Shaping the field of EU Data Law

by **Nine Riis**[*]

Abstract: The lawmakers in Brussels have worked relentlessly in recent years on enacting legislation targeting data. Yet, data legislation and the associated research have so far been conducted through the lenses of traditional fields of law, such as copyright law and fundamental rights law. While some authors do use the term "EU data law", almost no works exist that elaborate on the term and set out the value in conceptually working with an independent field of EU data law. To bridge this gap, the article demonstrates how EU data law can be classified as an autonomous legal field pursuant to the theory of factual classification. Furthermore, it shows how EU data law diverges from adjacent legal fields by striving to safeguard five distinct objectives stemming from data's particular characteristics. The objectives can be summarised as protection of the following: (i) a competitive market, (ii) fundamental rights, (iii) consumers, (iv) trustworthiness and (v) Open Data. The article argues that to effectively create, interpret and enforce data legislation, it is necessary for the EU lawmaker to take into account all of these objectives, thus making classification an essential tool for ensuring a coherent body of data legislation. Moreover, the article advances that there is a dichotomy within EU data law between economic goals and fundamental rights. While such a dichotomy is not an issue in itself, it is problematic if it is not taken adequately into account by the legislator when proposing and enacting data legislation. The article concludes that the EU legislator must actively acknowledge the effects of the dichotomy in order to ensure a coherent data legislation capable of sustaining a digital European society.

A. Introduction

1 The EU legislator has developed an avid interest in regulating data. The lawmakers in Brussels spare no time and they propose and enact new legislation targeting data at an unprecedented speed. Since 2018, the GDPR,[1] NPDR,[2]

P2B Regulation,[3] Open Data Directive,[4] Data Governance Act[5] and Digital Markets Act[6] have

---

[*] PhD Fellow at the Centre for Private Governance at the Faculty of Law, University of Copenhagen (nineriis@jur.ku.dk). I thank Associate Professor Sylvie Cécile Cavaleri for helpful feedback. Any errors are my own.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2018] OJ L 119/1 (GDPR).

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

OJ L303/59 (NPDR).

[3] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57 (P2B Regulation).

[4] 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 L172/56 (Open Data Directive).

[5] 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 (Data Governance Act).

[6] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022]

entered into force. Moreover, proposals for the Data Act[7] and the AI Act[8] are in progress and closely followed by scores of stakeholders both inside and outside the EU.

2 Despite the flurry of regulatory activity, data legislation and the resulting extensive research on data-related issues have mainly been conducted through the lenses of the traditional legal fields.[9] The most extensive activities have been undertaken within copyright law,[10] consumer protection law,[11] competition law,[12] data protection law,[13] and fundamental rights law.[14] This is a logical development as the increased use of data impacts many different parts of our society. Yet, the approach is problematic, because each legal field has

its own set of objectives and criteria for balancing such objectives against each other. When EU data regulation uncritically incorporates core elements from different legal fields, it creates an inherent tension in the legislation.[15] The tension is caused by the (often) contradictory objectives of the fields the legislator uses as steppingstones for the new legislation. Further, the approach results in a fragmented regulatory framework that governs unrelated legal issues within the same Directive or Regulation. On the whole, this obfuscates legal certainty.

3 Against this backdrop, the present article argues that EU data law is an autonomous legal field. The argument for a field of EU data law has been advanced before[16] and several authors use the term as an established concept.[17] In spite of this, there is almost no literature on the theoretical way of classifying the field and why it is valuable to treat data-related legal issues within EU data law. The present article fills this gap by using theories of classification to delimit EU data law and demonstrate that EU data law has its own objectives that diverge from those of adjacent fields of law. Further, it argues that insufficient awareness of EU data law as an independent field of law is an obstacle on the road to a coherent body of EU data legislation that can stand the test of time in the coming digital decades.

OJ L265/1 (Digital Markets Act).

7 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 (proposal for the Data Act).

8 Commission 'Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' (proposal for the AI Act).

9 Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Data Law* (Oxford University Press USA 2021) 903.

10 Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1995] OJ L77/20 (Database Directive) (currently under revision see <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-database-directive>accessed 20 December 2022) and proposal for the Data Act art. 35.

11 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28 (Sale of Goods Directive) and 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 L136/1 (Digital Content Directive).

12 Digital Markets Act, NPDR, Open Data Directive, Data Governance Act and proposal for the Data Act (in particular, chapters 2-4).

13 GDPR.

14 Commission 'Proposal for a European Declaration on Digital Rights and Principles for the Digital Decade' COM (2022) 28 final.

15 Streinz (n 9) 903; Joan Lopez Solano and others, 'Governing Data and Artificial Intelligence for All: Models for Sustainable and Just Data Governance.' (European Parliamentary Research Service 2022) 1.

16 The following works touch upon the topic: Christian Berger, 'Property Rights to Personal Data? – An Exploration of Commercial Data Law' (2017) 9 Zeitschrift für geistiges Eigentum (ZGE) 340; Björn Steinrötter, 'The (Envisaged) Legal Framework for Commercialisation of Digital Data within the EU' in Martin Ebers and Susana Navas (eds), *Algorithms and Law* (Cambridge University Press 2020); Streinz (n 9) Streinz is the most thorough work on the topic to date. Streinz' work has a broader scope than the present article by focusing on the evolution of EU data law and on its intersection with the general regulation in the EU.

17 See, for example, the abstract of Linda Kuschel and Jasmin Dolling, 'Access to Research Data and EU Copyright Law' (2022) 13 JIPITEC; Clarissa Valli Buttow and Sophie Weerts, 'Public Sector Information in the European Union Policy: The Misbalance between Economy and Individuals' (2022) 9 Big Data & Society 2 (who defines the term in a footnote as a body of legislating in EU regulating data as an object); Neil Cohen and Christiane Wendehorst, 'ALI-ELI Principles for a Data Economy' 19.

B. Classification of the law

4   On the one hand, it can be argued that classification of the law is an irrelevant and theoretical task. Classification does not normally influence the substantive legal analysis,[18] on the contrary, legal analysis is rarely bothered by a sharp division between different fields of law. If a lawyer is tasked with drafting a contract for IT services, they need to pay heed to contract law and implications from tax, competition, data protection and intellectual property law. This arguably makes classification appear a superfluous and formalistic task.

5   On the other hand, we operate with classification almost constantly when working as both practitioners and researchers. Many law firms and research institutions are organised in departments or working groups according to specialty. Further, few lawyers see themselves as generalists but rather specialise in one or several legal fields. This has, firstly, a practical purpose. The law and the number of legal sources is virtually unlimited and without any form of system, it is nearly impossible to know where to start when encountering a legal problem.[19] In the absence of classification, it would be an insurmountable task for a lawyer to master the law[20] and for law students to effectively embark upon their studies.[21] Secondly, classification allows for the identification of the distinct objectives of a legal field.[22] The objectives of a legal field are the values and interests the field persistently strives to safeguard. It is only with awareness of these objectives that legislators, practitioners and judges know how to create, interpret and enforce the law coherently.[23] This is, in particular, relevant for EU law as the Court of Justice of the EU (CJEU) often uses a teleological method of interpretation in the case of inconsistent provisions in EU legislation.[24]

Consequently, classification is crucial in the quest for legal certainty.

6   Yet, an important note in this regard is that classification is not an end in itself.[25] Rather, classification is a tool to effectively create, interpret and enforce the law. Accordingly, there is no universally correct form of classification and any attempt to identify one would be in vain. Instead, efforts should be made to argue why a specific form of classification is the most useful for creating a coherent field of law. The present article does not argue that the traditional fields of law within which data-related legal issues have so far been handled are irrelevant or obsolete. It argues that for the purpose of creating and enforcing data legislation, it is important to work within the field of EU data law to ensure that all relevant objectives are taken into account.

7   In the case of EU data law this article argues for internal factual classification based on the subject matter *data*. The classification is *internal*, because it only identifies the field of EU data law as opposed to classifying the whole of the law into different fields; the latter would take the form of *external* classification.[26] Factual classification is one of the most favoured classification forms.[27] Factual classification divides the law based on the part of social or economic life the relevant legal rules are most naturally associated with.[28] A particular relevant parameter in this regard is the subject

---

the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Columbia Journal of European Law 3, 31.

25   Pound (n 18) 944.

26   Albert Kocourek, 'Classification of Law' (1933) 11 New York University Law Quarterly Review 319, 322.

27   Authors arguing for factual classification are, for example, JA Jolowicz, 'Fact Based Classification of the Law' in JA Jolowicz (ed), *The division and classification of the law* (Butterworths 1970) 7; WL Twinning, K O'Donovan and A Paliwala, 'Ernie and the Centipede' in JA Jolowicz (ed), *Division and classification of the law* (Butterworths 1970) 29; Peter Seipel, *Computing Law - Perspectives on a New Legal Discipline* (LiberTryck 1977) 201 (naming it 'functional' classification). Please note that Seipel also reference both of the before mentioned works.

28   Note that the criteria used for factual classification vary. Jolowicz (n 27); Twinning, O'Donovan and Paliwala (n 27) 20 and; Seipel (n 27) 199f. focus more on the subject matter, for example, 'contracts' or 'computers' to which the legal rules apply, whereas Ross (n 19) 264 adopts a broader view of '[...] typical areas of life'.

---

18   Roscoe Pound, 'Classification of Law' (1924) 37 Harvard Law Review 933, 939.

19   Alf Ross, *On Law and Justice* (Jakob vH Holtermann ed, Uta Bindreiter tr, Oxford University Press 2019) 242; Pound (n 18) 943f.

20   Ross (n 19) 242.

21   See also Pound (n 18) 944.

22   Ross (n 19) 242f Ross does not use the term objectives, but refers to the '[...] principles and ideas which express the prevailing values within the legal area [...]'.

23   See also Pound (n 18) 944 who states: 'Legal precepts are classified in order to make the materials of the legal system effective for the ends of law'.

24   Koen Lenaerts and Jose A Gutierrez-Fons, 'To Say What

matter to which the legal rules apply.[29] For example, the field of construction law is commonly delimited based on the subject matter of construction agreements. Factual classification is in contrast[30] to conceptual classification, where the latter delimits the law according to the specific characteristics of the legal norms and their underlying concepts.[31] Pursuant to conceptual classification, it could, for example, be argued that public law consists solely of rules in the form competence norms.[32] Factual classification is likely favoured due to the ease of understanding the classification for persons outside the legal field.[33] Conceptual and factual classification are not the only forms of classification but the most common ones.[34]

8   However, there is an inherent risk in using factual classification. If the law is classified according to subject matter, an unlimited number of legal fields are identifiable at the risk of rendering classification meaningless: a danger that Easterbrook warns against in his infamous article "Cyberspace and the Law of the Horse".[35] Easterbrook's main argument is that even though horses are without a doubt a particular species, cases concerning horses do not give rise to any distinct legal issues. Tort or contract law cases on horses do not examine problems different from those within general tort and contract law. [36] Consequently, such a legal field "[…] is doomed to be shallow and miss unifying principles".[37] In order to avert the danger highlighted by Easterbrook, factual

classification must be supplemented by something more than subject matter. "Something more" is difficult to qualify. Assistance is offered by theorists of comparative law who have struggled with similar issues when classifying legal systems. Zweigert and Kötz argue that a specific legal system is distinguished by its *style*.[38] Zweigert and Kötz define style as, *inter alia*, the "[…] predominant and characteristic mode of thought in legal matters"[39] setting a legal field[40] apart from adjacent legal fields.[41] Arguably, the predominant and characteristic mode of thought is crystallized into the objectives of a legal field. By focusing on style, the obstacle of one-dimensional classification based only on one single criteria[42] (such as subject matter) is overcome. Accordingly, the danger of "the law of the horse" is averted.

9   Consequently, the field of EU data law is delimited based on subject matter—data—and the distinct objectives it persistently strives to safeguard. These objectives are identifiable in the data legislation proposed and enacted by the EU legislator as well as its accompanying policy documents. The objectives differ from those characterising traditional fields of law and stem from the issues created by data's particular characteristics. Data's particular characteristics and the corresponding objectives are more closely examined in the following section.

C. Delimiting the field of EU data law

I.   The characteristics of data and the objectives of EU data law

10   For the purposes of this article, data is defined 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".[43] The definition is found in several pieces of (proposed) EU legislation and is in alignment with the definitions advanced by

---

29   Jolowicz (n 27); Twinning, O'Donovan and Paliwala (n 27) 20 and; Seipel (n 27) 199f.

30   Note that some authors argue for an integrated form of classification that incorporate elements from both factual and conceptual classification, see Ross (n 19) 264 and to a certain extent; Seipel (n 27) 199.

31   Ross (n 19) 243; Seipel (n 27) 198.

32   Ross (n 19) 245.

33   Though Streinz does not explicitly address forms of classification, he seems to use the rationale of factual classification as well cf. Streinz (n 9) 902.

34   Ross (n 19) 243; Twinning, O'Donovan and Paliwala (n 27) 20; Seipel (n 27) 198; Note that the authors use slightly diverging terminology for the types of classification; factual classification is, for example, also known as functional classification, see, inter alia, ibid 201.

35   Frank H Easterbrook, 'Cyberspace and the Law of the Horse' [1996] University of Chicago Legal Forum 207.

36   ibid 207f.

37   ibid 207.

38   Hein Kötz and Konrad Zweigert, *An Introduction to Comparative Law* (3rd edn, 1998) 67.

39   ibid 68.

40   "Legal field" in the case of this article. Kötz and Zweigert examine "legal families".

41   Kötz and Zweigert (n 38) 68.

42   ibid 67.

43   Defined in the Digital Markets Act art. 2(19), Data Governance Act art. 2(1), and proposal for the Data Act art. 2(1). In alignment is also para. 30 of the Open Data Directive.

scholars.[44] The definition is useful and workable due to its broadness. Data can take many different forms and too narrow a definition risks inadvertently excluding some forms. Moreover, the definition emphasises that data must be *digital*, which is essential as data's value creation is intrinsically connected with digital technologies.[45] It is seldom that data in itself (and thereby the mere possession of data) generates value.[46] Generally, data's economic potential must be realised through different methods[47] where the most common is data analysis.[48] By analysing data, it is possible to derive insights with the potential of enabling better decision-making.[49] Such analysis becomes even more valuable when the analysis and the ensuing decision-making are automated as is the case with machine learning algorithms and artificial intelligence.[50] These technologies also create value as they autonomously improve themselves.[51] The value extraction from data analysis can impact both businesses, NGOs and public entities[52] and is thus extremely valuable for the EU economy. Data is therefore essential as an input to the operation and development of data analysis technologies.

11 Data differs from most other commodities in four main ways.[53] Firstly, data is *inexhaustible* meaning that it can be copied an endless number of times without being exhausted nor compromised in terms of quality.[54] It should be noted that such copying can be done at a very low cost.[55] Secondly, data is *non-rival* and can therefore be managed simultaneously by any number of users and processes.[56] Thirdly, data can be *utilised in different contexts* as the same data can constitute the input for different products and services.[57] Lastly, data-driven business models are often characterised by *network effects*[58] and *economies of scope*.[59] Network effects occur when the value of a

---

44   Thomas Tombal, *Imposing Data Sharing among Private Actors: A Tale of Evolving Balances* (Wolters Kluwer Law International 2022) 15 also uses the definition stated in the recently enacted and proposed data legislation. Similar definitions are advanced by; Steinrötter (n 16) 272; Thomas Hoeren and Philip Bitter, '(Re)Structuring Data Law: Approaches to Data Property' in Katrin Bergener, Michael Räckers and Armin Stein (eds), *The Art of Structuring: Bridging the Gap Between Information Systems Research and Practice* (Springer International Publishing 2019) 297f.

45   Commission 'Artificial Intelligence for Europe' (Communication) COM (2021) 205 final 2018 10; Jens Prüfer and Christoph Schottmüller, 'Competing with Big Data' (2021) 69 The Journal of Industrial Economics 967, 3; Daniel L Rubinfeld and Michal S Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339, 375ff.

46   'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective', vol 297 (2020) OECD Digital Economy Papers 297 10 <https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en> accessed 20 December 2022; Julia Wdowin and Stephanie Diepeveen, 'The Value of Data - Literature Review' (Bennett Institute for Public Policy 2020) 3 <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2020/12/Value_of_data_literature_review_26_February.pdf> accessed 20 December 2022.

47   Wdowin and Diepeveen (n 46) 19.

48   Commission 'Towards a common European data space' (Communication) COM (2018) 232 final 2018 2f.

49   Hai Wang and others, 'Towards Felicitous Decision Making: An Overview on Challenges and Trends of Big Data' (2016) 367–368 Information Sciences 747, 750.

50   Commission 'Artificial Intelligence for Europe' (Communication) COM (2021) 205 final (n 45) 10.

---

51   ibid.

52   Martin Wiener, Carol Saunders and Marco Marabelli, 'Big-Data Business Models: A Critical Literature Review and Multiperspective Research Framework' (2020) 35 Journal of Information Technology 66, 67; This perspective is also emphasised in Commission 'Staff Working Document: Guidance on sharing private sector data in the European data economy' 1.

53   See also the analysis of data as a commodity in Llewellyn D W. Thomas and Aija Leiponen, 'Big Data Commercialization' (2016) 44 IEEE Engineering Management Review 74, 83.

54   Charles I Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data' (2020) 110 American Economic Review 2819, 2819 Note that the authors do not distinguish between inexhaustible and non-rival.

55   Cohen and Wendehorst (n 17) 6; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final 2020 4.

56   Cohen and Wendehorst (n 17) 6; Stefan Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (Hart/Nomos 2017) 15; Jones and Tonetti (n 54) 2819.

57   Cohen and Wendehorst (n 17) 126; Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 10.

58   Rubinfeld and Gal (n 45) 355f; Prüfer and Schottmüller (n 45) 368. Note that these works have also been cited in; Nine Riis, 'The Duty to Supply Data under Art. 102 TFEU', *Konkurrenceretlige emner 2/2020* (Bech-Bruun 2020) 160ff.

59   Nestor Duch-Brown, Bertin Martens and Frank Mueller-

product increases proportionally with the amount of people using the product.[60] A classic example is a search engine algorithm improving in proportion with the number of entered search requests.[61] Economies of scope happen when combined analysis of several datasets yield more efficient insights than analysing each data set separately.[62]

12 The distinct characteristics of data described above create a risk of harm to different values and interests of the EU. The protection of these values and interests can be expressed as the five objectives of EU data law. Consequently, EU data law strives to safeguard (i) a competitive market, (ii) fundamental rights (iii) consumers, (iv) trustworthiness and (v) Open Data. The content of each of the objectives is elaborated on below.

1. A competitive market for data

13 The Commission has repeatedly stated that a competitive market for data must be established and protected.[63] There are many views on what constitutes a "competitive market", however, three main perspectives can be identified in relation to EU data law: (i) establishment of possibilities and incentives to trade data, (ii) removal of barriers to the internal market for data, and (iii) restrictions on large companies' use of data.

a) Establishment of possibilities and incentives to trade data

14 As stated above, data is a crucial input for the operation and development of a vast number of technologies[64] making access to data essential. One of

the best ways to gain access to data is through trade, however, data trade has not sufficiently taken off in the EU and is especially lacking in B2B relations.[65] Several explanations for this can be advanced. To start, data's inexhaustible and non-rival nature makes it difficult for a contracting party to control how the data is used once it has been shared. Further, as the same type of data is usable in a variety of contexts pricing data can be complicated[66] due to the fear of losing competitive edge. Both factors minimise companies' incentives to trade data.

15 As a reaction, the Commission has introduced several legislative and non-legislative[67] initiatives. On the side of legislation, the most relevant measures are the introduction of Article 34 of the proposal for the Data Act and Chapter 3 of the Data Governance Act. Article 34 of the proposal for the Data Act stipulates an obligation for the Commission to develop non-binding model contractual terms to support companies when they draft and negotiate agreements on data access and use. The rationale of the provision is to lower transactions costs and thus increase data trade.[68] Chapter 3 of the Data Governance Act adopts a different approach by providing a voluntary scheme for certifying data intermediation services. Data intermediation services are defined as services that aim to establish a commercial relationship between "an undetermined number of data subjects or data holders on one hand and data users on the other"[69] without using the provided data[70] itself nor improving it with the aim of licensing it for profit.[71] Accordingly, certified data intermediation services have a higher level of impartiality.[72] The rationale

---

(Communication) COM (2021) 205 final (n 45) 10; Rubinfeld and Gal (n 45) 375ff; Tombal (n 44) 88.

65   Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 7.

66   'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective' (n 46) 32.

67   One of the non-legislative initiatives is for example the establishment of the Support Centre for Data Sharing see <https://eudatasharing.eu/> accessed 20 December 2022.

68   See also paras. 55 and 83 of the proposal for the Data Act.

69   Data Governance Act art. 2(11).

70   Data Governance Act art. 12(a).

71   Data Governance Act art. 2(11)(a).

72   This is also supported by the fact that a data intermediation service provider complying with the requirements set out in articles 11 and 12 of the Data Governance Act is allowed to use the label "*data intermediation provider recognised in*

Langer, 'The Economics of Ownership, Access and Trade in Digital Data' [2017] European Commission, Joint Research Centre 9.

60   Riis (n 58) 160.

61   An example also mentioned in ibid 161.

62   Duch-Brown, Martens and Mueller-Langer (n 59) 9. Literature on economies of scope is extensive and further elaboration is outside the scope of this article.

63   Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1; Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final 1; Commission 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final 2014 2.

64   Commission 'Artificial Intelligence for Europe'

behind the provisions is that impartiality increases trust in the intermediation services with resulting incentives to trade data through intermediaries.

b) Removal of barriers to the internal market for data

16 The EU was founded with the main aim of establishing an internal market.[73] Accordingly, there should be no barriers to the free movement of data. This is, in particular, ensured by the NPDR explicitly prohibiting data localization requirements.[74] Moreover, the GDPR ensures the free movement of personal data.[75]

c) Restrictions on large companies' use of data

17 Data markets are prone to informational asymmetry,[76] network effects (both direct and indirect)[77] and economies of scope[78] all of which can act as barriers to entry.[79] Accordingly, it is difficult for new entrants to enter and establish themselves on the market. To address the risks stemming from these market characteristics, the proposal for the Data Act and the P2B Regulation impose *ex ante* restrictions on large companies' use of data in order to prevent market foreclosure and abuse of market power.[80]

18 Articles 4 and 5 of the proposal for the Data Act oblige data holders[81] to grant data users[82] access to data generated by the users' use of a product or related service.[83] Similarly, Article 9 of the P2B Regulation sets out information obligations for online intermediation services. The information obligations include a duty to inform the users about the data the intermediation service has access to and how the data is used.

19 Both Regulations employ *ex ante* mechanisms to address barriers to entry and thus prevent strong market actors from further strengthening their position within a specific data market or use their market power to leverage their position into an adjacent market.[84] Such *ex ante* mechanisms are commonly associated with EU competition law[85] and the rationales underlying the Regulations are to a great extent similar to those in competition law. The goals of EU competition law are ambiguous, but it is generally acknowledged that they include, at least, efficiency and consumer welfare.[86] These goals

---

the Union" and the accompanying logo as stipulated by art. 11(9) of the Act.

73 Consolidated Version of the Treaty on European Union [2016] OJ C202/13 (TEU) art. 3(3).

74 NDPR Art. 4(1).

75 GDPR art. 1(3)

76 Bertin Martens and others, 'Business-to-Business Data Sharing: An Economic and Legal Analysis' (2020) 27.

77 Rubinfeld and Gal (n 45) 355f; Prüfer and Schottmüller (n 45) 368.

78 Rubinfeld and Gal (n 45) 352ff; Martens and others (n 76) 24.

79 Rubinfeld and Gal (n 45) 349ff.

80 See also the analysis conducted by Ondrej Blazo, 'The Digital Markets Acts - Between Market Regulation, Competition Rules and Unfair Trade Practices Rules' [2022] Strani Pravni Zivot (Foreign Legal Life) 117, 131.

81 "Data holder" is defined as: "a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data" cf. art. 2(6) of the proposal for the Data Act. Note that SMEs are explicitly excluded from this definition cf. proposal for the Data Act art. 7(1).

82 "User" defined in art. 2(5) of the proposal for the Data Act. Access can also be granted to a third party designated by the user cf. art. 5 of the proposal for the Data Act.

83 See art. 2(2) and 2(3) of the proposal for the Data Act for definitions for "product" and "related service".

84 Luigi Zingales, Fiona Scott Morton and Guy Rolnik, 'Stigler Committee on Digital Platforms' 336, 37.

85 An illustrative example is the electronic communications sector, which has historically been a focus of competition law due to its specific market characteristics. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321/36 includes *ex ante* obligations similar to those in the P2B Regulation and the proposal for the Data Act, for example, information obligations cf. art. 69 and obligations to grant access cf. art. 61.

86 See the thorough empirical analysis in Konstantinos Stylianou and Marios Iacovides, 'The Goals of EU Competition Law: A Comprehensive Empirical Investigation' [2022] Legal Studies 1, 5ff with references. The goals of EU competition law have been discussed at length, however, the discussion is outside the scope of this article.

are also evident in the Regulations as they seek to increase both efficiency and consumer welfare[87] by facilitating access to data.

2. Protection of fundamental rights

20 The increased use of data and data analysis can collide with fundamental rights, in particular, (i) the right to protection of personal data cf. Article 8 of the EU Charter[88] and (ii) the prohibition against discrimination cf. Article 21 of the EU Charter. Further, there is (iii) a risk of compromising democratic values due to large companies' access to and use of data.

a) The right to protection of personal data

21 Legislation and case-law concerned with the protection of personal data is commonly referred to as *data protection law*.[89] Data protection has historically been one of the main forms of regulation of data in the EU[90] taking off with the enactment of the Personal Data Directive[91] in 1995. The rationale behind the Directive was partly harmonisation[92] and partly that the easiness of processing data digitally made it difficult for data subjects to exercise control over their personal data.[93] In 2018, the Directive was replaced by the GDPR,[94] which

ensures the continued protection of personal data[95] based on the same rationale as the Directive.[96] Yet, the GDPR includes additional obligations (and a stricter fine regime) in light of the increased risks from advanced surveillance technologies and tools facilitating unauthorised access to personal data.[97] Though the GDPR is often referred to in its capacity as a fundamental rights instrument, it also pursues an economic goal by ensuring the unrestricted movement of personal data in the EU.[98]

b) The prohibition against discrimination

22 Article 21 of the EU Charter includes a broad prohibition against discrimination applying to the Member States and the EU institutions.[99] Further, prohibitions against general and specific non-discrimination are included in secondary EU legislation[100] applying to the private sector.[101] Accordingly, non-discrimination law in the EU has a broad scope. The specific concern in regard to data is *algorithmic bias*. If the data used as input in machine learning algorithms or artificial intelligence is biased, the output risks being biased as well[102]— often articulated within data science as "Garbage in, garbage out".[103] Moreover, as the output is often used to further improve the algorithm, the bias becomes an inherent part of the design of the particular

---

87 P2B Regulation paras. 1 and 3 and Explanatory Memorandum to proposal for the Data Act pp. 3 and 12

88 Consolidated version of the Charter of Fundamental Rights of the European Union [2012] OJ 326/391 (EU Charter)

89 Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 14; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014) 4.

90 Together with the Database Directive.

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

92 Personal Data Directive paras. 5-7

93 Personal Data Directive para. 4. See also Lynskey (n 89) 3.

94 GDPR art. 94(1).

95 GDPR art. 1(1), 1(2), and para. 1.

96 GDPR para. 9.

97 GDPR para. 6; Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final (n 63) 3.

98 GDPR art. 1(3) and para. 13.

99 Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567, 6.

100 See 'Non-Discrimination' (*Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/equality/non-discrimination_en> accessed 20 December 2022 (also cited in; Wachter, Mittelstadt and Russell [n 99] 7).

101 Wachter, Mittelstadt and Russell (n 99) 7.

102 Commission 'Building Trust in Human-Centric Artificial Intelligence' (Communication) COM (2019) 168 final 2019 6.

103 See, for example, Bertie Vidgen and Leon Derczynski, 'Directions in Abusive Language Training Data, a Systematic Review: Garbage in, Garbage Out' (2020) 15 PLOS ONE e0243300,

algorithmic model.[104] The risk is further intensified in light of the network effects and economies of scope characterising data business models as these effects tend to exacerbate the bias. Algorithmic bias may be covered by current EU non-discrimination law[105] (though no cases have been tried in front of the CJEU), however, there are still gaps as well as evidence issues particular to cases of algorithmic bias.[106] One of the initiatives to remedy this is Article 10 of the proposal for an AI Act. Article 10(3) explicitly states that training, validation and testing data used in high-risk AI systems shall be, *inter alia*, "representative".

c) Risk of compromising democratic values due to large companies' access to and use of data

23 Large companies' (especially platforms') access to and use of data may compromise democratic values. The risk is different from the competition law concern examined above. The competition law concern is based on an economic theory of harm according to which the consumer risks paying the price for the abusive behaviour of a dominant undertaking. The risks for democratic values are harder to qualify. Recent studies have highlighted that companies with access to large amounts of data can cause non-economic societal harms.[107] With a wide reach and massive data sets large companies can, for instance, provide targeted news able to deliberately influence public opinion[108] or promote specific political agendas[109] jeopardizing the democratic values of the EU.[110] Such behaviour may also infringe fundamental rights, for instance, the right to free elections.[111] The preamble to the Digital Markets Act highlight these concerns by stating that the Act "[...] pursues an objective that is *complementary to, but different from that of protecting undistorted competition on any given market*, as defined in competition-law terms, which is to ensure that markets where gatekeepers are present are and remain contestable and fair, independently from the actual, potential or presumed effects of the conduct of a given gatekeeper covered by this Regulation on competition on a given market. This Regulation therefore aims *to protect a different legal interest from that protected by those rules* and it should apply without prejudice to their application" (author's emphasis).[112] The wording underlines that the conduct of large companies does not purely give rise to economic concerns.[113] The specific provisions of the Digital Markets Act, *inter alia*, prohibits gatekeepers'[114] use of certain categories of data[115] in competition with its business users.[116] Further, it obliges the gatekeeper to provide business users with access to data that has been either provided or generated by the business users through the gatekeeper's services.[117] These obligations are similar to *ex ante* competition law mechanisms and arguably the obligations will also affect the competitive conduct of gatekeepers. However, as stated above, the Digital Markets Act has a broader scope of protection than merely competition on the market.

---

104   Commission 'Building Trust in Human-Centric Artificial Intelligence' (Communication) COM (2019) 168 final (n 102) 6; Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final 2020 11.

105   Wachter, Mittelstadt and Russell (n 99) 29; Raphaële Xenidis and Linda Senden, 'EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination' (2020) 174.

106   Wachter, Mittelstadt and Russell (n 99) 29; Xenidis and Senden (n 105) 174.

107   See, for example, John W Cioffi, Martin F Kenney and John Zysman, 'Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century' (2022) 27 New Political Economy 820; 4 José van Dijck, David Nieborg and Thomas Poell, 'Reframing Platform Power' (2019) 8 Internet Policy Review; Christoph Busch and others, 'Uncovering Blindspots in the Policy Debate on Platform Power' 20ff.

108   Busch and others (n 107) 20 and 22 state that personal data can be used to provide targeted news and thus work as 'instruments for manipulation'. The quotation is taken from; van Dijck, Nieborg and Poell (n 107) 3.

109   Busch and others (n 107) 22.

110   See the values set out in art. 2 and 3 of the TEU.

111   Art. 3 of the Protocol of the European Convention on Human Rights (ascended by the EU cf. art. 6(2) of the TEU).

112   Digital Markets Act para. 11.

113   Busch and others (n 107) 17 also advance this interpretation.

114   As defined in art. 3 of the Digital Markets Act.

115   Data which has been either generated or provided by business users through their use of the core platform service (or supporting services), including data generated or provided by business users' customers cf. art. 6(2) of the Digital Markets Act.

116   Digital Markets Act art. 6(2).

117   Digital Markets Act art. 6(10).

---

3. Trustworthiness

24 The concept of *trust* and *trustworthiness* emerged in EU law concurrently with data-driven technologies. The Commission has emphasised that "[a] high level of trust is essential for the data-driven economy"[118] and almost all legislation regulating data put emphasis on the importance of trust.[119] The underlying rationale is that without trust in technology—and in particular trust that technology respects fundamental rights and European values—there will be no uptake in the use of such technology. Consequently, a lack of trust will prevent the effective development of a competitive EU market for data and the ensuing beneficial technologies.

4. Open Data

25 To encourage and ensure Open Data is an aim evident in EU data law. "Open Data" describes data in an open format that can be freely used, re-used and shared for both commercial and

non-commercial gains.[120] Open Data has been in focus since the entry into force of the Public Sector Information Directive[121] (now the Open Data Directive) in 2003. Open Data is desirable both from a fundamental rights and a competition law perspective. Open Data can be perceived as an extension of the right to receive and impart information as set out in Article 11(1) of the EU Charter.[122] Yet, Open Data is also advantageous for competition as the sharing and free availability of data grant companies new opportunities to

produce and improve products.[123] Open Data also advances the agenda of administrative law as it ensures transparency and accountability when the data relates to the public sector.[124] The two main instruments regulating Open Data is the Open Data Directive and the Data Governance Act. The Directive sets out a general obligation for Member States to ensure that documents held by public authorities[125] are re-usable for commercial and non-commercial purposes cf. Article 3. Similarly, the Data Governance Act includes an obligation for public authorities to make specific categories of data available for reuse under specific conditions cf. Article 5.

a) Consumer protection

26 Consumer protection is anchored in Article 169 TFEU[126] and in Article 38 of the EU Charter. One of the main goals of EU consumer protection law is to provide consumers with rights that enable them to establish a fair foundation for economic transactions.[127] This is, *inter alia*, obtained by granting consumers appropriate and effective remedial rights in contractual relations as protected by the Sale of Goods Directive since 1999. Yet, these rights have been under growing pressure due to the increase in generated data.[128] An example is the surge in business models based on consumers providing data as remuneration for (monetary) free services. A reaction to these business models has been a revision of the Sale of Goods Directive and the introduction of the Digital Content Directive. The Directives introduce contractual rules favourable to consumers procuring digital content, digital services[129] and physical goods interconnected with or incorporating such content or services.[130] The rationales underlying the two directives are twofold. Firstly, the quality of the provided content and services using data improve

---

118 Commission 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final (n 63) 3.

119 GDPR para. 7, Data Governance Act para. 23, NPDR, para. 33, P2B Regulation, para. 3, proposal for the Data Act paras. 48 and 78 and proposal for the AI Act paras. 45 and 62 Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final (n 63) 3; Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 1; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1 and 11; Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final (n 104) 1.

120 Open Data Directive para. 16

121 See paras. 4 – 5 of 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 L345/90.

122 Open Data Directive para. 5.

123 Open Data Directive paras. 8 – 9.

124 Open Data Directive para. 14.

125 However, several exceptions are set out in art. 1(2).

126 Consolidated Version of the Treaty on the Functioning of European Union [2016] OJ C202/47 (TFEU).

127 Agustin Reyna, Natali Helberger and Frederik Zuiderveen Borgesius, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427, 1427.

128 Sale of Goods Directive para. 5.

129 Digital Content Directive art. 3(1).

130 Sale of Goods Directive 2(5)(b).

as consumers can exercise remedial rights in case of non-conformity[131] leading to better products on the market. Secondly, the rules encourage consumers' trust in technologies, because consumers know that the companies providing the data-driven services are contractually liable.

D. The inherent dichotomy in EU data law and the way forward

27 By defining the field of EU data law, all the objectives concerning data deemed important by the EU legislator are fleshed out. The objectives stem from the distinct issues created by data's particular characteristics and differ from the objectives characterising traditional fields of law. Consequently, the classification of EU data law contributes to an enhanced understanding of the values and interests that are relevant to take into account when creating, interpreting, and enforcing data legislation. This, in turn, provides for a coherent field of law that ensures legal certainty.

28 When examining the objectives of EU data law, it is clear that there is an inherent dichotomy between economic goals on the one hand and fundamental rights on the other hand.[132] Data has an enormous economic potential exacerbated by its ability to make an economic impact across a vast number of industries.[133] Data-driven technologies have a broad scope; they can provide better and faster medical diagnosis,[134] improve sustainability[135] and innovate an uncountable number of products and services.[136] It is exactly the broadness of data's use that warrants the catchphrase "data is the new oil".[137] Yet, data

also has the ability to compromise the democratic values upon which the EU is built and the potential to infringe fundamental rights. The extent of the risks ensuing from algorithmic bias or from large companies' potentially far-reaching power are difficult to fully comprehend as our society may be impacted in ways we cannot yet imagine. The dichotomy is also evident when considering the subjects of protection in current data legislation. Arguably, there is a difference in the approach to regulation depending on if the subject of protection is a consumer assessing a product or the public seeking to navigate in a risk zone for fundamental rights.[138]

29 Both economic goals and protection of fundamental rights are important and the legislator must decide how to balance them against each other, which the EU legislator has not sufficiently done.[139] A relevant example is the continuous distinction between personal and non-personal data in EU legislation.[140] The distinction relies on the assumption that data sets of personal and non-personal data are easily separated and that parallel application of different legal rules is possible. However, this is not necessarily aligned with reality[141] and is problematic because the stricter mandatory requirements for processing of personal data (while justifiable from a fundamental rights perspective) effectively impede data trade. Consequently, there is an ensuing risk that the legal provisions mainly pursuing economic goals cannot efficiently achieve such objective. As an illustration, Article 12 of the Data Governance Act lists the requirements that must be satisfied in order to become a certified data intermediation

---

131 Digital Content Directive paras. 5 and 8 and Sale of Goods Directive para. 32.

132 See also Streinz (n 9) 934 in agreement.

133 Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 2.

134 It can, for example, (earlier and faster) detect skin cancer as well as calculate the chances of relapse for certain medical conditions cf. Jenni AM Sidey-Gibbons and Chris J Sidey-Gibbons, 'Machine Learning in Medicine: A Practical Introduction' (2019) 19 BMC Medical Research Methodology 64, 2.

135 Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 2.

136 ibid.

137 'The World's Most Valuable Resource; Regulating the Data Economy' (2017) 423 The Economist.

138 Solano and others (n 15) 53.

139 ibid 1; Streinz (n 9) 903.

140 Something often noted and criticized, see, inter alia, Christiane Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Reiner Schulze, Dirk Staudenmayer and Stefan Lohsse (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (Nomos 2017); Inge Graef, Raphaël Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation.' 44 European Law Review 605; Inge Graef and Raphael Gellert, 'The European Commission's Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing' [2021] SSRN Electronic Journal 2 <https://www.ssrn.com/abstract=3814721> accessed 3 February 2023.

141 Graef, Gellert and Husovec (n 140) 5.

service provider.[142] Article 12 stipulates different requirements dependent on the provided data being personal or non-personal[143] requiring stricter requirements for processing personal data. However, the provision does not take into account cases of mixed datasets or cases where non-personal data becomes personal due to the dynamic interpretation of what constitutes personal data.[144] The latter situation is likely to arise due to the vast amount of different datasets available in data intermediation services. The sparse guidance in the Data Governance Act in this regard risks limiting the intended effect of Article 12 as providers may have difficulties satisfying the requirements of the provision and thus qualify for the certification.

30　It can be argued that the objective of trustworthiness can, in some cases, solve the dichotomy between economic goals and protection of fundamental rights. In other words, without fundamental rights protection (that is, *trust*) no EU citizen or company will use new technologies.[145] However, the soundness of this rationale should be subject to closer examination. It is a convenient way to solve a complex matter, but when taking into account how all of our lives (and modern comforts) depend on new forms of data-driven technology, the argument seems weak.

31　An inherent dichotomy is not detrimental to a legal field, in fact, it is what characterizes almost all fields of law. However, it is important to acknowledge a field's contrary stances and decide how to balance them against each other. This is, in particular, important when taking into account how speedily the EU legislator is proposing and passing data legislation. If the legislator does not acknowledge the different objectives of EU data law and their inherent tension, the risk is that none of the objectives will be effectively achieved. Further, legal uncertainty is in-

creased as businesses and individuals have considerable difficulties navigating an increasing amount of legislation safeguarding opposing objectives.

32　The aim of EU data law is not to solve the dichotomy between the field's objectives. In the words of Roscoe Pound, "Classification is not an end".[146] Classification is a tool used to construct a solid foundation for creating, interpreting and enforcing the law. By classifying EU data law, the present article brings to light the field's objectives and their inherent tensions. This clarity can assist the EU legislator in making the decisions necessary for creating better and more consistent data legislation to sustain a digital European society in the coming digital decades.

142　The distinction used in art. 12 is also criticized by the European Data Protection Board and the European Data Protection Supervisor in 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) (2021) 28f. Note that some of the criticism issued in the opinion have been mitigated in the final approved text of the Data Governance Act.

143　See, for example, art. 12(j) – (n) operating with the distinction.

144　Wendehorst (n 140) 331; Graef, Gellert and Husovec (n 140) 3f.

145　Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final (n 104) 1; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1.

146　Pound (n 18) 944.