringements requiring an online intermediary to install a system for filtering all information stored on its servers, exclusively at its expense and for an unlimited period of time would be contrary to Article 15.1 ECD[53]. The CJEU emphasized that a fair balance must be struck between the fundamental rights protected by the CFEU[54]. A filtering system of this type that seeks to protect intellectual property rights (Article 17.2 CFEU) does not respect the principle of proportionality insofar as it implies, on the one hand, a substantial infringement of the intermediary's freedom to conduct business (Article 16 CFEU); and, on the other hand, it would significantly affect the right to the protection of personal data of users (Article 8 CFEU) and their right to freedom of expression (Article 11 CFEU) due to the risk that the system would not adequately distinguish between lawful and unlawful content[55].

26 Finally, in *Glawischnig-Piesczek* the CJEU stated that it is not contrary to Article 15.1 ECD an injunction ordering a social network to remove information the content of which is identical or equivalent to information which was previously declared to be defamatory, or to block access to that information, irrespective of who the author is. Such an injunction would not entail a disproportionate impact on the right to freedom to conduct a business, as: "The monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies"[56].

27 The CJEU seems to ignore that human communication is culturally sensitive and that it is highly complex at a technical level to capture the context of a publication. Identical content can have different meanings; for example, swear words or insults can be harmless when addressed to a close person[57]. Despite progress in IA, automatic moderation systems cannot reliably distinguish between defamation and its critique, news coverage or satire[58].

28 As for equivalent content, AG Szpunar warned that: "A reproduction of the information that was characterized as illegal containing a typographical error and a reproduction having slightly altered syntax or punctuation constitutes equivalent information. It is not clear, however, that the equivalence referred to in the second question does not go further than such cases"[59]. AG Szpunar's concerns were ultimately confirmed when the CJEU concluded that: "Injunction[s] must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal"[60], provided

50 Art 6(4) and recital 25 DSA.

51 *L'Oréal and others* (n 33) paras 139-141.

52 Case C-494/15 *Tommy Hilfiger Licensing and Others v Delta Center* (CJUE, 7 July 2016) para 34.

53 Case C-360/10 *SABAM* (CJUE, 16 February 2012) para 38; Case C-70/10 *Scarlet Extended* (CJUE, 24 November 2011) para 40.

54 GC Case C-275/06 *Promusicae* (CJUE, 29 January 2008) para 68.

55 *SABAM* (n 53) paras 46–50; *Scarlet Extended* (n 53) paras 48–53. On the compatibility of arts 11, 16 and 17(2) CFEU with injunctions to prevent copyright infringements see also Case C-314/12 *UPC Telekabel Wien* (CJEU, 27 March 2014) and Case C-484/14 *Mc Fadden* (CJEU, 15 September 2016).

56 Case C-18/18 *Glawischnig-Piesczek* (CJEU, 3 October 2019) para 46.

57 T Dias Oliva, D M Antonialli, A Gomes, Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online. *Sexuality & Culture*, 2021, 25, 706 ("In-group/out-group status may help create contextual conditions that predispose particular experiences of language. A word that is experienced as a slur when hurled by an outsider can be experienced as a joke when used by an in-group member. LGBTQ people reclaim slurs by using them within the community. A word that might normally convey malice here conveys solidarity").

58 D Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69(6) *GRUR International* 618; J Daskal and K Klonick, 'When a Politician Is Called a "Lousy Traitor," Should Facebook Censor It?' (*The New York Times* 27 June 2019) <https://www.nytimes.com/2019/06/27/opinion/facebook-censorship-speech-law.html> accessed 23 June 2025.

59 *Glawischnig-Piesczek* (n 56) Opinion of AG Szpunar para 67.

60 *Glawischnig-Piesczek* (n 56) para 41.

that injunctions contain specific elements, such as the name of the victim, the circumstances in which the infringement was determined and equivalent content to that which was declared to be illegal, "so that the hosting provider concerned is not required to carry out an independent assessment of that content"[61].

29 The problem, again, is that detecting equivalent content requires considering the actual meaning of the publication at issue, and in most cases, it is impossible to do without human oversight[62]. As AG Saugmandsgaard Øe points out: "Although intermediary providers are technically well placed to combat the presence of certain illegal information disseminated through their services, they cannot be expected to make 'independent assessments' of the lawfulness of the information in question. Those intermediary providers do not generally have the necessary expertise and, above all, the necessary independence to do so – particularly when they face the threat of heavy liability. They cannot therefore be turned into judges of online legality, who are responsible for coming to decisions on legally complex questions"[63].

30 The CJEU suggests using algorithmic content moderation systems to avoid making an independent assessment of the lawfulness. Nevertheless, as discussed in the next section, such mechanisms are prone to false positives and false negatives.

C. The Standard of Conduct of Online Platforms in Defamation Cases

I. Required Standard of Conduct

31 The required standard of conduct is that of a reasonable (legal) person in the circumstances of the case[64]. Assessing the defendant's conduct involves considering legal provisions, as well as the custom or best practices of the relevant economic sector, which may be reflected in the corresponding codes of conduct[65]. In the absence of the above, negligence should be established by balancing the expected risk, on one hand, and the cost of precautionary measures, on the other[66].

32 Under Article 4:102 (1) PETL, the required standard of conduct depends, among other factors, on the nature and value of the protected interest involved, the foreseeability of the damage, as well as the availability and the costs of precautionary or alternative methods[67]. Likewise, the US Restatement Third, Torts: Liability for Physical and Emotional Harm § 3 states that the principal factors to consider in ascertaining whether a person's conduct lacks reasonable care are: the foreseeable likelihood that the person's conduct will result in harm, the foreseeable severity of any harm that may ensue, and the burden of precautions to eliminate or reduce the risk of harm.

33 This approach has its origins in the reasoning of Judge Learned Hand in *United States v Carroll Towing Co*[68]. Following Hand's liability formula for negligence, a potential injurer is negligent if and only if B < PL, where B is the burden of taking precautions, P is the probability of loss, and L is the gravity of loss. The balancing approach rests on and expresses a simple idea: conduct is negligent if its disadvantages outweigh its advantages. In other words, the actor's conduct is negligent if the magnitude of the risk outweighs the burden of risk prevention[69].

1. Risk of Harm

34 The foreseeability of disseminating illegal content depends on the type and popularity of platforms.

61 ibid para 45. See also Case C-401/19 *Poland v Parliament and Council* (CJEU 26 April 2022) para 90 'The providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright'.

62 E Rosati, 'Material, personal and geographic scope of online intermediaries' removal obligations beyond *Glawischnig-Piesczek* (C-18/18) and defamation' (2019) 41(11) *European Intellectual Property Review* 676.

63 *Poland* (n 61) Opinion of AG Saugmandsgaard Øe para 197. See also A/HRC/38/35 para 17 'Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic'.

64 Art 4:102(1) *Principles of European Tort Law* (PETL); Art VI – 3:102 *Draft Common Frame of Reference*.

65 There is currently no code of conduct for combating online defamation. On disinformation see Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065 (OJ C, C/2024/3014, 26.4.2024).

66 C van Dam, *European Tort Law* (2nd edn, Oxford University Press 2013) 236.

67 P Widmer, 'Art 4:102 Required standard of conduct' in European Group on Tort Law, *Principles of European Tort Law: Text and Commentary* (Springer 2007) 75–79.

68 159 F2d 169 (2nd Cir 1947).

69 American Law Institute, *Restatement Third, Torts: Liability for Physical and Emotional Harm* (2010) comment e 30.

As outlined in the introduction to this paper, defamation is one of the main reasons for users' complaints under Article 16 DSA. The permissibility of anonymity is also relevant, as it facilitates wrong by eliminating accountability[70]. As Citron notes: 'Online, bigots can aggregate their efforts even when they have insufficient numbers in any one location to form a conventional hate group. They can disaggregate their offline identities from their online presence, escaping social opprobrium and legal liability for destructive acts. Both of these qualities are crucial to the growth of anonymous online mobs'[71].

35 Platform operators are aware that users sometimes post illegal content. Nonetheless, foreseeability cannot be assessed in abstract terms; it must be evaluated in relation to whether the party who caused the harm could have reasonably foreseen the specific outcome of their conduct. Platform operators should be held liable only when they have actual knowledge or become aware of a specific illegal content, as it is not foreseeable in advance that one of their millions of users would commit a specific infringement.

36 In terms of the severity of harm, Article 2.102 (2) PETL sets forth that: 'Life, bodily or mental integrity, human dignity and liberty enjoy the most extensive protection'. The right to honour derives from human dignity, aiming to preserve both the feeling that a person has of their qualities (subjective honour) and reputation (objective honour)[72].

37 Online defamation usually causes non-pecuniary losses. In general, these losses are recoverable only when the infringement of the protected interest causes substantial harm to the victim's emotional well-being[73]. Nonetheless, Article 9.3 of the Spanish Organic Act 1/1982 establishes an irrebuttable presumption of non-pecuniary damages. This presumption is justified both on the grounds of the difficulty of the proof as well as in the fact that the specific nature of the protected interests that have been infringed permits the reasonable presumption that a non-pecuniary loss has taken place[74].

70 *McIntyre v Ohio Elections Com'n*, 514 US 334 (1995) 1537.

71 DK Citron, 'Cyber Civil Rights' (2009) 89 *Boston University Law Review* 64.

72 A De Cupis, *I diritti della personalità* (2nd edn Giuffrè Editore 1982) 251–252.

73 C von Bar, *The Common European Law of Torts*, vol II (Clarendon Press 2000) 20.

74 M Martín-Casals and J Solé Feliu, 'The protection of personality rights against invasions by mass media in Spain' in H Koziol and A Warzilek (eds), *The Protection of Personality Rights Against Invasions by Mass Media* (Springer 2005) 329.

2. Benefits of the Conduct

38 The benefits of the conduct should be assessed by considering both the interests of platforms and users. On the one hand, online platforms enjoy the right to freedom to conduct a business as provided for in Article 16 CFEU. This right encompasses the freedom for any platform to use, within the limits of liability for its own acts, the economic, technical and financial resources available to it. Additionally, platforms benefit from the freedom to impart information as guaranteed by Articles 11 CFEU and 10 ECHR.

39 To resolve the question of whether the domestic courts' decisions holding an online intermediary liable for defamatory comments were in breach of its freedom of expression, the ECtHR identified the following aspects as relevant for its analysis: a) the context and content of comments, b) the measures taken by the intermediary to prevent or remove the comments, c) the liability of the actual authors of the comments as an alternative to the intermediary's liability, d) the prior conduct of the injured party, e) the consequences of the domestic proceedings for the intermediary, and f) the consequences of the comments for the injured party[75].

40 Based on these criteria, in *Delfi v Estonia* the ECtHR held that it had been justified to order a news portal to pay damages (approximately 320€) for anonymous comments posted on its site, given its failure to take measures to remove clearly illegal comments, which amounted to hate speech or incitements to violence, without delay[76]. In contrast, in *MTE and Index.hu Zrt v Hungary*, the ECtHR found that strict liability of news portals for defamatory comments was incompatible with Article 10 ECHR. It held that there was no reason to state that, accompanied by effective procedures allowing for rapid response, the notice-and-take-down system had not functioned as an appropriate tool for protecting commercial reputation[77].

41 On the other hand, users have the right to freedom of expression, which applies not only to information or ideas that are favorably received but also to those that offend, shock or disturb[78]. For Article 8 ECHR to come into play, the attack on a person's reputation must attain a certain level of seriousness, in a manner causing prejudice to personal enjoyment

75 *Delfi* (n 7) para 142; *MTE* (n 41) paras 72–88; *Høiness v Norway* no 43624/14 (ECtHR, 19 March 2019) para 67; *Jezior v Poland* no 31955/11 (ECtHR, 4 June 2020) para 53; *Sanchez v France* no 45581/15 (ECtHR [GC], 15 May 2023) para 167.

76 *Delfi* (n 7) para 159.

77 *MTE* (n 41) para 91.

78 *Handyside v United Kingdom* no 5493/72 (ECtHR, 7 December 1976) para 49.

of the right to respect for private life[79]. Despite millions of users posting content online every day[80], many of those comments are likely to be too trivial for them to cause any significant damage to another person's reputation[81]. In this sense, in *MTE and Index.hu Zrt v Hungary* the ECtHR indicated that: 'Without losing sight of the effects of defamation on the Internet, especially given the ease, scope and speed of the dissemination of information (...) regard must be had to the specificities of the style of communication on certain Internet portals. For the Court, the expressions used in the comments, albeit belonging to a low register of style, are common in communication on many Internet portals - a consideration that reduces the impact that can be attributed to those expressions'[82].

3. Cost of Precautionary Measures

42 Article 16 DSA addresses one of the gaps in the ECD by obligating hosting service providers to establish notice and take-down mechanisms[83]. These mechanisms must be easy to access and user-friendly and must allow for the submission of notices exclusively by electronic means. Additionally, they should facilitate the submission of notices that are sufficiently precise and adequately substantiated[84].

43 In defamation cases, before notification the costs of detection and removal usually exceed the expected harm due to the limited information that the platform has about the truthfulness of the information. In contrast, the receipt of a notification that complies with the requirements mentioned in Article 16.2 DSA considerably reduces the burden on the platform operator. Therefore, the standard of conduct expected from platforms depends, to a large extent, on the diligence previously exercised by the victim[85].

44 Platforms generally have teams of reviewers and algorithmic content moderation systems to fight against illegal content. For example, according to the Facebook and Instagram Transparency Reports, Meta has a team of 212 moderators that review content in English[86]. Even if platforms have sufficient content reviewers who understand the language, cultural, political and social context of the publications, incorrect decisions cannot be ruled out, as non-lawyers must decide in just a few seconds whether a message is likely to harm a person's dignity in a given country.

45 Investing in the development of algorithmic content moderation systems is costly, so it is a viable option only for large platforms[87]. Requiring the same level of diligence from SMEs as from Big Tech companies would stifle market participation and free competition, making it extremely difficult for new businesses to enter or forcing out those that cannot afford the costs. For this reason, the additional obligations imposed under the DSA on providers of online platforms do not apply to providers that qualify as micro or small enterprises[88].

46 Hiring third-party services to carry out content moderation tasks is possible, but many of these services are not designed to detect defamatory content, and the few that can detect text toxicity have a high error rate. For example, Perspective - a free API developed by Jigsaw and Google - automatically evaluates messages and ranks them according to attributes such as toxicity, severe toxicity, identity attack, insult, profanity and threat.

79 *Axel Springer AG v Germany* no 47940/99 (ECtHR [GC], 7 February 2012) para 83.

80 DOMO, 'Data Never Sleeps 12.0' (2024) <https://www.domo.com/learn/infographic/data-never-sleeps-12> accessed 23 June 2025.

81 *Tamiz v United Kingdom* no 3877/14 (ECtHR, 19 September 2017) para 80; Çakmak *v Turkey* no 45016/18 (ECtHR, 7 September 2019) para 50.

82 *MTE* (n 41) para 77.

83 Art 14(3) and art 21(2) Directive 2000/31/EC on Electronic Commerce (ECD).

84 Recital 50 DSA; P Wolters and R Gellert, 'Towards a better notice and action mechanism in the DSA' (2023) 14(3) *JIPITEC* 413–418.

85 M Husovec, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which Is Superior? And Why?' (2018) 42 *Columbia Journal of Law & the Arts* 66.

86 Content moderators by official EU language for Facebook and Instagram combined: Bulgarian (55), Croatian (56), Czech (63), Danish (39), Dutch (154), Estonian (6), Finnish (24), French (630), German (470), Greek (37), Hungarian (44), Irish (0), Italian (427), Latvian (4), Lithuanian (11), Maltese (1), Polish (112), Portuguese (2088), Romanian (74), Slovak (49), Slovenian (8), Spanish (3110), Swedish (78). For languages widely spoken outside the EU (French, English, Spanish and Portuguese) there are additional reviewers for reports from non-EU countries. *Regulation (EU) 2022/2065 Digital Services Act* Transparency Report for Facebook (25 April 2025) <https://transparency.meta.com/reports/regulatory-transparency-reports/> accessed 23 June 2025.

87 Buiten, de Streel and Peitz (n 23) 153 ("Large platforms may be able to save on costs of detection, monitoring and removal because of economies of scale. It may pay off for large hosting platforms to invest in developing or acquiring software tools to identify and filter out illegal content. Large hosting platforms can spread the high fixed costs of such software tools over all instances of illegal material (...). Investments in advanced software tools might not pay off for smaller platforms, forcing them to do more detection and monitoring work manually, at higher costs and often with less precision per instance of illegal material").

88 Arts 19 and 29 DSA.

However, Hosseini *et al*. showed that the system has a high false negative rate, as it is relatively easy to deceive[89]. The developers of Perspective themselves have admitted its fallibility: "Our models are not perfect and will make errors. It will be unable to detect patterns of toxicity it has not seen before, and it may incorrectly detect toxicity in healthy comments that contain patterns similar to previous toxic conversations. Because of this, Perspective is not intended for use cases such as fully automated moderation"[90].

47 In summary, a diligent economic operator should not be required to conduct *ex ante* or proactive control of defamatory content. Such an obligation would not only contradict Article 8 DSA - interpreted in light of Recital 30 DSA -, but also would not respect the principle of proportionality, because platforms do not have the technical and human resources necessary to proactively identify and remove defamatory content with a sufficient level of accuracy.

48 A different question is whether, given the current state of the art, online platforms can be subjected to notice-and-stay-down obligations to prevent the reappearance of previously notified defamatory content.

II. Content Moderation Mechanisms for Preventing Defamatory Content

49 Online platforms generally employ two automated techniques for content moderation: matching systems and predictive systems[91]. The former checks if a piece of content is identical to another previously identified as defamatory, while the latter predicts the likelihood that previously unseen content is defamatory.

1. Matching Systems

a.) Word Filters

50 Word filters compare words or expressions against a database to prevent, block or remove undesired text. Most social networks allow users to personalize blacklists. For instance, Facebook lets users choose up to 1.000 keywords in any language to block from comments on their profiles[92]. Many of these platforms also have their own blacklists. Still, the functioning of these filters is opaque, as no platform provides a definition or examples of what it considers offensive or inappropriate.

51 In *Alone in the Dark*, the German Federal Court of Justice concluded that it was technically and economically reasonable for an online intermediary to use word filters to prevent copyright infringements[93]. The Frankfurt Regional Court reached the same conclusion in a reputation protection case[94]. Nonetheless, word filters have important limitations. Firstly because of the lack of exhaustiveness of all words or combinations of words that may constitute a defamatory comment. Secondly, users can easily circumvent the system by introducing small modifications to the text[95]. Thirdly, filters do not consider context, and therefore generate a high rate of false positives. For example, YouTube deleted several accounts of well-known YouTubers due to a filter error when it interpreted the acronym "CP" as referring to "child pornography" when it meant "combat points" concerning the Pokemon GO video game[96].

b.) Hashing

89 H Hosseini, S Kannan, B Zhang and others, 'Deceiving Google's Perspective API Built for Detecting Toxic Comments' (2017) 2–3 <https://arxiv.org/abs/1702.08138> accessed 23 June 2025.

90 'Perspective FAQs' <https://developers.perspectiveapi.com/s/about-the-api-faqs?language=en_US> accessed 23 June 2025.

91 N Chowdhury, 'Automated Content Moderation: A Primer' (2022) 2 <https://cyber.fsi.stanford.edu/news/automated-content-moderation-primer> accessed 23 June 2025.

92 See <https://www.facebook.com/help/131671940241729> accessed 23 June 2025.

93 BGH 12 July 2012 I ZR 18/11 paras 33–35 'Die Eignung eines Wortfilters mit manueller Nachkontrolle für die Erkennung von Urheberrechtsverletzungen wird nicht dadurch beseitigt, dass er mögliche Verletzungshandlungen nicht vollständig erfassen kann'.

94 Landgericht Frankfurt am Main 14 December 2022 no 2-03 O 325/22 ECLI:DE:LGFFM:2022:1214.2.03O325.22.00 para 3 'Die Kammer kann angesichts dessen nicht erkennen, warum diese Identifizierung der rechtsverletzenden Tweets für die Antragsgegnerin technisch und wirtschaftlich, beispielsweise anhand der von der Antragstellerseite vorgeschlagenen Stichworte, unzumutbar sein sollte'.

95 E Llansó, 'No amount of AI in content moderation will solve filtering's prior restraint problem' (2020) 7(1) *Big Data & Society* 2.

96 T Gerken, 'YouTube backtracks after Pokemon child abuse ban' (*BBC* 18 February 2019) <https://www.bbc.com/news/technology-47278362> accessed 23 June 2025.

52 A hash value is an alphanumeric string that serves to identify an individual digital file as a kind of digital fingerprint[97]. Hashing consists of two phases: the generation and storage of the hash in a database, and the comparison of hashes for matches. For example, to prevent the reappearance of a meme, the algorithm must transform the image (meme.jpg) into a hash (a996be1eb1e210958219e0bb015d5420) and record that value in a database. Identical files have the same hash so if a user tries to post a copy of the meme, the system will prevent it.

53 Hashing can be cryptographic or perceptual. The advantages of cryptographic hashing are that it requires little data storage capacity, does not involve a large investment as open-source solutions are available, it is relatively easy to implement, and can accurately identify exact duplicates of a digital file[98]. However, one of its major disadvantages is its lack of robustness[99], since even the slightest manipulation results in a completely different hash[100].

54 In contrast, perceptual hashing does not attempt to determine whether two files are identical but whether they are sufficiently similar[101]. In the case of images, perceptual hashing extracts a fingerprint based on certain characteristics that resist possible modifications such as compression, color changes, rotation, the addition of text, or any other that does not fundamentally change the underlying content but alters the pixel values[102]. For example, in 2007, YouTube launched Content ID to identify matches of copyright-protected content[103]; in 2009, Microsoft Corporation developed PhotoDNA to prevent the dissemination of known child exploitation material[104]; and in 2017, the Global Internet Forum to Counter Terrorism created a hash-sharing database of terrorist and violent extremist content[105].

55 The judgement of 8 April 2022 of the Frankfurt Regional Court held that Facebook was liable for disseminating a defamatory meme because it did not take reasonable measures to prevent further identical or similar infringements. For the Frankfurt Regional Court, it was decisive that Facebook could have prevented them by using hashing[106]. However, like word filters, hashing is also prone to false positives, given the difficulties of discerning the publication context.

2. Predictive Systems

a.) Data Collection and Classification

56 For a system to predict the probability that content is illegal it must be trained with numerous examples to identify common characteristics. Each piece of training data is called "document", and a compilation of documents is called "corpus"[107].

57 Training data can be obtained through manual searches or from pre-existing databases. For example, the Hate Speech Dataset Catalogue includes open datasets for hate speech, online abuse, and offensive language[108]. Likewise, the Offensive Language Identification Dataset consists of an open corpus

97 *United States v Wellman* 663 F3d 224 (4th Cir 2011). See also E Engstrom and N Feamster, 'The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools' (2017) 12–13 <https://www.engine.is/the-limits-of-filtering> accessed 23 June 2025.

98 European Union Intellectual Property Office, *Automated Content Recognition: Discussion Paper – Phase 1 Existing Technologies and Their Impact on IP* (2020) 8–9.

99 R Gorwa, R Binns and C Katzenbach, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) 7(1) *Big Data & Society* 4.

100 This can be verified through the following link: <https://www.md5.cz> accessed 23 June 2025.

101 C Shenkman, D Thakur and E Llansó, 'Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis' (Centre for Democracy & Technology 2021) 39 <https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/> accessed 23 June 2025.

102 H Farid, 'An Overview of Perceptual Hashing' (2021) 1(1) *Journal of Online Trust and Safety* 5.

103 'How Content ID works' <https://support.google.com/youtube/answer/2797370?hl=en-GB&sjid=14937822664490622239-EU> accessed 23 June 2025.

104 Microsoft, 'PhotoDNA' <https://www.microsoft.com/en-us/photodna> accessed 23 June 2025.

105 GIFCT, 'Hash-Sharing Database' <https://gifct.org/hsdb/> accessed 23 June 2025.

106 Landgericht Frankfurt am Main 8 April 2022 no 2-03 O 188/21 ECLI:DE:LGFFM:2022:0408.2.03O188.21.00 para 3 'Es ist zwischen den Parteien unstreitig, dass zum Ausgangspost identische Bilder über den Vergleich der Hashwerte automatisiert identifiziert werden können (...) Es ist zwischen den Parteien ebenfalls unstreitig, dass es technische Möglichkeiten gibt, nicht nur fast identische, sondern sogar ähnliche Bilder zu erkennen, indem man Abstriche hinsichtlich des Grads der Übereinstimmung beim Hashwert macht und die so gefundenen Kandidaten mittels PDNA und OCR überprüft'. The judgment of 25 January 2024 of the Frankfurt Court of Appeals (16 U 65/22) upheld the judgment of first instance.

107 A Stefanowitsch, Corpus Linguistics: A Guide to the Methodology (Language Science Press 2020) 22.

108 'Hatespeechdata' <https://hatespeechdata.com/> accessed 23 June 2025. The dataset is maintained by Leon Derczynski, Bertie Vidgen, Hannah Rose Kirk, Pica Johansson, Yi-Ling Chung, Mads Guldborg Kjeldgaard Kongsbak, Laila Sprejer and Philine Zeinert.

of 14200 English language documents on offensive language[109]. Both databases are useful for training a natural language processing (hereinafter NLP) system to detect this type of language. However, a tool developed using datasets in English may not function well when used to moderate speech in other languages[110].

58 Once the initial corpus has been compiled, crowdsourcing services are usually hired to classify or annotate the documents. Each document is often analyzed by 3-5 people and only those that pass a minimum threshold of consensus among the classifiers are incorporated into the final corpus. In order to correctly classify documents, it is essential to establish a clear, simple and consistent definition of what constitutes illegal content[111]. The problem arises from the lack of a universal definition of "defamation". Attempting to simplify it may result in misclassifying messages whose illegality requires a more complex analysis, which can vary from country to country. Additionally, definitions with subjective components pose a risk of introducing bias[112], as well as under-representation of language or expressions used by or against certain groups of people[113]. As Llansó *et al*. note: "If these datasets do not include examples of speech in different languages and from different groups or communities, the resulting tools will not be equipped to parse these groups' communication"[114].

59 To address these challenges, the Council of Europe recommends evaluating and testing algorithmic systems with sufficiently diverse and representative sample populations, without drawing on or discriminating against any particular demographic group[115]. Regarding high-risk AI systems, Article 10.3 AIA states that: "Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose", and Article 10.4 that: "Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used". Nevertheless, AI systems used for content moderation are, in principle, not high-risk systems and therefore do not fall under Chapter III of the AIA.

b.) Pre-Processing of Data

60 After collection and classification, the next step is pre-processing data through NLP. Pre-processing involves preparing and reducing all data to facilitate its computational representation. This process includes various methods such as tokenization[116], removing stop words[117], punctuation marks or special characters, and transforming symbols into words.

61 Next, it is necessary to extract a numerical representation of the corpus using vector representation models, such as Bag of Words (hereinafter BoW). BoW involves creating a vocabulary of all the words in the corpus and then generating a matrix where each row represents a document, and each column represents a word from the corpus. The matrix values indicate the frequency or importance of that word in the corresponding

109 'OLID' <https://sites.google.com/site/offensevalsharedtask/olid> accessed 23 June 2025. The dataset was created by Marcos Zampieri, Shervin Malmasi, Preslav Nakov, Sara Rosenthal, Noura Farra and Ritesh Kumar; M Zampieri, S Malmasi, P Nakov and others, 'Predicting the Type and Target of Offensive Posts in Social Media' in *Proceedings of NAACL-HLT 2019* 1415–1420.

110 A Marsoof, A Luco and H Tan, 'Content-filtering AI systems – limitations, challenges and regulatory approaches' (2023) 32(1) *Information & Communications Technology Law* 78.

111 M Barral Martínez, 'Platform regulation, content moderation, and AI-based filtering tools: some reflections from the European Union' (2023) 14(1) *JIPITEC* 216.

112 A Balayn, J Yang and Z Szlavik, 'Automatic Identification of Harmful, Aggressive, Abusive, and Offensive Language on the Web: A Survey of Technical Biases Informed by Psychology Literature' (2021) 4(3) *ACM Transactions on Social Computing* 26; R Binns, M Veale and M van Kleek, 'Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation' in GL Ciampaglia, A Mashhadi and T Yasseri (eds), *Social Informatics: 9th International Conference, SocInfo 2017 (Part II)* (Springer 2017) 411–12.

113 A Díaz and L Hecht-Felella, 'Double Standards in Social Media Content Moderation' (2021) 11 <https://www.brennancenter.org/es/node/9225> accessed 23 June 2025; N Duarte, E Llansó and A Loup, 'Mixed Messages? The Limits of Automated Social Media Content Analysis' (Center for Democracy & Technology 2017) 16 <https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/> accessed 23 June 2025.

114 E Llansó, J van Hoboken, P Leerssen *et al*, 'Artificial Intelligence, Content Moderation, and Freedom of Expression' (Transatlantic Working Group 2020) 8 <https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf> accessed 3 March 2025.

115 Committee of Ministers, 'Recommendation CM/Rec(2020)1 to member States on the human rights impacts of algorithmic systems' (adopted 8 April 2020 at the 1373rd meeting of the Ministers' Deputies) C.3.2.

116 A token is a contiguous sequence of characters with a semantic meaning. See Aggarwal, C.C. *Machine Learning for Text*. New York: Springer, 2022, 21.

117 Common prepositions, conjunctions, pronouns, and articles are considered stop words.

document[118]. This allows the system to detect the words that appear most frequently in defamatory messages and predict new ones. Nonetheless, a significant limitation of BoW is that it does not consider the order of words or their relationship to the rest of the document. Words that may be offensive in isolation can have a harmless meaning when combined with other words in the document.

62 Using neural networks to represent words as numerical vectors in a multidimensional space is also possible. Methods such as word embedding capture the semantic information of words, so similar terms, related terms or terms with the same connotation are placed close together in the vector space[119]. Word embedding also has its limitations, as it reproduces implicit biases in the corpus[120]. Bolukbasi *et al.* demonstrated that word embedding reproduces gender stereotypes by associating professions such as architect, economist, philosopher, computer programmer, pilot or captain with men, and housewife, nurse, receptionist, librarian, hairdresser or nanny with women[121]. Likewise, Caliskan *et al.* found that the concepts most associated with men include areas such as technology, engineering, religion and sports; while the concepts most associated with women include areas such as beauty, cooking, fashion and luxury[122].

c.) System Training

63 Algorithmic content moderation systems are generally trained through supervised learning, meaning that the system learns from labelled data to generalize or infer their common characteristics to classify new content. To train a system to predict defamatory content, the nodes of the artificial neural network can consider factors such as whether a message contains insults, comes from an anonymous user, or is directed at a specific person. Each parameter is assigned a weight based on its importance, with a higher weight indicating a more significant influence on the final result. When a node receives a value through its input connections, it multiplies it by the weight associated with each variable. If the result exceeds a certain threshold, the information passes through the output connections until it reaches the final layer, where the system provides its ultimate prediction.

64 Nonetheless, artificial neural networks do not offer explanations for their outputs, a phenomenon known as the black box problem[123]. As Burrell points out: "When a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension. Machine optimizations based on training data do not naturally accord with human semantic explanations"[124]. Understanding how the algorithm interacts with the learning environment to get the final prediction, even when the input variables are known, is extremely complex[125]. Moreover, decision-making is obscured by a code typically protected by intellectual property rights[126].

d.) Evaluation

65 The final step before implementing a prediction system is its evaluation. Classification errors can lead to false positives, i.e. identifying content that is lawful as unlawful[127], and false negatives, i.e., identifying as lawful content that is unlawful. False positives lead to over-blocking, while false negatives lead to under-blocking[128].

118 J Eisenstein, Introduction to Natural Language Processing (MIT Press 2019) 13–16.

119 D Jurafsky and JH Martin, Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition (3rd edn 2023) 105–108.

120 H Gonen and Y Goldberg, 'Lipstick on a Pig: Debiasing Methods Cover up Systematic Gender Biases in Word Embeddings But Do Not Remove Them' (2019) <arXiv:1903.03862> accessed 23 June 2025; A Caliskan, JJ Bryson and A Narayanan, 'Semantics Derived Automatically from Language Corpora Contain Human-like Biases' (2017) 356(6334) *Science* 183–186.

121 T Bolukbasi, KW Chang, J Zou *et al*, 'Man is to computer programmer as woman is to homemaker? Debiasing word embeddings' (2016) <arXiv:1607.06520> accessed 23 June 2025.

122 A Caliskan, PP Ajay, T Charlesworth *et al*, 'Gender Bias in Word Embeddings: A Comprehensive Analysis of Frequency, Syntax, and Semantics' (2022) <arXiv:2206.03390> accessed 23 June 2025.

123 D Castelvecchi, 'The Black Box of AI' (2016) 538 *Nature* <https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731> accessed 23 June 2025.

124 J Burrell, 'How the machine "thinks": Understanding opacity in machine learning algorithms' (2016) 3(1) *Big Data & Society* 10.

125 C Rudin and J Radin, 'Why are we using Black Box Models in AI when we don't need to? A lesson from an Explainable AI competition' (2019) 1(2) *Harvard Data Science Review* 3.

126 M Maggiolino, 'EU Trade Secrets Law and Algorithmic Transparency' (Bocconi Legal Studies Research Paper No 3363178, 2019) 6–9.

127 F Reda, 'When filters fail: These cases show we can't trust algorithms to clean up the internet' <https://felixreda.eu/2017/09/when-filters-fail/> accessed 23 June 2025.

128 Four types of measures are usually used to assess the performance of a system: accuracy, precision, recall and specificity. See G Sartor, A Loreggia, The impact of algorithms for online content filtering or moderation.

66 Machine learning systems are based on probabilistic methods, so errors cannot be avoided[129]. The error rate is higher when the unlawfulness depends on language nuances and social and cultural particularities. As Bender and Koller claim: "In contrast to some current hype, meaning cannot be learned from form alone[130]. This means that even large language models (...) do not learn meaning; they learn some reflection of meaning into the linguistic form"[131]. Nowadays, the highest accuracy rates of automatic offensive language detection systems do not exceed 80%[132]. Even the most advanced large language models, such as GPT-4o, have limitations in terms of context understanding[133].

67 Principle 1 of the Santa Clara Principles on Transparency and Accountability in Content Moderation recommends that companies use automatic content moderation systems only when there is sufficiently high confidence in the quality and accuracy of those processes[134]. In a similar vein, Recital 26 DSA states that online intermediaries should take reasonable measures to ensure that, where automated tools are used to detect, identify and act against illegal content, the relevant technology is sufficiently reliable to limit the rate of errors to the maximum extent possible.

68 In summary, AI systems cannot achieve accurate outcomes when content decisions require a high degree of contextual understanding[135]. As observed in the European Parliament resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed: "Current automated tools are not capable of critical analysis and of adequately grasping the importance of context for specific pieces of content, which could lead to unnecessary takedowns and harm the freedom of expression and the access to diverse information, including on political views, thus resulting in censorship"[136]. Similarly, in *Poland v Parliament and Council*, the CJEU stressed that: "A filtering system which might not distinguish adequately between unlawful content and lawful content (...) would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter, and would not respect the fair balance between that right and the right to intellectual property"[137].

69 For the above reasons, user notifications should not trigger a stay-down obligation that is an obligation to prevent the reappearance of previously notified defamatory content. This is without prejudice to any injunction that may be issued in a specific case ordering the prevention of identical or similar infringements in line with the Glawischnig-Piesczek doctrine.

Upload filters. 2020, 45 <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)657101> accessed 23 June 2025.

129 E Douek, Content moderation as systems thinking. *Harvard Law Review*. 2022, 136(2), 552 ("Error choice is baked in at the moment of *ex ante* system design and depends on a number of factors including the importance of speed, an assessment of the level of risk in a particular context, and the level of technological capacity for moderating a certain kind of content").

130 The authors define "form" as any observable realisation of language, such as marks on a page, pixels or bytes in a digital representation of text, or movements of the articulators.

131 EM Bender and A Koller, 'Climbing towards NLU: On Meaning, Form, and Understanding in the Age of Data' in D Jurafsky *et al* (eds), *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*(Association for Computational Linguistics 2020) 5193.

132 F Zufall, M Hamacher, K Kloppenborg *et al*, 'A Legal Approach to Hate Speech – Operationalizing the EU's Legal Framework against the Expression of Hatred as an NLP Task' (2021) 7 <arXiv:2004.03422> accessed 23 June 2025; A Zagidullina, G Patoulidis and J Bokstaller, 'Model Bias in NLP: Application to Hate Speech Classification Using Transfer Learning Techniques' (2021) 8–11 <arXiv:2109.09725> accessed 23 June 2025.

133 E Vargas Penagos, 'ChatGPT, can you solve the content moderation dilemma?' (2024) 32 *International Journal of Law and Information Technology* 25–26.

134 'The Santa Clara Principles' <https://santaclaraprinciples.org/> accessed 23 June 2025.

135 A Marsoof, A Luco, H Tan *et al*, 'Content-filtering AI systems – limitations, challenges and regulatory approaches' (2023) 32(1) *Information & Communications Technology Law* 83.

136 European Parliament, 'Resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed' 2020/2022(INI) para 12.

137 *Poland* (n 61) para 86. See also JP Quintais, C Katzenbach and SF Schwemer *et al*, 'Copyright Content Moderation in the European Union: State of the Art, Ways Forward and Policy Recommendations' (2024) 55 *International Review of Intellectual Property and Competition Law* 17.

D. Remedies for Non-Compliance with Due Diligence Obligations

I. Public and Private Enforcement of the DSA

70 Chapter IV of the DSA contains a set of provisions on supervision and enforcement by the competent public authorities. Digital Services Coordinators (Article 49.2 DSA) have investigative and enforcement powers (Article 51 DSA), including the power to impose fines (Article 52 DSA), in respect of conduct by providers of intermediary services falling within the competence of their Member State[138]. Digital Services Coordinators may exercise those powers on their own initiative or following a request pursuant to Article 53 DSA: "Recipients of the service and any body, organization or association mandated to exercise the rights conferred by this Regulation on their behalf[139] shall have the right to lodge a complaint against providers of intermediary services alleging an infringement of this Regulation with the Digital Services Coordinator of the Member State where the recipient of the service is located or established"[140].

71 The Member State in which the main establishment of the provider of intermediary services is located has, in general, exclusive powers to supervise and enforce the DSA (Article 56.1 DSA)[141]. However, the powers of supervision and enforcement of due diligence obligations against providers of very large online platforms (hereinafter VLOP) and of very large online search engines (hereinafter VLOSE)[142] are shared by the European Commission and by the national competent authorities (Article 56.3 DSA)[143], and the former has exclusive powers of supervision and enforcement of the additional obligations to manage systemic risks imposed on these providers (Article 56.2 DSA)[144].

72 The European Commission may initiate proceedings against a provider of a VLOP or a VLOSE if it suspects it has infringed any of the provisions of the DSA (Article 66.1 DSA). If the European Commission finds that the provider does not comply with one or more provisions of the DSA, it will adopt a non-compliance decision (Article 73.1 DSA) and may impose fines not exceeding 6 % of the provider's total worldwide annual turnover (Article 74.1 DSA). To date, the European Commission has initiated formal proceedings against AliExpress[145], Facebook/Instagram[146], Temu[147], TikTok[148], and X[149].

73 Public enforcement addresses a collective action

138 'Digital Services Coordinators' <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs> accessed 23 June 2025.

139 Article 86 DSA. Rademacher argues that the *ius standi* should be extended to all parties negatively affected by an alleged infringement of a provider against provisions of the DSA, including notifiers. See T Rademacher, Article 53 Right to lodge a complaint. In B Hofmann/F Raue, (dirs.). *Digital Services Act: Article-by-article commentary*. Baden-Baden: Nomos. 2024, 937.

140 Recitals 118-119 DSA.

141 Recital 123 DSA.

142 The European Commission has designated as VLOPs: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Stripchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube and Zalando; and as VLOSEs: Bing and Google Search.

143 Recital 125 DSA.

144 I Buri, 'A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer' *VerfBlog* (31 October 2022) <https://verfassungsblog.de/dsa-conflicts-commission/> accessed 23 June 2025.

145 European Commission, 'Commission opens formal proceedings against AliExpress under the Digital Services Act' (14 March 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485> accessed 23 June 2025.

146 European Commission, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (16 May 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664> accessed 23 June 2025; European Commission, 'Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act' (30 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373> accessed 23 June 2025.

147 European Commission, 'Commission opens formal proceedings against Temu under the Digital Services Act' (31 October 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622> accessed 23 June 2025.

148 European Commission, 'Commission opens formal proceedings against TikTok on election risks under the Digital Services Act' (17 December 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> accessed 3 March 2025; European Commission, 'Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward program in the EU' (22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227> accessed 3 March 2025; European Commission, 'Commission opens formal proceedings against TikTok under the Digital Services Act' (19 February 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926> accessed 23 June 2025.

149 European Commission, 'Commission sends preliminary findings to X for breach of the Digital Services Act' (12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761> accessed 23 June 2025.

problem, as victims may lack sufficient incentive to pursue private actions when the impact of an infringement is minimal[150]. Nevertheless, public enforcement is inherently selective due to the limited resources of supervisory authorities[151]. As Husovec points out: "Only practice will tell how the European Commission will exercise its competence in cases when VLOPs or VLOSEs violate standard due diligence obligations. It is likely that the resource-limited Commission will prioritize cases based on their importance"[152]. The limitations of public enforcement can be mitigated by private claims[153], mainly through the claim for compensation provided for in Article 54 DSA.

II. The Right to Compensation under Article 54 DSA

74 Where the conditions for applying the safe harbor provided for in Article 6.1 DSA are not met, platforms may be held liable for hosting defamatory content in accordance with each Member State's rules on tort liability.

75 When the damage is the result of non-compliance with the due diligence obligations regulated in Chapter III of the DSA, the victim can also opt for the compensation remedy provided for in Article 54: "Recipients of the service shall have the right to seek, in accordance with Union and national law[154], compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation". As indicated by Raue, this article establishes an imperfect liability rule because it lacks provisions on the subjective requirements for damages, the burden of proof, or defenses such as the statute of limitations[155].

76 Under Article 54 DSA, victims must demonstrate: being a recipient of an intermediary service[156], the infringement of any due diligence obligations of the DSA, the existence of fault of the platform's operator[157], the existence of damages, and the causal link between the infringement and the damage.

1. Infringement of Due Diligence Obligations

77 Non-compliance with certain due diligence obligations under the DSA may result in harm affecting a user's right to honor. This may occur when platforms fail to suspend the provision of their services to users who frequently provide defamatory content (Article 23 DSA) or when they do not designate a single point of contact to enable users to communicate directly and rapidly with them (Article 12 DSA). In this sense, before the DSA, the judgement 72/2011, of 10 February, of the Spanish Supreme Court confirmed the liability of the owner of a website for hosting defamatory messages on the grounds that the illegality was evident, and that the defendant had failed to comply with the obligation to designate a means of contact[158]. The infringement of this obligation prevented the plaintiff from being able to communicate with the defendant in an easy and direct manner to stop the dissemination of the defamatory content[159].

150 S Shavell, Liability for Harm versus Regulation of Safety. *The Journal of Legal Studies*. 13 (2) 1984, 363 ("One reason that a defendant can escape tort liability is that the harms he generates are widely dispersed, making it unattractive for any victim individually to initiate legal action").

151 A Rubí Puig, 'Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de Datos y otras acciones en derecho español' (2018) 34 *Derecho Privado y Constitución* 209.

152 M Husovec, *Principles of the Digital Services Act* (Oxford University Press 2024) 424; D Jackson and B Szóka, 'The Far Right's War on Content Moderation Comes to Europe' *TechPolicy.press* (11 February 2025) <https://www.techpolicy.press/the-far-rights-war-on-content-moderation-comes-to-europe/> accessed 23 June 2025.

153 Z Clopton, 'Redundant Public-Private Enforcement' (2016) 69 *Vanderbilt Law Review* 308–311.

154 Recital 121 DSA clarifies that: "Such compensation should be in accordance with the rules and procedures set out in the applicable national law and without prejudice to other possibilities for redress available under consumer protection rules". The detailed procedural rules governing actions for safeguarding an individual's rights under UE law must be no less favorable than those governing similar domestic actions (principle of equivalence) and must not render practically impossible or excessively difficult the exercise of rights conferred by EU law (principle of effectiveness).

155 F Raue, 'Article 54 Compensation' in B Hofmann and F Raue (eds), *Digital Services Act: Article-by-Article Commentary*(Nomos 2024) 951.

156 Recipient of the service means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible (Article 3 b) DSA).

157 Within the European legal systems, fault-based liability provides the backbone of the law of torts. See G Wagner, Liability Rules for the Digital Age, *Journal of European Tort Law*, 13(3) 2022, 194.

158 See Article 5 ECD and Article 10 of the Law 34/2002 of 11 July 2002 on information society services and electronic commerce. The latter transposed the ECD into Spanish law.

159 Judgment 72/2011 (Supreme Court (Civil Chamber) 10 February 2011) para 4 (ECLI:ES:TS:2011:559).

78 The majority of DSA's due diligence obligations appear to confer rights which can be violated by a single act of non-compliance. For instance, Article 17.1 DSA obliges hosting service providers to provide a clear and specific statement of reasons to any affected user for any restriction imposed on their content. The statement of reasons shall at least contain, among other information, a reference to the legal ground relied on and explanations as to why the information is considered to be illegal content on that ground (Article 17.3 d) DSA), and clear and user-friendly information on the possibilities for redress available to the recipient of the service in respect of the decision (Article 17.3 f) DSA). Failure to comply with this provision may prevent the user from realizing that their content has been removed and, consequently, from being able to complain about the decision in time. Other DSA's due diligence obligations require an assessment of the platform's behavior on a systemic level to be able to establish violations (e.g., Articles 20.4, 21.2, 22.2, or 23 DSA)[160].

79 It is unclear whether Articles 34 and 35 DSA can be enforced through private actions[161]. In accordance with these provisions, providers of VLOPs and VLOSEs must diligently identify, analyze and assess any systemic risks in the Union, including the dissemination of illegal content through their services (Article 34.1 a) DSA), stemming from the design of their recommender systems and any other relevant algorithmic system (Article 34.2 a) DSA). After the risk assessment, the above-mentioned subjects must put reasonable, proportionate, and effective mitigation measures in place, with particular consideration given to the impact on fundamental rights. Such measures may include testing and adapting their recommender systems (Article 35.1 d) DSA).

80 Following the well-established case law of the CJUE, individuals who have been harmed have a right to compensation where the rule of EU law infringed intended to confer rights on them, and those rights arise not only where provisions of EU law expressly grant them, but also by reason of positive or negative obligations which those provisions impose in a precise, clear and unconditional manner, whether on individuals, on the Member States or on the EU institutions[162]. The problem is that Articles 34-35 DSA grant the providers of VLOP and VLOSE and the Commission broad discretion. Therefore, as Husovec notes: "Prior to the Commission concretizing what risk mitigation measures are appropriate given the practice of the provider, it is hard to infer specifically what an individual can personally expect from such rules"[163].

2. Fault

81 Article 82 of 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 (hereinafter GDPR) provides a right to compensation to any person who has suffered material or non-material damage as a result of an infringement of the GDPR.

82 This provision, like Article 54 DSA, does not specify the subjective requirements for damages. Some authors argue that Article 82 GDPR does not require the existence of fault when establishing the liability of controllers or processors[164], while others maintain that a strict liability rule should apply in cases of infringement of obligations of result[165]. However, the CJEU has held that it is apparent from a combined analysis of Articles 82.2 and 82.3 that this article provides for a fault-based regime, in which the controller is presumed to have participated in the processing constituting the breach of the GDPR in question[166]. Article 54 DSA is much narrower than Article 82 GDPR, so it is uncertain whether the CJEU will reach the same conclusion.

83 It should be noted that, unlike Article 54 DSA, Article 74 DSA does include a reference to the requirement

160 M Husovec, Principles of the Digital Services Act (Oxford University Press 2024) 434.

161 In favor of this possibility, see F Raue, Article 54 Compensation. In B Hofmann/F Raue (dirs.). *Digital Services Act: Article-by-article commentary*. Baden-Baden: Nomos. 2024, 958.

162 The CJUE established the principle of direct effect of EU law in Case C-26/62 *van Gend & Loos* (5 February 1963).

163 M Husovec, *Principles of the Digital Services Act* (Oxford University Press 2024) 431. See also M del Moral Sánchez, 'The Devil is in the Procedure: Private Enforcement in the DMA and the DSA' (2024) 9(1) *University of Bologna Law Review* 33.

164 G Zanfir-Fortuna, 'Article 82. Right to compensation and liability' in C Kuner, L Bygrave and C Docksey (eds), *The EU General Data Protection Regulation* (Oxford University Press 2020) 1176.

165 MJ Santos Morón, 'Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art 82 RGPD (asuntos C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21)' (2024) 16(2) *Cuadernos de Derecho Transnacional* 1420; A Rubí Puig, 'Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD' (2018) 5(4) *Revista de Derecho Civil* 62–63.

166 Case C-667/21 *Krankenversicherung Nordrhein* (CJEU, 21 December 2023) para 103; Case C-687/21 *MediaMarktSaturn*(CJEU, 25 January 2024) para 52; Case C-741/21 *Iuris* (CJEU, 11 April 2024) para 46.

of fault when it establishes that: "The Commission may impose on the provider of the very large online platform or of the very large online search engine concerned fines not exceeding 6 % of its total worldwide annual turnover in the preceding financial year where it finds that the provider, *intentionally or negligently*: (a) infringes the relevant provisions of this Regulation (...)".

3. Damages

84 Since Article 54 DSA does not contain any provision intended to define the rules on the assessment of damages, it is for the legal system of each Member State to prescribe the criteria for determining the extent of the compensation payable in that context, subject to compliance with principles of equivalence and effectiveness[167].

85 When the infringement of the DSA's due diligence obligations affects the right to honor, the extent of non-pecuniary losses should be assessed considering factors such as the number of views of the defamatory content and the duration it remained publicly accessible[168]. In online defamation cases, Spanish courts have awarded damages against online intermediaries ranging from 1000€ to 18000€ depending on these criteria[169].

86 For example, the judgement of the Court of Appeals of Malaga, section 4, 82/2018, of 5 February, ordered a news portal to pay compensation of 1200€ for hosting defamatory comments. The judgement took into account that the defamatory comments were a minority compared to the rest of the comments, that the number of users was not significant, and that the news item referred to a limited territorial scope (Marbella)[170]. In contrast, the judgement of the Court of Appeals of Murcia, section 1, 9/2020, of 13 January, ordered another news portal to pay compensation of 20000€ for hosting defamatory comments. The Court of Appeals considered that the comments received a total of 89462 visits in order to quantify non-pecuniary losses[171].

E. Concluding Remarks

87 Online platforms are liable for hosting defamatory content only once they have knowledge or awareness of its illegality, as harm is not foreseeable before that moment. They have reactive duties which, pursuant to Article 16 DSA, include implementing notices and take-down mechanisms to react rapidly against defamatory content. In contrast, platforms should not be subjected to proactive prevention duties, as this would entail general monitoring or active fact-finding obligations, both expressly prohibited under Article 8 DSA. Given the current state of the art, platforms should also not be required to prevent the reappearance of previously notified defamatory content. However, the lack of notice and stay-down obligations does not preclude courts from ordering measures to prevent the publication of identical or similar illegal content.

88 When platforms cannot benefit from the safe harbor, their liability for hosting defamatory content must be based on the Member State's rules on tort liability. Additionally, liability may be established under Article 54 DSA if the damage results from the platform's actions or omissions. In such cases, the victim must demonstrate that they are the recipient of an intermediation service, that the platform infringed one or more due diligence obligations under the DSA, the fault of the platform operator, the damage suffered, and a causal link between the infringement and the damage.

167 Case C-300/21 Österreichische Post (CJEU, 4 May 2023) para 54; Joined Cases C-182/22 and C-189/22 *Scalable Capital*(CJEU, 20 June 2024) para 27.

168 *Kozan v Turkey* no 16695/19 (ECtHR, 1 March 2022) para 66; *Sanchez* (n 75) para 193; *Danileț v Romania* no 16915/21 (ECtHR, 20 February 2024) para 76.

169 Judgment of the Court of Appeal of Madrid, sec 19, 50/2006, 6 February, ECLI:ES:APM:2006:266 (compensation of €18,000); Judgment of the Court of Appeal of Islas Baleares, sec 3, 65/2007, 22 February, ECLI:ES:APIB:2007:200 (compensation of €6,000); Judgment of the Court of Appeal of Madrid, sec 13, 420/2008, 22 September, ECLI:ES:APM:2008:18214 (compensation of €6,000); Judgment of the Court of Appeal of Badajoz, sec 3, 280/2010, 17 September, ECLI:ES:APBA:2010:871 (compensation of €2,000); Judgment of the Court of Appeal of Barcelona, sec 14, 707/2010, 29 November, ECLI:ES:APB:2010:8805 (compensation of €12,000); Judgment of the Court of Appeal of Madrid, sec 11, 221/2011, 31 March, ECLI:ES:APM:2011:2467 (compensation of €9,000); Judgment of the Court of Appeal of Málaga, sec 4, 540/2011, 24 October, ECLI:ES:APMA:2011:1605 (compensation of €10,000); Judgment of the Court of Appeal of Madrid, sec 12, 47/2015, 4 February, ECLI:ES:APM:2015:4445 (compensation of €10,000); Judgment of the Court of Appeal of Santa Cruz de Tenerife, sec 3, 1/2022, 13 January, ECLI:ES:APTF:2022:97 (compensation of €5,000).

170 The Spanish Supreme Court upheld this judgement. See Judgement 235/2020, of 2 June (ECLI:ES:TS:2020:1534).

171 The judgement of the Spanish Supreme Court 226/2021, of 27 April (ECLI:ES:TS:2021:1570) reduced the compensation to 15000€ considering that the right to privacy was not violated, only the right to honour.

The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry

by **Stephanie Rossello** *

Abstract: On the basis of EU case-law, guidelines and scholarship, it is unclear whether opinions can be rectified under Article 16 GDPR and, if yes, what rectifying opinions means in practice. Yet, such ambiguity cannot be explained on the basis of the text of Article 16 GDPR, which allows the rectification of any type of personal data. This article inquires into the historical origins of the facts versus opinions dichotomy for the purpose of the right to rectification in Dutch data protection legislation. It examines how and why this distinction emerged during the preparation of the first Dutch data protection law as well as how it influenced the interpretation and application of the right over time by Dutch courts and the Dutch DPA. This study can help explain what distinguishes opinions from so-called facts for the purposes of rectification, why such differentiation exists and how it can affect the interpretation and application of the right. The analysis leads to the conclusion that, at the Dutch level, the facts versus opinions dichotomy is a by-product of two fundamental uncertainties. The first one concerns the notion of accuracy and the standard of proof required to prove an inaccuracy. The second one relates, more generally, to the relation between data protection law on the one hand, and other (often national) legal regimes, such as administrative law or tort law, on the other, with which data protection law will often intersect.

Keywords: Accuracy, Completeness, Facts, Opinions, Rectification

Recommended citation: Stephanie Rossello, The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry, 16 (2025) JIPITEC 270 para 1.

A. Introduction

1 Consider the following fictitious example. A university student fails an exam in a course named "General Data Protection Regulation (GDPR)".[1] After some initial disappointment, she realizes that the score she received does not accurately reflect her knowledge of the subject. The student, hence, decides to dispute the score before the university's examination board, following the procedure set out by the university regulations. At the same time, she requests the university to correct her grade on the basis of Article 16 GDPR. This provision requires the controller to rectify inaccurate data concerning the data subject and to complete personal data that is incomplete for the purpose of the processing. Based on existing case-law of the Court of Justice of the European Union (CJEU), guidance of European data protection supervisors and international data protection scholarship on the right to rectification of personal data, it is unclear whether the student's rectification request is likely to be granted and, if yes, how rectification should practically take place. The main reason for this is that the request concerns the rectification of personal data in the form of a third-party evaluation (or so-called 'opinion').

2 Whereas rectifying inaccurate 'facts' by substituting them with accurate ones is often uncontroversial, carrying out the same process for opinions is far more contentious. What lies at the core of the discussion is the (un)verifiability of the accuracy of personal data in the form of opinions. In essence, the accuracy

* PhD candidate Open Universiteit and KU Leuven.

1 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

of opinions would often be more difficult to verify and prove, because of the lack of an unambiguous and/or undisputed benchmark against which to assess these data.[2] By contrast, the accuracy of facts (e.g. someone's height) can be more easily verified because there is one clear objective standard against which to evaluate them.[3]

3 Crucially, the distinction between facts and opinions is absent from the wording of Article 16 GDPR and its predecessor, Article 12 (b) of the Data Protection Directive 95/46/EC (DPD).[4] Data protection scholarship on the right to rectification of personal data does not address the origins and rationale of this dichotomy.[5] In this article, I thus explore the roots and justification of this differentiation, using The Netherlands as a case-study.[6] I chose The Netherlands because Dutch courts have, and often still do, hold that the right to correction of personal data "is not intended to correct or erase personal data that represent impressions, opinions or conclusions with whom the data subject does not agree".[7] Against this backdrop, I aim to answer the following research questions. First, why are, in the Dutch data protection legal framework, opinions often said not to be suitable for being corrected or erased through the right to rectification of Article 16 GDPR or its predecessors under Dutch data protection law? Second, what does this imply, in practice, for the rectification of opinions?

4 I answer these questions by looking at the genealogy of the right to rectification in Dutch data protection law, practice (advises, guidance, decisions) of the Dutch Data Protection Authority (DPA) and relevant case-law. Specifically, the paper is based on a review of the main documents used to prepare Dutch data protection laws as well as the laws themselves, namely: the *Wet persoonsregistraties* of 1988 (Wpr),[8] the *Wet bescherming persoonsgegevens* of 2000 (Wbp)[9] and the law implementing the GDPR, the *Uitvoeringswet Algemene verordening gegevensbescherming* of 2018 (UAVG).[10] In parallel, I have conducted a review of a selection of published guidelines, advises, reports and decisions of the Dutch DPA – from its early establishment in the form of the *Registratiekamer*, until today[11] – and published case-law on Article 16 GDPR and its predecessors under Dutch data protection law.[12] Since the review is limited to only published documents and case-law, it may not be entirely representative of these authorities' view on the topic. Moreover, I have not reviewed case-law on the right to rectification in sectorial data protection laws (e.g. laws dealing with the processing of personal data by law enforcement authorities). Additionally, when useful to interpret the preparatory legislative works, laws and decisions and case-law mentioned above, I have consulted academic literature on Dutch data protection law in general, and the principle of accuracy and the right to rectification,

2 Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Colum. Bus. L. Rev 494; Diana Dimitrova, 'The Rise of the Personal Data Quality Principle. Is It Legal and Does It Have an Impact on the Right to Rectification?' (2021) 12 EJLT <https://www.ejlt.org/index.php/ejlt/article/view/768/1042> accessed 15 November 2021; Dara Hallinan and Frederik Zuiderveen Borgesius, 'Opinions Can Be Incorrect (in Our Opinion)! On Data Protection Law's Accuracy Principle' (2020) 10 IDPL 1.

3 Wachter and Mittelstadt (n 3) 548; Hallinan and Zuiderveen Borgesius (n 3) 8.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

5 Wachter and Mittelstadt (n 3); Bart Custers and Helena Vrabec, 'Tell Me Something New: Data Subject Rights Applied to Inferred Data and Profiles' (2024) 52 CLSR 105956; Dimitrova (n 3); Andreas Nicolas Häuselmann, *EU Privacy and Data Protection Law Applied to AI: Unveiling the Legal Problems for Individuals* (2024, Doctoral dissertation, Universiteit Leiden) <https://scholarlypublications.universiteitleiden.nl/handle/1887/3747996> accessed 15 July 2024.

6 See also: Stephanie Rossello, 'De (on)juistheid en rectificatiemodaliteiten van zachte persoonsgegevens in het Nederlands recht', forthcoming in: (2025) 2 P&I, 72.

7 See paragraph 4.1 below.

8 Wet van 28 december 1988 houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (Wet persoonsregistraties) (*Stb* 1988, 665).

9 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) (*Stb* 2000, 302).

10 Wet van 16 mei 2018 houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (*Stb* 2018, 144).

11 The published decisions, reports, advises and guidelines of the Dutch DPA and its predecessors were found by means of a search on the Dutch DPA's online archives and scholarly contributions that published part of the decisions. The keywords used were the Dutch translations of "correction" and "rectification". The research includes decisions published before 3 July 2024.

12 The case-law was found mainly by means of a search on the online repository of Dutch case-law (rechtspraak.nl). The keywords used were Dutch translations of "correction personal data" in combination with "GDPR" and "rectification personal data" in combination with "article 16 GDPR". In total, approximately 250 cases were reviewed. The research includes cases published before 3 July 2024.

in particular. Finally, it should be stressed that the research concerns only the right to rectification under Article 16 GDPR and its predecessors under Dutch data protection law. Closely related rights, such as the right to erasure of Article 17 GDPR or the right to restriction of Article 18 GDPR, although undoubtedly relevant for the discussion concerning the distinction between the accuracy of facts and opinions, are outside the scope of this study.

5 Before delving into the substance of the paper, I shall offer a final clarification. In this article I use the terms 'facts' and 'opinions' because these are terms that are often used in relevant data protection sources to delineate the different interpretation and application of the notion of accuracy and rectification to two different types of personal data. Other terms that, in the reviewed sources themselves, are used as synonyms of facts are, for instance, 'objective personal data' or 'hard data'. Conversely, opinions are often referred to as or assimilated with 'subjective personal data', 'soft data', 'assessment or evaluation', 'conclusion', 'impression', 'inference' or 'research result'. The work presented in this article consists of looking at how the right to rectification has been applied to personal data that – in the reviewed sources themselves – are defined as 'opinions' (or one of the aforementioned terms), compared to personal data that, in the reviewed sources themselves, are referred to as 'facts' (or one of the aforementioned concepts). At this point, I do not intend to set forth my own definition of facts or opinions for the purposes of the right to rectification. In this article, I chose the facts versus opinions terminology simply because it is the most straightforward one. Yet, I recognize that, in every-day language, the term opinion is not necessarily a synonym of, for instance, 'inference' or 'research result'. I also note that – for the purposes of this article – I do not differentiate between human opinions on the one hand, and algorithmic opinions on the other. However, I do observe that the majority of the sources reviewed at a national level appear – from the facts of the case as described in the document – to refer to human opinions.

6 In Section B, I briefly present how existing CJEU case-law, guidance of EU data protection bodies and international data protection scholarship has approached the rectification of facts and opinions. Subsequently, I expand on the original meaning and the purpose of the right to rectification as interpreted by the Dutch legislator (Section C). Next, I detail how the right has been interpreted and further clarified by the Dutch DPA and courts (Section D).

B. The Rectification of Opinions in EU Data Protection Law

7 Until now, the only case where the CJEU has explicitly (albeit only transversally) dealt with the rectification of (third-party) opinions is the *Nowak* case.[13] The main question raised in that case was whether Mr. Nowak's examination script qualified as his personal data. When dealing with this question, both the Advocate General Kokott (AG) and the Court briefly discussed whether Mr. Nowak's exam answers, the evaluator's comments on the script and the exam questions could be rectified and, if yes, under which circumstances. Both the AG and the Court deemed that the accuracy of personal data under Article 6 (1) (d) Data Protection Directive 95/46/EC (DPD) had to be judged by reference to the purpose of the collection of the data.[14] Since the purpose of collecting exam answers was to assess a candidate's level of knowledge, answers showing gaps in that knowledge did not qualify as inaccurate under Article 6 (1) (d) DPD.[15] Consequently, these answers could not be rectified a posteriori. By contrast, errors such as the attribution of the data subject's answers to another exam candidate or the loss of a part of the answers (i.e. what can be called material errors) would give rise to a right to correction.[16] The AG and the Court came to the same conclusion in relation to the evaluator's comments. Specifically, according to the Court, the comments could be rectified when they would not accurately reflect the examiner's opinion.[17] However, when the comments were not "objectively justified",[18] the AG added, they would not be liable to being corrected under data protection law, since "any objections to the comments had to be dealt with as part of a challenge of the evaluation of the script".[19] Finally, the Court considered that the exam questions were not capable of qualifying as personal data.[20] Neither the Court, nor the AG explicitly distinguished facts, on the one hand, from opinions on the other. Nevertheless, their position on the rectifiability of

13 *Peter Nowak v Data Protection Commissioner* [2017] Court of Justice of the European Union, ECLI:EU:C:2017:994.

14 *Opinion AG Kokott Peter Nowak v Data Protection Commissioner* [2017] ECJ ECLI:EU:C:2017 :582 at para 35; *Peter Nowak v. Data Protection Commissioner* (n 14) at para 53.

15 *Opinion AG Kokott. Peter Nowak v. Data Protection Commissioner* (n 15) at para 35; *Peter Nowak v. Data Protection Commissioner* (n 14) at para 53.

16 *Opinion AG Kokott. Peter Nowak v. Data Protection Commissioner* (n 15) at para 36; *Peter Nowak v. Data Protection Commissioner* (n 14) at para 54.

17 *Peter Nowak v. Data Protection Commissioner* (n 14) at para 54.

18 *Opinion AG Kokott. Peter Nowak v. Data Protection Commissioner* (n 15) at para 54.

19 ibid at para 55.

20 *Peter Nowak v. Data Protection Commissioner* (n 14) at para 58.

the three types of personal data mentioned above is indicative of their standpoint on the question whether opinions (i.e. the evaluator's comments) can be rectified by the data subject. As similarly argued by Wachter and Mittelstadt (see below) and other authors[21], the CJEU's ruling in *Nowak* seems to suggest that opinions can be corrected under data protection law only insofar as the correction concerns a material error. Errors in reasoning, affecting the content of the opinion, by contrast, cannot be rectified. In the earlier *YS and others* case, the Court reached a somewhat similar conclusion.[22] In that case, the CJEU held that the Dutch Immigration Authority's legal analysis, which had been used to support that authority's decision on whether to grant the data subjects a residence permit, did not qualify as personal data under Article 2 (a) DPD.[23] The CJEU explained this by referring to (among others) the objective of the DPD, specifically the rights that the DPD conferred to data subjects.[24] Verification of the accuracy of (the content of a) legal analysis, the latter's rectification (and, consequently, access to it) would be matters which do not, according to the Court, fall within the scope of the right to privacy.[25]

8 The European Data Protection Board (EDPB)'s predecessor, i.e. the Article 29 Working Party (WP29), and the European Data Protection Supervisor (EDPS) have also alluded to a difference between facts and opinions in relation to the right to rectification of personal data. Specifically, in the context of profiling in the sense of Article 4 (4) GDPR, the WP29 appears to suggest that a medical profile that puts an individual into a category that is more likely to get a heart disease would not necessarily be inaccurate under article 16 GDPR, even if the individual never gets such disease. That profile, the WP29 explains, "may still be factually correct as a matter of statistics".[26] According to the WP29, the medical profile could, however, be complemented – taking into account the purpose of the processing – with a supplementary statement based on a more advanced medical examination.[27] Additionally, in its 2014 Guidelines on the rights of individuals with respect to the processing of their personal data under Regulation 45/2001 on the protection of personal data by European Union institutions and bodies[28], the EDPS stated that "the right to rectification applies only to objective and factual data, not to subjective statements (which, by definition, cannot be factually wrong)".[29] Opinions (such as appreciations done in the context of an HR recruitment procedure,[30] HR performance assessments, [31] or medical opinions[32]), the EPDS added, can be rectified to the extent that the correction concerns the fact that the appreciation had been made, not the content of the assessment. According to the EDPS, opinions can, however, be complemented with the viewpoint of the data subject, to ensure their completeness.[33]

9 In academic literature, Wachter and Mittelstadt have interpreted the CJEU's ruling in *Nowak* as meaning that the right to rectification does not apply to the content of what they call subjective inferences, such as the evaluator's exam comments.[34] On the basis of *Nowak* and *YS and others* cases, they conclude that the CJEU does not conceive of guaranteeing the accuracy of inferences (and decisions based on these inferences) as falling within the remit of data protection law.[35] Contrary to Wachter and Mittelstadt, the scholars Ausloos, Mahieu and Veale, have argued that the right to rectification of Article 16 GDPR is also applicable to opinions and inferences.[36] If the controller disagrees with the rectification proposed by the data subject, they submit, the right to rectification should be conceived as a right to add the data subject's perspective on the (in)accuracy, without repealing the original opinion.[37] The scholars Häuselmann and Custers have also contended, on the basis of a teleological interpretation of article 16 GDPR, that the right to rectification should apply to any type of personal data, including personal data in the form of opinions, predictions or emotion data.[38] Similarly, Hallinan and Zuiderveen-Borgesius state that also opinions can be (in)accurate under data protection law. [39] If the interpretative framework

21 Custers and Vrabec (n 6) 9–10.

22 *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v Ms* [2014] Court of Justice of the European Union ECLI:EU:C:2014:2081.

23 ibid at para 40.

24 ibid at para 41 and 44.

25 ibid at para 45 and 46.

26 Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (wp251rev.01 22 August 2018) 18.

27 ibid.

28 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L 8, 12.1.2001.*

29 EDPS, 'Guidelines on the Rights of Individuals with Regard to the Processing of Personal Data' (2014) 18–19.

30 ibid 19.

31 ibid.

32 ibid 20.

33 ibid 19.

34 Wachter and Mittelstadt (n 3) 534.

35 ibid 550.

36 Jef Ausloos, René Mahieu and Michael Veale, 'Getting Data Subject Rights Right' (2019) 10 JIPITEC 283, 302.

37 ibid.

38 Andreas Häuselmann and Bart Custers, 'The Right to Rectification and Inferred Personal Data' (2024) 15 EJLT < https://ejlt.org/index.php/ejlt/article/view/1004/1097> accessed 2 February 2025.

39 Hallinan and Zuiderveen Borgesius (n 3) 6.

used to produce a certain opinion is not "adequately precise"[40] for a given purpose (the scholars provide the example of the use of smell to diagnose broken ribs), then the personal data contained in the opinion will be inaccurate under the GDPR. What will be adequately precise, the authors argue, will be informed by sector-specific standards (e.g. medical standards) and, where these do not exist, by the specific context of the case.[41] Finally, on the basis of the line of argumentation developed by Hallinan and Zuiderveen-Borgesius, the scholar Dimitrova advocates for a broad interpretation of the right to rectification that encompasses, next to the correction of the input data, also the modification of the interpretative framework that has generated the inaccurate opinion, and the opinion itself.[42]

10 As will be seen below (Sections C and D), elements of the debate concerning the different application and/or interpretation of the right to rectification to facts compared to opinions at the EU level also emerge in the context of discussions on the right to rectification under Dutch data protection law.

C. The Rectification of Opinions in Dutch Data Protection Law

I. Three Generations of Data Protection Laws Containing a Right to Correction

11 An early version of the right to rectification of personal data entered the Dutch legal framework in 1983 through Article 10.3 of the Dutch Constitution. This provision reads as follows: "The law provides rules concerning individuals' requests for access and correction ("*verbetering*") of data about them as well as the use made of such data".[43] Five years later, to implement this constitutional provision, Article 31.1 of the Wpr was adopted. This provision reads as follows: "the person who has been informed about the fact that personal data are being registered [about them] according to Article 29 [of the said law], can request in writing that the holder of such data corrects ("*verbeteren*") them, completes them or erases them, if the data are factually incorrect, incomplete for the purposes of the registration, irrelevant or registered in violation of a legal obligation. [...]".[44]

12 The right to correction as enshrined in Article 36.1 Wbp, which replaced the Wpr and transposed the DPD, underwent little changes compared to its predecessor. Specifically, it provided that "the person who has been informed about the fact that personal data are being processed [about them] according to Article 35 [of the said law], can request that the controller corrects such data ("*verbeteren*"), completes them, erases them or blocks them, if the data are factually incorrect, incomplete or irrelevant for the purposes of the processing or processed in violation of a legal obligation. [...]".[45]

13 Finally, on 25 May 2018, the GDPR became applicable in The Netherlands, with Article 16 GDPR providing the following: "the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement." The GDPR was, moreover, implemented through the UAVG, which does not contain specific provisions on the right to rectification.

II. Meaning and Purpose of the Right to Correction as Originally Conceived by the Dutch legislator

1. The Right to Correction, the Right to Correct Factual Inaccuracies, and the Right to Complete Incomplete Personal Data

14 It appears from the text of the abovementioned provisions and preparatory works of the Wpr and Wbp that the right to correction could carry two distinct meanings. On the one hand, it was an umbrella term used to denote what could be defined as, in fact, distinct data subject rights, namely:

- the right to correct factually inaccurate data;
- the right to complete personal data that were incomplete for the purpose of the processing;

40 Hallinan and Zuiderveen Borgesius (n 3) 9.

41 Hallinan and Zuiderveen Borgesius (n 3) 9.

42 Dimitrova (n 3).

43 Artikel 1.10 of the Dutch Constitution read as follows: "1. Everyone has, except when the law provides otherwise, the right to respect of his personal sphere. 2. The law lays down rules concerning the protection of the personal sphere with respect to the determination and dissemination of personal data. 3. The law lays down rules concerning individuals' requests for access of the data concerning them and the use made of these data, as well as correction of these data". Article 1.10 Gw.

44 Art. 31.1 Wpr (n 9).

45 Art. 36.1 Wbp (n 10).

- the right to erase data that were irrelevant for the purpose of the processing; and
- the right to erase (and under the Wbp block) data that had been registered/processed in contravention of a legal obligation.[46]

15 The right to correction could also, however, carry a more limited meaning, referring, as mentioned above, to the correction of data due to their factual inaccuracy.[47] In the following paragraphs, I will refer to the former as the right to correction and the latter as the right to correct factually inaccurate personal data.

16 It should be clarified that – by the text of the three provisions – the right to correction under Articles 31.1 Wpr and 36.1 Wbp cannot simply be equated with the right to rectification under Article 16 GDPR. Specifically, the wording of the provisions suggests that the right to correction under Articles 31.1 Wpr and 36.1 Wbp is i) either broader than the right to rectification as presented in the text of Article 16 GDPR (encompassing, for instance, also the right to erase irrelevant personal data) or ii) more limited (encompassing only the right to correct factually incorrect data, but not the right to complete them). The text of Articles 31.1 Wpr and 36.1 Wbp on the one hand, and Article 16 GDPR on the other, indicates that these provisions have two common denominators, namely: the right to correct inaccurate personal data and the right to complete incomplete personal data for the purpose of the registration/processing. Below, I will, hence, first clarify the meaning of the right to correction (Section C.II.2.). Subsequently, I will explain the meaning of the right to correct factually inaccurate data (Section C.II.3) and complete incomplete data (Section C.II.4) on the basis of the preparatory works of the Wpr and Wbp.

2. The Right to Correction as a (Merely) Indirect Enabler of Qualitative Decisions Concerning the Individual

17 From its inception, the right to correction was linked to the impact that inaccurate data could have on an individual's "professional career and reputation, without that individual being aware of it".[48] Specifically, it had to be seen in light of the purpose served by the broader right to personal data protection, which it formed a part of. The right to personal data protection was seen as a bundle of entitlements individuals had with respect to the image generated by their personal data.[49] In particular, such image should not be the result of a collection of personal data undertaken for illegal purposes and should not be "misleading"[50], or, in other words, generated on the basis of data that were "inaccurate, irrelevant and/or incomplete"[51]. The creation of a misleading image about a person was seen as particularly problematic when the data could potentially be used for important actions (including decisions) concerning an individual. This appears from the fact that the first draft data protection law proposed by the State Committee Koopmans[52] foresaw an exception to the right to correction in cases where data were collected exclusively for scientific research or statistical purposes. In these cases, the Committee considered, the personal data were not meant to be used to make decisions about an individual.[53] The conceptualization of the right to correction (and the notion of accurate data) as a safeguard for qualitative decisions (on e.g. employment, credit, health) concerning an individual, arguably, remained in later stages of the legislative evolution of the right up until the Wpr[54], and, subsequently, the Wbp.[55]

46 See e.g.: P.J. Hustinx and G. Baert, 'Preadviezen over de bescherming van de persoonlijke levenssfeer bij de toepassing van de computer' (Vereniging voor de Vergelijkende Studie van het Recht van België en Nederland) Zwolle: W.E.J. Tjeenk Willink 1973, p. 36–37; *Privacy en Persoonsregistratie: Interimrapport van de Staatscommissie Bescherming Persoonlijke Levenssfeer in Verband Met Persoonsregistraties* (Staatsuitgeverij, s-Gravenhage 1974), p. 13; *Privacy en Persoonsregistratie: Eindrapport van de Staatscommissie Bescherming Persoonlijke Levenssfeer in Verband Met Persoonsregistraties* (Staatsuitgeverij, s-Gravenhage 1976), p. 109; *Kamerstukken II* 1984/'85, 19095, nr. 3, p. 46 (MvT); F. De graaf, *Bescherming van de Persoonlijkheid, Priveleven, Persoonsgegevens*, Alphen aan den Rijn: Tjeenk Willink 1977, p. 217; *Kamerstukken II* 1997/'98, 25892, nr. 3, p. 160 (Mvt).

47 *Kamerstukken II* 1981/ '82, 17207, nr. 3, p. 38–39 (MvT); *Kamerstukken II* 1986/'87, 19095, nr. 6, p. 15 (MvAII).

48 *Eindrapport van de Staatscommissie van advies inzake de Grondwet en de Kieswet* (Staatsuitgeverij 'Gravenhage 1971), p. 239.

49 *Privacy en Persoonsregistratie: Eindrapport* (n 47) p. 26-27.

50 *Privacy en Persoonsregistratie: Eindrapport* (n 47) p. 25; p. 26-27.

51 ibid

52 The State Committee Koopmans was appointed by the Dutch Government in 1972 to advise on legislative or other measures necessary to protect the personal sphere in relation to the use of automated registration systems for personal data. Automated registration systems were later defined by the State-Committee Koopmans itself as "collections of personal data which had been rendered accessible in an automated way" *Privacy en Persoonsregistratie: Eindrapport,* (n 47) p. 97.

53 *Privacy en Persoonsregistratie: Eindrapport* (n 47) p. 83.

54 *Kamerstukken II* 1984/'85, 19095, nr. 3 (n 47), p. 47 (MvT); *Kamerstukken II* 1984/'85, 19095, A-C, p. 7; *Kamerstukken II* 1986/'87, 19095, nr. 6 (n 48) p. 6 (MvAII); Art. 33.a Wpr (n 9).

55 Art. 44.1 Wbp (n 10).

18 Although the right to correction was intended to facilitate qualitative decisions (and consequently, third-party opinions on which decisions are often based), it was originally not (like the broader right to personal data protection) aimed at governing decision-making itself.[56] This also appears from the End-Report of the State Committee Koopmans, which provides explicitly that data protection law was not meant to govern the quality of administrative or private decisions, even if they could have an important impact on an individual's life.[57] The reason for this was that Dutch administrative law already foresaw specific procedures for disputing administrative decisions.[58] Additionally, in the private sector, the Committee went on, the principle of contractual freedom prevailed, which meant that, in principle, when (evaluating and) deciding upon important aspects of an individual's life, private parties were, in general, not bound by any legal obligations.[59] This has important implications for the scope of the right to correction: personal data in the form of 'decisions' would, as originally envisaged by the Dutch data protection legislator, not be liable to being corrected through Article 31.1 Wpr.

19 Compared to the Wpr, the preparatory works concerning the Wbp and Uavg say little about the underlying purpose of the right to correction and, in particular, how such right (and, the Wbp or Uavg, in general) relates to decisions negatively affecting the individual. Specifically, nothing in the preparatory works or text of the Wbp or Uavg indicates that these laws were, contrary to the Wpr, meant to also directly safeguard the quality of decisions (and reasoning underlying them).

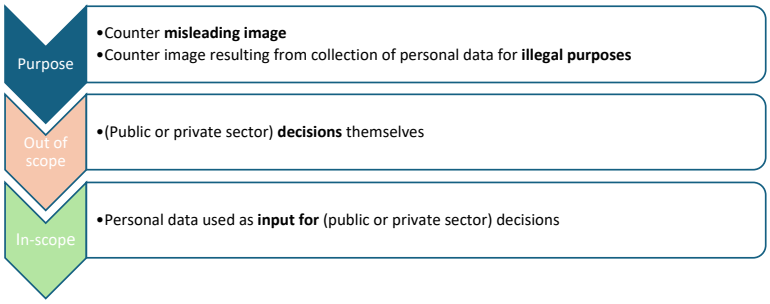

Figure 1. Purpose and material scope of application of the right to correction of Article 31.1 Wpr

3. The Right to Correct Factually Inaccurate Data in the Preparatory Works of the Wpr and Wbp

20 Neither the Wpr or Wbp themselves, nor their preparatory works explain explicitly under which circumstances data would qualify as factually (in) accurate (as opposed to merely (in)accurate). Below I have sought to interpret the meaning of factual (in)accuracy in the Wpr and Wbp on the basis of preparatory works that touch upon the meaning of the right to correct factual inaccuracies. This source indicates that the adjective factual was often used as a proxy for cases where verifying the accuracy would not require complex investigations but could be achieved easily. In other words, data were factually (in)accurate when assessing their accuracy was a (relatively) straightforward task.

21 When discussing the right to correction, the State Committee Koopmans (and some of its individual members) appeared concerned that the (in)accuracy of certain data, also called "soft data",[60] would be difficult to ascertain.[61] One type of data envisaged were evaluative data, such as personal impressions, evaluations or opinions.[62] With respect to these data, the State Committee held that, to the extent possible, it was preferable that the registered data was factual[63] and that the evaluative nature of soft data be clarified in the registration.[64] The second category of data whose accuracy was difficult to verify were (presumably, soft or hard) data that represented decisions that could be contested in the context of specific (national) procedures concerning the substance of the decision.[65] With respect to these data, the assumption was indeed that, in line with the legislator's general conception of data protection law (see above Section C.II.2), if there were other (legal) means to dispute their accuracy, these should be prioritized over the right to correction proposed in the Wpr.[66] In cases where none of the options presented above was viable, it would have been the judge's task to adjudicate, according to standards of reasonableness, upon situations where the accuracy of the data was difficult to verify.[67] Although only the first category of data explicitly concerns opinions, also the second category is relevant for the purposes of correcting opinions. In particular, as will be

56 *Kamerstukken II* 1986/'87, 19095, nr. 9, p. 11.
57 *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 29–30.
58 ibid.
59 ibid.
60 Hustinx and Baert (n 47), p. 36.
61 Hustinx and Baert (n 47), p. 36; *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 48.
62 ibid.; *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 48.
63 *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 48.
64 Hustinx and Baert (n 47), p. 36; *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 48.
65 ibid.
66 ibid.
67 *Privacy en Persoonsregistratie: Eindrapport* (n 47), p. 48.

detailed below (Section D.I.), what emerges from the examined case-law is that, (administrative or civil) decisions that can be disputed through specific (national) mechanisms are often based on opinions (e.g. legal assessments) concerning the individual affected by the decision. Consequently, a number of Dutch courts have been inclined to rule that, like the decision itself, the accuracy of opinions used as a basis for decisions that can be contested under other domains than data protection law should be evaluated by making use of the specific national procedure foreseen in those domains (see below Section D.I.3).

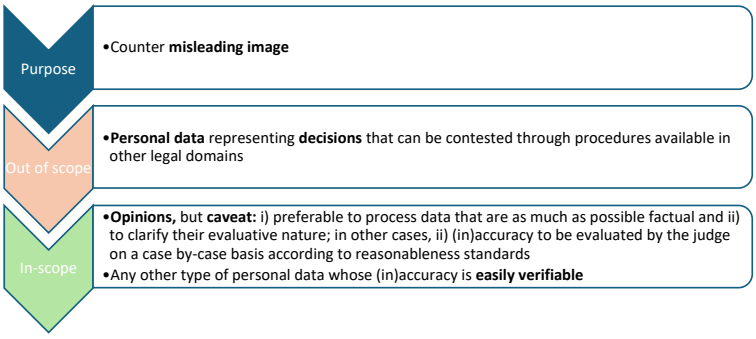

Figure 2. Purpose and material scope of application of the right to correction of factually inaccurate data of article 31.1 Wpr

22 Finally, as will be seen below (Sections D.I. and D.II.), the practice of the Dutch DPA and relevant case-law on the right to correction of factually inaccurate data suggests that this right presumably implied the modification of the inaccurate data, by means of replacing them with accurate data or erasing them altogether.

4. The Right to Complete Incomplete Data in the Preparatory Works of the Wpr and Wbp

23 The preparatory works of the Wpr and Wbp devote little attention to the right to complete personal data that were incomplete for the purposes of the registration / processing. They do, however, indicate that, like the broader right to correction, the right to complete personal data was intended to prevent the data held or processed about an individual would project a misleading image of that individual (see above Section C.II.2). In particular, by giving the data subject the right to add personal data to incomplete data, the legislator aimed to ensure that the personal data did not provide a "one-sided representation" of the data subject.[68] Contrary to factual (in) accuracy, which was arguably a binary concept, the completeness of the data was purpose-dependent.[69] Crucially, the Dutch DPA and courts have relied on this right, when the data subject challenged the accuracy of personal data in the form of opinions. As will be discussed below (Section D.I.2), this right has indeed, on multiple occasions, been understood as including the possibility to add the data subject's perspective to the disputed opinion. Moreover, in some limited instances, it has also been interpreted as granting the right to add new personal data, potentially resulting in a new opinion (Section D.II.2).

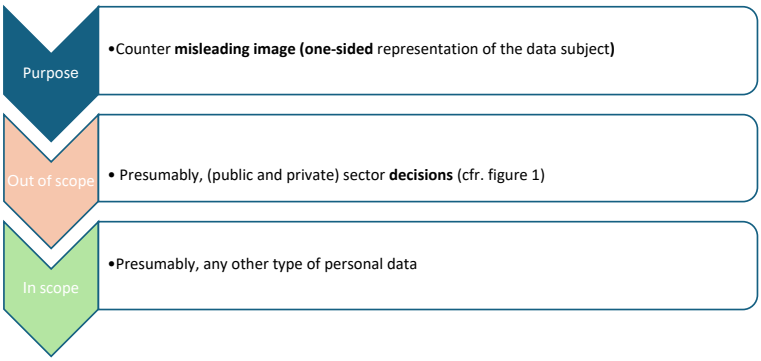

Figure 3. Purpose and material scope of application of the right to complete incomplete data of article 31.1 Wpr

68 *Kamerstukken II* 1981/ '82, 17207, nr. 3 (n 48), p. 39 (MvT).

69 Michael Teekens, 'Privacy En Computer-Registratie' (1975) Ars Aequi, p. 181–29.

D. The Right to Correct Factually Inaccurate Data and Complete Incomplete Data in the Practise of the Dutch DPA and Case-Law

I. The Right to Correct Factually Inaccurate Data as not being "Intended" for the "Correction or Erasure of Opinions with which the Data Subject Does not Agree"

24 Broadly speaking, two main approaches to the rectification of opinions can be detected in the analysed practice of the Dutch DPA and relevant case-law. The approach discussed in this paragraph – which I found in a majority of the reviewed decisions and case-law – consists of interpreting the notion of "factual inaccuracy" as excluding the possibility to correct or erase opinions with which the data subject does not agree, on the basis of Articles 31.1 Wpr and 36.1 Wbp. Below, I first explain how the notion of factual inaccuracy has been interpreted as excluding the correction or erasure of opinions, and as covering only "easily and objectively verifiable inaccuracies" (Section D.I.1). Next, I expand on what this implies for the rectification of opinions in the reviewed practice of the Dutch DPA and relevant case-law (Sections D.I.2 and D.I.3).

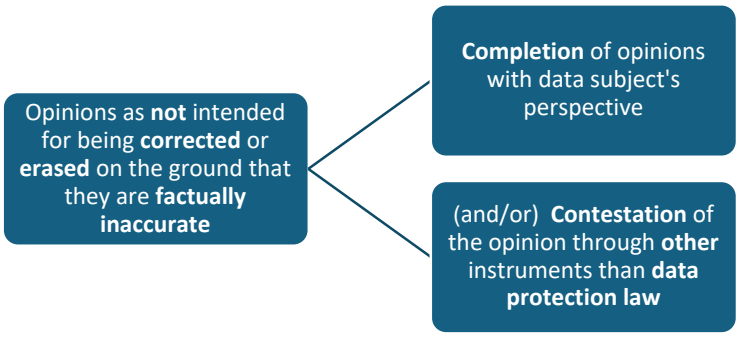

Figure 4. Approach excluding opinions from correction or erasure on the ground that they are factually inaccurate

1. "Factual Inaccuracy" as Excluding the Correction or Erasure of Opinions

25 An analysis of decisions of the Dutch DPA and case-law on the right to correction under the Wpr and Wbp illustrates what data were, often, considered not capable of qualifying as factually (in)accurate. This was often the case for what was defined as "opinions", "(expert) assessments", "impressions", "observations", "conclusions", "research results" "concerning the data subject", "with whom the data subject does not agree". According to a frequently recurring formula which was first introduced by the Dutch DPA in 1995,[70] the right to correction [in the Wpr/[71] Wbp][72] "is not intended to correct or erase" the aforementioned type of personal data. Initially, the Dutch DPA decisions and judgments containing this formula provided little clarification on the reasoning behind it. The first explanation can be found in a judgment by the administrative division of the Council of State of 2006 (the Council).[73] In this case, the data subject, an unemployed individual, sought the correction or erasure of its classification into "category 4" by the administrative authority responsible, among others, for estimating the data subject's likelihood of re-employment. After stating that the right to correction under Article 36.1 Wbp was not intended to erase "impressions, judgments or conclusions, such as the classification of the data subject in category 4", the Council explained that, the aforementioned classification "did not amount to factual data that could qualify as inaccurate under Article 36.1 Wbp".[74] Other examples of personal data that, according to the Dutch DPA and relevant case-law, qualified as "opinions, impressions, or conclusions with whom the data subject did not agree" and that could not be corrected or erased on the ground that they were factually inaccurate were: i) (medical) opinions used in the context of an

70 Registratiekamer 21 June 1995, *z95B027* in *Persoonsgegevens beschermd - uitspraken van de Registratiekamer* (SDU 1997) p. 269.

71 Registratiekamer 23 August 2001, z2001-0423, <https://autoriteitpersoonsgegevens.nl/uploads/imported/z2001-0423.pdf>; Registratiekamer 21 June 1995, *z95.B.027* in *Persoonsgegevens beschermd - uitspraken van de Registratiekamer* (SDU 1997) p. 269 (n 71).

72 Raad van State 3 March 2004, ECLI:NL:RVS:2004:AO4783; Raad van State 16 March 2005, ECLI:NL:RVS:2005:AT0510; College Bescherming Persoonsgegevens 27 May 2005, z2004-1152, p. 3 <https://www.autoriteitpersoonsgegevens.nl/uploads/imported/z2004-1152.pdf>; Raad van State 3 February 2010, ECLI:NL:RVS:2010:BL1852; Raad van State 16 February 2011, ECLI:NL:RVS:2011:BP4759; Raad van State 16 October 2013, ECLI:NL:RVS:2013:1543; Raad van State 20 February 2019, ECLI:NL:RVS:2019:520; Rechtbank Arnhem 24 September 2009, ECLI:NL:RBARN:2009:BK0880.

73 Raad van State 22 February 2006, ECLI:NL:RVS:2006:AV2256.

74 ibid para. 2.3.

evaluation by a municipal agency of the individual's capacity to accept employment opportunities;[75] ii) a governmental file used as a basis for evaluating whether or not the data subject should be entitled to a prolongation of their disability benefits;[76] iii) the classification of a detainee as posing a high flight-risk by the detention facility in which the individual resided.[77]

26 As of 2009, the aforementioned formula was often paired with another one which required the "factual (in)accuracy" under Article 36.1 Wbp to be "easily and objectively verifiable".[78] The case in which this test was first adopted concerned a neurologist whom had been dismissed by its employer on the basis of a third-party advise, which concluded that the neurologist was unfit for his job.[79] The data subject requested the controller and, subsequently, the judge to find that the aforementioned advise was (factually) inaccurate under Article 36.1 Wbp. Interestingly, the neurologist acknowledged using the right to correct inaccurate data as a way to avoid initiating civil liability proceedings against the third party that had provided the disputed advise. The court held that Article 36.1 Wbp could not be used as a substitute for civil (liability) procedures. It, further, specified that the factual inaccuracy triggering the right to correction under Article 36.1 Wbp had to be "easily" and "objectively verifiable", which would, for instance, be the case with "non-disputed facts".[80] The court, hence, concluded that, since the evidence provided by the data subject did not sufficiently prove that the disputed advise was inaccurate, its inaccuracy could not be "easily and objectively" verified. Therefore, the court continued, the inaccuracy of the disputed personal data was merely subjective. Consequently, the individual could not obtain a correction or erasure of these data on the ground that they were factually inaccurate under Article 36.1 Wbp. As frequently done by the Dutch DPA and other courts in cases of subjective inaccuracies (see below Section D.I.2), the court did, however, allow the individual to supplement the disputed data with their perspective on the inaccuracy.

27 Following this ruling, a considerable number of the reviewed cases concerning Articles 36.1 Wbp and 16 GDPR continued to exclude "opinions the data subject disagrees with" from being eligible for correction or erasure, frequently justifying this, either implicitly or explicitly, by stating that the inaccuracy at issue could not be "easily and objectively verified". Personal data that were often treated in this manner comprised (often, professional) third-party opinions concerning the data subject that (often) formed part of a file used as input for a decision with important (legal or other) consequences for the individual. Several examples are offered below:

- the opinion of a social services employee entrusted with making assessments about a child's safety;[81]
- the findings of an investigation carried out by the governmental agency entrusted with inquiring what the best interest of the child are, in the context of judicial proceedings;[82]
- the qualification of the data subject as having a fiscal debt;[83]
- the content of a medical diagnosis concerning the data subject;[84]
- the findings of an inquiry carried out by the competent immigration authority, in the context of the data subject's asylum application; [85]
- a third party's anonymous statement concerning the brother-sister relationship of the data subject and another individual, forming part of an immigration file concerning the data subject;[86]
- information contained in a governmental agency's advice used as basis for determining whether to prolong a catering permit provided to the data subject; [87]
- a doctor's description of the data subject's

75 Raad van State 16 March 2005, ECLI:NL:RVS:2005:AT0510 (n 73).

76 Raad van State 3 March 2004, ECLI:NL:RVS:2004:AO4783 (n 73).

77 Registratiekamer 23 August 2001, z2001-0423 <https://autoriteitpersoonsgegevens.nl/uploads/imported/z2001-0423.pdf (n 72).

78 Raad van State 24 May 2023, ECLI:NL:RVS:2023:2006; Raad van State 26 January 2022, ECLI:NL:RVS:2022:230; Raad van State 12 May 2021, ECLI:NL:RVS:2021:1020.

79 Gerechtshof s'Hertogenbosch 27 May 2009, ECLI:NL:GHSHE:2009:BI6357.

80 ibid.

81 Gerechtshof 's-Hertogenbosch 13 January 2022, ECLI:NL:GHSHE:2022:80.

82 Raad van State 6 October 2010, ECLI:NL:RVS:2010:BN9526.

83 Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437; Rechtbank Den Haag 22 April 2021, ECLI:NL:RBDHA:2021:3984; Raad van State 23 October 2019, ECLI:NL:RVS:2019:3571.

84 Raad van State 24 May 2023, ECLI:NL:RVS:2023:2006 (n 79).

85 Raad van State 3 February 2010, ECLI:NL:RVS:2010:BL1852 (n 73).

86 Raad van State 16 October 2013, ECLI:NL:RVS:2013:1543 (n 73).

87 Raad van State 20 February 2019, ECLI:NL:RVS:2019:520 (n 73).

home situation, in the context of proceedings concerning the individual's entitlement to certain illness benefits;[88]

- the description of the data subject as "being careful about making certain statements", contained in a medical file;[89]
- the description by an administrative authority (entrusted with the management and guidance of unemployed people) of the data subject as "not being willing to apply for jobs underneath the individual's level of education";[90]
- the description by an administrative authority of the data subject as being "unwilling to shake hands" and "shaking because of anger".[91]

28 These cases offer several important insights. First, what, often, matters in the reviewed decisions and case-law is not the nature of the personal data being assessed (i.e. facts versus opinions), but the nature of the inaccuracy that is alleged by the data subject. Specifically, as per the test developed in the aforementioned 2009 case, for an alleged inaccuracy to be eligible for correction or erasure the crucial criteria are (i) the ease with which such inaccuracy can be proven and (ii) whether the inaccuracy can be substantiated according to a somewhat universally agreed upon standard (i.e. is objective). If the data subject cannot prove that the personal data are "manifestly inaccurate"[92], the practice and case-law discussed in this paragraph choose to maintain the status-quo, by not altering (i.e. "correcting or erasing") the personal data at issue.

29 Second, as also pointed out by other scholars,[93] rather than focussing on the nature of the disputed accuracy, certain case-law, focuses on the nature of the personal data that contains the alleged inaccuracy (e.g. easily and objectively verifiable statements, contained in an individual's immigration file).[94] In these cases, the disputed accuracy (e.g. the content of the statements) is conflated with the opinion (e.g. the immigration file) and, at times, subsequent decision to which it gives rise. Consequently, probably also because Dutch data protection law was originally not intended to govern the accuracy of decision-making (and underlying reasoning) (see Sections C.II.2 and C.II.3), the (in) accuracy is treated as uncorrectable or unerasable by default, even in cases where it does meet the standard of being easily and objectively verifiable.

30 Third, and related to the previous points, the reviewed decisions and cases highlight the courts' need to delineate the boundaries between the right to correction of factually incorrect data in data protection law, on the one hand, and remedies allowing to challenge an opinion or decision, foreseen in other legal domains, on the other. Some judgments holding that opinions cannot be corrected or erased because they are factually inaccurate can, indeed, be interpreted as being symptomatic of a certain fear to adjudicate upon matters that (also) pertain to other legal domains (e.g. civil liability[95] or fiscal law[96]). A recent ruling by the Council, arguably, illustrates this.[97] In that case, an individual had been denied a passport because they appeared in the database of the tax administration as having a fiscal debt. The data subject challenged this qualification with the fiscal court on the basis of tax law and, in parallel, sought the controller to correct or erase it on the ground that it was inaccurate under Article 16 GDPR. Upon the controller's refusal to do so, the matter was brought before the Council. The Council held that the controller had rightly rejected the request to correct the description of the data subject as having a fiscal debt under Article 16 GDPR because, at the time at which that request was made, the fiscal judge had not yet ruled on the question brought before them under fiscal law. The Council went on stating that, "since the inaccuracy [of the data] had not been established yet by the fiscal judge [on the basis of fiscal law], the controller could assume that the [disputed] data were accurate [under Article 16 GDPR]".[98] In short, requiring that the (in)accuracy of certain data can lead to the alteration of the data (through correction or erasure) only when the inaccuracy is manifest, minimizes the risks of interference (and, possibly, contradiction) with what may be decided by another court or authority ruling on, fundamentally, the same question, but on the basis of other legal rules than data protection law.

31 To provide an answer to the first research question, the reason why the Dutch DPA and Dutch case-law often exclude opinions from being corrected or erased on the ground that they are inaccurate, very likely lies in the fact that the right to correct

88 Raad van State 16 February 2011, ECLI:NL:RVS:2011:BP4759 (n 73).

89 Rechtbank Arnhem 24 September 2009, ECLI:NL:RBARN:2009:BK0880 (n 73).

90 Raad van State 10 July 2022, ECLI_NL_RVS_2022_2053.

91 Raad van State 20 April 2011, ECLI:NL:RVS:2011:BQ1871.

92 Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437 (n 84).

93 G Overkleeft-Verburg, 'Annotation of: 200903967/1/H3' [2010] JB 2010/66.

94 See e.g.: Raad van State 3 February 2010, ECLI:NL:RVS:2010:BL1852 (n 73).

95 Gerechtshof s'Hertogenbosch 27 May 2009, ECLI:NL:GHSHE:2009:BI6357 (n 80).

96 Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437 (n 84); Raad van State 23 October 2019, ECLI:NL:RVS:2019:3571 (n 84).

97 Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437 (n 84).

98 ibid.

inaccurate personal data has historically, in the text of the Wpr and Wbp, been limited to data that could qualify as factually inaccurate. As of 2009, factual inaccuracy has often been interpreted in the reviewed practice of the Dutch DPA and courts as an inaccuracy that is easily and objectively verifiable. Since personal data in the form of opinions are often (presumed to be) unlikely to meet the standard of being easily and objectively verifiable, they will often not be capable of being corrected or erased on the ground that they are factually inaccurate. Finally, it should also be noted that, despite the fact that the text of Article 16 GDPR does not require data to be factually inaccurate, the Dutch DPA[99] and a considerable number of Dutch courts[100] continue, also under Article 16 GDPR, to exclude opinions from being capable of being corrected or erased on the ground that they are factually inaccurate. This raises the question whether the notion of accuracy triggering an alteration of the disputed data (i.e. in the form of correction or erasure) under Article 16 GDPR should also, like its predecessors under the Wpr and Wbp, be interpreted as being limited to factual accuracy.

2. ... but (in Several Instances) Allowing Data Subjects to Complete the Subjectively Inaccurate Data With Their Perspective

32 As already mentioned above (see Section C.II.4), frequently, when they rejected requests for correction or erasure of an opinion, the Dutch DPA and courts have allowed the data subject to supplement the disputed personal data with their vision on the (in)accuracy.[101] Interestingly, this approach is, at times, linked in the examined practice of the Dutch DPA[102] and case-law,[103] to the right foreseen under Articles 31.1. Wpr and 36.1 Wbp to complete personal data that are incomplete for the purpose of the processing (see above Section C.II.4).

3. ... and/or (in Other Instances) Directing Data Subjects to Dispute Mechanisms Available in Other Legal Domains Than Data Protection Law

33 Another trend detected in practice and case-law denying that opinions could be corrected or erased because of their factual inaccuracy consists in directing data subjects to dispute mechanisms available in other domains than data protection law (mostly, administrative law).[104] Sometimes this is done after granting the data subject the aforementioned right to supplement the subjective inaccuracy with their view, sometimes such right is not granted and the data subject's right to correction (in any form, whether modification, erasure or completion of the data) is simply denied. Most of the case-law I have reviewed that adopted this approach was taken under the Wbp. What seems to resonate throughout this case-law is the aforementioned caveat made by the Wpr's drafters concerning the purpose of the right to correction (and data protection law, more broadly) in relation to decisions affecting the individual (see Sections C.II.2 and C.II..3 above). Since decisions that can be disputed through specific (national) mechanisms are often based on opinions (e.g. medical or legal assessments), some courts have referred disputes concerning the accuracy of these opinions to the same mechanisms available for contesting the decisions based on such opinions.

99 Autoriteit Persoonsgegevens, 'Recht op rectificatie' <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/recht-op-rectificatie>.

100 Rechtbank Zeeland West Brabant 21 April 2021, ECLI:NL:RBZWB:2021:1970; Gerechtshof s'Hertogenbosch 13 January 2022, ECLI:NL:GHSHE:2022:80 (n 82); Rechtbank den Haag 11 April 2024, ECLI_NL_RBDHA_2024_4984; Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437 (n 84); Rechtbank Limburg 22 May 2024, ECLI:NL:RBLIM:2024:2275; Rechtbank Den Haag 25 February 2022, ECLI:NL:RBDHA:2022:2432.

101 Registratiekamer 21 June 1995, *z95B027* in *Persoonsgegevens beschermd - uitspraken van de Registratiekamer* (SDU 1997) p. 269 (n 71); Raad van State 3 March 2004, ECLI:NL:RVS:2004:AO4783 (n 73); Registratiekamer 2000, A ter Linden and CG Zandee, 'Zorg Voor Gegevens Bij Indicatiestelling', p. 58 <https://www.autoriteitpersoonsgegevens.nl/uploads/imported/rap_2000_indicatiestelling.pdf>; College Bescherming Persoonsgegevens 27 May 2005, z2004-1152 <https://www.autoriteitpersoonsgegevens.nl/uploads/imported/z2004-1152.pdf> (n 73); Gerechtshof s'Hertogenbosch 27 May 2009, ECLI:NL:GHSHE:2009:BI6357 (n 80); Raad van State 24 May 2023, ECLI:NL:RVS:2023:2006 (n 79); Rechtbank den Haag 25 February 2022, ECLI:NL:RBDHA:2022:2432 (n 98); Gerechtshof s'Hertogenbosch 13 January 2022, ECLI:NL:GHSHE:2022:80 (n 82); Rechtbank Zeeland West-Brabant 21 April 2021, ECLI:NL:RBZWB:2021:1970 (n 101).

102 College Bescherming Persoonsgegevens 27 May 2005, z2004-1152 <https://www.autoriteitpersoonsgegevens.nl/uploads/imported/z2004-1152.pdf> (n 73).

103 Gerechtshof s'Hertogenbosch 27 May 2009, *ECLI:NL:GHSHE:2009:BI6357* (n 80).

104 Raad van State 10 April 2024, ECLI:NL:RVS:2024:1437 (n 84); Rechtbank Limburg 22 May 2024, ECLI:NL:RBLIM:2024:2275 (n 101); Raad van State 23 October 2019, ECLI:NL:RVS:2019:3571 (n 84); Raad van State 20 February 2019, ECLI:NL:RVS:2019:520 (n 73); Raad van State 16 October 2013, ECLI:NL:RVS:2013:1543 (n 73); Raad van State 3 February 2010, ECLI:NL:RVS:2010:BL1852 (n 73); Raad van State 6 October 2010, ECLI:NL:RVS:2010:BN9526 (n 83).

II. The Right to Correct Factually Inaccurate Data and Complete Incomplete Personal Data as Leading to the Erasure and, at times, Correction of Opinions

34 A limited number of decisions and case-law reviewed under Articles 31.1 Wpr and 36.1.Wbp indicates that personal data in the form of opinions can, under certain circumstances, be modified, i.e. corrected or erased. Broadly speaking, I have detected two different ways in which the Dutch DPA and/or courts reach this outcome. These are discussed below and summarized in figure 5.

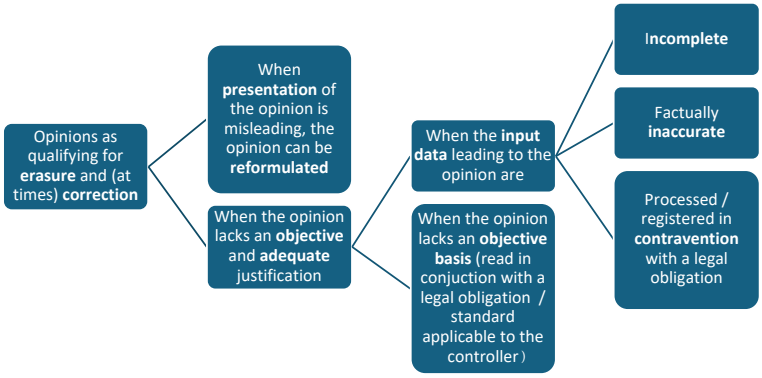

Figure 5. Approach allowing the erasure and, at times, correction of opinions

1. Reformulation of the Opinion

35 One approach consists in reformulating the opinion to better fit the context in which the opinion is processed. Under this approach, it is rather the presentation of an opinion, not its content, that is modified. This approach was adopted, for instance, in a case concerning a request for correction under Article 36.1. Wbp of the data subject's description as being "paranoid".[105] In that case, the court requested the controller to clarify what it precisely meant with this term, specifically whether it should be interpreted as the result of a medical diagnosis. Since the controller specified that this was not the case, but that the adjective was intended to convey its impression of the data subject as someone who appeared "suspicious", the court held that "paranoid" had to be replaced with, for instance, "coming across as suspicious".[106] According to the court, this was necessary to avoid that the use of the adjective would be interpreted as if it were the outcome of a medical diagnosis. In other words, the rewording was required to avoid a misleading image of the individual, considering the context in which their personal data were processed.

36 The approach taken in this case, in my view, only slightly departs from the one discussed in the aforementioned paragraph (Section D.I.). In particular, the opinion at issue was reformulated in accordance with what the controller itself had specified, namely that paranoid should be interpreted as "coming across as suspicious". The content of the opinion, was, thus, fundamentally, not modified, only its presentation was.

2. Erasure or correction of the personal data underlying an opinion leading to the erasure of the opinion itself

37 A second, more far-reaching approach detected in a (very) limited number of decisions of the Dutch DPA and case-law, consists of erasing an opinion on the grounds that it lacks an objective and adequate justification. Contrary to the majority of the cases mentioned above (Section D.I.), the focus in these cases is more granular, as it concerns the processing of the input personal data leading to the contested opinion (and, if applicable, ensuing decision), rather than the opinion itself.

38 One case in which this approach was detected concerned a request for correction brought before the Dutch DPA (presumably under Article 31.1 Wpr) of a person's creditworthiness score.[107] The DPA ruled that the score had been calculated using factually inaccurate and incomplete personal data, because it had been determined on the basis of the person's residence address, without including additions to the person's house number (e.g. house number + A, B, C etc).[108] This skewed the data subject's risk-score towards the scores of other people living on the same house number. Hence, the DPA ruled that, for the sake of accurately determining a person's creditworthiness risk, the person's house number addition also had to be taken into account and added up to the specific processing at hand.[109] De facto, this meant that the data subject's risk score had to be re-assessed.

39 Similarly, in a case concerning a data subject's

105 Raad van State 20 April 2011, ECLI:NL:RVS:2011:BQ1871 (n 92).

106 ibid.

107 Registratiekamer 23 June 1999, *99V036302* < https://archief17.archiefweb.eu/archives/archiefweb/20230427062025/https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z1999-0363.pdf>.

108 ibid.

109 ibid.

request for correction under Article 31.1 Wpr of the flight risk that had been assigned to them by the detention facility where the individual resided, the DPA concluded that such risk had been determined on the basis of incomplete data and in contravention with a legal obligation.[110] In particular, the flight risk had been determined solely on the basis of two criteria, namely the individual's wealth and the fact that the they had been found guilty to lead a criminal organisation. After reviewing the procedure that the detention facility had to follow when assessing a detainee's flight risk, the DPA observed that this procedure required the facility to seek the Public Prosecutor's assessment of the detainee's flight risk, particularly in cases where the detainee would – without this additional information – have received a high risk score. In the case at hand, however, the controller failed to request such advice and other additional information (e.g. whether the detainee had been violent when committing criminal activities or whether they had shown good behaviour in the course of the detention) which could have resulted in a lower risk-score. Consequently, the DPA held that the personal data concerning the detainee had not been "adequately" and "diligently" (i.e. fairly) processed.[111] The Authority added that the process leading to the determination of the risk-score had contravened the legal framework applicable to the detention facility.[112] This meant, according to the DPA, that the flight-risk score was "incomplete, alternatively, registered in contravention with a legal obligation."[113] The Authority, hence, advised that the individual's risk score be re-evaluated and, if necessary, modified to take into account the additional information that the controller had initially overlooked.[114]

40 One judgment of the Hoge Raad (i.e. the Dutch Supreme Court) concerning a request for correction or erasure under Article 36.1 Wbp came to a somewhat similar conclusion. Specifically, the case concerned a data subject's request to remove certain passages from a so-called youth support plan, a term used to outline the assistance and support foreseen to a young person.[115] The support-provider who had drafted such plan had come to several conclusions that put the data subject (i.e. the father of the person the plan was meant to help) in a bad light. These unfavourable opinions were based on what another party (i.e. the data subject's ex-wife) had been saying about the data subject and had not been independently verified by the support provider. In so doing, the support provider had violated their professional code of conduct. The court held that impressions of the support-provider were inherently subjective and that, therefore, they could, in principle, not be erased on the ground that they were inaccurate.[116] Nevertheless, it continued, the principle of accuracy as enshrined in Article 11.2 Wbp required opinions to have an "objective basis".[117] Since the support provider had failed to independently verify the accuracy of the opinion expressed by the data subject's ex-wife, before presenting it as if it was their own conclusion, the opinion lacked an objective basis. Therefore, it had to be erased.

41 These cases are remarkable in the sense that they amount to an erasure of opinions under Articles 31.1 Wpr and 36.1 Wbp but not on the formal ground that the opinions were factually inaccurate. A common denominator across these cases is that they required the controller to provide an objective and adequate justification for the opinion. The focus, in other words, lied on the input (personal data) leading to the opinion, not the opinion itself. In particular, the decisions of the DPA revolved mainly around the question whether the opinion at hand was sufficiently justified, in light of the specific circumstances of the case, including the (non-data protection) legal framework applicable to the controller (specifically, in the case concerning the flight risk score, the framework applicable to the detention facility). In the case brought before the Supreme Court, the main issue concerned the lack of an objective justification for the opinion. Whether such justification needed to be provided and what it entailed was determined in accordance with (non-data protection law) standards applicable to the controller, specifically the controller's professional code of conduct, which required it to come to an independent, non-biased assessment of a certain situation.

42 It is important to highlight, once again, that the aforementioned cases relate to Articles 31.1 Wpr and 36.1 Wbp. As I explained above (see Section C.II.1), while these provisions share some commonalities with Article 16 GDPR, they are not the direct equivalent of it. It is, hence, unclear whether the approach consisting in correcting opinions by erasing them on the ground that they lack an objective and adequate justification can be transposed to Article 16 GDPR. In fact, I did not find any Dutch decisions or case-law under Article 16 GDPR corroborating this.

43 To answer the second research question, the tendency of the Dutch DPA and Dutch courts to

110 Registratiekamer 23 August 2001, z2001-0423, <https://autoriteitpersoonsgegevens.nl/uploads/imported/z2001-0423.pdf> (n 72).

111 ibid, p. 9.

112 ibid, p. 10.

113 ibid.

114 ibid, p. 11.

115 Hoge Raad 16 July 2021, ECLI:NL:HR:2021:1169.

116 ibid.

117 ibid.

exclude opinions from correction or erasure on the ground that they are factually inaccurate has not always resulted in the non-rectifiability of this type of data under data protection law. Specifically, these authorities have, often, interpreted the right to correction of opinions as a right to add up the data subject's perspective on the disputed data. Moreover, in other instances, they have allowed opinions to be reformulated to better match the context of the processing. Finally, on other occasions, they have gone one step further, and granted the erasure (and, at times, ensuing correction) of opinions because the processing of personal data leading to the contested opinion was either factually inaccurate, incomplete, and/or, simply, unjustified in light of the specific (legal) obligations and standards applicable to the controller.

E. Conclusion

44 Let us go back to the example presented in the introduction. What emerges from the findings discussed in the preceding paragraphs is that there are several ways in which the Dutch DPA and Dutch courts have, throughout time, dealt with comparable requests. According to a predominant approach, the exam score itself is unlikely to be amended (i.e. corrected or erased) on the ground that it is factually inaccurate. A major reason for this is that such score is likely to qualify as data whose accuracy is not easily and objectively verifiable, hence, subjective. The student could, however, be given the opportunity to correct the score by adding her view to it. Cumulatively or alternatively, she may be given the option to contest the content of the score with the university's examination board. Imagine further that the university guidelines required the examiner to test the student's knowledge of the material, territorial and personal scope of application of the GDPR, principles of data processing, data subject rights and international data transfers. Yet, the exam only contained questions on the GDPR's territorial scope of application. In that case, the student could arguably obtain correction in the form of a reformulation of the title of the exam that she had failed. Her score sheet could report that she had failed an exam concerning the "Territorial scope of application of the GDPR", not the "GDPR". Finally, according to another approach detected in some of the reviewed cases, the student could arguably obtain an erasure of the score, on the ground that the examination procedure established by the university and leading to the assessment had not been followed. In this scenario, the score could be erased because the personal data used to determine it (i.e., the exam answers) were incomplete, given the purpose of the processing, which was to assess the student's knowledge on more aspects of the GDPR than just its territorial scope of application. Additionally, one could argue that the score was the result of a processing in violation of a standard applicable to the examiner (i.e. the university guidelines). Consequently, the score would not be sufficiently justified, in light of such standard.

45 As already mentioned, this research does not show that all the shades of "accuracy", "completeness" and "rectification" present in the reviewed Dutch practice on Article 16 GDPR and its predecessors under Dutch law can simply be transposed to Article 16 GDPR. However, an inquiry into the limited CJEU case law, guidance from EU data protection supervisors, and international scholarship concerning the right to rectification of personal data under Article 16 GDPR and its predecessor under the DPD shows that similar (different and, at times, contradictory) approaches to those identified in Dutch law animate the discussion at the EU level. Hence, one of the most significant questions that needs to be tackled now is, in my view, whether research undertaken into the genealogy of the right to rectification of personal data into other EU Member States leads to comparable results as the one undertaken in this article and whether the latter is useful to interpret Article 16 GDPR.

46 The research also shows that distinguishing facts from opinions for the purposes of rectification is likely to be misleading. When dealing with the right to rectification of personal data, the focus of the debate should not lie on the nature of the personal data being processed (i.e. whether it is a fact or an opinion) but on the notion of accuracy that is liable to being rectified under data protection law. The majority of Dutch case-law and decisions analysed in this article suggest that only easily verifiable and objective inaccuracies can be rectified through correction or erasure, i.e. measures involving a modification of the inaccurate data themselves. One of the questions that, hence, warrants further investigation is whether opinions can meet this standard and, if yes, how this standard should be operationalised.

47 Finally, the study illustrates that the issue of rectification of personal data in the form of opinions is tied to a broader, and more fundamental question concerning the purpose and essence of data protection law, its relation with other legal domains with which it may intersect, and whether, and how Member States have dealt with such intersection. Specifically, ascertaining the accuracy of personal data in the form of an opinion may require the use of normative standards present in other (legal and non-legal) disciplines. Requiring that the inaccuracy of data is easily and objectively verifiable or manifest in order to correct or erase its content may be a strategy adopted by national authorities and courts presented with requests for correction or erasure of personal

data to avoid potential conflicts with other courts confronted with, essentially, the same question but raised under other legal domains. Further research could, therefore, address whether and how national Member States have adopted (procedural) rules to avoid such possible overlap.

The European Union's Pursuit of Digital Sovereignty Through Legislation

by **Lukas von Ditfurth** *

Abstract: In recent years, calls for promoting Europe's digital sovereignty have gained traction in Europe, including in EU policy circles. A digitally sovereign Europe, it is hoped, will be able to more effectively and autonomously control the use of digital technologies, services, and data in Europe. This Article aims to shed light on the concept of digital sovereignty and its relevance for the EU's ongoing efforts to (re-)shape the rules of cyberspace through legislation. To this end, the Article attempts to develop a coherent understanding of digital sovereignty. Based on this understanding, the Article then analyzes how the EU has attempted to promote its digital sovereignty through legislation. It argues that the pursuit of digital sovereignty can be seen as an overarching goal and framework for a wide range of recent legal acts, including the Artificial Intelligence Act, the Digital Services Act, and the Digital Markets Act. The Article concludes by discussing the desirability of digital sovereignty as a legal and political goal and by considering some of the main criticisms of the EU's pursuit of digital sovereignty.

Keywords: Digital Sovereignty, European Union, Data Strategy, Tech Sovereignty, Technological Independence, Digital Markets, Artificial Intelligence

Recommended citation: Lukas von Ditfurth, The European Union's Pursuit of Digital Sovereignty Through Legislation, 16 (2025) JIPITEC 286 para 1.

A. Introduction

1 Digital Sovereignty has been the leitmotif of the European Commission's digital agenda during Ursula von der Leyen's first term as president. Going back to her candidacy in 2019, von der Leyen has advocated for the EU to become technologically sovereign and a global standard-setter in the digital realm.[1] Since then, the notion of digital sovereignty has featured prominently in speeches and documents from representatives and members of EU institutions.[2] At

* Dr. Lukas von Ditfurth, LL.M. (Chicago) is Associate at Hengeler Mueller Partnerschaft von Rechtsanwälten mbB, Berlin. The author is publishing this Article in his personal capacity and does not represent the views of the firm or its clients. He would like to thank the anonymous reviewer from whose thoughtful comments this Article has benefited substantially.

1 See Ursula von der Leyen, 'A Europe that strives for more: my agenda for Europe' (2019) 13 <https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf>. Even prior to von der Leyen's candidacy, the idea of European digital sovereignty had gained some traction in both scholarly and policy circles. In 2016, then Commissioner Viviane Reding stressed the crucial importance of digital sovereignty for Europe's future; see Viviane Reding, 'Digital Sovereignty: Europe at a Crossroads' (2016) <https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf >. For an overview of the discourse on digital sovereignty see Rocco Bellanova, Helena Carrapico & Denis Duez, 'Digital/sovereignty and European security integration: an introduction', (2022) 31 European Security 337, 346-49; Georg Glasze et al., 'Reception and Elaboration of "Digital Sovereignty" in Three European Discourse Arenas: France, Germany, and the EU', (2023) 28 Geopolitics 928, 929-31; Stephane Couture & Sophie Toupin, 'What does the notion of "sovereignty" mean when referring to the digital?', (2019) 21 New Media & Society 2305, 2312-13.

2 See, e.g., Thierry Breton, then Commissioner for Internal

its core, digital sovereignty is about the autonomous and effective control of digital technologies and services. In this vein, Ursula von der Leyen described European digital sovereignty as "*the capability that Europe must have to make its own choices, based on its own values, respecting its own rules*".[3] The ascent of digital sovereignty on the EU's political agenda has not been limited to the rhetoric of its officials. Rather, digital sovereignty can be seen as the guiding normative ideal of the EU's approach to regulating data, digital technologies, and online activities. Although only few proposals and legislative acts explicitly reference the notion of digital sovereignty, the goals of extending EU values, laws, and norms to the digital space and strengthening the EU's autonomous control over online activities underlie a wide range of legislative acts.

2 The EU's recent embrace of digital sovereignty contrasts sharply with the internet's traditional self-understanding as a global space of freedom where, according to John Perry Barlow's famous Declaration of the Independence of Cyberspace, states would exercise no sovereignty and their legal systems would not apply.[4] State Sovereignty and the digital space were thought to be incompatible. Whereas state sovereignty would require effective and monopolized control over a bounded territory, the digital space was to be borderless, global, and characterized by horizontal power relations.[5] In reality, the digital space was never as independent from state interference as cyber-libertarians envisioned it to be. States have always used their control of the internet's underlying physical infrastructures to regulate the online activities of individuals and organizations in order to, for example, steer the exchange of communication and data or protect intellectual property rights.[6] Nevertheless, the degree of control that states in the West have exercised over the digital space could justifiably be described as relatively weak.[7] Due to the fast pace of digital innovation and the economic and social promises of a global internet, European and North American countries were reluctant to interfere too strongly with the organization of the digital space through private actors.[8] Against this background, the EU's embrace of digital sovereignty as a normative ideal represents the culmination of a paradigm shift away from supporting an open internet that is based on liberalized markets and transnational connectivity towards a regulatory approach that intervenes more actively in the organization of the digital space.

3 The EU's new emphasis on digital sovereignty is motivated by a perceived loss of its autonomy, competitiveness, and security in the digital space.[9]

Market, 'Speech at Hannover Messe Digital Days' (July 15, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/speech_20_1362>; Charles Michel, then President of European Council, 'Speech at "Masters of digital 2021": Digital sovereignty is central to European strategic autonomy' (Feb. 3, 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event>; European Parliament Research Service, 'Digital Sovereignty for Europe' (2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf>; Programme for Germany's Presidency of the Council of the European Union, 'Together for Europe's recovery' (2020) 8 <https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf>.

3 Ursula von der Leyen, 'Shaping Europe's digital future' (Feb. 19, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260>.

4 See John P. Barlow, 'A Declaration of the Independence of Cyberspace' (Feb. 8, 1996) <https://www.eff.org/cyberspace-independence>; see further Edoardo Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives' in Federico Fabbrini, Edoardo Celeste & John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (2021) 211, 214.

5 Celeste (n. 4), 212; Thorsten Thiel, 'Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation' in Jeanette Hofmann, Norbert Kersting, Claudia Ritzi & Wolf J. Schünemann (eds), *Politik in der digitalen Gesellschaft: zentrale Problemfelder und Forschungsperspektiven* (2019) 47, 48.

6 Celeste (n. 4), 214; Jack Goldsmith & Tim Wu, Who controls the Internet? (2006) 65-85; Julia Pohle, Digital Sovereignty. A new key concept of digital policy in Germany and Europe (2020) 9; Thiel (n. 5), 48-49.

7 In contrast, digital sovereignty has been an integral part of the digital policies of many (autocratic) states, notably China and Russia, for many years; see, e.g., Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realisation' in Dennis Broeders & Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 107, 115; Anqi Wang, 'Cyber Sovereignty at its boldest: A Chines Perspective', (2020) 16 Ohio St. Tech. L.J. 395; Lizhi Liu, 'The Rise of Data Politics: Digital China and the World', (2021) 56 Studies in Comparative International Development 45; Louis Pétiniaud et al., 'Russia's Pursuit of "Digital Sovereignty": Political, Industrial and Foreign Policy Implications and Limits', (2023) 28 Geopolitics 924, 925.

8 For an analysis of the German discourse of the 1990s and 2000s on online state interventions see Finn Dammann & Georg Glasze, '"Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!" Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer "digitalen Souveränität" in Deutschland' in Georg Glasze, Eva Odzuck & Ronald Staples (eds), *Was heißt digitale Souveränität?* (2022) 29, 31-35.

9 The terms digital space and cyberspace are used interchangeably and understood broadly in this Article.

There are valid concerns that European values and the European legal, moral, and economic order have been undermined in cyberspace. This development has been attributed primarily to the dominant positions of powerful digital platforms within the economic and social spheres of the digital space. The predominantly American platform operators, in particular Meta, Apple, Alphabet, Amazon, and Microsoft, are considered to hold "*de facto sovereignty*".[10] They own essential digital infrastructures and, as *private legislators*, set important rules for social and economic interactions in the digital space.[11] Because of their infrastructural and quasi-legislative power, large digital platforms are able to steer the trajectory of the digital space, perform quasi-governmental functions of market regulation, and shape social and economic interactions on the internet in a way that can conflict with the EU's values and interests.[12]

4 Furthermore, from a foreign policy and security perspective, serious threats to Europe's cybersecurity and political order emanate from hostile states and other malicious actors. Cyberattacks pose a threat on multiple levels: they can violate citizens' privacy, harm the European economy through business sabotage or espionage, and disrupt the functioning of government services and critical infrastructures.[13] State-sponsored disinformation, initiated in particular by Russia, is spread through digital channels and can distort public discourse and undermine fair elections.[14] In addition, there is the widespread economic concern that Europe suffers from a lack of digital competitiveness and technological self-sufficiency.[15] Digital innovation may threaten the future success of Europe's traditionally strong but slow-to-adapt industrial sector and it is feared that Europe will be left behind, as the majority of digital cutting-edge technologies and services, including Artificial Intelligence (AI), are funded and developed outside of the EU.[16] These developments may jeopardize Europe's economic welfare and lead to a precarious dependency on foreign businesses.[17] In the long-term, this dependency could undermine sovereignty goals relating to Europe's cybersecurity and its regulatory and geostrategic autonomy.[18]

5 This Article explores how the EU is reacting against these threats by promoting its digital sovereignty through legislation. To this end, the Article aims to develop a coherent and analytically useful definition of digital sovereignty based on traditional political and legal understandings of the concept of state sovereignty (**B.**). This definition serves to distinguish the EU's digital sovereignty from other related concepts that are also sometimes discussed under the notion of digital sovereignty, i.e., Europe's technological independence, on the one hand, and the autonomous control of individuals and private organizations over their data, on the other hand. Based on a clear understanding of the concept of digital sovereignty, the Article proceeds by outlining through which legal acts and for which purposes the EU has promoted its digital sovereignty and technological independence (**C.**). The Article concludes with a high-level evaluation of the quest

Following Milton Mueller, the digital space is defined here as "*the virtual space for interaction created by joint use of compatible data communication protocols*"; see Milton Mueller, 'Against Sovereignty in Cyberspace', (2020) 22 International Studies Review 779, 788. This digital space is made up of infrastructures, technologies, and data, and includes all online content, online activities, and online interactions among humans and between humans and computers; see Benjamin Peters, 'Digital' in Benjamin Peters (ed), *Digital Keywords* (2016) 93, 94.

10 Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', (2020) 33 Philosophy & Technology 369, 372.

11 Julia Pohle & Thorsten Thiel, 'Digital sovereignty', (2020) 9 Internet Policy Review 1, 4;, at 6-7; Pohle (n. 6), 7; Ulrich Dolata, 'Plattform-Regulierung: Koordination von Märkten und Kuratierung von Sozialität im Internet', (2019) 29 Berliner Journal für Soziologie 179, 194; Jacques Crémer et al., Competition policy for the digital era (2019) 60-63.

12 Floridi (n. 10), 372; Dolata (n. 11), 194.

13 Matthias Bauer & Fredrik Erixon, 'Europe's Quest for Technological Sovereignty: Opportunities and Pitfalls', (2020) ECIPE Occasional Paper No. 02/2020, 26 <https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf>; Lokke Moerel & Paul Timmers, *Reflection on Digital Sovereignty* (2021), 9 <https://ssrn.com/abstract=3772777>.

14 Richard A. Clarke, 'Hostile State Disinformation in the Internet Age', (2024) 153 Daedalus 45, 45-56; Andrew M. Guess & Benjamin A. Lyons, 'Misinformation, Disinformation, and Online Propaganda' in Nathaniel Persily & Joshua Tucker (eds), *Social Media and Democracy* (2020) 10, 13-16.

15 European Parliament Research Service (n 2), 2.

16 Bauer & Erixon (n. 13), 13; Benjamin Farrand & Helena Carrapico, 'Digital Sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity', (2022) 31 European Security 435, 448; European Parliament Research Service (n 2), 2.

17 For a comprehensive overview of, e.g., Germany's technological dependencies see Bundesministerium für Wirtschaft und Energie, *Schwerpunktstudie Digitale Souveränität* (2021) 15-30 <https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6>.

18 See also Bellanova, Carrapico & Duez (n. 1), 348; Dammann & Glasze (n. 8), 48; Moerel & Timmers (n. 13), 11; Linda Monsees & Daniel Lambach, 'Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity', (2021) 31 European Security 377, 379.

for digital sovereignty and discusses some of its pitfalls (**D.**).

B. The Concept of Digital Sovereignty

6 Calls for strengthening Europe's digital sovereignty raise a variety of different issues that are to some extent interrelated, but address different actors and require different solutions.[19] They can refer to the control exercised by individual citizens and private organizations over their data, the ability of the EU and its Member States to autonomously govern cyberspace and to ensure cybersecurity, or the technological independence of the European economy. Furthermore, the term digital sovereignty is used in political and academic discourses for a variety of other claims, notions, and narratives, which are not related to the EU.[20] The discursive versatility of the term digital sovereignty and its intuitive applicability to different subject matters contribute to its popularity as a catch-all term.[21] Yet, the widely divergent uses of the term complicate analyses of the content of claims about digital sovereignty and their justifications.[22]

7 For the sake of conceptual and analytical clarity, it is therefore necessary to untangle different notions and meanings and to define digital sovereignty in a way that differentiates it from other (related) concepts.[23] In particular, the concept of digital sovereignty shall be delineated from the concepts of individual and organizational data autonomy and of Europe's technological and economic independence, which are also frequently discussed under the heading of European digital sovereignty.

I. Individual and Organizational Data Autonomy

8 The terms digital sovereignty or data sovereignty are sometimes used to refer to the autonomous control of individuals or private organizations over "their" data.[24] This individual digital (or data) sovereignty is typically understood to refer to the "*abilities and possibilities of individuals and institutions to be able to exercise their role(s) in the digital world independently, self-determinedly and securely*".[25] Using the term digital (or data) sovereignty to refer to the concepts of factual self-determination and autonomy of individuals is, however, misleading. For one, it is contrary to traditional legal and political understandings of sovereignty, which refer to the autonomy and control of states.[26] The same is true with regard to the discourse on digital sovereignty, in which digital sovereignty is predominantly understood to refer to state power and control in the digital space and the term data sovereignty typically refers to the state's control over data flows and is most coherently viewed as an element of the state's digital sovereignty.[27] Furthermore, individual data sovereignty has misleading connotations as the term sovereignty seems to imply an individual's legal or moral *right* to control their data.[28] Yet, according to the most wide-spread definitions, individual data sovereignty only refers to the *de facto control* exercised by individuals or organizations over the collection, use, and sharing of their data. Therefore,

19 This Section builds on Lukas von Ditfurth, *Datenmärkte, Datenintermediäre und der Data Governance Act* (2023) 193-201.

20 For in-depth analyses of the discourse about digital sovereignty see Couture & Toupin (n. 1); Patrik Hummel et al., 'Data sovereignty: a review', (2021) Big Data & Society 1, 2; Daniel Lambach & Kai Oppermann, 'Narratives of digital sovereignty in German political discourse', (2023) 36 Governance 693.

21 Lambach & Oppermann, (n. 20), 705; Dammann & Glasze (n. 8), 50.

22 See also Hummel et al. (n. 20), 2.

23 The Article's aim is not to interpret the use of the term by EU officials in speeches, but to develop a coherent and analytically useful concept of digital sovereignty based on traditional and established academic understandings of the term.

24 See, e.g., Pohle & Thiel (n. 11), 11; Pohle (n. 6), 16; Steffen Augsberg & Petra Gehring, Datensouveränität: Positionen zur Debatte (2022); Clara Beise, 'Datensouveränität und Datentreuhand', (2021) Recht Digital [RDi] 597; Alexander Roßnagel, 'Digitale Souveränität im Datenschutzrecht', (2023) Multimedia und Recht [MMR] 64.

25 Gabriele Goldacker, *Digitale Souveränität* (2017) 3 <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>.

26 See also Christian Rückert et al., 'Souveränität, Integrität und Selbstbestimmung: Herausforderungen von Rechtskonzepten in der digitalen Transformation' in Georg Glasze, Eva Odzuck & Ronald Staples (eds), Was heißt digitale Souveränität? (2022) 159, 160.

27 Couture & Toupin (n. 1), 2313; Anupam Chander & Haochen Sun, 'Sovereignty 2.0', (2023) 55 Vand. J. Transnat'l L. 283, 294.

28 For example, Gerrit Hornung and Sabrina Schomberg see a close parallel between the term data sovereignty and the right to informational self-determination as developed by the German Constitutional Court, see Gerrit Hornung & Sabrina Schomberg, 'Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Data Governance Acts', (2022) Computer und Recht 508, 510.

it is more accurate to refer to the data autonomy of individuals and organizations instead of their digital or data sovereignty.

II. Digital Sovereignty

9 At its most abstract level, digital sovereignty is defined here as state sovereignty in the digital space.[29] In order to flesh out this abstract definition, this Section will first briefly explore the well-established understanding of state sovereignty in jurisprudence and political science and then extend it to the digital space.

1. Dimensions of State Sovereignty

10 Although sovereignty is a shifting concept that has taken on many different shades over the course of centuries[30], there has remained a core meaning of the concept which still serves "*as the chief organizing principle of the international states system*".[31] At its core, sovereignty is defined as supreme authority within a territory.[32] This supreme authority is traditionally (and still today) held and exercised by the state. The core definition of sovereignty can be broken down into different facets and elements, some of which are central to the concept of digital sovereignty. On a fundamental level, an important distinction is to be made between the sovereignty *within* the state and the sovereignty *of* the state.[33]

11 As sovereignty within the state refers to the organization of authority within a political community[34], it is only the sovereignty of the state that is relevant to the concept of digital sovereignty. The sovereignty of the state can be divided into three separate but related dimensions: its internal sovereignty, its external sovereignty, and its legal sovereignty under public international law. The internal sovereignty of the state manifests itself in the ability and authority of the state to set binding legal rules for its subjects on its territory and to enforce them effectively by means of its monopoly on the use of force.[35] This internal sovereignty is composed of two essential elements – control and authority. Control refers to the actual ability or power of the state to direct and determine activities and developments within its territory.[36] Authority is the mutually recognized *right* of an actor to set rules, to command and to be obeyed.[37] This way, a state's sovereignty is to some extent linked to the legitimacy of state and government.[38]

12 External sovereignty refers to the exclusion of foreign states from interfering with the control and authority of a state within its territory.[39] Internal and external sovereignty are two sides of the same coin; each presupposes the other.[40] At its core, external sovereignty is the basis for the existing international order, in which "*states exist in specific territories, within which domestic authorities are the sole arbiters of legitimate behavior*".[41] External sovereignty is lost when a state relinquishes its supreme control and authority over a territory to a foreign actor, for example, through foreign intervention or voluntary invitation.[42]

13 International legal sovereignty is based on the recognition of states.[43] Generally, the sovereignty

29 Similarly, Anupam Chander and Haochen Sun understand the term digital sovereignty "to mean the application of traditional state sovereignty over the online domain", see Chander & Sun (n. 27), 292.

30 For a comprehensive historical account see generally Francis H. Hinsley, *Sovereignty* (2d edn, 1986).

31 Daniel Philpott, 'Sovereignty' in George Klosko (ed), *The Oxford Handbook of the History of Political Philosophy* (2011) 561, 561.

32 Ibid; Samantha Besson, 'Sovereignty' in *Max Planck Encyclopedias of International Law* (2011) para. 1 <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=MPIL>.

33 Albrecht Randelzhofer, '§ 17 Staatsgewalt und Souveränität' in Josef Isensee & Paul Kirchhof (eds), Handbuch des Staatsrechts II (3rd edn, 2004) 143, 145 para. 4; Christian Hillgruber & Hans Otto Seitschek, 'Souveränität' in Görres-Gesellschaft (ed) Staatslexikon V (8th edn, 2021).

34 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (1999) 11. It was this dimension of sovereignty and the questions of who the absolute sovereign is and ought to be, which the early theorists of sovereignty, in particular Jean Bodin and Thomas Hobbes, were primarily concerned with.

35 Randelzhofer (n. 33), 160 para. 39; Hillgruber & Seitschek (n. 33); Enrico Peuker, Verfassungswandel durch Digitalisierung (2020) 197.

36 Krasner (n. 34), 12.

37 Krasner (n. 34), 10; Robert P. Wolff, *In Defense of Anarchism* (2nd edn, 1998) 2.

38 Philpott (n. 31), 561; Huw Roberts et al., 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', (2021) 10 Internet Policy Review 1, 6.

39 Philpott (n. 31), 563; Krasner (n. 34), 20; Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (7th edn, McGraw-Hill 2006) 319-20.

40 Randelzhofer (n. 33), 154 para. 24; Philpott (n. 31), 563; Besson (n. 32), para. 73; Robert Jackson, Sovereignty: the evolution of an idea (2007) 12.

41 Krasner (n. 34), 20.

42 Krasner (n. 34), 20; Morgenthau, (n. 39), 319-26.

43 Krasner (n. 34), 14. Public international law enshrines the sovereignty of states. According to Article 2(1) of the UN Charter, the UN is based on the principle of the sovereign equality of all its members.

of a state under public international law presupposes its internal and external sovereignty.[44] Nevertheless, this relation between international legal sovereignty and the actual control exercised by a state over its territory is fickle. In the past, states that had little actual control over their internal affairs have been recognized as sovereign states under public international law.[45]

2. State Sovereignty in the Digital Space

14 The traditional concept of state sovereignty can be applied to the digital realm. Accordingly, digital sovereignty is to be understood as state sovereignty in the digital space. To the concept of digital sovereignty, both the internal and external dimensions of state sovereignty are relevant. For a state to be fully digitally sovereign, two conditions must be met. First, the state must have the authority and control to autonomously shape the rules of the digital space within its territory. It must have the right and ability to set its own autonomous rules for all online activities and developments that take place within or directly affect its territory, rather than being subject to external rules set by foreign states or private organizations. Second, the state must be able to effectively uphold and enforce the rules it has established within its territory and to keep foreign states from interfering with its control. It must have the *de facto* power to ensure that by and large its laws are respected in the digital space insofar as its own physical territory is concerned.

15 Digital sovereignty thereby complements the traditional or analogue sovereignty of states.[46] It is one element of full state sovereignty in the digital age.[47] Since the supreme authority and control over a territory nowadays also requires authority and control over the online activities occurring within or directly affecting this territory, there is no tension between the traditional concept of sovereignty rooted in the territory of the state and its modern counterpart of digital sovereignty.[48] On the contrary, the notion of digital sovereignty is still tied directly to a state's territory. Digital sovereignty refers to the authority and control over online activities that either originate in the state's territory or that affect persons, organizations, or infrastructures within the state's territory.

16 There are two main objections leveled against this and similar understandings of digital sovereignty. First, one could argue that sovereignty applied to the digital space must be fundamentally different from traditional understandings, as the sovereignty of states is *de facto* shared with private organizations, which have gained control over essential activities and infrastructures of the digital space.[49] Although it is true that some digital platforms have attained extraordinary economic and social power in the digital space, this claim is unconvincing. No private company in the digital space holds the supreme authority and control required to qualify as sovereign. In the digital space, states continue to set authoritative laws for their people and no private company has been recognized as having such authority, i.e., the *right* to command and be obeyed.[50] Furthermore, sovereignty not only requires a great amount of control over a (digital) territory, rather it requires that the sovereign's authority and control is the highest.[51] As, for example, the severe restrictions imposed on foreign digital companies in China and Russia as well as the US law aimed at banning TikTok have shown, the supreme authority over their digital territories still lies with states, not with private organizations.[52]

17 The second objection is raised against the very possibility of state sovereignty in the digital space. According to Milton Mueller, no state actor can have the monopoly on force over all of cyberspace to be considered sovereign.[53] Rather, there is only a shared global cyberspace and states can merely leverage their sovereignty over actors and infrastructures in their territory to influence the use of certain sites or applications.[54] Although it is true that supreme authority over the entire global digital space cannot realistically be achieved by a single state, it does not follow that the complete rejection of the concept

44 Randelzhofer (n. 33), 154 para. 25; Martin Nettesheim, '§ 5 Die Souveränität' in Klaus Stern, Helge Sodan & Markus Möstl (eds), Das Staatsrecht der Bundesrepublik Deutschland I (2nd edn, 2022) 261, 273 para. 37.

45 Krasner (n. 34), 15-16.

46 Floridi (n. 10), 375.

47 See also Hummel et al. (n. 20), 7.

48 Chander & Sun (n. 27), 291.

49 See, e.g., Luciano Floridi's claim that "corporate digital sovereignty" is a "political reality", Floridi (n. 10), 373; see also Anna Tiedeke, 'Die (notwendige) Relativität digitaler Souveränität', (2021) Multimedia und Recht [MMR] 624, 626.

50 See also Huw Roberts, 'Digital Sovereignty and Artificial Intelligence: A Normative Approach', (2024) 70 Ethics and Information Technology 1, 6-8.

51 Philpott (n. 31), 561-62.

52 See also Andrew K. Woods, 'Litigating Data Sovereignty', (2018) 128 Yale L.J. 328, 360-63 ; Thiel (n. 5), 52-53; Ciaran Martin, 'Geopolitics and Digital Sovereignty' in Hannes Werthner, Erich Prem, Edward A. Lee & Carlo Ghezzi (eds), Perspectives on Digital Humanism (2022) 227, 229. As Jack Goldsmith and Tim Wu already emphasized in 2006, governments are able to exercise control over the internet through their control of the physical infrastructures underlying the network within their borders, see Goldsmith & Wu (n. 6), 50-58, 65-85.

53 Mueller (n. 9), 790.

54 Mueller (n. 9), 790.

of digital sovereignty is necessary or appropriate. The usefulness and timeliness of the concept of digital sovereignty derives from its suitability for capturing the current efforts of states to control digital activities emanating from and affecting their territories. It is neither necessary nor useful to define the concept of digital sovereignty, as Milton Mueller does, in a way that is wholly detached from states' territories.[55] Instead, the term digital sovereignty can reasonably be used to refer to the authority and control that a state exercises over its domestic digital space or territory, i.e., over the online activities of persons within its geographical territory and over online activities originating from third countries that directly affect persons, organizations, and objects located within the territory of the EU. Such activities include, for example, the provision of foreign digital services in the EU, the posting and publishing of online content accessible from within the EU, and data flows to and from servers located in the EU.

3. Digital Sovereignty of the EU

18 Applying the concept of digital sovereignty to the EU raises the unresolved question of whether and how the EU itself can be (digitally) sovereign. After all, the effects of the European integration on the sovereignty of the EU and its Member States are complex and controversial.[56] Whereas, for example, the German Constitutional Court rejects the notion of a sovereign EU and assumes that all sovereignty continues to remain with the Member States[57], many European law scholars hold the view that sovereignty is in fact shared or pooled between the EU and its Member States.[58] For the purposes of this Article, the internal sovereignty relationship between the EU and the member states need not be explored further. In relation to the pursuit of European digital sovereignty against foreign states and private enterprises, the EU and its Member States can be regarded as a single entity. In this Article, European digital sovereignty will therefore be understood as the autonomous and effective exercise of sovereign power by EU institutions together with the Member States.

III. Technological and Economic Independence

19 Although related in practice, the technological and economic independence of a state or the EU is conceptually different from its (digital) sovereignty. After all, the authority of a sovereign state to enact and enforce laws of its own volition is not abrogated by *de facto* economic or technological dependencies.[59] As long as goods and services are autonomously and effectively regulated by a state, its sovereignty is not undermined by the fact that those goods and services are offered by foreign businesses.[60] Nevertheless, a lack of technological and economic independence can indirectly affect Europe's control over the digital space, just as it can lead to a loss of economic prosperity. For example, the presence of European tech companies could facilitate the enforcement of EU law, as authorities of the Member States have the legal authority to issue and execute legal orders against domestic companies on their territory. Besides, EU cybersecurity may benefit from more digital services provided from within the EU.

C. EU Legislation and the Quest for Digital Sovereignty

20 Full digital sovereignty, defined as the complete authority and ability of the EU and its Member States to autonomously shape the rules of the digital space within their territory and to effectively enforce those rules, represents an ideal state that is neither fully achievable in practice nor necessary for a state to be considered sovereign.[61] The possession of (digital) sovereignty is best understood as a gradual property and not as a binary property. Although the EU and its Member States still exercise a

55 Only if based on this understanding, would the concept of digital sovereignty denote something that is unachievable and contradictory.

56 See, e.g., Dieter Grimm, *The Constitution of European Democracy* (2017) 39-56.

57 According to the German Federal Constitutional Court, the Member States merely delegate individual (incomplete) state powers to the EU; see Bundesverfassungsgericht [Federal Constitutional Court], Jun. 30, 2009, 123 BVerfGE 267, 380-406; see also Ferdinand Wollenschläger, 'Artikel 23 GG' in Horst Dreier (ed), Grundgesetz Kommentar II (3rd edn, 2015), para. 88-93.

58 See John Peterson, 'The European Union: Pooled Sovereignty, Divided Accountability', (1997) 45 Political Studies 559; William Wallace, 'The Sharing of Sovereignty: the European Paradox', (199) 47 Political Studies 503; Lisa-Marie Lührs, 'Europäische Souveränität als mehrdimensionaler Rechtsbegriff', (2022) Europarecht [EuR] 673, 680; Utz Schliesky, *Souveränität und Legitimität von Herrschaftsgewalt* (2004) 507-586.

59 Morgenthau, (n. 39), 319-22.

60 Chander & Sun (n. 27), 310.

61 The claim that Europe's control over the digital space is weakened does not imply that it has lost its (digital) sovereignty (fully). As Rocco Bellanova et al. put it: "*Sovereignty is an unfulfilled political goal, insofar it is never truly absolute nor undisputed*", see Bellanova, Carrapico & Duez (n. 1), 340.

considerable amount of sovereignty over the digital space, there are valid concerns that Europe's digital sovereignty, specifically its control over the digital space, has been relatively weakened.[62] The objective of strengthening Europe's digital sovereignty refers to efforts to increase the relative level of control exercised by the EU and its Member States over the digital space. In particular, but not exclusively, the EU is seeking to strengthen its internal sovereignty, as it sees powerful private businesses as the main threat to its digital sovereignty.[63]

21 Although the term digital sovereignty is rarely mentioned explicitly in the EU's legislative acts[64], this Section will attempt to show that digital sovereignty can be regarded as an overarching objective and framework of EU digital policy that connects different EU legal acts.[65] This approach is consistent with recent findings that there have been broad shifts in EU digital policy towards more autonomy and control, even if the language of digital sovereignty has not been used to the same extent in all relevant policy sub-areas.[66] Based on the definition of digital sovereignty developed above, it will be outlined how the EU attempts to autonomously (re-)shape the rules of the digital space through legislation (**I.**). Subsequently, the EU's efforts to improve its legal enforcement mechanisms and to promote compliance with its laws in the digital space will be examined (**II.**). Furthermore, since the cybersecurity of the EU and its Member States is an important building block for Europe's internal and external sovereignty, the EU's measures to protect the cybersecurity of state institutions and critical infrastructures will be explored (**III.**). Finally, because they are closely related to the EU's pursuit of digital sovereignty and because EU institutions do not make as clear a distinction between digital sovereignty and technological independence as the definition above[67], key legal efforts to improve Europe's technological independence will be described briefly (**IV.**).

I. Shaping the Rules of the Digital Space

22 Central to the EU's quest for digital sovereignty are its efforts to re-shape the rules of the digital space in accordance with the European values and principles enshrined in Articles 2 and 3 of the Treaty on European Union (TEU).[68] Strictly speaking, these legislative efforts are themselves an exercise of the EU's digital sovereignty, as they are an instance of the EU using its authority to shape the rules of the domestic digital space. They are still included here as part of the EU's pursuit of greater digital sovereignty, because they are intended to align the rules of cyberspace more closely with the autonomous values and interests of the EU. By supplanting the informal digital order shaped by tech companies with formal legislation, these legislative efforts serve to extend the EU's autonomous control over its domestic cyberspace, thereby promoting the EU's digital sovereignty.

23 The values pursued by the EU include, in particular, the strong protection of individual human rights, the safeguarding of democracy, and the promotion of competition and fairness in digital markets. In view of the EU's legislative competencies, it is not surprising that these objectives are pursued primarily via the regulation of the single market.[69] There is a natural fit between this market-based regulatory approach and the EU's sovereignty objective, because the EU's attempts to re-shape the rules of digital space are primarily directed against the activities of powerful digital businesses and not against foreign states.[70] According to the European Commission, it is the informal digital order created by digital platforms that has led to harms for individual rights, democracy, and competition

62 In general, claims about the weakening of a state's sovereignty typically refer to a lack of control, not to a lack of authority, see Krasner (n. 34), 12.

63 Chander & Sun (n. 27), 307.

64 Only Recital 2 of the Chips Act explicitly mentions the enhancing of digital sovereignty as one of its objectives. There, digital sovereignty is understood as technological independence, see European Commission, Chips Act Explanatory Memorandum, COM(2022) 46 final, 4. The Explanatory Memorandum to the AI Act emphasizes the need for common action at Union level to "*protect the Union's digital sovereignty and [...] to shape global rules and standards*"; see European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 6.

65 This claim in no way implies that the strengthening of digital sovereignty is the only or primary objective of these legal acts.

66 Gerda Falkner et al., 'Digital Sovereignty – Rhetoric and Reality', (2024) 31 Journal of European Public Policy 2099.

67 See Theodore Christakis, 'European Digital Sovereignty, Data Protection, and the Push toward Data Localization' in Anupam Chander & Haochen Sun (eds), *Data Sovereignty* (2023) 371, 372.

68 Consolidated Version of the Treaty on European Union OJ C 202, 7.6.2016, 13. See also Celeste (n. 4), 221; Pohle (n. 6), 7.

69 Most legal measures discussed here are based on Article 114 TFEU, according to which the EU may adopt legal measures which have as their object the establishment and functioning of the internal market. This includes the DSA, DMA, DGA, DA, AI Act Proposal, and EMFA Proposal. In addition to Article 114 TFEU, the AI Act Proposal is also based on Article 16 TFEU. The GDPR is based exclusively on Article 16 TFEU.

70 Chander & Sun (n. 27), 307.

in Europe.[71]

1. Protecting Fundamental Rights

24 The EU's most fundamental goal is to build a human centered digital economy that respects individual human rights, in particular human dignity and privacy.[72] Cornerstone of this rights-based approach is still the General Data Protection Regulation (GDPR)[73], which predates von der Leyen's presidency and seeks to protect the personal data of natural persons within the EU in accordance with Article 8(1) of the Charter of Fundamental Rights of the EU (the Charter) and Article 16(1) of the Treaty on the Functioning of the EU (TFEU).[74] Building on the EU Data Protection Directive[75], the EU introduced the GDPR to respond to the rapid technological developments and the ever-increasing collection and sharing of personal data by implementing strong safeguards for the protection of personal data.[76] By establishing strict principles and narrow justifications for the processing of personal data, the GDPR restricts both the commercial exploitation of personal data and the unrestrained use of personal data for state surveillance purposes.[77] In particular, the GDPR seeks to counter the data capitalism of the digital economy, in which businesses profit from personal data at the expense of data subjects' privacy and their control over personal information.[78]

25 While the GDPR will remain the central regulation for protecting personal data for the foreseeable future, the EU has recently adopted complementary regulations aimed at increasing data protection levels within the EU. The Data Governance Act[79] shall set up a legal framework for data intermediaries to strengthen the control of data subjects over their personal data.[80] Furthermore, the Digital Services Act (DSA)[81] imposes special risk management obligations on so-called Very Large Online Platforms (VLOPs), which are intended to safeguard the privacy and other fundamental rights of individuals.[82] Both the GDPR and the DGA not only promote the EU's digital sovereignty but also strengthen the data autonomy of individuals to some extent.[83]

26 The regulation of Artificial Intelligence is the other main area where the EU is trying to establish a robust legal framework for protecting individual rights with the Artificial Intelligence Act (AI Act)[84].[85] Under the risk-based and multi-tiered approach of the AI Act, AI systems with unacceptable risks are fully prohibited, high-risk AI systems are subject to strict regulation, and low-risk systems must comply only with moderate obligations.[86] AI practices that are

71 European Commission, COM(2020) 66 final, 3, 5.

72 See, e.g., European Commission, COM(2020) 66 final, 4; Recital 4 GDPR; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 1.

73 Regulation (EU) 2016/679.

74 See Article 1(1) and (2) GDPR, Recitals 1 and 2 GDPR.

75 Directive 95/46/EC.

76 See only Recital 6 GDPR and Gerrit Hornung & Indra Spiecker gen. Döhmann, 'Introduction' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), *General Data Protection Regulation: Article-by-Article-Commentary* (2023) 1, 64 para. 195; see further on the history of EU data protection legislation and its objectives Orla Lynskey, *The Foundations of EU Data Protection Law* (2016) 47-75.

77 See Articles 5 and 6 GDPR as well as Recitals 39-50 GDPR.

78 On the notion of data or surveillance capitalism see further European Parliament Research Service (n. 2), 3; Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).

79 Regulation (EU) 2022/868.

80 See Recitals 5, 32, 38 DGA. See further Lukas von Ditfurth & Gregor Lienemann, 'The Data Governance Act: Promoting or Restricting Data Intermediaries?', (2022) 23 Competition and Regulation in Network Industries 270; Heiko 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; Gabriele Carovano & Michèle Finck, 'Regulating data intermediaries: the impact of the Data Governance Act on the EU's data economy', (2023) 50 Computer Law & Security Review 105830.

81 Regulation (EU) 2022/2065.

82 See Articles 34(1)(b) and 35 DSA as well as Recital 81 DSA.

83 The main examples of GDPR provisions aimed at promoting individual data autonomy include Articles 6(1)(a), 9(1), 13, 14, 16, 17, and 21 GDPR. However, the extent to which the GDPR promotes individual data autonomy should not be overstated. Neither the official objectives of the GDPR nor its main principles explicitly mention the self-determined control of data by the data subjects as a basic concern of the GDPR. Furthermore, the lawful processing of data does not necessarily require the consent of the data subject, but may also be based on, e.g., legitimate interests of the processor; see further Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?', (2021) 12 JIPITEC 246, 249-59; Opinion of Advocate General Campos Sanchez-Bordona, Case C-300/21 – UI v. Österreichische Post (Oct. 6, 2022), ECLI:EU:C:2022:756, para. 68-77.

84 Regulation (EU) 2024/1689.

85 Recitals 1, 2, 3, and 8 AI Act; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final,1; European Commission, COM(2020) 65 final, 1; Jonas Schuett, 'Risk Management in the Artificial Intelligence Act', (2023) European Journal of Risk Regulation 1, 5-6;. For a closer look at the risks posed by AI to the values of privacy and democracy see Karl Manheim & Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy', (2019) 21 Yale J.L. & Tech. 106.

86 See Recital 26 AI Act; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 12; Schuett,

fully prohibited because of their negative impact on individuals and their rights include, for example, the use of AI systems that deploy subliminal techniques in order to materially distort a person's behavior in a manner that is likely to cause harm as well as AI systems that exploit the vulnerabilities of a specific group of persons due to their age or physical or mental disability.[87] AI practices that are considered to be high-risk due to their potential negative effects on individuals relate to, *inter alia*, the use of AI for determining access of natural persons to educational institutions, for making decisions on promotions and terminations of employees, and for evaluating the creditworthiness of natural persons.[88] Through these obligations, the AI Act is designed to protect the human dignity, autonomy, safety, and equality of natural persons from the intentional or negligent misuse of AI systems.[89]

2. Safeguarding Democracy

27 In keeping with its mandate under Article 3(1) TEU, the EU has introduced novel rules to protect the interrelated public values of democracy and media freedom and pluralism, which are threatened by foreign state interference as well as by content selection and display mechanisms of information intermediaries, such as social networks. The low costs of disseminating information on the internet and the lack of epistemic authorities controlling the accuracy of that information have enabled the spread of misinformation and disinformation, the latter sometimes being sponsored by hostile foreign states.[90] The spread of misinformation and disinformation has been acerbated by the inability or unwillingness of social networks to effectively stop the spread of false information on their platforms and their tendency to create filter bubbles and echo chambers around their users.[91] It is feared that these features of digital interaction have led to sharp increases in political manipulation and polarization that threaten the foundations of democracy.

28 In the absence of legislative foreign policy competences[92], the EU has used its internal market competence to impose due diligence obligations on VLOPs through the DSA in order to curb the spread of misinformation and disinformation and to reduce their potential for distorting democratic processes.[93] Providers of VLOPs, in particular social networks and search engines, need to carry out risk assessments for identifying any actual or potential negative effects on civil discourse and electoral processes stemming from the functioning of their service and its related systems.[94] If any relevant risks have been identified, the providers of VLOPs are under an obligation to put in place reasonable, proportionate, and effective mitigation measures specifically addressing these risks.[95] In addition, in the event of a crisis that poses a serious threat to public security or public health, the European Commission may order VLOPs to assess the impact of their services on the crisis and to take measures to mitigate that impact.[96]

29 The obligations of VLOPs under the DSA demonstrate

(n. 85), 4; David Bomhard & Marieke Merkle, Europäische KI-Verordnung: Der aktuelle Kommissionsentwurf und praktische Auswirkungen, (2021) Recht Digital [RDi] 276, 279.

87 See Article 5(1)(a) and (b) AI Act; see further Kalojan Hoffmeister, 'The Dawn of Regulated AI: Analyzing the European AI Act and its Global Impact', (2024) Zeitschrift für europarechtliche Studien [ZEuS] 182, 197-199.

88 Article 6(2) AI Act in conjunction with Annex III No. 3, 4, and 5. These high-risk systems are regulated strictly. For example, in order to minimize the risks of errors, biases, and discrimination stemming from technical inaccuracies of AI systems due to inaccurate training data or weaknesses of the underlying algorithms, Articles 9 and 10 AI Act require developers and users to establish a risk management system and to set in place appropriate data governance practices; see further Hoffmeister (n. 87), 202.

89 See Recitals 28, 31, 48, 59 AI Act.

90 On the lack of epistemic authorities on the internet see Brian Leiter, 'The Epistemology of the Internet and the Regulation of Speech in America', (2022) 20 Geo. J.L. & Pub. Pol'y 903, 918-921; on misinformation and disinformation see Andrew M. Guess & Benjamin A. Lyons, 'Misinformation, Disinformation, and Online Propaganda' in Nathaniel Persily & Joshua Tucker (eds), *Social Media and Democracy* (2020) 10.

91 For an overview see Luis Roberto Barrosoa & Luna van Brussel Barroso, 'Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth', (2023) 24 Chi. J. Int'l L. 51, 56-61. The extent to which filter bubbles and echo chambers actually exist is heavily debated. For an overview of the current state of research *see* generally Pablo Barbera, 'Social Media, Echo Chambers, and Political Polarization' in Nathaniel Persily & Joshua Tucker (eds), Social Media and Democracy (2020) 34; Peter M. Dahlgreen, 'A critical review of filter bubbles and a comparison with selective exposure', (2021) 42 Nordicom Review 15.

92 See Article 24(1) TEU.

93 See Recital 9 DSA.

94 See Article 34(1)(b) DSA and Recitals 9, 82, and 104 DSA. Among others, the EU Commission has designated Facebook, YouTube, Instagram, and TikTok as VLOPs. For a critical assessment of the DSA's approach to fighting disinformation see Alain Strowel & Jean De Meyere, 'The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?', (2023) 14 JIPITEC 66, 71-77.

95 See Article 35(1) DSA.

96 See Article 36 DSA; see further Strowel & De Meyere (no. 92), 77.

the EU's willingness to implement a European approach to regulating speech on the internet vis-à-vis the mostly American VLOPs, whose moderation of content practices are influenced by the American legal culture and its emphasis on the strong protection of free speech.[97] Whereas the First Amendment of the US Constitution imposes strict limits on the regulation of the content of speech, including for many types of false speech, the European legal culture is more open to regulating speech as the freedom of expression is not considered an absolute right and may be limited for reasons of public interest.[98]

30 The regulation of VLOPs under the DSA is complemented by the European Media Freedom Act (EMFA).[99] With the EMFA, the EU aims to protect media freedom and plurality from restrictions by Member States, but also from certain risks resulting from the increasing dependencies of media outlets on online information intermediaries.[100] Indirectly, the EMFA contributes to the protection of democracy, as media services perform important democratic functions as reliable news sources and public watchdogs.[101] The EMFA complements the DSA by regulating the treatment of certain independent and credible media services by VLOPs. It seeks to preserve media freedom and plurality by protecting independent media providers from deliberate and inadvertent abuses of the position of VLOPs as important gateways to journalistic content.[102] In particular, VLOPs must be transparent in their decisions to suspend their intermediation services with respect to content provided by such media service providers and they must remove any unjustified restrictions or suspensions.[103]

3. Promoting Fairness and Competition in Digital Markets

31 The EU has further adopted important legislation to promote European ideals of market fairness and competition in increasingly concentrated digital markets, including data markets. Whereas the Digital Markets Act (DMA)[104] imposes *ex ante* regulation on digital platforms that act as gatekeepers in already important digital markets, the DGA and the Data Act (DA)[105] regulate different aspects of the nascent European data economy in order to enable the emergence of well-functioning data markets.

32 The DMA targets the multi-dimensional power positions of the major digital platforms that supposedly constitute a threat to Europe's consumers and its lagging digital economy. In particular, the DMA reacts to the competition risks posed by the strong positive economies of scale and network effects of digital platform markets.[106] In combination with certain unfair practices employed by the providers of large and important digital platforms (gatekeepers), these effects have undermined the contestability and fairness of markets for certain crucial digital services, so-called core platform services.[107] These core platform services include,

97 Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', (2018) 131 Harv. L. Rev. 1598, 1618-1622.

98 Ioanna Tourkochoriti, 'The Digital Services Act and the EU as the Global Regulator of the Internet', (2023) 24 Chi. J. Int'l L. 129, 131-32. On the protection of false speech under the First Amendment see Leslie G. Jacobs, 'Freedom of Speech and Regulation of Fake News', (2022) 70 Am. J. Comp. L. 278, 280-86: Erwin Chemerinsky, 'False Speech and the First Amendment', (2018) 71 Okla. L. Rev. 1. Under EU law, limitations imposed on the right to freedom of expression pursuant to Article 11 of the Charter and Article 10(1) of the European Convention on Human Rights are permissible, if they are proportionate and necessary to fulfill certain objectives of public interest; see Lorna Woods, 'Art 11 – Freedom of Expression and Information' in Steve Peers, Tamara Hervey, Jeff Kenner & Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, 2021), para. 11.59 et seq.

99 Regulation (EU) 2024/1083.

100 See Recitals 2, 3, and 18 EMFA. The EMFA's shall contribute to the upholding of Article 11(2) of the Charter, according to which, the freedom and pluralism of the media are to be respected.

101 See Recitals 1, 40; European Commission, EMFA Explanatory Memorandum, COM/2022/457 final, 6; European Commission, COM(2020) 790 final, 11.

102 See Recitals 3, 50, and 55 EMFA.

103 Article 17(4) and (6) EMFA.

104 Regulation (EU) 2022/1925.

105 Regulation (EU) 2023/2854.

106 See Recital 2 DMA. For an overview of the competitive issues raised by these characteristics of platform markets see generally Stigler Committee on Digital Platforms, *Final Report* (2019), 34-43 <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf>; and Geoffrey Parker, Georgios Petropoulos & Marshall Van Alstyne, *Digital Platforms and Antitrust*, (2020) Bruegel Working Paper 06/2020 <https://www.bruegel.org/sites/default/files/wp_attachments/WP-2020-06-1.pdf>.

107 See Recitals 2 and 15 DMA. Gatekeepers are the providers of core platform services which meet certain qualitative and quantitative criteria and have been designated as such by the EU Commission, see Article 3 and Recitals 15 and 16 DMA. To date, the EU Commission has designated as gatekeepers Alphabet (Google), Amazon, Apple, ByteDance, Meta (Facebook), Microsoft, and Booking.com; see European Commission, 'Digital Markets Act: Commission designates six gatekeepers' (Sep. 6, 2023) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328>;

inter alia, search engines, social networks, web browsers, and video-sharing platforms.[108] Due to the lack of contestability and fairness on these core platform markets, their (competitive) functioning is impaired to the detriment of prices, quality, and innovation in the digital sector.[109] It is the goal of the DMA to ensure and restore the contestability and fairness of core platform markets by placing *ex ante* obligations on the provision of core platform services by gatekeepers.[110] These obligations correspond to certain practices of gatekeepers which are seen as harmful.[111] Obligations aimed at improving the contestability and fairness of core platform markets include, *inter alia*, restrictions on the data collection practices of gatekeepers, data access rights for end users and business users, and rules aimed at enabling the switching and multi-homing of end users and business users.[112]

33 The DGA is another piece of legislation that seeks to ensure competition and fairness on digital markets. While its primary goal is to promote trust in data intermediation services in order to facilitate the emergence of functioning data markets[113], the DGA also aims to ensure that data intermediation services will be provided in a competitive and fair environment.[114] The EU is determined to prevent undesirable market developments at an early stage by introducing a strict *ex ante* regulation for data intermediaries.[115] Hence, the DGA is designed to protect vertical and horizontal competition on data intermediation markets and to fend off the entry and domination of data intermediation markets by already powerful digital conglomerates.[116] In addition, data markets are to be regulated by the DA, which sets rules for the fair access to data generated by the use of products connected to the internet and for the invalidity of unfair contractual terms regarding the sharing of data.[117] Essentially, the DA seeks to empower the users of connected products and to spread the benefits derived from data generated by the Internet of Things more fairly.[118] In particular, manufacturers of connected products are obligated to make the data generated by the use of a connected product available to the respective product user free of charge.[119] These data can then be used by third parties to provide aftermarket or ancillary services.[120] Unlike the DMA and DGA, the DA is not aimed directly against the major digital platforms.[121] Rather, the DA addresses the lack of data sharing by manufacturers, many of which are European companies from traditional industry sectors.[122]

II. Effective Enforcement of European Law in the Digital Space

34 The EU further seeks to strengthen its digital sovereignty by improving its enforcement mechanisms to promote legal compliance in the

European Commission, 'Commission designates Booking as a gatekeeper' (May 13, 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2561>.

108 See Article 2(2) and Recitals 13 and 14 DMA.

109 See Recitals 3 and 4 DMA. Contestability refers to the presence of low market entry barriers as a condition for vigorous and dynamic inter-platform competition for core platform markets; see Recital 32 DMA and Jacques Crémer et al., 'Fairness and Contestability in the Digital Markets Act', (2023) 40 Yale J. on Reg. 101, 117-31. Unfairness is understood in the DMA as an imbalance in the bargaining power of gatekeepers and other market participants, which leads to an unfair and one sided distribution to gatekeepers of the benefits resulting from innovation and other efforts in core service markets; see Recital 33 DMA and Crémer et al., id., 108-17; Rupprecht Podszun et al., 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers', (2021) Journal of European Consumer and Market Law [EuCML] 60, 62.

110 See Articles 5(1) and 6(1) DMA. The DMA departs from traditional antitrust law approaches to regulation and instead relies on an ex ante regulatory approach similar to those for network industries; see Wolfgang Kerber, 'Taming tech giants with a per se rules approach? The Digital Markets Act from the "rules vs. standard" perspective', (2021) N° 3-2021 Concurrences 28; Podszun et al. (n. 109), 61.

111 See Recital 31 DMA.

112 See Articles 5 and 6 DMA and Recitals 36-64 DMA.

113 See infra Part C.IV.3.

114 See Recital 33 DGA; von Ditfurth & Lienemann (n. 80), 280-81.

115 For an extensive analysis see von Ditfurth (n. 19), 207-209 (2023).

116 von Ditfurth & Lienemann (n. 80), 288-90.

117 See Articles 3-13 DA. Other provisions of the DA related to the fair and pro-competitive regulation of the digital economy are the rules on switching between data processing services (Articles 23-31 DA), such as cloud services. For an analysis of the data access rights under the DA see Moritz Hennemann et al., *Data Act: An Introduction* (2024) 71-140.

118 See European Commission, Data Act Explanatory Memorandum, COM(2022) 68 final, 2-3; Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives', (2023) 72 GRUR International 120, 122.

119 See Articles 3 and 4 DA and Recitals 5, 6, and 20 DA.

120 See Recital 6 DA.

121 Nevertheless, the DA does include a mechanism to prevent that data access rights can be exploited by powerful digital platforms. According to Article 5(3) DA, product users may not request the sharing of the product data with undertakings that have been designated as gatekeepers under the DMA. Furthermore, gatekeepers may not oblige or incentivize product users to share their product data with them.

122 See Recital 2 DA; European Commission, SWD(2020) 295 final, 9-10; European Commission, SWD(2022) 34 final, 9-10.

digital space. Specifically, the EU is concerned with removing barriers to legal enforcement that are caused by distinctive features of the digital space, i.e., the transnational nature of cyberspace and the mobility of data. As a result of these features, the national territory as the physical place where states wield their authority has become less important for enforcing legally compliant online behavior. The EU has reacted to these developments by adopting legal measures aimed at improving European control over data access and global data flows (**1.**), extending the territorial scope of EU law (**2.**), requiring foreign organizations to designate representatives within the EU (**3.**), and obliging providers of digital platforms to regulate and moderate the content available on their platforms (**4.**).

1. Controlling Data Access and Data Flows

35 States have been struggling to control and monitor the (cross-border) movements of data for years. This issue has been exacerbated by increases in cloud usage for the storage of individual and organizational data.[123] Because of their mobility and divisibility, data are moved around in the cloud and stored in different server locations, including extraterritorial locations.[124] The global nature of the internet and the uptake of cloud usage have led to a situation where an individual or an organization and their data "*are now often separated by great distances and possibly several jurisdictions*".[125] Consequentially, a large amount of data held by EU citizens is located abroad which affects European law enforcement in two important ways. First, law enforcement agencies struggle to access data required as evidence for criminal proceedings.[126] Second, once data leave the jurisdiction of the EU and enter the jurisdiction of a third state, European agencies lack the effective means to ensure that third countries and private organizations comply with European legal rules.[127] The EU has taken legislative measures to address both of these issues.[128]

a.) Ensuring Access to Digital Evidence

36 The EU has adopted the E-Evidence Regulation[129] to ensure the effective access by Member States' law enforcement agencies to digital evidence stored in other EU and non-EU countries. The E-Evidence Regulation introduces an EU-wide legal framework for direct cooperation between judicial authorities in one Member State and digital service providers in another Member State, without actively involving the latter state.[130] Under certain conditions, the competent authorities of a Member State may directly order service providers offering their services in the EU to produce or to preserve certain electronic evidence data.[131] Service providers covered by the E-Evidence Regulation include, *inter alia*, instant messaging and email services as well as online marketplaces and hosting services provided via cloud computing.[132]

37 Importantly, the obligations to produce or preserve electronic evidence apply to service providers regardless of the location of the requested data as long as these data are related to services offered in the EU.[133] Thus, service providers may be required to hand over data to European law enforcement agencies that are located on servers in third countries. With

123 Woods (n. 52), 352. According to Statista, in 2022, 60% of worldwide corporate data were stored in the cloud, see <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data>.

124 Jennifer Daskal, 'The Un-Territoriality of Data', (2015) 125 Yale L.J. 326, 366-69.

125 Andrew K. Woods, Against Data Exceptionalism, 67 Stan. L. Rev. 729, 742 (2016); see also Daskal (n. 124), 373; Aude Géry & Florian Nicolai, 'Law Enforcement and Access to Transborder Evidence: the Quest for the Exercise of Digital Sovereignty?', (2023) 28 Geopolitics 941, 941-42.

126 Woods (n. 125), 739; Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective', (2022) 85 Modern Law Review 997, 1002-3; Géry & Nicolai, (n. 125), 941-42.

127 See with respect to the protection of personal data Peter Schantz, 'Article 44' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), *General Data Protection Regulation: Article-by-Article-Commentary* (2023) 775, 776 para. 4; Christopher Kuner, 'Article 44' in Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (2020) 755, 757.

128 The control exercised by a state over data flows within its borders and data flows from and to its territory is sometimes referred to as "data sovereignty", see Couture & Toupin (n. 1), 2312-13; Chander & Sun (n. 27), 293. In this Article, data sovereignty is understood to be just one aspect of the broader concept of digital sovereignty.

129 Regulation (EU) 2023/1543.

130 Theodore Christakis, *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive* (2023) 1-2 <https://ssrn.com/abstract=4306874>.

131 See Article 4 E-Evidence Regulation. The conditions for issuing evidence production orders or preservation orders are laid down in Article 5 and 6 E-Evidence Regulation respectively. Such orders may be issued for, e.g., the pursuit of criminal offences and must be necessary and proportionate. The orders may cover, inter alia, the production or preservation of IP data, traffic data, and content data, such as text, videos, or images.

132 See Article 2(4) E-Evidence Regulation and Recital 27 E-Evidence Regulation.

133 See Article 1 (1) and Recitals 21, 26 E-Evidence Regulation.

its extraterritorial reach, the E-Evidence Regulation mirrors the US CLOUD Act of 2018[134], which requires service providers to disclose all data in their control to US law enforcement agencies regardless of the location of the data.[135] Due to its extraterritorial reach, the E-Evidence Regulation will in many cases conflict with foreign laws. For example, the US Electronic Communications Privacy Act (ECPA) generally prohibits service providers from disclosing the content of electronic communications directly to foreign governments.[136] In order to minimize such conflicts, the E-Evidence Regulation provides for a judicial review procedure in cases where complying with evidence production orders would violate foreign laws.[137] However, even if there is an actual conflict between the E-Evidence Regulation and foreign laws, the courts of Member States may still decide to uphold the order to disclose evidence.[138] Thus, in case of conflict, the E-Evidence Regulation claims the primacy of EU law over foreign laws.

b.) Regulating International Data Transfers

38 Data transfers to third countries pose significant risks for the circumvention of the level of data protection under EU law, as there are few means available to European authorities to ensure compliance with EU law in foreign states. The EU and its Member States can only effectively control international data flows as long as the data is still on their territory.[139] Therefore, the EU has adopted legal rules to regulate international transfers of both personal and non-personal data. Most importantly, the GDPR governs the transfer of personal data to third countries.[140] Personal data may only be transferred to a third country, if the EU Commission has decided that the third country ensures an adequate level of data protection or if the controller or processor transferring the data has provided appropriate safeguards to guarantee the effective protection of data.[141] This way, the GDPR aims to ensure that the personal data of Europeans will enjoy a level of protection in third states that is essentially equivalent to that of the EU.[142]

39 With the adoption of the DGA and the DA, the EU has recently extended the regulation of international data flows to non-personal data. Both the DGA and the DA include similar statutes which restrict international transfers of non-personal data to third countries and the access of foreign governments to such data where such transfer or access would create a conflict with or contravene European law.[143] These provisions primarily aim to protect the trade secrets and intellectual property rights of businesses as well as national security interests of Member States.[144]

2. Extending the Territorial Reach of EU Law

40 The global and borderless nature of cyberspace poses another problem for the EU's sovereignty, as it allows digital services to be provided in the EU without the provider being established in the EU.[145] If EU laws merely apply to subjects within its own domestic territory, its rules could be easily circumvented by foreign actors who can offer their digital goods or services within the EU despite being established in third countries. The EU has addressed this potential regulatory gap by extending the scope of its legislation beyond its territory. It includes within the scope of its laws all persons who are active on its territory, regardless of whether they are established in the EU or in a third country. This extension of territorial scope is a key feature of the GDPR. Under its marketplace principle, the GDPR applies not only to data processing activities in the EU, but also to data processing activities by foreign entities that affect data subjects in the EU.[146] In doing so, the GDPR imposes obligations on data controllers and data processors, regardless of their actual geographic location or legal seat.[147] Mirroring

134 Clarifying Lawful Overseas Use of Data Act, contained in Consolidated Appropriations Act, 2018, PL 115-141, Division V.

135 Christakis (n. 130), 18. On the CLOUD Act see Stephen W Smith, 'Clouds on the Horizon: Cross-Border Surveillance under the US CLOUD Act', in Federico Fabbrini, Edoardo Celeste & John Quinn eds, Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (2021) 119.

136 See 18 U.S.C. § 2702(a)(3); Congressional Research Service, Cross-Border Data Sharing under the CLOUD Act (Apr. 23, 2018) 10-11) <https://www.everycrsreport.com/files/20180423_R45173_c8a82f6a7cee392e23453b5836546d6a68e5e779.pdf>.

137 Article 17 and Recitals 74-79 E-Evidence Regulation.

138 Article 17(6) E-Evidence Regulation.

139 Christoph Kuner, *Transborder Data Flows and Data Privacy Law* (2013) 105.

140 See Articles 44-49 GDPR.

141 See Articles 45 and 46 GDPR. For analyses of the GDPR regime for international data transfers see Leonie Wittershagen, *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit* (2022) 52-82; Tobais Naef, *Data Protection without Data Protectionism* (2022) 115-221.

142 See Recital 104 GDPR; Schantz (n. 127), 777 para. 6.

143 See Article 31(1) DGA; Article 32(1) DA.

144 See Recital 20 DGA and Recital 101 DA.

145 Adèle Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation', (2018) 9 JIPITEC 126, 127.

146 See Article 3(2) GDPR.

147 Stephan Koloßa, 'The GDPR's Extra-Territorial Scope: Data Protection in the Context of International Law and

the GDPR's approach, the marketplace principle has also been adopted for the DSA, DGA, DA, and AI Act.[148]

3. Requiring Representation of Foreign Providers of Online Services

41 A further mechanism used by the EU legislator to improve compliance with its rules is the requirement for international businesses to designate representatives within the EU territory.[149] Because of the global reach of the internet, it can be difficult to enforce obligations under EU law against foreign providers of digital services that do not have an establishment in the EU but are still subject to EU law due to the marketplace principle.[150] In particular, European authorities may struggle to communicate with foreign service providers and they lack the legal authority to deliver official orders on foreign territories.[151] Thus, the purpose of designating representatives is to promote the effectiveness and efficiency of information requests by European authorities. The designated representatives shall serve as points of contacts for all requests concerning the provision of their services within the EU and their compliance with EU law.[152]

4. Law Enforcement Responsibilities of Online Services

42 Online content can be easily and rapidly copied and shared over the internet. This characteristic enables mass infringements of intellectual property rights and personality rights. Since the early 2000s, there has been a large number of copyright infringements on the internet as a result of wide-spread file sharing practices.[153] In addition, the emergence of social media has been accompanied by an increase in the creation and dissemination of disinformation, misinformation, and online content that violates the personality rights of individuals or that can be classified as hate speech.[154]

43 Due to the large volume and rapid distribution of illegal online content, the effort required to monitor and prevent such legal violations exceeds the resources of law enforcement agencies. This situation has been exacerbated by the relatively liberal regulation of internet intermediaries in the EU and the US. Under the EU E-Commerce Directive[155] as well as the US Communication Decency Act[156] and the US Digital Millennium Copyright Act[157], online service providers were largely exempted from liability for illegal conduct of their users.[158] Partially departing from its traditionally liberal stance towards intermediary regulation, the EU has recently adopted legislation to improve online compliance by requiring certain internet intermediaries to ensure the legally compliant behavior of their users themselves. Thereby, the EU legislator is leveraging the *de facto* control exercised by powerful internet intermediaries over the digital space to improve the enforcement of EU law.

44 The DSA is the centerpiece of EU efforts to utilize digital service providers for law enforcement through mandatory self-regulation.[159] In principle,

Human Rights Law', (2020) 80 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht [ZaöRV] 791, 795; Gerrit Hornung, 'Article 3' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), General Data Protection Regulation: Article-by-Article-Commentary (2023) 116, 155 para. 36.

148 See Article 2(1) DSA; Article 11(3) and Recital 42 DGA; Article 1(3) DA; and Article 2(1) AI Act. Other countries, including Japan and Brazil, have also adopted similar mechanisms for ensuring the extraterritorial applicability of their data protection laws; see, e.g., Article 75 of the Japanese Act on the Protection of Personal Information and Article 3 of the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais).

149 See Article 27 GDPR; Article 13 DSA; Article 11(3) DGA; Article 3 of Directive (EU) 2023/1544 (E-Evidence Directive).

150 See Recital 1 E-Evidence Directive; Schantz (n. 127), 776 para. 4.

151 Hannes Krämer, 'Extraterritoriale Wirkungen des Unionsrechts – eine normanalytische Skizze', (2021) Europarecht [EuR] 137, 144.

152 See Recital 80 GDPR and Recital 42 DGA.

153 See, eg., Felix Oberholzer-Gee & Koleman Strumpf, 'File Sharing and Copyright', (2010) 10 Innovation Policy and the Economy 10; Goldsmith & Wu (n. 6), 105-118.

154 See, e.g., Barrosoa & van Brussel Barroso, (n. 91), 56-61; Danielle K. Citron & Helen Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age', (2011) 91 B.U. L. Rev. 1435, 1447-1453; Majid Yar, 'A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media', (2018) 1 International Journal of Cybersecurity Intelligence & Cybercrime 5, 6-9. Typical personality rights include the right to privacy, the right to one's own image, and the prohibition of defamation, see Susanna Lindroos-Hovinheimo, 'Jurisdiction and personality rights – in which Member State should harmful online content be assessed?', (2022) 29 Maastricht Journal of European and Comparative Law 201, 204.

155 Directive 2000/31/EC.

156 47 U.S.C. § 230(c)(2).

157 17 U.S.C. § 512(g)(1).

158 For an in-depth analysis of online intermediary liability in the EU and the US see Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (2020).

159 Similar enforcement obligations are also present in Article 17(4) of the EU Digital Single Market Directive

the DSA retains the liability rules of the preceding E-Commerce Directive, according to which providers of online intermediary services are generally not legally responsible for third-party content, as long as they remain neutral intermediaries and are not aware of the potential illegality of the content.[160] However, the DSA introduces new and stricter procedural obligations for providers of hosting services and providers of online platforms, the latter being a sub-type of hosting services.[161] All providers of hosting services are required to put notice and action mechanisms in place, which allow third parties to inform them of the presence of illegal content on their services and enable the providers themselves to remove such content.[162] In addition, providers of online platforms must implement effective mechanisms and systems to handle internal complaints, to provide out-of-court dispute settlement for affected parties, and to cooperate with trusted flaggers of illegal content.[163] They are also required to suspend the provision of their services to users that frequently upload illegal content.[164] These obligations aimed at ensuring a legally compliant online environment are supplemented by additional obligations for VLOPs, which are obligated to conduct risk assessments to identify whether the dissemination of illegal content occurs through their services and whether their services have any negative effects on fundamental rights.[165] If such risks are identified, the VLOP providers must take effective mitigation measures, such as adapting their algorithmic recommender systems or adding to their content moderation personnel.[166]

III. Securing European State Institutions and Critical Infrastructures

45 The capacity of the EU and its Member States to effectively enforce their laws in cyberspace is an essential prerequisite for strengthening European digital sovereignty. This capacity requires the unimpaired functioning of state institutions and critical infrastructures, which are threatened by cyberattacks.[167] Cyberattacks are launched not only by cybercriminals but also by foreign states that engage in espionage and pseudo-military operations in cyberspace.[168] Hostile cyber activities by foreign states include, for example, large-scale infiltration and surveillance of government networks, power grid disruptions, and disruptions of public health services.[169]

46 The EU's approach to strengthening European cybersecurity is multi-pronged. It includes investments, policy, and legal instruments. One important policy instrument that specifically addresses the cybersecurity risks stemming from foreign technology providers is the 5G Toolbox. It is a set of non-binding recommendations for a common EU approach to ensuring the security of 5G networks in view of potential risks posed by the Chinese supplier Huawei.[170] In this regard, the promotion of Europe's cybersecurity crucially depends on the advancement of its technological independence.[171] On the legislative side, the EU

("upload filters") and Article 12 (j) DGA. On upload filters see Thomas Spoerri, 'On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market', (2019) 10 JIPITEC 173. On enforcement obligations under the DGA see von Ditfurth & Lienemann (n. 80), 287

160 See Articles 4-8 and Recital 17 DSA; Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation', (2021) 12 JIPITEC 361, 369; Martin Eifert et al., 'Taming the Giants: The DMA/DSA Package', (2021) 58 Common Mkt. L. Rev. 987, 1005-8.

161 See Recital 13 DSA. In particular, online platforms encompass social networks and online marketplaces. Other hosting services include cloud computing, web hosting, and file storage and sharing services, see Recital 29 DSA. For an overview over the layered obligations for special types of intermediary services (i.e. hosting services, online platforms, and VLOPs) see Buiten (n. 160), 368; Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules', (2024) 38 Berkeley Tech. L.J. 883, 900.

162 See Article 16 and Recitals 50-54 DSA. Pursuant to Article 17 DSA, they are further required to provide a specific statement of reasons to users affected by content takedowns or similar actions. See further Husovec (n. 161), 900-2; Eifert et al. (n. 160), 1009-13.

163 See Articles 20-22 and Recitals 58-62 DSA.

164 See Article 23 and Recital 64 DSA.

165 See Article 34(1)(a) and (b) and Recitals 80 and 81 DSA. See further Husovec (n. 161), 902-8.

166 See Article 35 and Recitals 87 and 88 DSA.

167 Roberts et al. (n. 38), 12; European Commission, JOIN(2020) 18 final, 4; see also Farrand & Carrapico (n. 16), 447.

168 See only Dennis Broeders & Bibi van den Berg, Governing Cyberspace: Behavior, Power, and Diplomacy in Dennis Broeders & Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 1, 1-2.

169 Lucas Kello, 'Cyber legalism: why it fails and what to do about it', (2021) 7 Journal of Cybersecurity 1, 9.

170 NIS Cooperation Group, Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (2020) <https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf>; European Commission, COM(2020) 50 final; European Commission, JOIN(2020) 18 final, 4. See further Monsees & Lambach (n. 18) 36, 384-86.

171 European Commission, COM(2020) 50 final; European Commission, JOIN(2020) 18 final, 11; NIS Cooperation Group (n. 170), 3.

has issued regulations and directives aimed at strengthening European cybersecurity in general and the cybersecurity of government institutions and critical infrastructures in particular. General measures include the Cybersecurity Act, which has fortified the role of the EU Agency for Cybersecurity (ENISA) and has established a security certification framework for digital products and services offered on the common market.[172] It is being complemented by the Cyber Resilience Act, which introduces horizontal cybersecurity requirements for all digital products and services in the EU.[173]

47 In addition, the EU has adopted legislative acts that are specifically aimed at improving the cybersecurity of EU institutions, Member State institutions, and critical infrastructures. The recent Cybersecurity Regulation requires the institutions, bodies, and agencies of the EU to establish internal cybersecurity risk management and control mechanisms.[174] The cybersecurity levels of the institutions and critical infrastructures of Member States are directly addressed by the NIS 2 Directive from 2022.[175] In particular, the NIS 2 Directive requires each Member State to adopt a national cybersecurity strategy and to establish or designate authorities responsible for cybersecurity and the management of large-scale cybersecurity incidents and crises.[176] Furthermore, Member States shall adopt laws to ensure that essential and important public and private entities take technical, operational and organizational measures to manage cybersecurity risks and minimize the impact of security incident on the recipients of their services.[177] Essential and important entities include, *inter alia*, public administration entities of the central government, providers of important digital infrastructures and certain large companies that are active in the healthcare, transport, or energy sector.[178] The NIS 2 Directive is complemented by sector-specific measures, including the European Electronic Communications Code (EECC)[179] and the Digital Operational Resilience Act (DORA)[180].[181]

48 Finally, the capacity of the EU and its Member States to fend off cyberattacks and related incidents shall be further strengthened by the Cyber Solidarity Act.[182] The Cyber Solidarity Act aims to strengthen European capacities to detect and respond to cybersecurity threats and incidents through the deployment of a pan-European infrastructure of Security Operation Centers to enhance detection capabilities (European Cyber Shield), the creation of a Cybersecurity Emergency Mechanism to support Member States in responding to and recovering from large-scale cybersecurity incidents, and the establishment of a review mechanism for large-scale incidents.[183]

IV. Strengthening Europe's Technological Independence

49 In addition to promoting its digital sovereignty, the EU is implementing legislation specifically aimed at advancing its technological and economic independence by increasing the availability of essential digital technologies, infrastructures, and data within Europe. These measures – although serving a conceptually different purpose – are closely related to the EU's pursuit of digital sovereignty, because an increase in Europe's technological independence and capabilities can also facilitate the EU's *de facto* control over its domestic cyberspace.[184] Key legislative measures to improve Europe's technological independence target the increased production of semiconductor chips in Europe (**1.**), the development and use of AI in Europe (**2.**), and the fostering of a competitive European data economy (**3.**).

1. Availability of Semiconductors

50 As semiconductors have become an essential input

172 Regulation (EU) 2019/881. For an account of the development of EU cybersecurity law see further Lee A. Bygrave, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes', (2025) 56 Computer Law & Security Review 106071.

173 Regulation (EU) 2024/2847. For an introduction to the Cyber Resilience Act see Pier Chiara, 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', (2022) 3 International Cybersecurity Law Review 255.

174 See Articles 5-9 and Recitals 6 and 7 of the Cybersecurity Regulation (Regulation (EU, Euratom) 2023/2841).

175 Directive (EU) 2022/2555.

176 See Articles 7-9 and Recitals 48-57 NIS 2 Directive.

177 See Article 21 and Recitals 77-89 NIS 2 Directive.

178 See Article 3 and Recitals 15-19, 31-35 NIS 2 Directive.

179 Directive (EU) 2018/1972.

180 Regulation (EU) 2022/2554.

181 Among other goals, the EECC shall ensure that providers of public electronic communications networks and services take appropriate technical and organizational measures to manage the (cyber) security risks posed to their networks and services; *see* Article 40 and Recitals 94-98 EECC. The objective of DORA is to achieve a high level of digital operational resilience in the financial sector; see Article 1(1) and Recital 12 DORA. Pursuant to Article 1(2) DORA and Article 4 NIS 2 Directive, the NIS 2 Directive does not apply to financial entities covered by DORA.

182 Regulation (EU) 2025/38..

183 See Article 1(1) and Recitals 7, 8, 13-15, 30, 35-38, and 50 of the Cyber Solidarity Act.

184 See infra Part D.II.

for the production of electronic goods[185], the EU Chips Act[186] presents an important building block in the EU's efforts to improve its technological independence. Its overarching goal is to provide "*a framework for increasing the Union's resilience in the field of semiconductor technologies*".[187] It primarily aims to do so by establishing the *Chips for Europe Initiative*, by improving the security and resilience of supply chains, and by supporting the government structures required for monitoring the semiconductor sector and responding rapidly to potential supply shortages.[188] In particular, the *Chips for Europe Initiative* will provide generous financial support to the establishment of factories for semiconductor production and related research in Europe.[189]

2. Leadership in AI

51 The EU intends to improve the AI capacities of European businesses and to promote the uptake of this new technology in Europe.[190] From a legal side, this goal shall be supported by the AI Act. In addition to mitigating the risks associated with AI, the AI Act aims to promote the development, use, and adoption of AI technologies in Europe by establishing harmonized rules for AI and improving the EU's internal market.[191] Furthermore, the AI Act provides for the establishment of regulatory sandboxes for the development, testing, and validation of innovative AI systems.[192] The purpose of regulatory sandboxes is to "*foster AI innovation by establishing a controlled experimentation and testing environment*" under the supervision of regulatory authorities.[193]

3. Data Economy

52 The EU is further determined to provide European businesses with better access to data as a key resource for innovation in order to reshape the competitive balance of the global data economy.[194] Consequently, the EU aims to increase the level of data sharing within the EU by amending the legal framework for data sharing through the DGA, the DA and the Common European Data Spaces.[195]

53 The DGA aims at facilitating the emergence of functioning data markets by promoting trust in so-called data intermediation services through the strict *ex ante* regulation of these services.[196] Besides improving the control of data subjects over their personal data[197], these regulated data intermediaries shall act as matchmakers on C2B and B2B data markets. In particular, they shall support data holders and data subjects in making their respective data available to potential data users, thereby increasing the availability of data for European businesses.[198] The DA is intended to improve data access for European businesses by removing certain barriers to data sharing which currently prevent an optimal allocation of data.[199] It does so by introducing access rights of product users and certain third parties to the data generated by the use of products connected to the internet.[200] These data access rights shall not only empower the users of connected products and achieve a fairer distribution of the benefits based on data generated by connected products.[201] They shall also unlock large amounts of data for innovation purposes of businesses and thus create significant economic welfare gains for the European economy.[202]

54 Finally, these two cross-sectoral legislative measures aimed at improving data availability are complemented by efforts to establish Common European Data Spaces in sectors of high importance, such as the health sector, the financial sector, or the agricultural sector.[203] This sector-specific approach reflects the need to take into account the individual circumstances of certain sectors and industries and

185 Monsees & Lambach (n. 18), 386.
186 Regulation (EU) 2023/1781.
187 Recital 2 of the Chips Act.
188 See Chapters 2-4 of the Chips Act. For a closer look see Dennis-Kenji Kipker, 'Technologie-Souveränität durch europäische Gesetzgebung? – Der Entwurf des neuen EU Chips Act und sein regulatorisches und politisches Framework', (2022) Kommunikation & Recht [K&R] 47.
189 See Articles 3(2) and 4(1) of the Chips Act.
190 European Commission, COM(2020) 65 final, 1. On the EU's approach to counter the legal and ethical risks associated with the use of AI see supra Part C.I.1.
191 See Recitals 1 and 8 AI Act.
192 See Articles 57-63 AI Act.
193 Recital 139 of the AI Act.
194 Pascal D. König, 'Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept', (2022) 8 European Policy Analysis 484, 497; Roberts et al. (n. 38), 9; von Ditfurth & Lienemann (n. 80), 272.
195 European Commission, COM(2020) 66 final, 12-14, 21-23.
196 See Recitals 5, 32 and Article 12 DGA; see also von Ditfurth & Lienemann (n. 80), 278.
197 See supra Part C.I.1.
198 Recital 27 DGA; European Commission, SWD(2020) 295 final, 1, 19-20; von Ditfurth & Lienemann (n. 80), 277.
199 See Recitals 2 and 4 DA.
200 On the data access rights under the DA see supra Part C.I.3.
201 See supra Part C.I.3.
202 See European Commission, Data Act Explanatory Memorandum, COM(2022) 68 final, 2-3; European Commission, SWD(2022) 45 final, 26-27, 40; Kerber, (n. 118), 122.
203 European Commission, COM(2020) 66 final, 21-23; European Commission, SWD(2022) 45 final, 1; European Commission, SWD(2024) 21 final, 17-38.

to assist them in developing tailor-made rules for data use and sharing.[204]

D. Evaluation

55 As the previous Section has shown, the EU has adopted extensive legislation in order to enhance its control over the digital space and to promote EU values and interests. However, while it is natural for the EU to seek to strengthen its control over cyberspace, the pursuit of digital sovereignty also raises questions about the overall desirability and appropriateness of the EU's approach to regulating cyberspace.

I. The Value of Digital Sovereignty

56 Digital sovereignty is inherently tied to the values of autonomy and the rule of law. The ability to shape the domestic law in a way that is not or only to a relatively limited extent controlled or influenced by foreign actors allows a state to pursue its objectives in a self-determined manner. And a state having the capabilities to effectively enforce its rules for the digital space ensures conformity with its domestic law, which is essential for securing whatever purposes the law is intended to serve.[205] At the same time, these virtues of digital sovereignty can also lend themselves to states' pursuit of immoral or imprudent purposes. Ultimately, the (moral) value of digital sovereignty thus depends on the goals that are being pursued through the exercise of sovereignty. Digital sovereignty can therefore be seen as a second-order goal, one that is pursued in order to further other first-order goals. The range of first-order goals for which digital sovereignty can be pursued is broad. A state's control over the digital space could be used to promote human rights or to maintain autocratic regimes and suppress dissent.[206] In this sense, digital sovereignty is morally neutral.

57 As seen in the previous Section, the EU's pursuit of digital sovereignty is primarily aimed at promoting human rights, democracy, and market fairness and competition as first-order goals. The promotion of these first-order goals is *prima facie* justified and desirable. Yet, whether the EU's pursuit of digital sovereignty will turn out to be successful ultimately depends on the suitability of its legislative measures for promoting these first-order goals. Conclusively answering this complex question would require an in-depth assessment of each legislative act related to the EU's quest for digital sovereignty, a task that cannot be accomplished here.[207] Instead, only some of the more general issues raised by the EU's quest for digital sovereignty will be discussed in this Section.

II. Lack of Coherence

58 The EU's pursuit of digital sovereignty, on the one hand, and of technological and economic independence, on the other hand, suffers from a lack of coherence. It is marred by a tension between the goals of protecting the rights of EU citizens and of promoting Europe's digital economy.

59 In theory, the two objectives of promoting European digital sovereignty and technological independence could complement each other. The existence of leading European technology companies and digital services providers could contribute to the effective enforcement of EU values and rules in cyberspace. For example, the emergence of high-quality European online services would mitigate current enforcement risks due to international data transfers.[208] Moreover, the emergence of European technologies can help spread and implement European values and interests in Europe and globally. European developers of AI systems could be more sensitive to European rights and values and infuse them into their systems. In the digital space, technological capabilities are not only vital for a region's economic competitiveness but also for its political power to shape the rules and

204 European Commission, COM(2020) 66 final, 6. As of today, the establishment of the European Health Data Space has progressed the furthest. Regulation (EU) 2025/327 on the European health data space has entered into force on March 26, 2025 and will start applying in 2029.

205 On this value of the rule of law see Joseph Raz, *The Authority of Law* (2nd edn, 2009) 223-226.

206 Pohle & Thiel (n. 11), 9-10; Chander & Sun (n. 27), 289, 293-298.

207 For example, the expected effects of the DMA are controversial. Some scholars support the DMA's goals and design, *see*, e.g., Cabral et al., *The EU Digital Markets Act: a Report from a Panel of Economic Experts* (2021) 30-32 <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122910/jrc122910_external_study_report_-_the_eu_digital_markets_acts.pdf>; Anne C. Witt, 'The Digital Markets Act: Regulating the Wild West', (2023) 60 Common Mkt. L. Rev. 625. Others are more skeptical, see, e.g., Carmelo Cennamo et al., 'Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act', (2023) 14 Journal of European Competition Law & Practice 44; Yunsieg P. Kim, 'A Revolution Without A Cause: The Digital Markets Act and Neo-Brandeisian Antitrust', (2023) Wis. L. Rev. 1247.

208 It is for this reason that Alexander Roßnagel, the Data Protection Commissioner of the German state of Hesse, claims that Article 8 of the Charter requires the EU and its Member States to promote the emergence of European digital services, see Roßnagel, (n. 24), 67.

values of cyberspace.[209]

60 Conversely, the exercise of sovereignty through digital regulation could also promote the technological and economic independence of Europe. The EU strategy for regulating data and digital markets not only pursues the protection of European values and rights, but also aims to advance Europe's economic interests.[210] In particular, the EU regulation of digital and data markets through the DMA, DGA, and DA can be seen as an attempt to promote the emergence of a competitive European data economy by reigning in the market power of dominant foreign competitors and reducing competitive disadvantages of European tech companies due to a lack of data availability.[211]

61 In practice, however, the two objectives seem to be at odds rather than complementing each other. It is likely that the EU's attempts to comprehensively regulate the digital economy weaken the European technology sector by limiting the use of new and innovative technologies and imposing high compliance costs on businesses. In particular, the GDPR, the centerpiece of European data regulation, likely has negative effects on innovation, competition, and economic welfare in the EU.[212] For instance, the GDPR's restrictions on collecting, retaining, and sharing data limit the availability of data necessary for training AI systems.[213] Furthermore, its strict principles of data minimization and purpose limitation work against the EU's objective of facilitating the broad use and sharing of data for business purposes through the DGA and DA.[214] This may lead to a pragmatic conflict between the GDPR and data sharing laws, as they promote diverging states of affairs that practically cannot coexist with each other.[215] Against this background, it is not surprising that European businesses regard the GDPR as the main obstacle to using and exchanging data for innovative purposes.[216]

62 In addition, the EU's recent approach of promoting digital technologies and services through rights-based regulation, which underlies both the AI Act and the DGA, is unlikely to succeed. The AI Act seeks to promote the development and uptake of AI in the EU by implementing harmonized rules for AI, which shall ensure a high level of protection of health, safety, and fundamental rights.[217] It is more likely, however, that its additional and often uncertain rules will further reduce the ability and willingness of European businesses to develop and use such technologies.[218] Similarly, the DGA is supposed to facilitate the emergence of data intermediation services by increasing trust in these services through strict regulation.[219] Yet, this approach is likely to backfire, as the strict and highly uncertain rules of the DGA will complicate the provision of data intermediation services and lead to high compliance costs.[220] In these instances, the EU's approach of promoting innovation through strict regulation is likely to end up harming rather than promoting Europe's innovative capabilities and technological independence.

209 Monsees & Lambach (n. 18), 380.

210 European Commission, COM(2020) 66 final, 1, 3; Bauer & Erixon (n. 13), 6.

211 König (n. 194), 497; Roberts et al. (n. 38), 9; von Ditfurth & Lienemann (n. 80), 272.

212 See, e.g., Michal S. Gal & Oshrit Aviv, 'The Competitive Effects of the GDPR', (2020) 16 Journal of Competition Law & Economics 349; Rebecca Janßen, 'GDPR and the Lost Generation of Innovative Apps', (2022) NBER Working Paper 30028 <https://www.nber.org/papers/w30028>.

213 Andrea Calderaro & Stella Blumenfelde, 'Artificial intelligence and EU security: the false promise of digital sovereignty', (2022) 31 European Security 415, 428; Erik Brattberg, Raluca Csernatoni & Venesa Rugova, 'Europe and AI: leading, lagging behind, or carving its own way?', (2020) Carnegie Endowment for International Peace Working Paper, 33 <https://carnegie-production-assets.s3.amazonaws.com/static/files/BrattbergCsernatoniRugova_-_Europe_AI.pdf>.

214 On this inherent tension in EU data law see generally Christiane Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (2017) 327. Neither the DGA nor the DA successfully address this tension, see Hennemann et al. (n. 117), 40-42.

215 On pragmatic conflict between laws see Raz (no. 205), 201.

216 See Jan Büchel et al., *Anreizsystem und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft* (2022) <https://ieds-projekt.de/wp-content/uploads/2022/03/IEDS-Whitepaper-1.pdf>; Bitkom, *After 5 years: GDPR only receives the grade "sufficient"* (Oct. 5, 2023) <https://www.bitkom.org/EN/List-and-detailpages/Press/5-years-GDPR-receives-grade-sufficient>.

217 See Article 1(1) and Recitals 8, 176 of the AI Act.

218 See, e.g., Bomhard & Merkle (n. 86), 283; Michael Veale & Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach', (2021) Computer und Recht international [Cri] 97, 112; Philipp Hacker, 'A legal framework for AI training data: from first principles to the Artificial Intelligence Act', (2021) 13 Law, Innovation and Technology 257, 298.

219 See Recitals 5, 32 DGA.

220 Richter (n. 80), 465; von Ditfurth & Lienemann (n. 80), 290.

III. Unilateralism

63 Traditionally, the EU has pursued a strategy of open markets and a multilateral approach to international diplomacy and this long-standing commitment is reflected in the EU Treaties.[221] According to Article 21(1) and (2)(h) TEU, the EU "*shall promote multilateral solutions to common problems*" and "*promote an international system based on stronger multilateral cooperation and good global governance*". The EU's pursuit of digital sovereignty is at odds with its multilateralist commitments, as it seeks to unilaterally regulate the digital space.[222] Due to the transnational nature of the digital space, this approach inevitably affects the autonomy (and thus the sovereignty) of other states. In particular, EU digital legislation can influence *de jure* or *de facto* rules in third states (**1.**), contribute to the fragmentation of cyberspace (**2.**), and promote economic protectionism (**3.**).[223]

1. Extraterritorial Influence of EU Legislation

64 Some EU regulations, in particular the GDPR, the AI Act, the DGA, and the E-Evidence Regulation, share certain characteristics by which they influence the laws of foreign states and the behavior of foreign citizens and businesses.

65 The GDPR extends its geographic reach beyond the borders of the EU and directly covers certain online activities of individuals and businesses in third states.[224] Under its marketplace principle, the GDPR unilaterally extends the EU's legal authority over persons and organizations in third states.[225] In addition, the GDPR influences the laws of third states via its regulation of international data transfers. Personal data may only be transferred to a third country, if the EU Commission has decided that the third country ensures an adequate level of data protection or if the controller or processor transferring the data has provided appropriate safeguards to guarantee the effective protection of data.[226] The prospect of obtaining an adequacy decision from the EU Commission creates significant incentives for third states to align their data protection law with the GDPR.[227] For example, the pressure to satisfy EU adequacy requirements had an enormous influence on the emergence and shape of African data protection legislation.[228] These extraterritorial legal effects are reinforced by the Brussels Effect, which describes the unilateral extension of a state's laws beyond its borders through market mechanisms, leading to a *de facto* global reach of some EU rules.[229]

66 It is likely that other recent legal acts which include mechanisms similar to those of the GDPR will soon also exert their extraterritorial influence on foreign states. The GDPR's marketplace principle has been copied by the DSA, DGA, DA, and AI Act, extending their scopes to all relevant businesses operating in the EU's internal market, regardless of where these are established.[230] In addition, the DGA and DA mirror the GDPR's approach to regulating cross-border data flows data by restricting international transfers of non-personal data to third countries.[231]

67 Due to the borderless nature of the digital space, the implementation of legal mechanisms with extraterritorial effects can be necessary to effectively

221 Marise Cremona, 'Extending the Reach of EU Law: The EU as an International Legal Actor', in Marise Cremona & Joanne Scott (eds), *The EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019) 64, 66.

222 This is not surprising. Since the 20th century, the ideal of sovereignty has been frequently criticized for supposedly undermining multilateral cooperation and international law; see Philpott (n. 31), 568-571.

223 This Article will not delve into an analysis of the compatibility of the EU's regulation of cyberspace with international (trade) law. On this issue see Nehra Mishra, *International Trade Law and Data Governance* (2024); Roman Kalin, *Digital Trade and Data Privacy* (2024).

224 Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona & Joanne Scott (eds), *The EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019) 112; Koloßa (n. 147), 795; Federico Fabbrini & Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders', (2020) 21 Ger. Law J. 55, 61.

225 See supra Part C.II.2.; Azzi (n. 145), 130. This extension of the GDPR beyond EU borders raises problems under public international law, as it may conflict with the principles of legal sovereignty and non-interference, see Koloßa (n. 147), 798-807; Azzi (n. 145), 130-32.

226 Articles 44-49 GDPR; see supra Part C.II.1.(b).

227 Kuner (n. 224), 133; Mishra, (n. 223), 133.

228 Lukman Abdulrauf, 'African Approach(es) to Data Protection Law' in Raymond Atuguba, Moritz Hennemann, Patricia Boshe & Sena Afua Dei-Tutu (eds), *African Data Protection Laws* (2024) 36-39.

229 Anu Bradford, 'The Brussels Effect', (2012) 107 Nw. U. L. Rev. 1, 3; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (2020) 1-2. On the GDPR's tangible impact on Canada see René Mahieu et al., 'Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?', (2021) 11 Journal of Information Policy 301.

230 See supra Part C.II.2.x

231 See Article 31(1) DGA; Article 27(1) DA.

regulate domestic online activities.[232] For example, it would be easy to circumvent the high standard of data protection in the EU if personal data could be exported from Europe to third states without any conditions or restrictions.[233] Yet, the EU's approach goes beyond simply ensuring the effectiveness of its domestic regulations in a defensive manner and, in some instances, seeks to assert its values as universal values and to set global standards.[234] It was in this spirit that former EU Commissioner Viviane Reding advocated for the GDPR to become the "gold standard" for the world.[235] Similarly, the AI Act explicitly aims to shape global norms for AI.[236] Most notably, the E-Evidence Regulation disregards the territorial sovereignty of third states by requiring foreign service providers to hand over evidence data located on servers in third countries to European law enforcement agencies and by asserting the primacy of EU law in case of a conflict with foreign laws.[237]

68 Such offensive exercises of normative power can provoke conflicts with the interests and values of third countries.[238] It is hardly surprising then that foreign countries perceive the EU's *de jure* or *de facto* global regulation of cyberspace as attacks on their own digital sovereignty.[239] Therefore, the EU's extraterritorial regulation carries some risk of undermining multilateral cooperation and provoking sovereignty conflicts with third countries, if they decide to mirror the EU's approach.[240] Furthermore, it is possible that the extraterritorial imposition of EU legal values ignores important cultural and economic differences and is therefore ill-suited to address the needs and interests of some third countries.[241] The extraterritoriality of its legislation thus saddles the EU with a global responsibility that is difficult to fulfil.[242]

2. Fragmentation of Cyberspace

69 The EU's promotion of its digital sovereignty can also contribute to the fragmentation of cyberspace, thereby posing a threat to the global uniformity of the internet. According to Milton Mueller, digital sovereignty is "*inimical to [the internet's] liberalized order of information around common technical standards and the free flow of information*".[243] By disrupting global information flows as well as digital trade and services, national efforts to establish sovereign digital territories could divide the cyberspace. In this case, internet users around the world would no longer share the same online experience and this would have undesirable social, economic, and technical consequences.[244] For example, the restrictive regulation of online speech and content in some states may lead to the emergence of different cultural and social spheres on the internet.[245]

70 From an economic perspective, the proliferation of divergent national rules for digital technologies and online services increases compliance and transaction costs and jeopardizes global competition and free trade on the internet.[246] For instance, the emergence of a large number of divergent national adequacy standards for international data transfers has led to a fragmentation of data protection standards around the world, which especially harms businesses from the global south and small and medium-sized enterprises.[247] Ultimately, the divergent approaches to internet regulation may also affect the underlying hardware and networks themselves.[248] Fragmentation at the technical level could undermine the interoperability of hardware and disrupt the interconnectedness of the internet.[249]

232 See supra Part C.II.2.; Azzi (n. 145), 130.

233 Kuner (n. 139), 107.

234 Kuner (n. 224), 136; Glasze et al. (n. 1), 932; André Barrinha & G. Christou, 'Speaking sovereignty: the EU in the cyber domain', (2022) 31 European Security 356, 369.

235 See Viviane Reding, 'A data protection compact for Europe' (Jan. 28, 2014) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_62>. The European Commission has also articulated the GDPR's universal ambition in some of its official documents; see European Commission, COM(2017) 7 final, 2.

236 See European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 5.

237 See supra Part C.II.1.(a).

238 On the EU's normative power see Ian Manners, 'Normative Power Europe: A Contradiction in Terms?', (2002) 40 Journal of Common Market Studies 235.

239 Celeste (n. 4), 224.

240 Kuner (n. 224), 138; Celeste (n. 4), 225.

241 See, e.g., Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets', (2021) 53 Vand. L. Rev. 685, 706; Anne Bernzen, "Data Colonialism?' Big Data's Adverse Impact on the (Global) South' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 171, 180-81; Payal Arora, 'General Data Protection Regulation – A Global Standard?: Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South', (2019) 17 Surveillance & Society 717, 718.

242 Kuner (n. 224), 142. See also Celeste (n. 4), 226; Matthias Braun & Patrik Hummel, 'Sovereign Power: Artificial Intelligence and Europe's Digital Sovereignty', (2023) 28 Geopolitics 932, 934.

243 Mueller (n. 9), 780.

244 Mark A. Lemley, 'The Splinternet', (2021) 70 Duke L.J. 1397, 1399.

245 Lemley, ibid, 1409.

246 Mueller (n. 9), 794.

247 Anupam Chander & Paul Schwartz, 'Privacy and/or Trade', (2023) 90 U. Chi. L. Rev. 49, 54, 107-8.

248 Lemley (n. 244), 1410-18.

249 See, e.g., on China's attempt to introduce its own technical standards Stacie Hoffmann et al., 'Standardising the

71 Not all of the EU's recent regulatory efforts necessarily contribute to the fragmentation of the internet.[250] To a certain extent, the internet can still function well if it is uniform in some respects and diverse in others.[251] This is illustrated by the EU's regulation of online speech. Although certain social media platforms operating in Europe, such as X (Twitter) or Facebook, have responsibilities under the DSA to moderate speech on their platforms in a manner that may be incompatible with the First Amendment, this has not led to a significant disruption of these platforms as transatlantic channels of communication.[252] However, from an economic perspective of free trade and competition, the EU's pursuit of digital sovereignty can be more problematic. Foreign businesses, especially SMEs, may find it difficult to navigate the complex web of the EU's digital regulatory environment and could be kept from entering the European market due to pre-emptive compliance costs. The stringent regulation of novel technologies in the EU, such as AI, can also lead to a divergence in the types of services and applications offered to users inside and outside the EU.[253] In some instances, this can deprive Europeans of access to innovative technologies and services.[254]

3. Economic Protectionism

72 Partly due to their fragmenting impact, many of the EU's digital policies and legislative acts have been accused of protectionist rationales.[255] Critics regard the EU's pursuit of digital sovereignty and technological independence as a pretext for a hidden protectionist agenda.[256]

73 In the US, it is particularly the EU's regulation of large online platforms through the DMA that is perceived as a protectionist attack on its largest and most successful Internet companies, as five of the seven designated gatekeepers covered by the DMA are American (Alphabet, Amazon, Apple, Meta, and Microsoft).[257] Another frequent target of anti-protectionist criticisms are the EU rules on international transfers of data.[258] These are regarded by some as "data localization" measures, i.e., measures that specifically restrict cross-border data transfers.[259] Critics of such measures argue that these measures are often motivated (at least implicitly) by the aim to promote domestic economic development, but instead end up harming domestic and foreign businesses and consumers by raising costs, limiting access to foreign services, and impeding technological progress.[260]

74 It is hard to determine to what extent these accusations are justified. As Christoph Kuner has

splinternet: how China's technical standards could fragment the internet', (2020) 5 Journal of Cyber Policy 239, 252-254.

250 Lemley (n. 244), 1401.

251 Woods (n. 52), 368.

252 See also Nick Clegg, 'The Future of Speech Online: International Cooperation for a Free & Open Internet', (2024) 153 Daedalus 65, 70.

253 European Parliament Research Service, *'Splinternets': Addressing the renewed debate on internet fragmentation* (2022) 42 <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf>.

254 For example, Apple delayed the EU release of the iPhone 16's AI feature for 18 months due to concerns over its compliance with the DMA; see Dwayne Cubbins, 'Apple Intelligence in Europe: What's happening and why the hold-up?', Tech-Issues Today (Sep 10, 2023) <https://techissuestoday.com/apple-intelligence-europe-availability>. This shows that not every EU regulatory act will necessarily lead to the Brussels Effect. In cases where the provision of services can be split between different territories at a reasonable cost, businesses will not need to comply with EU laws extraterritorially.

255 Pohle & Thiel (n. 11), 11; Dennis Broeders et al., 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions', (2023) Journal of Common Market Studies 1, 8; Chander & Sun (n. 27), 310.

256 See, e.g., Charlene Barshefsky, 'EU digital protectionism risks damaging ties with the US', Financial Times (Aug. 2, 2020) <https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103>.

257 For example, a bipartisan group of members of Congress sent a letter to then President Biden stating that "*as European leaders have made clear, the DMA as currently drafted is driven not by concerns regarding appropriate market share, but by a desire to restrict American companies' access to Europe in order to prop up European companies*" <https://delbene.house.gov/uploadedfiles/eu_digital_markets_act_letter.pdf>; see further EU Commission, *Digital Markets Act: Commission designates six gatekeepers* (Sep. 6, 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328>.

258 Susan A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', (2019) 18 World Trade Review 541, 557-562; Henry Farrell & Abraham Newman, 'The Transatlantic Data War', Foreign Affairs (Feb. 2016) <https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war>.

259 Anupam Chander & Uyên P. Lê, 'Data Nationalism', (2015) 64 Emory L. J. 677, 680; Naef, (n. 141), 235. Due to these restrictive effects, the regulation of international data flows under the GDPR has raised doubts about its compatibility with the non-discrimination obligations of the WTO's General Agreement on Trade in Services (GATS); see, e.g., Svetlana Yakovleva & Kristina Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation', 114 AJIL Unbound, 10 (2020); Mira Burri, 'Interfacing Privacy and Trade', (2021) 53 Case W. Res. J. Int'l L. 35, 62-67.

260 Chander & Lê, ibid, 721; Martina F. Ferracane, 'The Costs of Data Protectionism' in Mira Burri (ed), *Big Data and Global Trade Law* (2021) 69.

pointed out, it is often difficult to accurately identify protectionist policy rationales and distinguish them from other underlying motivations.[261] Because of cultural differences in their views on the nature and value of data protection, strict data protection laws may appear legally and morally justified to a European and protectionist to an American.[262] This observation also applies to other areas of digital regulation that are central to the EU's quest for digital sovereignty, such as the regulation of online speech, AI, and competition in digital markets. In defense of the EU, it can be argued that both the DMA and the regulation of international data transfers pursue rational and legitimate aims. The DMA's objectives of strengthening the contestability and fairness of markets for core platform services are based on justified economic concerns and do not arbitrarily disadvantage foreign companies. Similarly, the GDPR aims to prevent circumventions of EU law and to guard against concrete risks for personal data in other countries, such as broad data access rights for law enforcement authorities or intelligence agencies.[263] Still, it cannot be ruled out that these laws may have *de facto* protectionist effects.

75 More problematic than these value-based regulations are the EU's efforts to strengthen its technological independence, which carry overt protectionist connotations.[264] After all, the objective of technological independence is driven by the desire to substitute foreign technology providers with local ones and to increase the market shares of domestic tech companies. In some cases, there are plausible policy reasons for strengthening the technological and digital capabilities of European companies. Heavy reliance on foreign technology providers can sometimes undermine Europe's cybersecurity and its autonomy.[265] However, there is a fine line between policies based on such legitimate reasons and policies whose protectionist effects are not justified by adequate policy rationales.[266] The mere fact that certain technologies or services are developed abroad should not serve as a blanket excuse for the preferential treatment of local providers.

261 Christopher Kuner, 'Data Nationalism and its Discontents', (2015) 64 Emory L.J. Online 2089, 2097.

262 For an overview of the different visions of data privacy in the EU and the US see Paul M. Schwartz & Karl-Nikolaus Pfeifer, 'Transatlantic Data Privacy Law', (2017) 106 Geo. L.J. 117, 121-137.

263 Kuner (n. 261), 2093; Kuner (n. 139), 107-116.

264 Bauer & Erixon (n. 13), 22.

265 Theodore Christakis, *European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy* (2020) 54-55 <https://ssrn.com/abstract=3748098>.

266 Christakis, ibid, 54.

E. Conclusion

76 Ultimately, it is easy to see why the ideal of a digitally sovereign EU has such a broad appeal. At a time when many undesirable social, economic, and political effects of the internet have become apparent, the EU understandably feels the need to actively and self-determinedly shape and enforce the rules governing cyberspace on its own digital territory. By embracing digital sovereignty as a normative ideal, the EU's digital agenda has shifted towards prioritizing control over its domestic cyberspace.[267] Digital sovereignty serves as the overarching goal that connects different pieces of legislation, all of which share the aim of redefining the prevailing rules of the digital space and restoring the EU's control over its digital territory. By implementing rules to protect the rights of individual citizens, the functioning of democracy and competition in digital markets, the EU is pursuing a regulatory path that sets itself apart from both the market-centric approach of the US and the state-centric approach exemplified by China.[268]

77 It is likely that the EU will continue to focus on its digital sovereignty during the second term of von der Leyen's commission presidency. This is indicated by the fact that the European Commission has for the first time appointed a Vice-President for Tech Sovereignty, Security and Democracy, whose goals include developing a Digital Fairness Act and promoting EU digital norms and standards internationally.[269] In general, this approach deserves support. As sovereigns, the EU and its Member States have the legal right and the legitimacy to set the rules governing Europe's digital space and the values pursued by the EU deserve protection.[270] Moreover, since the second Trump administration took office in the US, the need to continue to assert EU values and interests in cyberspace has only grown.

78 However, there are also inherent risks to openly embracing a legal policy centered on the pursuit of digital sovereignty. First, it can lead to false expectations and regulatory hubris. Digital regulation is characterized by a high degree of informational

267 See also Falkner et al. (n. 66), 2112.

268 See further Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (2023).

269 European Parliament Research Service, *Briefing: Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy* (2024) 3 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762455/EPRS_BRI(2024)762455_EN.pdf>.

270 Contrary to the ideology of early cyber-exceptionalists, states have remained the "*single greatest source of legitimate rules for different peoples with varied community values and experiences on a diverse planet*", *see* Woods (n. 52), 369.

uncertainty.[271] The difficulty of regulating a rapidly evolving technological environment with significant uncertainty about future developments and disruptions can lead to regulatory lag, off-target regulation, and other unintended consequences. Examples include the slow reaction of regulators to strategic acquisitions of emerging start-up competitors by big tech companies[272], the GDPR's long-winded legislative process and its failure to take into account looming big data and AI trends[273], and the neglect of general purpose AI, such as ChatGPT, in the European Commission's original Proposal for the AI Act.[274] Thus, the ideal of digital sovereignty may create expectations of a level of control over the digital space that is illusory and there is a risk that it may lead EU regulators to overestimate the accuracy and effectiveness of new potential legislation. In addition, the EU's control over the digital space can be constrained by its limited foreign policy competences, which may impair the EU's ability to strengthen its external digital sovereignty against interference by hostile states[275], and by the decentralized enforcement of EU law, which has often not been sufficiently effective, especially in cross-border contexts.[276]

79 Second, the embrace of digital sovereignty as a legislative ideal sits uneasily with the EU's traditionally multilateral and trade-friendly approach to international politics. More than most other areas of domestic policy, the regulation of the inherently transnational cyberspace can have direct legal, economic, and political effects on foreign states and their citizens.[277] Some of these effects may be unwelcome. Unilaterally pursuing EU values and interests through extraterritorial legislation may lead third countries to reciprocate[278], which would further fragment the rules of cyberspace. Already, the proliferation of laws with extraterritorial effects from different jurisdictions creates legal conflicts and dilemmas for the legal subjects who must choose whether to comply with the laws of one jurisdiction or another. For example, organizations may face incompatible legal obligations when confronted with data access requests under the US CLOUD Act on the one hand, and GDPR obligations not to disclose the data on the other.[279] A similar dilemma may arise soon as a result of the conflict between the E-Evidence Regulation and the US ECPA.[280]

80 As these examples also show, the EU exercises its digital sovereignty for both defensive and offensive purposes. In the first example, it is the US CLOUD Act that that challenges the EU's sovereignty and that is legitimately countered by the GDPR's defensive mechanisms for controlling data exports in order to protect the rights of EU data subjects. In contrast, the E-Evidence Regulation follows a more offensive approach. The EU intends to abandon the traditional concept of territoriality, which is tied to the location of the data, for its own data access requests, while still preserving its territorial sovereignty against foreign data access requests.[281] Such offensive exercises of digital sovereignty by the EU can understandably be perceived by foreign states as threats to their own digital sovereignty.

81 For these reasons, the EU should take a measured approach towards promoting its digital sovereignty, rather than pursuing digital sovereignty unconditionally and for its own sake. This requires the EU to critically assess the domestic and

271 Urs Gasser & Moritz Hennemann, 'Unlocking the Potential of the Data Age: Key Tasks and Challenges of Data Strategies' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 11, 15.

272 See Christophe Carugati, 'Which mergers should the European Commission review under the Digital Markets Act?', (2022) Bruegel Policy Contribution 24/2022, 2 <https://www.bruegel.org/system/files/2022-12/PC%2024%202022.pdf>.

273 See Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', (2017) 47 Seton Hall L. Rev. 995.

274 See the adopted position of the Council of the EU from Nov. 25, 2022, 2021/0106(COD), 6 <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

275 On the EU's disjointed approach to combating state-sponsored disinformation see Andreu Casero-Ripollés et al., 'The European approach to online disinformation: geopolitical and regulatory dissonance', (2023) 10 Humanities and Social Sciences Communications 657, 7; Matthias Kachelmann & Wulf Reiners, 'The European Union's Governance Approach to Tackling Disinformation: Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty', (2023) 396 L'Europe en formation 11, 17-21.

276 See, e.g., on the issues surrounding the GDPR's cross-border enforcement Giulia Gentila & Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR', (2022) 71 International & Comparative Law Quarterly 799. As a result, the EU Commission is seeking to improve the GDPR's cross-border mechanisms, see Chapter III of its Proposal for a Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final.

277 Chander & Sun (n. 27), 307; Moritz Hennemann, 'Global Data Strategies: An Introduction' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 1, 1.

278 Kuner (n. 224), 138.

279 See Jessica Shurson, 'Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law', (2020) 28 International Journal of Law and Information Technology 167, 179-80.

280 See supra Part C.II.1.(a).

281 Suzan Hüttemann, 'Die E-Evidence-Verordnung: Pioniermodell für das digitale Zeitalter oder Preisgabe der Staatlichkeit?', (2024) Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht [NZWiSt] 81, 92.

international implications of existing and new legislation in order to ensure that it coherently and appropriately regulates the domestic cyberspace and avoids international legal conflicts.[282] Domestically, the EU will need to better align its goals of digital sovereignty and technological independence, as the current regulatory framework for digital technologies is likely to stifle innovation, development, and use of new technologies within the EU. Internationally, the EU should continue to avoid unilateral solutions where this is possible and seek multilateral cooperation among like-minded states.[283] In theory, a multilateral approach enables the EU to protect important values and interests while simultaneously respecting the sovereignty of third countries.[284]

82 Of course, a multilateral approach is only feasible if third states are willing to cooperate and compromise. Given the current tense international political climate and the diverging values and interests of some other major international powers, multilateral efforts alone are unlikely to effectively protect and promote EU values and interests in the digital space. In particular, the EU faces external pressures from the US and China, which are each advancing their own competing visions for regulating cyberspace.

83 China exports its illiberal and state-centric model for regulating the digital space through the provision of its homegrown digital infrastructures abroad and through its growing influence on international institutions, such as the United Nations or the International Electronical Commission (IEC).[285] The US model for governing the digital space, which is based on weak digital regulation and strong protections for free speech, is exported primarily through the commercial success of US tech companies.[286] During the second Trump administration, this laissez-faire approach towards digital regulation is likely to be more actively promoted by the US government, including in relation to the EU.[287] Already, members of the Trump administration have voiced harsh criticism of the EU's regulation of speech and AI.[288] There are also concerns that the Trump administration's actions could target the enforcement of the DMA[289] or unravel the EU-US Data Privacy Framework, putting data transfers from the EU to the US at risk.[290]

84 Where multilateral cooperation is thus unrealistic and there is a need to safeguard the EU's autonomy against external pressures, the pursuit of digital sovereignty for defensive purposes is necessary and legitimate to effectively protect European interests and values in accordance with Article 3(5) TEU.

282 Currently, impact assessments and evaluations of EU legislation are limited to domestic effects and do not take into account potential consequences for third countries; see Kuner (n. 224), 142.

283 Examples of this approach include the agreements on cross-border data transfers with Japan and the US and the recently concluded digital trade agreement with South Korea.

284 See also Woods (n. 52), 368-69. In some instances, the promotion of digital sovereignty may strengthen the EU's bargaining position, allowing it to gain more concessions from third countries.

285 See further Bradford (n. 268), 290-308, 388-93; Erie & Thomas Streinz, 'The Bejing Effect: China's Digital Silk Road As Transnational Data Governance', (2021) 54 N.Y.U. J. Int'l L. & Pol. 1, 35-47; Willem Gravett, 'Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa,' (2020) 20 Afr. Hum. Rts. L.J. 125, 138-42.

286 Bradford (n. 268), 33-52, 259.

287 See Jan Philipp Albrecht, 'Trump and Big Tech: Europe's Sovereignty at Stake', Heinrich Böll Stiftung (Jan 24, 2025) <https://www.boell.de/en/2025/01/24/trump-and-big-tech-europes-sovereignty-stake>.

288 See, e.g., Emily Atkinson, 'JD Vance attacks Europe over free speech and migration", BBC News (Feb 15, 2025) <https://www.bbc.com/news/articles/ceve3wl21x1o>; Clea Caulcutt, 'JD Vance warns Europe to go easy on tech regulation in major AI speech, Politico (Feb 11, 2025) <https://www.politico.eu/article/vp-jd-vance-calls-europe-row-back-tech-regulation-ai-action-summit/>.

289 See Stefan Krempl, 'Suspension of the DMA? – Concerns about horse-trading between the EU and the USA (Jun 26, 2025) <https://www.heise.de/en/news/Suspension-of-the-DMA-Concerns-about-horse-trading-between-the-EU-and-the-USA-10461509.html>

290 See Brian Hengesbaugh & Lukas Feiler, 'How could Trump administration actions affect the EU-US Data Privacy Framework?', IAPP (Feb. 26, 2025) <https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework>.

An EU Copyright Framework for Research: Opinion of the European Copyright Society

by **Caterina Sganga, Christophe Geiger, Thomas Margoni, Martin Senftleben, Mireille van Eechoud***

Executive Summary: Research and academic freedom are at the core of the EU project. Yet, the relationship between EU copyright law and research is intricate. Research and education interests have traditionally been recognized within copyright law to some degree, however, the current EU copyright *acquis* is not really conducive to an effective research environment. This jeopardises the fulfilment of the EU's ambitions in the field.

Building on the pillars of action of the European Research Area (ERA) Policy Agenda 2022-2024 and its follow-up, the ECS emphasises the need for a copyright framework that fosters research, and supports the call for immediate action on the EU copyright framework to address the most pressing challenges it raises for European researchers and their institutions.

This Opinion stresses the need to ensure a proper balance between IP rights, protected under Article 17(2) CFREU, and the freedom of art and science (Article 13 CFREU), coupled with the 'right to research', as enshrined in international legal instruments (UDHR and ICESCR), the objectives of the EU treaties, and the CFREU and ECHR. Various EU and national legal instruments are in place that facilitate access and reuse of scientific works, but these have several shortcomings. They weaken the effective balance between copyright, research policy needs, and the fulfilment of ERA policy goals, including the EU Open Science agenda.

This opinion focuses on the flaws in key provisions aimed at balancing copyright and research needs: the general InfoSoc Directive research exception, the text and data mining exception of the CDSM Directive and national secondary publication rights. It also briefly assesses the interface between copyright and (research) data regulation. We propose several policy interventions to address the identified shortcomings. These include the introduction of an EU-wide secondary publication right with specific characteristics; the amendment of text and data mining exceptions; the creation of a general mandatory research exception overcoming the challenges raised by Article 5(3)(d) InfoSoc; and a more careful legislative drafting to reduce legal complexity and ensure consistency across copyright and data legislation.

Recommended citation: Caterina Sganga, Christophe Geiger, Thomas Margoni, Martin Senftleben, Mireille van Eechoud, An EU Copyright Framework for Research, 16 (2025) JIPITEC 312 para 1.

1. The Importance of Research

1 In the face of the complex challenges the EU is facing, there is an acute awareness that research must be put "at the heart of our economy"[1] and that education (skills) is of vital importance to ensure prosperous fair societies.

2 Research and academic freedom have been at the core of the EU project. This is evident from the creation of the European Research Area (ERA) 25 years ago, the progressively increasing targets for EU R&D investment, the consolidated multi-annual research Framework Programs (currently Horizon) and the extensive Commission policy agenda in the field. The EC's Open Science (OS) agenda and work towards an European Open Science Cloud (EOSC) foregrounds the importance of academic integrity, citizen involvement and access to research. In all this, academic freedom is a core value. Or, as Article 13 of the Charter of Fundamental Rights of the European Union (CFREU) and its precursors mandate, "The arts and scientific research shall be free of constraints. Academic freedom shall be respected".

3 In many cases there is no tension between academic

* The European Copyright Society (ECS) was founded in January 2012 with the aim of creating a platform for critical and independent scholarly thinking on European Copyright Law and policy. Its members are scholars and academics from various countries of Europe, seeking to articulate and promote their views of the overall public interest on all topics in the field of authors rights, neighbouring rights and related matters. The ECS is neither funded nor instructed by any particular stakeholders. Its Opinions represent the independent views of a majority of ECS members.

1 See European Commission, "A new plan for Europe's sustainable prosperity and competitiveness" and https://commission.europa.eu/priorities-2024-2029/competitiveness_en

freedom and intellectual property. However, when this happens, the clash should be resolved by striking a fair balance between conflicting fundamental rights, since Article 17(2) CFREU provides that "Intellectual property shall be protected'.

4 Research and education interests have traditionally been recognized within copyright laws to some degree, but the current copyright *acquis* is not conducive to an open and innovation-friendly research environment, thus jeopardising fulfilment of the EU's ambitions in the field.

5 Against this background, the most recent ERA Policy Agenda 2022-2024[2] identified four pillars of action: (i) to deepen a truly functioning internal market for knowledge"; (ii) to take up together the challenges posed by the twin green and digital transition, and increasing society's participation in the ERA; (iii) to amplify access to research and innovation excellence across the Union; and (iv) to advance concerted research and innovation investments and reforms.

6 Copyright law does not provide a specific regime for scientific works or, more generally, for works that stem from research activities. Save for circumscribed research exceptions, it does not grasp nor reflect in its structure the different needs, incentive drivers and characteristics of scientific authors and their outputs as compared to creators operating in the realm of cultural and creative sectors and industries (CCSIs), which traditionally constitute the core and *raison d'être* of copyright law. Still, the copyright-research interface is rich and multifaceted. It comes into play for the regulation of publishing contracts and the relationship between scientific authors and publishers; when a researcher would like to share freely their published works through institutional or subject-specific repositories, or to get access to a resource their institution has not subscribed to, or to reuse a work they have lawfully acquired; when research consortia try to pool together the resources each partner has individual lawful access to; when a research team needs to perform text and data mining activities over a protected database. And the list may continue. Despite such numerous interactions, research is covered only with limited and fragmented copyright exceptions.

7 This lack of a holistic consideration of the interplay between copyright law and research and the need to shed light on the impact of copyright (and data) law on the fulfilment of EU research policy goals have been subject to analysis and comments in decades of studies and scholarly contributions, which have highlighted how "the freedom to access, use and reuse diverse knowledge resources – from repositories of literary and artistic works to more general data collections – is indispensable for research"; how "knowledge resources required for research are often subject to specific regulations that limit access and use",[3] from IP law (copyright, patent, trade secrets) to hybrid regimes such as database protection law; and how academic publishing and its governance of IP rights have become yet another stumbling block in the realization of a more equitable global research ecosystem.[4]

8 It does not come as a surprise, then, that among the actions envisioned under the first pillar of the ERA Policy Agenda 2022-2024, the second top priority is to "propose an EU copyright and data legislative and regulatory framework fit for research". To realize these objectives, the EC funded a study aimed at assessing the impact of EU and Member States' copyright and data legislation on access to and reuse of data and publications for research purposes. The study, published in 2024,[5] added yet another wealth of data and evidence of the wide array of obstacles copyright law poses to the realisation of a fully functioning European Research Area. Without the intention of being exhaustive, but only to focus on the most pressing challenges that the EU copyright framework raises for European researchers and their institutions, this Opinion offers a brief assessment of the shortcomings of the main existing instruments that have been introduced to balance copyright enforcement against research needs and goals (general research exception; text and data mining exception; secondary publication right; interface copyright-data regulation). On this basis, it proposes high-priority policy interventions to address such

2 European Commission - Directorate-General for Research and Innovation, "European Research Area Policy Agenda – Overview of actions for the period 2022-2024", Publication Office of the European Union, 2021.

3 Martin Senftleben, Kacper Szkalej, Caterina Sganga, Thomas Margoni, 'Towards a European Research Freedom Act: A Reform Agenda for Research Exceptions in the EU Copyright Acquis', forthcoming in IIC, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5130069.

4 Caterina Sganga, Thomas Margoni, Martin Senftleben, Kacper Szkalej, 'Towards a European Research Freedom Act: A Proposal for an EU-wide Secondary Publication Right' (January 12, 2025), available at https://ssrn.com/abstract=5134238.

5 European Commission: Directorate-General for Research and Innovation, 'Improving access to and reuse of research results, publications and data for scientific purposes – Study to evaluate the effects of the EU copyright framework on research and the effects of potential interventions and to identify and present relevant provisions for research in EU data and digital legislation, with a focus on rights and obligations', Publications Office of the European Union, 2024, available at https://data.europa.eu/doi/10.2777/633395 (last accessed 27 March 2023) (hereinafter ERA Study 2024). Disclosure: Margoni, Senftleben, Sganga and Van Eechoud were part of the team that authored this report.

flaws and create the conditions for an EU copyright framework fit for research and for the fulfilment of ERA policy goals.

9 For the purpose of the Opinion, the concept of "research" is intended as covering all forms of scientific[6] research (defined as such for they employ a scientific method, regardless of the domain of knowledge involved) performed in the interest of advancing public knowledge. In this sense, the definition is purposefully broader than the one adopted in Article 2 CSDMD, which the European Copyright Society has already criticized for its incapability to encompass all forms of scientific research activities fulfilling public interest goals (e.g. by excluding independent researchers or for-profit research endeavours).[7]

2. Research within the Context of Fundamental Rights

10 A 'right to research' as such does not exist explicitly in any of the international or European human right documents. However, it is implicitly included within international legal instruments and the two main European human rights instruments, as well as the objectives of the EU treaties.[8] The tension between copyright and research is contained at the very foundation of international human rights law. The Universal Declaration of Human Rights (UDHR),[9] on the one hand, guarantees "the right to freely participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits" while also requiring that authors receive protection for the "moral and material interests resulting from any scientific, literary or artistic production." Similarly, Article 15 of the International Covenant on Economic, Social and Cultural Rights (ICESCR)[10] contains a commitment from the signatories of the covenant to "respect the freedom indispensable for scientific research and creative activity."[11] In the same provision, two separate rights are expressed: on the one hand, everyone should have the right to "enjoy the benefits of scientific progress and its applications", on the other hand all persons should "benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author."[12] However, it can be argued that these seemingly separate statements are complementary and therefore systematically linked.

11 While the international human rights framework informs the interpretation of the rights and obligations arising under the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights,[13] at the EU level, the right to research can be constructed through a combined reading of several fundamental rights such as freedom of expression (Article 10 ECHR, Article 11 EU Charter), freedom of art and science (Article 13 EU Charter) and the right to education (Article 14 EU Charter). Furthermore, the right to research can be rooted in the objectives of the EU treaties, such as sustainability, scientific advancement and the commitment to a social market economy. For example, Article 3 (3) TEU calls for the establishment of an internal market, which is to "work for *sustainable development* of Europe based on balanced economic growth and price stability, a highly competitive *social market economy*, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment. It shall promote *scientific and technological advance*",[14] for which research is a fundamental prerequisite. Sustainable development has been defined in the EU context to mean "stimulating and encouraging economic development (e.g. more jobs, creativity, entrepreneurship and revenue), whilst protecting and improving important aspects (at the global and European level) of nature and society (inter alia natural assets, public health and fundamental rights) for the benefit of present and future generations."[15]

6 Note that the term "scientific" is used in the broadest sense, encompassing all disciplines and realms of knowledge and not only pure and applied sciences.

7 ECS, Comment of the European Copyright Society addressing selected aspects of the implementation of Articles 3 to 7 of Directive (EU) 2019/790 on Copyright in the Digital Single Market, 3 May 2022, available at https://europeancopyrightsociety.org/2022/05/03/https-europeancopyrightsocietydotorg-files-wordpress-com-2022-05-ecs_exceptions_final-1-pdf/.

8 See detailed Christophe Geiger and Bernd Justin Jütte, 'Conceptualizing a 'Right to Research' and its Implications for Copyright Law, An International and European Perspective', American University International Law Review 2023, Vol 38, Issue 1, p. 1. The next paragraph draws on this research.

9 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

10 International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966 UNGA Res 2200 A (XXI) (ICESCR), UNTS vol. 993, p. 3.

11 ICESCR, art. 15(3), see also art. 27(1) UDHR.

12 ICESCR, art. 15(1)(b) and (c).

13 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

14 Emphasis added.

15 See Sander R.W. van Hees, 'Sustainable Development in the EU: Redefining and Operationalizing the Concept', [2014] 10 Utrecht Law Review 62, at p. 75. See also at international level the so-called Brundtland-definition, based on the homonymous 1987 UN Commission (World Commission

12 Since research and education are key in order to develop new creative works while at the same time guaranteeing that access to knowledge is available for future generations, the principle of sustainability has started to be used to conceptualize an obligation of the EU to foster research through secondary legislation and calls for a "sustainable copyright law" have emerged.[16] In any case, research plays an important and very prominent role in the law and policy of the EU in recent years, as demonstrated by the numerous policy documents produced by the European Commission to emphasize the need to create a vibrant European ecosystem for research.[17] Therefore, a copyright framework that hinders research can be in direct conflict with the international and EU fundamental rights framework as well as with the policies developed by the EU.

3. The State of the Art: Where the Problems Lie

13 Despite the positive availability of a multitude of legal instruments in the EU *acquis* and national legislations that are meant to facilitate access to and reuse of scientific works,[18] a number of shortcomings in each of these provisions and in the general architecture of copyright law weaken the effective balance between copyright and research policy needs.

14 Challenges stem from the EU legislative strategy and drafting techniques, resulting in the inconsistent or vague language and contractual overridability of most research exceptions and limitations (E&Ls), and in the lack of coordination between general (InfoSoc Directive) and subject-specific (Software and Database Directives) provisions. They arise from the fragmentation of Member States' legislative solutions and judicial interpretations, chiefly caused by the optional nature of the great majority of research E&Ls, or by the vague language of some mandatory exceptions. The same can be said for the problematic interplay and misalignment between copyright and data-related legislations, and for the large room left to freedom of contract and its impact on the balance of conflicting interests set by copyright law. Several critiques have also targeted specific E&Ls, such as Article 3 CDSMD on text and data mining, or entire acts, such as the Database Directive, for their restrictive rather than enabling impact on access to and reuse of copyright-protected materials. More generally, the lack of harmonization of copyright contract law[19] in the field of publishing of scientific works is commonly understood as a major obstacle for the fulfilment of ERA policy goals.

15 Within the context of ERA, the EU promotes greater access and reuse of scientific knowledge through Open Science (OS) policies, of which Open Access (OA) to scientific outputs is a major component. The backbone of EU OS goals has been first outlined in the EC Recommendation on access to and preservation of scientific information (2012),[20] which invited Member States to develop "clear policies for the dissemination of scientific publications produced within publicly funded research activities and open access to them"[21] by, *inter alia*, mandating OA for publications that stem from publicly funded research activities, immediately and in any case not more than six/twelve months after the date of first publication.[22] The objective was later operationalised in two further Recommendations, calling for the facilitation of open sharing of metadata[23] and the formulation of clear policies to preserve and reuse scientific information.[24] OA and Open Data Policies are now integrated in the EU's framework programme. All research products funded through Horizon Europe must in principle be made available as OA, and research data published as FAIR (findable,

on Environment and Development (WCED), Our Common Future, 1987, Chapter 2, para. 1.), where sustainability is commonly defined as "meeting the needs of the present whilst ensuring future generations can meet their own needs."

16 See e.g. with further references Christophe Geiger and Bernd Justin Jütte, 'The Right to Research as Guarantor for Sustainability, Innovation and Justice in EU Copyright Law', in: T. Pihlajarinne, J. Mähönen and P. Upreti (eds.), *Rethinking the Role of Intellectual Property Rights in the Post Pandemic World: An Integrated Framework of Sustainability, Innovation and Global Justice*, Edward Elgar, 2023, p. 138 sq.;

17 For further references, see above section 1 of the Opinion; Geiger and Jütte, note 9; Christophe Geiger and Bernd Justin Jütte, 'Copyright, the Right to Research and Open Science: About Time to Connect the Dots', in E. Bonadio and C. Sganga (eds), *A Research Agenda for EU Copyright Law*, Edward Elgar, 2025, p. 149.

18 The term "scientific work" is hereby used to refer to all research outputs in all disciplines and realms of knowledge, and not only in pure and applied sciences, in line with the specification provided supra (n 6).

19 The EU competence in the field may be based on the same ground (Article 115 TFEU) that supported the intervention on copyright contracts and author's remuneration with Articles 18 et seq CDSMD.

20 Commission Recommendation of 17 July 2012 on access to and preservation of scientific information, OJ L 194, 21/07/2012, p. 39–43.

21 Ibid Recommendation 1.

22 Ibid.

23 Commission, 'OSPP-REC - Open Science Policy Platform Recommendations' (Directorate-General for Research and Innovation, 2018), <https://data.europa.eu/doi/10.2777/958647> (last accessed 27 March 2025).

24 Commission Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information, C/2018/2375, OJ L 134, 31.5.2018, p. 12–18.

accessible, interoperable, and reusable).

16 Since 2012, OS initiatives have been undertaken at different levels and with a different pace across Member States, mostly via soft law tools, and in line with the EU priorities.[25] Ambitious objectives, however, have often remained aspirational statements lacking effective implementation measures, as testified by the very low percentage of OA publications (mostly Green OA) circulating within the ERA also in recent years.[26] Various reasons are put forward to explain the limited success of OS policies - legal, economic, organisational, as well as technological. Along with scientific practices and regulatory approaches to hiring/promotion and research evaluation processes, which favour high-impact, often proprietary journals and well-functioning proprietary databases, important legal obstacles stem from a lack of true harmonization of national E&L and copyright contract rules. In combination with the territorial nature of copyright, this has resulted in continued legal uncertainty and related chilling effects on scientific authors and institutions willing to engage in OS actions, particularly when cross-border activities are involved.[27] In addition, the effectiveness of E&L has been curtailed by their contractual overridability and by the application of technological protection measures, while publishing contracts have often banned the possibility to resort to free (Green) OA options.

17 Against this background, the EC report "Open Science and Intellectual Property Rights" (2018)[28] explicitly highlighted the misalignment between the EU OS agenda and the approach followed in the context of the harmonization of EU copyright and database laws, followed by the ERA Policy Agenda 2022-2024 and its priority of proposing "an EU copyright and data legislative and regulatory framework fit for research".

18 The ECS wishes to support the call for an immediate action on the EU copyright framework to address the most pressing challenges the EU copyright framework raises for European researchers and their institutions. To this end, this Opinion offers an overview of the flaws affecting the key instruments that have been introduced to balance copyright enforcement against research needs (general research exception; text and data mining exception; secondary publication right; interface copyright-data regulation). On this basis, it offers concise policy recommendations to tackle such challenges and create the conditions for an EU copyright framework fit for research and for the fulfilment of ERA policy goals.

a.) General Research Exception

19 With Article 5(3)(a) ISD, Articles 6(2)(b) and 9(b) of the Database Directive (DBD) and Article 10(1)(d) of the Rental, Lending and Related Rights Directive (RLRD), the copyright acquis provides for an exception that globally refers to use for purposes of "scientific research." Article 5(3)(a) ISD, for instance, reads as follows:

> *Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 [the reproduction right and the right of communication to the public] in the following cases: (a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;...*

20 Evidently, the provision is not confined to specific forms of research or specific research tools, methodologies, collaborations, research settings etc. It deals with scientific research in a broad, general manner. The same can be said about its DBD and RLRD counterparts. At first sight, these provisions, thus, seem to inject considerable flexibility into the EU copyright and database protection system. However, a closer look reveals several conceptual problems.

21 First, Article 5(3)(a) ISD, Articles 6(2)(b) and 9(b) DBD and Article 10(1)(d) RLRD are "may" provisions. This optional nature implies that Member States are not bound to implement the exemption of use for scientific research purposes in a standardised form. As a result, national research provisions based on Article 5(3)(a) ISD – the most widely transposed research exception of the EU acquis – differ in relation to beneficiaries, works covered, the scope of permitted use, the exclusive rights covered (reproduction and/or communication to the public), conditions of applicability, remuneration requirements and safeguards against contractual

25 For an overview, see ERA Study 2024, pp 399-452.

26 In 2018, only 36% of publications were in OA, with percentages varying from 52% in the United Kingdom to 49% in the Netherlands, 43% in Spain, 41% in France, and 40% in Italy. The most widespread format is the Green OA model (between 70 and 80%), while the Gold version usually covers around 15-20% of the total.

27 This problem has been repeatedly highlighted by researchers and research performing organizations participating at the survey conducted within the framework of the ERA Study 2024, pp 78-80.

28 Commission, 'Open Science and Intellectual Property Rights' (Directorate-General for Research and Innovation, 2022) <https://data.europa.eu/doi/10.2777/347305> (last accessed 27 March 2025).

override. Quite clearly, this diversity is not conducive to cross-border research activities. It poses challenges to joint research activities in transnational consortia. Research use that is permissible in one Member State may amount to infringement in other Member States that have followed a more restrictive implementation strategy.

22 Second, legal uncertainty with a corrosive effect on research activities can arise from conceptual inconsistencies, mostly due to the improper juxtaposition of teaching and research under the same exceptions. In the context of Article 5(3)(a) ISD and Articles 6(2)(b) and 9(b) DBD, for instance, it is unclear whether the illustration requirement only concerns teaching or is intended to cover use for research purposes as well. Divergent national implementation practices show that both interpretations have informed lawmaking in EU Member States.

23 Third, the research exceptions in the EU *acquis* differ with regard to the spectrum of exclusive rights. While Article 5(3)(a) ISD covers both reproduction and communication to the public, Article 9(b) DBD only covers acts of reproduction ("extraction" in the terminology used in the context of the sui generis database right). The Software Directive (SWD) does not even contain a scientific research provision, and it is unclear whether the existing rules on studying, testing and decompiling computer programs are capable of providing comparable breathing space for research use. The asymmetry between the general research provisions in different EU directives is likely to pose difficulties in the context of research projects. The lack of an entitlement to make protected elements of a database available to the public can lead to a situation where researchers in a larger consortium are inhibited from sharing data resources (extracted from a protected database) with colleagues. It cannot be ruled out that the circle of researchers belonging to a broader research consortium, such as a group of researchers consisting of several teams in different EU Member States, is deemed a relevant public in the sense of copyright and sui generis database law. Accordingly, the sharing of protected database contents within this circle of researchers amounts to an act of making available to the public. As the research exemption in Article 9(b) DBD does not cover the re-utilisation – the making available to the public – of protected database contents, this use falls outside the scope of the use privilege and requires an authorisation for each protected database element. In addition, the missing limitation of the right of making available to the public will prevent researchers from sharing research results with the broader academic community – or the public at large – if these research results contain protected elements of a database. Hence, it is hardly possible to check the replicability of the scientific analysis and verify research results.

24 Fourth, the requirement of use for a "non-commercial purpose" further enhances the legal complexity surrounding the exceptions laid down in Article 5(3)(a) ISD and Articles 6(2)(b) and 9(b) DBD. The requirement also appears outdated, especially in light of the evolving nature of research practices that increasingly involve collaborations with private partners and public-private partnerships, often encouraged and even required by European and national research funding schemes. When the non-commercial use requirement is applied strictly, the mere possibility of research yielding results that can be exploited commercially may already bar researchers from invoking the research exception. As a result, even the commercialisation of research output by technology offices of publicly funded research institutions may create legal complications for researchers who initially – while conducting the research – relied on the research exemption under the assumption of non-commercial use and learned only afterwards – when the project was completed – that the results would be exploited commercially.

25 Fifth, the current lack of a research exception in the area of computer programs leads to imbalances. The EU acquis treats copyright holders in the realm of software (no exposure to an exception for scientific research according to the SWD) more favourably than other right holders who must tolerate certain research freedoms. Conversely, the absence of a general research provision in the SWD disadvantages researchers who need software resources, when their position is compared with colleagues who can invoke the aforementioned research provisions with regard to other work categories and databases.

26 Sixth, it must not be overlooked that in addition to the described issues arising from the wording of the research provisions themselves, the EU acquis poses additional hurdles. The overarching requirement to ensure compliance with the three-step test laid down in Article 5(5) ISD gives rise to the question whether researchers must explain – potentially even with regard to each individual project – that the intended use of resources enjoying protection constitutes a "special case." Moreover, they may have to rebut allegations that the use carried out in a research project has a corrosive effect on the normal exploitation of protected works and/or unreasonably prejudices legitimate interests of right holders.

27 Finally, legal uncertainty and use restrictions can follow from Technological Protection Measures (TPMs) that serve as electronic fences preventing access and use for research purposes. Article 6(4), subparagraph 4, ISD makes this additional legal issue even more pressing. According to this provision,

contractual terms prevail over the research exemption in Article 5(3)(a) ISD in the context of online uses. This decision of the EU legislature exposes researchers to contractual clauses that may exclude use for research purposes altogether.

b.) Text and Data Mining Exceptions

28 Two Text and Data Mining (TDM) exceptions were introduced at the EU level in 2019 by the CDSM Directive. The first of these exceptions is imperative and available to research organizations and cultural heritage institutions acting for research purposes (Article 3 CDSMD); the other is available to any beneficiary, but it is subject to an "opt-out" by rightsholders who have the possibility to reserve the uses for TDM in an appropriate form (Article 4 CDSMD).

29 The configuration of TDM activities as in need of copyright exceptions, while intended to introduce much needed legal certainty in the area (see Recital 8 CDSMD), also implicitly assumed that uses that extract (unprotected) informational value from works, but which do not "use works as works" (so called non-consumptive uses) fall into copyright exclusivity. Formally, this recognition relies upon the broadly defined right of reproduction under Article 2 ISD, not on the recognition of property rights in the informational value of works, as Recital 9 ISD indicates. Simply put, a TDM exception is not needed because the informational value of a work is protected, but because, in order to reach that informational value (e.g., the statistical correlations between the various words and sentences in a text), a number of technical copies are usually made. TDM exceptions are needed to excuse these often temporary, partial and non-literal copies which are nonetheless suitable to trigger Article 2 ISD, as the CJEU confirmed in *Infopaq I* and *II*.[29]

30 Regarding the content of the exceptions, despite the aforementioned important difference in scope, they share several similarities. They enjoy that same, wide, definition of TDM contained in Article 2(2) CDSMD; both are exceptions (mainly) to the right of reproduction; both require lawful access to content - though the respective recitals employ different wording; both allow the retention of copies for scientific research and for text and data mining, respectively; and both have the same intricate relationship with TPMs, as provided in Article 6(2) InfoSoc (see also Article 7(2), second sentence CDSMD).

31 The adoption in 2024 of the AI Act has added an additional layer of complexity to the role of the TDM exceptions. The AI Act has in fact confirmed that Articles 3 and 4 CDSMD are the legislative interfaces between copyright exclusivity and the training of General-Purpose AI (GPAI) models, which rely on TDM as a data acquisition and analysis technique (Recital 105 and Article 53 AIA).

32 The resulting picture is complex and multifaceted. On the one hand, EU actors now have two legal provisions addressing TDM which have indisputably brought legal clarity in important areas (e.g., the imperativeness of Article 3 CDSMD, the possibility to retain copies, etc). At the same time, other conditions are still in need of further elaboration to reach the intended effects, such as, for instance, the precise form of the reservation of rights under Article 4 CDSMD.

33 From the standpoint of research organizations and cultural heritage institutions, a number of issues remain unanswered. The many conditions found in Article 3 CDSMD (e.g., beneficiaries, lawful access, focus on right of reproduction, TPMs, public-private partnerships, etc), considerably reduce the usefulness of the exception for research organizations. In more abstract terms, approaching a basic analytical technique (this is TDM) through the regulatory mechanism of a copyright exception, instead of the more structural approach of a fundamental rights (e.g., right to research), almost inevitably leads to the compression of constitutionally protected rights. Against this background, it should be assessed whether the presence of Article 4 CDSMD and its elevation to a sort of Copyright-Generative AI interface may further dilute the importance of an already too narrow provision, such as Article 3, intended to exempt activities falling under the umbrella of public interest research. That said, as the first national pronouncements have demonstrated, the decried peril to "circumvent" Article 4 via Article 3 has been proven fictitious. In other words, commercial actors interested in using datasets developed on the basis of Article 3 require a proper license from rightsholders if the opt-out was exercised.

c.) Secondary Publication Right

34 Funders of research in the EU and in Member States increasingly require that research outputs be made openly available. In many cases publishers control copyright, which is either transferred or exclusively

29 See Case C-5/08, *Infopaq I*, EU:C.2009:465, and C-302/10 *Infopaq II*, EU:C.2012:16. Cf. Thomas Margoni, Martin Kretschmer, 'A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology', GRUR Int, vol.71(8), 2022, pp.685-701.

licensed as a precondition for publication. The development towards open access through reform of the publishing system has so far been a slow process, involving complicated negotiations between research organisations and commercial publishers. A statutory secondary publication right is an important means to ensure at least some level of openness.

35 Until now, six Member States (Germany, France, Belgium, Austria, the Netherlands and Bulgaria) have introduced, either in their copyright statutes or in an independent act, a secondary publication right (SPR). The SPR attributes to the author of a scientific work, variously defined (see below), the right to make it publicly available after a certain period of time (the so-called "embargo" period) following its first publication, openly and free of charge, subject to certain conditions. Usually framed as not overridable by contract, the SPR represents a safety valve to facilitate the dissemination in OA of scientific works regardless of the conditions set by publishing contracts.

36 All national solutions converge on the definitions of the basic requirements for SPR to operate, although divergences remain. The subject-matter is generally limited to scientific contributions published in periodicals (e.g. journal articles), with the exclusion of monographs or book chapters. However, the language used is not homogeneous. Germany and Austria require "a scientific contribution", France a "scientific writing", Belgium a "scientific article", the Netherlands a "short scientific work", with the additional requirement (but not in the Netherlands and Bulgaria) of inclusion in outlets published periodically (Belgium) or at least once (France) or twice (Austria, Germany) a year. There is no full convergence either on the version of the product to which the SPR applies. While Germany, Austria, Belgium and France admit only the so-called author-accepted manuscript (AAM, that is the post-peer review draft without typesetting), the Dutch definition does not impose any limitation.

37 All Member States require the work to originate from research that has been funded wholly or partially by public funds. However, the percentage (from 50% to "at least partially") as well as other specific requirements vary. The same variations appear with regard to the duration of the embargo period that should pass between the first publication and the exercise of the SPR. Options range from one year without distinctions (Germany and Austria) to six months for natural sciences and one year for the humanities and social sciences (France and Belgium), with Bulgaria opting for no embargo, and the Netherlands referring to a "reasonable period". Additional requirements may be present, such as the agreement of all co-authors (France). Member States converge, instead, in declaring the provision unwaivable and not overridable by contract, making any contrary clause null and void, and in requesting the indication of the original source and the republication to be for non-commercial uses only (with the exception of Belgium).

38 National SPRs have been introduced with the aim of offering to authors of scientific works who do not want or cannot afford opting for paying OA (the "Gold" route) the possibility to republish for free in repositories the AAM version of their work ("Green" OA), and thus comply with the OA obligations set by an increasing number of funding institutions, without struggling with the acceptance and subsequent compliance with non-negotiable standard model publication agreements that may ban Green OA practices.

39 Surveys and studies conducted in the past years have demonstrated a general lack of awareness among stakeholders about the availability of SPRs.[30] This circumstance, coupled with copyright territoriality, have negatively impacted on the effectiveness of the instrument, which have been only moderately used, and only in the context of publishing agreements governed by the law of one of the six Member States featuring SPRs. In fact, these reforms had limited or no impact on the practice of international journals whose standard agreements are subject to other national laws. At the same time, divergences among national solutions have also created further barriers to the development of common practices among publishers and stakeholders in different Member States, further reducing the potential impact of existing SPRs, and triggering the risk of forum shopping to avoid the application of national SPR provisions.

40 At the same time, specific features of existing SPRs have already proven their shortcomings in the implementation phase. The discrimination between journal articles and other publications or products have substantially circumscribed the number of research outputs eligible for SPR. Longer embargo periods have substantially frustrated the potential impact of a broader dissemination in OA of research results in sectors or topics where findings get fast outdated, conflicting with the basic OS goal of achieving greater and more immediate access to scientific findings. Similarly, the uncertain interpretation of the public funding benchmark has triggered chilling effects in the application of SPR in instances such as publications by non-tenured staff members or those funded by private funds, or outputs stemming from multiple projects within extended partnerships, where the percentage of public funding could be difficult to calculate

30 Cf ERA Study 2024 at p.54 et seq.

with certainty. The same can be said for the non-commercial use requirement. In contemporary research practices, public-private partnerships are not only increasingly common, but often a prerequisite under national funding schemes. Limiting SPRs to non-commercial uses creates legal uncertainties in projects conducted with private partners, particularly in cases where the funding scheme requires a commercial use of the project's results.

41 While being a positive addition and a remarkable step forward in aligning national copyright frameworks with the EU Open Science and research policy goals, the actual implementation of national SPRs have evidenced flaws that, due to their inevitable cross-border nature and impact on the ERA, clearly call for an EU-wide intervention.

d.) Interface Copyright-Data Regulation

42 The growing body of data legislation at EU level intersects with existing copyright law. The AI Act, Digital Services Act and Digital Market Act are well-known examples[31]. In the copyright realm there is less attention for the interface with the Open Data Directive ("ODD"), Data Governance Act ("DGA") and Data Act ("DA").[32] From the perspective of research and academic freedom, the most significant interface with copyright is in the ODD and DGA.[33]

43 The Open Data Directive obliges public sector bodies to allow re-use of information they hold for commercial and non-commercial purposes as freely as possible. This includes the re-use of copyrighted materials, unless these are subject to third-party (intellectual property) rights. The position of public research organisations is not entirely clear. They qualify as public sector body under the ODD's definitions, but the ODD also contains a specific provision mandating that free use be allowed of "research data" (a broad term, also encompassing IPR protected materials including academic publications) made public in repositories (Article 10(2) ODD). This means that the ability to exercise copyright prerogatives freely by researchers and research organisations (esp. academics at public universities) is restricted by the ODD. Such restrictions can also result from the 'open access' policies for research data that Member States are obliged to develop (Article 10(1) ODD).

44 Of note, where obligations under the ODD *curb* the freedom to keep access to research outputs controlled, also through the use of copyright, a secondary publication right can in fact *help* academics make research outputs more open, especially if the SPR is structured as a rights retention. In any case, to prevent possible conflict and legal uncertainty, the obligations and objectives of the ODD should be taken on board in the crafting of a harmonized SPR. What is also worth noting is that the ODD is blind to the fact that the academic freedom of individual researchers may be at odds with a public institution's policy. Notably, copyright is a key instrument for individual academics to retain control over how their work is used (e.g. in predatory OA journals, in onerous contexts that harm academic integrity or reputation). Being forced to publish open access under a permissive license (such as CC-BY) effectively means relinquishing control, which can be at odds with academic freedom.

45 The Data Governance Act (DGA) addresses a variety of issues. What is relevant for the purposes of this Opinion is that it extends the principle of openness from the ODD to public sector-held information that is subject to third party copyright or other intellectual property rights. The DGA does not regulate the position of public sector bodies in the research and education field specifically and there is some ambiguity about their position, e.g. to what extent they must try to retain copyright, or try to secure copyright permissions of third parties, with a view to opening up research data and outputs.

46 The law is silent on how the re-use provisions of the ODD and DGA relate to the TDM exceptions of

31 As highlighted also by previous ECS Opinions. See, e.g., European Copyright Society Comment on Copyright and the Digital Services Act Proposal, 17 January 2022, available at https://europeancopyrightsociety.org/wp-content/uploads/2022/01/2022-01-17-ecs-comment-on-copyright-and-the-digital-services-act-proposal-4.pdf; Opinion of the European Copyright Society on selected aspects of the proposed Data Act, 12 May 2022, available at https://europeancopyrightsociety.org/wp-content/uploads/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf; Copyright and Generative AI: Opinion of the European Copyright Society, January 2025, available at https://europeancopyrightsociety.org/wp-content/uploads/2025/02/ecs_opinion_genai_january2025.pdf

32 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information ("ODD")); 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 | "DGA"); 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 | "DA"). The Data Act becomes effective on 12 September 2025.

33 See Mireille van Eechoud, 'Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research', Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2777/71619 and ERA Study 2024, pp 205-208.

the CDSM Directive, or to any other limitations or exemptions relevant to research and education for that matter. This results in legal uncertainty, which triggers chilling effects on researchers and research-performing organisations and thus weakens the potential of such provisions to operate concurrently to pursue OS goals.

47 Finally, the ODD and DGA prohibit public sector bodies from exercising their sui generis database rights (not their copyright in databases). At the same time, Article 43 of the Data Act excludes data generated by Internet-of-Things products from sui generis database protection regardless of who the database producer is. The introduction of such limits outside copyright/intellectual property instruments adds to the complexity of the system as a whole.

4. The Way Forward: Policy Recommendations

48 Against the flaws and challenges raised by the current regulatory state of the art, the ECS believes that the EU legislator should carefully consider the opportunity to proceed with the following interventions, listed in order of time feasibility (short-term vs medium-term).

a.) Introduction of an EU-Wide Secondary Publication Right

49 It is clear that, to achieve a unified ERA inspired by shared OS principles, the introduction of a harmonized EU-wide SPR that builds on the experiences already developed by six Member States may represent the most time-effective and realistic policy solution, tackling one of the currently greatest stumbling blocks to the full realisation of a fairer and more accessible internal market for research. Also, in light of the national fragmentations triggered by local legislative initiatives, such a harmonized solution would also prevent nationality-based or geographic discrimination, achieve greater legal certainty, and avoid forum shopping in the scientific publishing sector.

50 One of the key challenges to tackle is striking a proper balance between conflicting fundamental rights (Articles 11-13 vs Article 17(2) CFREU), taking into account the effective bargaining powers of the parties involved, without unduly curtailing the operation of the SPR and thus frustrating the fulfilment of its function of leverage to attain ERA's OS goals. Conditions of applicability and other requirements should be carefully tailored and defined with precision, in order to avoid legal uncertainties (and related chilling effects) and fragmentation in national implementations, should the EU-wide SPR be introduced via a Directive. This would perpetuate the challenges currently faced by researchers when dealing with different national SPR regimes, with no benefit for the correct functioning of the ERA.

51 Against this background, it is clear that the EU legislator should exercise utmost care when defining the parameters and requirements of the EU SPR regime, by taking into account, *inter alia*, the evolution of business models in the scientific publishing sectors (e.g. APC and double-dipping, transformative agreements, greater value generated by additional platform/data aggregation services, etc.), the variety of research output produced by researchers, trends of public-private partnerships, evolving practices of research funding organisations and their expectations, differences in the practices of various scientific disciplines. This constitutes the basic background to perform a comprehensive impact assessment of a reform that aims at striking a fair balance between conflicting interests while effectively enhancing OA to research outputs, thus supporting the development of a unified ERA built on OS principles.

52 To properly fulfil this function, an EU-wide SPR should have a number of minimum features.

1) First, the SPR should have a mandatory and imperative nature against contractual overridability. This represents an inevitable prerequisite for any SPR to perform its institutional function of rebalancing the bargaining power of scientific authors and publishers and avoid contractual carve-outs of Green OA options.

2) With regard to the subject-matter, it is also advisable to consider extending the scope of the SPR to cover a wider range of research outputs. The problems and uncertainties engendered by different national solutions require a harmonizing intervention that also takes into account the diversification of academic practices in different fields and the related greater variety of research products that go beyond the mere category of journal articles. This approach would also be more aligned with the protection and fulfilment of the fundamental right to research, based on Articles 11 and 13 CFREU, and more adequate to strike a fair balance between the related need to protect research openness and autonomy and the protection of copyright under Article 17(2) CFREU. Against this background, it is necessary to consider the possibility to extend the scope of an EU-wide SPR to cover a broader range of products, especially to the benefit of those

disciplines where journal articles constitute only a limited share of research outputs. To the extent other products such as data collections, blog posts and other outputs are covered by IP rights and pose similar barriers to OA practices, this circumstance should be properly taken into account when framing the subject-matter of a harmonized SPR. In this sense, it is advisable to set the external boundaries of the objective scope of the right on the basis of a thorough impact assessment, which should shed light on the detriments publishers would suffer from the inclusion of each and any form of scientific output, compared to the benefits such an inclusion would produce in terms of greater OA availability of research results for researchers and the society at large.

3) Similar caution should be exercised when setting any public funding requirement. Introducing a high threshold may carve out from the scope of the SPR a great part of the results of projects based on public-private funding schemes. At the same time, the setting of any threshold should be accompanied by a very detailed definition of the elements that are relevant for the definition of "public" or "private" funding, in order to limit to the maximum extent possible the uncertainties that have tainted the application of national SPRs in the past years. More generally, the identification of the public funding benchmark should be based on an assessment of the impact the requirement may have on the legitimacy of private exploitation interest. A high quota of public funding decreases the legitimacy of private interest in exploiting research results, since the output is offered to the publisher free of charge. However, this does not change in the case of public-private partnerships, since in no case is the publisher that finances the research from which the article or other output stemmed, and its investments are limited to the management of the peer-review and editorial process and the marketing of the final product. In this sense, there seems to be no objective basis to justify the subordination of the SPR to a public funding requirement. The EU legislator may decide to limit the instrument to the mere function of making publicly funded research outputs available to the public in OA, or to aim at a greater range of scientific knowledge available in OA by lowering the threshold (or eliminating it), thus including also a larger number of outputs stemming from more public/private research partnerships.

4) The introduction of an embargo period should be carefully considered. From the perspective of researchers, immediate access to scientific fundings is of fundamental importance to stay abreast of the state of the art and build their own research on this basis. From the perspective of publishers, embargo periods limit the impact of SPR on their business model and primary markets, for it postpones the dissemination of a substitute of their published products to a later stage and makes them retain their competitive advantage for the interim period between first and second publications. When deciding on this requirement, the EU legislator should perform a careful assessment and balancing between such conflicting interests. An additional element to be considered is that the added value of a proprietary journals database subscription may lie more in their nature of one-stop-shop (with connected data-related services and internal connections between results), while the secondary publication of a single article may only act as a substitute for a single contribution. Additionally, attention should be paid to the fact that embargo periods have different legal effects depending on the copyright management strategies adopted by the publisher. When the relationship between author and publisher is based on a non-exclusive license, or on an implied contract where neither the transfer nor an exclusive license in favour of the publisher is provided, embargoes translate such agreements into a de facto exclusive license. This effect and the distinction should be carefully taken into account and reflected upon when devising an EU-wide SPR.

5) Another feature introduced by the majority of national SPR is the limitation of the right to the author-accepted manuscript (AAM) version only. The choice is dictated by the aim of avoiding a pure substitution effect between the first and second publication, which it is argued would happen were the SPR to allow the free distribution of the version of record (VOR, i.e. the publisher's edited version with typesetting). From the perspective of researchers, extending the SPR to the VOR would be preferable, as this would ensure the circulation of a single version of the work, certainty on the final/correct version, and a consistent and proper referencing and verification. From the perspective of publishers, the abovementioned substitution effect is perceived as a threat to their return on investment on the review, typesetting and pagination processes, which would in turn act as a disincentive to invest and lead to lower publication quality. While the actual impact on publishers' interests depends on whether their copyright management strategy uses exclusive or non-exclusive assignment schemes, in order to adopt the right policy option, the EU legislator will nevertheless need to strike a fair balance between these two conflicting

sets of needs and objectives. Elements to be considered are the potentially different impact of covering the VOR for different types of outputs (journal articles, books, book chapters, datasets etc) if appropriate; the presence of publishers' exclusive rights on the layout and typographical arrangements; referencing and verification habits of different academic sectors; effective substitution effects and their impact in different disciplines.

6) The last element to be carefully evaluated when devising an EU-wide SPR is the opportunity to introduce a non-commercial use limitation. As mentioned, Member States have adopted remarkably divergent stances on the matter. From an OS perspective, such a limitation is not advisable in light of the uncertainties it may trigger, with related chilling effects on researchers. From the publishers' perspective, the requirement acts as a guarantee against exercises of the SPR which may directly compete with the first publication. Here, the same considerations made on the embargo period and related substitution effects apply. The evolution of publishers' business models sees article processing charges (APC) offered to authors willing to pay to have their works in OA, flanked with more expensive subscription models and structured databases that also offer additional resources (particularly data and their aggregations), which tighten the dependency of researchers and academic institutions on publishers beyond the mere access to single published articles. In this sense, the added value and competitive advantage of granting exclusive access to single publications is much lower than in the past. This element should also be considered when conducting an assessment of the impact on SPR exercised for commercial uses, and weighted against the impact that such a limitation may have on the range of products available in OA.

b.) Introduction of a General Mandatory Research Exception

53 In line with CJEU jurisprudence, the reconciliation of competing fundamental rights must take place internally: within the system of exclusive rights and limitations in EU copyright and sui generis database law. As the analysis has shown, the current EU acquis is unlikely to offer sufficient breathing space for this balancing task. The existing research rules have structural deficiencies, ranging from fragmented and overly restrictive research exceptions to opaque lawful access provisions, outdated non-commercial use requirements, legal uncertainty arising from the three-step test, obstacles posed by the protection of paywalls and other technological measures, and exposure to contracts that override statutory research freedoms. To arrive at a copyright framework that is conducive to research in line with the described ERA goals, it should be considered to:

1) clarify that the requirement of use as an "illustration" in Article 5(3)(a) ISD and Articles 6(2)(b) and 9(b) DBD only concerns the teaching branch of the use privilege and does not relate to scientific research;

2) abandon the outdated requirement of use for a "non-commercial purpose" and only require compliance with the three-step test, following the model in Article 10(1)(d) and (3) RLRD;

3) clarify that, regardless of the volume of use, scientific research constitutes a "special case" in the sense of the three-step test of Article 5(5) ISD because of the fundamental rights underpinning following from Articles 11(1) and 13 CFREU;

4) declare the fourth subparagraph of Article 6(4) ISD inapplicable to use for the purposes of scientific research, as already done in Article 7(2) CDSMD with regard to scientific TDM, and ensure that the application of TPMs does not hinder the exercise of Article 5(3)(a) ISD;

5) declare any contractual provision contrary to use privileges for scientific research unenforceable, as already stated in Article 7(1) CDSMD.

54 In contrast to the current, optional research exceptions in Article 5(3)(a) ISD, Articles 6(2)(b) and 9(b) DBD and Article 10(1)(d) RLRD, a more flexible and robust exemption with these conceptual contours should constitute a mandatory "shall" provision to ensure a harmonised application across Member States and comparable conditions for research teams in different countries. Moreover, the strengthened provision should cover both the right of making copies for research purposes (reproduction) and the right of sharing these copies (making available to the research group). Finally, it is advisable to implement the proposed more flexible and robust use privilege for scientific research not only in the field of copyright, related rights and sui generis database protection but also in the area of computer programs, where an open-ended research provision is currently missing.

55 Proposing these amendments, benefits for society as a whole must not be overlooked. An open-ended research provision with the described conceptual contours can render EU copyright and sui generis database law capable of keeping pace with the rapid

evolution of new technologies and changing research approaches and methodologies. A narrow research exception that only supports known research needs and methodologies will inevitably fail to offer a basis for new, previously unknown approaches. In contrast to a specific, narrow research privilege, a general provision enables the research community to analyse developments in the increasingly digital and algorithmic information society – with all rapid changes in information technology and modes of communication. It would strengthen research autonomy by providing a basis for exploratory research projects and methodologies that fall outside traditional approaches and categories.

c.) Amendment of the Text and Data Mining Exceptions

56 Text and Data Mining, defined as "any automated analytical technique aimed at analysing text and data in digital form" is a broad definition that, in the digital environment, is capable of capturing most activities conducted by scientific researchers. Consequently, any restriction applied to the concept or scope of TDM is suitable to directly restrict research activities. It is therefore of utmost importance for a thriving research environment to safeguard a broad and protected space for research, including research performed via TDM, and to only introduce restrictions to this space in clearly defined and well justified cases.

57 Against this background, the main features of Article 3 CDSMD that may constitute an unnecessary or not well defined limitation to research done via TDM are: the requirement of lawful access, the beneficiaries of the provision, the purposes covered, the rights of economic exploitation exempted, the faculty to retain copies, as well as the impact of technological and integrity measures on Article 3 CDSMD. In order to offer an interpretation of these concepts that complies with the aforementioned principles, the following policy recommendations are proposed.

1) Lawful access. The concept of lawful access in Article 3 CDSMD should be conceived broadly and, as it has been argued in the literature, not be linked to the current standards developed by the CJEU for the cases of lawful sources (e.g. *ACI Adams*[34]) or to the concept of consent in relation to communication to the public (e.g. *Renckhoff*[35]). On the contrary, lawful access should: a) focus on the acts carried out by the researcher; and b) build upon the examples offered in Recital 14 CSDMD, particularly the expression "freely available online" in relation to the content that can be lawfully accessed.

2) Beneficiaries. The current text of the CDSMD offers a detailed definition of research organizations.[36] As recent national case law has indicated, this definition is capable of covering research activities carried out by non-academic institutions. However, individual researchers, not affiliated with a research institution, seem to fall outside the scope of this provision. Given the rise of non-institutional scientific research, such as citizen science, it would be important to further elaborate this concept in order to avoid excluding individual contributors to scientific research, a practice that is particularly important to "democratise" the scientific process.

3) Purposes. The purpose of scientific research appears both as an element in the main text of Article 3 CSDMD, as well as a definitory component of the concept of research organizations in Article 2 CDMSD. This redundancy may not necessarily be problematic. However, as it has been pointed out, research purposes do not cover some important, and arguably research-related, activities, such as investigative journalism.[37] This limitation to the scope of Article 3 CDSDM should be further assessed as it could create unjustifiable differential treatment to equally protected rights.

4) Rights and subject matter (software) exempted. The current text of Article 3 CSDMD exempts the right of reproduction for copyright and the right of extraction and re-utilization for the sui generis database right in databases; the right of reproduction for works and other subject matter covered by Article 2 ISD; and the right of reproduction and making available to

34 Case C-435/12 *ACI Adam BV and Others v Stichting de Thuiskopie*, EU:C:2014:254.

35 Case C-161/17 *Land Nordrhein-Westfalen v Dirk Renckhoff*, EU:C:2018:634.

36 "A university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research: (a) on a not-for-profit basis or by reinvesting all the profits in its scientific research; or (b) pursuant to a public interest mission recognized by a Member State; in such a way that the access to the results generated by such scientific research cannot be enjoyed on a preferential basis by an undertaking that exercises a decisive influence upon such organization".

37 Similarly, see ECS, Comment of the European Copyright Society addressing selected aspects of the implementation of Articles 3 to 7 of Directive (EU) 2019/790 on Copyright in the Digital Single Market, supra at n 6.

the public of press publications under Article 15 CDSMD. The strong focus on the right of reproduction and the absence of software from the scope of Article 3 CDSMD stand out and have the potential to create uncertainty and legal fragmentation. For instance, Article 5(3)(a) ISD which was the basis for pre-2019 national TDM exceptions also exempts the right of communication to the public. This is particularly important since the CDSMD clarifies that "The existing exceptions and limitations in Union law should continue to apply, including to text and data mining ... as long as they do not limit the scope of the mandatory exceptions or limitations provided for in this Directive". The absence of software in the scope of Article 3 CDSMD raises interpretative uncertainty, particularly in the light of the fact that software is present in the scope of Article 4 CDSMD. It should be clarified whether the absence is intended to allow Member States to decide whether to include software in their national implementations or on the contrary whether such absence is intended as a form of negative pre-emption.

5) The retention of copies. Article 3(2) CDSMD permits the storage of copies made during TDM "for the purposes of scientific research, including for the verification of research results". This is a very important element of the EU TDM framework, particularly in the case of research. However, it is not clear whether these copies can be further shared with fellow researchers, particularly outside the research institution. These practices are essential for the purpose of "scientific research" and for the verification of results. However, the potential to trigger the (not exempted) right of communication to the public may deter researchers and their institutions from sharing these copies and thus frustrate an essential element of the scientific process.

6) Technological and integrity measures. While Article 7 CDSMD importantly clarifies the unenforceability of contractual limitations to Article 3 CDSMD, a similar degree of clarity in relation to TPMs is absent. An additional element of uncertainty refers to the unclear relationship between TPMs and the new concept of "security and integrity measures" of Article 3(3) CDSMD which right holders are allowed to adopt. Whereas in principle this category and its function are justifiable (for example the use of application programming interfaces (APIs) for a safe and efficient access to a resource), the unclear definition and the relationship with TPMs creates unnecessary ambiguity (for example the use of APIs so restrictive that frustrate the scope of scientific research central to Article 3 CDSMD).

d.) Interface Copyright-Data Regulation

1) As the growing body of data legislation in the EU affects scientific research at the level of institutions and individual researchers and also has multiple copyright dimensions, it is advisable to maximize efforts to reduce legal complexity and ensure consistency across instruments. The legal complexity of the system of rules impacting research can be reduced by pursuing a more holistic approach. Specifically, the introduction of copyright related rules in multiple legislative instruments [outside of copyright law] should be avoided. Should this not be possible - as in the case of a potential European Research Act, the EU legislator should exercise utmost care in streamlining definitions and ensure consistency with the EU copyright acquis and its key tenets.

2) The Open Science policies (including open access) currently have little consideration for the academic freedom of individuals, especially as regards the ways in which limiting the exercise of copyright prerogatives can adversely affect academic freedom. Certainly, where Open Science policy is increasingly expressed in binding norms, it is important to ensure these norms are consistent with key principles of copyright such as the centrality of the natural person as creator.

3) To prevent possible conflict and legal uncertainty, the design of any harmonized secondary publication right should be consistent with the obligations and objectives of the Open Data Directive and Data Governance Act that promote access and re-use of research outputs.

Drafting Committee:
Caterina Sganga, Christophe Geiger, Thomas Margoni, Martin Senftleben, Mireille van Eechoud

Signatories

Prof. Lionel Bently, Professor of Intellectual Property Law, University of Cambridge, United Kingdom

Prof. Estelle Derclaye, Professor of Intellectual Property Law, University of Nottingham, United Kingdom

Prof. Séverine Dusollier, Professor, Sciences Po Paris,

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu