The Laws of Big Data

Lena Mischau

The Laws of Big Data

How Data Protection Law, Competition Law and Contract Law Deal with the Challenges of a Data-Driven World

Lena Mischau[1,2]

[1] Weizenbaum Institute for the Networked Society, Hardenbergstraße 32, 10623 Berlin, Germany; Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin, Germany.

[2] This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) under grant No. 16DII111 ("Deutsches Internet-Institut").

lena.mischau@rewi.hu-berlin.de

Abstract. This paper presents a selection of legal topics in the context of data analytics and Big Data from a lawyer's perspective. After introducing the reader to the role of law, both in the analogue and the digital world (1), the paper gives a systematic overview of some of the currently most relevant data-related legal topics (2). While digitalisation and data processing poses new questions to all areas of law, this paper focusses on the role Big Data plays in competition, data protection and contract law, as those are closely interlinked and address similar data-related phenomena. The paper was written from a mainly European perspective and presents some specific approaches European law takes to address the challenges we face with the advent of Big Data.

Keywords: Competition Law, Data Protection Law, Contract Law.

1. Introduction – the Role of Law in a Data-Driven World

Law serves multiple functions in society. Contract law, for instance, aims to provide a clear legal framework for diverse parties to conclude contracts and exchange goods and services in a fair manner. It aims to rebalance interests and asymmetries of information or negotiation power between businesses and consumers, but also between businesses themselves. For instance, European consumer law imposes information and transparency obligations on sellers [1], prohibits particularly unfair and problematic provisions in General Terms and Conditions [2], and imposes certain rights and duties on the parties in cases where the product is not in conformity with the contract [3]. Competition law, in turn, wants to protect and foster competition with all its positive effects by prohibiting cartels and any abuse of dominant market positions, and by controlling mergers with regards to the impact they will likely have on competition [4]. Data protection law first and foremost aims at protecting privacy and self-determination of data subjects, that is, of individuals [5].

All of these areas of law existed long before the rise and success of the online platform economy and data ecosystems involving the Internet of Things ("IoT"). Nevertheless, they apply to the digital world just as they do to the analogue one. It used to be a widespread misperception that the digital world and the Internet in particular were "free" from the law. However, no space – neither analogue nor virtual – exists that is not subject to any legal rules at all. Law continues to pursue its respective societal objectives in digital environments. Power asymmetries should be rebalanced, consumers protected and self-determination and privacy ensured online too. The legal imperatives are all the more vital given the increasing blurring of lines between the online and offline world , for instance, with regards to smart products and IoT. However, it is true indeed that *enforcing* the law in digital contexts is often much more difficult than in analogue ones. Irrespective of the question of enforcement, the legal rules as such often do not even need to be adapted to digital cases and it does not make any difference from a legal point of view whether a certain event takes place online or offline.

Example: Under European law, for instance, the buyer of a laptop has the same legal rights should the laptop prove to be defective a few months after purchase, regardless of whether he bought it in a physical shop next door or via an online shop [6]. Similarly, competition law works according to the same principles regardless of whether an undertaking does business in a traditional market or in a digital market, such as for online search engines. In both cases, the same essential rules apply. Finally, data protection law treats data processing in mainly the same way, regardless of whether the data processor is, for instance, a company that asks you to fill in a paper questionnaire that will be integrated into a filing system, or whether the company sends you an email with a link to an online form.

Nevertheless, digitalisation is confronting our societies with a number of novel phenomena that the law in its current state is not always able to address adequately. The unprecedented availability of enormous quantities of data – often of very high quality – that can be processed at high speed ("Big Data") [7] is one of these new phenomena. Big Data paves the way for progress that the whole of society can benefit from [8]. For instance, Big Data can help us make processes more efficient, increase knowledge by demonstrating correlations we would otherwise not be able to see, and improve forecasts [9]. Businesses and public bodies can benefit from using Big Data applications in very similar ways [10]. As a result, Big Data can have very positive impacts for individuals and for society. For instance, patients might enjoy better healthcare services thanks to optimised medical treatment or early identification of individual health risks [11]. Technology based on Big Data such as intelligent traffic systems and data use in urban systems could increase security and the mobility of citizens [12]. In addition, the environment could also benefit from Big Data, where more efficient processes help avoid pollution and unnecessary waste of resources, or where Big Data applications help stabilise energy grids to be able to cope with the volatility of renewable energy sources, such as solar or wind power [13]. At the same time, we need to be aware of and fight the dangers that come with Big Data, such as potential discrimination, erroneous decision-making based on inaccurate data, and privacy breaches [14]. It is up to the law to establish a legal framework that enables us to benefit from the opportunities while protecting us from the risks of Big Data.

2. A Selection of Legal Topics in the Context of Big Data

Big Data poses specific and complex challenges for data protection law, competition law and contract law. It makes sense to shed light on these three areas of law together, as they interact very closely, pursuing objectives that are sometimes very similar, other times very different [15].

2.1. Big Data and Data Protection Law

Data protection law is the main legal field dealing with Big Data. Throughout the last years, we have witnessed a large number of data protection scandals [16], such as Cambridge Analytica [17], that illustrate both the various dangers of collecting personal data on a large scale and the importance of effective privacy protection.

According to the European General Data Protection Regulation ("GDPR") [18], any processing of personal data is forbidden unless the processing is justified by a legal ground listed in Art. 6(1) GDPR [19]. Such a justification may be given where the data subject – in other words, the natural person whose data are being processed – has freely given her explicit consent for the specific purpose of data processing (Art.6(1)(a) GDPR). In addition to the receipt of explicit consent, data processing can also be legitimate if it is necessary to perform a contractual obligation (Art. 6(1)(b) GDPR), if it is necessary to comply with a legal obligation of the data controller (Art.6(1)(c) GDPR), if it is necessary to protect vital interests of the data subject or another natural person (Art. 6(1)(d) GDPR) or if it is necessary to perform a task carried out in the public interest (Art.6(1)(e) GDPR). However, the processing may also be justified due to legitimate interests of the controller or third parties, provided that these interests are not overridden by the data subject's interests (Art.6(1)(f) GDPR). In any case of data processing, basic principles need to be respected, for instance, the principles of lawfulness, fairness and transparency (Art. 5(1)(a) GDPR), and the principles of integrity and confidentiality (Art. 5(1)(f) GDPR). Moreover, the GDPR provides specific rules for certain aspects of Big Data, such as data processing on a large scale, systematic monitoring of publicly available areas and profiling, as those are considered as particularly risky [20].

Example: A consumer would like to make use of an online food delivery service. Before he can make an order, he is asked to fill in his name, address and bank account details in an online form. In addition, he is asked to answer certain questions, such as how he became aware of that particular food delivery service, what his favourite dishes are, whether he likes cooking as a hobby, and whether he has any specific allergies or illnesses that require certain diets.

Regarding his name, address and bank account details, no consent would be needed, because the food delivery service could not provide the service without the information (Art. 6(1)(b) GDPR). In contrast, any processing of the additional information mentioned above would only be justified if the consumer grants his consent (Art. 6(1)(a) GDPR). The information about potential allergies falls within the scope of health data and merits special protection (Art. 9 GDPR). In all cases, the service provider needs to inform the consumer about certain aspects of the data processing, including, for example, its purpose, the storage period and the consumer's rights, such as the right to access his data (Art. 13(1)(c), (2)(a)(b) GDPR).

Although these rules seem restrictive at first glance, effective data protection faces a large number of difficulties in practice. To start with, data protection policies are usually very long and complex, and consumers usually do not read them [21]. Consumers therefore lack sufficient information as to what happens to their data and are not able to give consent in an informed and self-determined way. Several initiatives and projects try to tackle this issue. For instance, so called "privacy icons" aim to visualise certain data processing aspects and to help consumers better understand the way their data will be processed [22]. Personal Information Management Systems (PIMS) promise to support consumers in enforcing their privacy preferences by, for example, automatically allowing or forbidding data processing according to these preferences [23]. Others, in contrast, consider moving away from consent and instead determining on a societal – rather than individual – level what kinds of data processing should be allowed or forbidden [24].

Another issue in this regard is closely connected to both contract law and competition law. Many digital businesses claim to provide digital goods or services to the consumer "for free", that is they do not ask for any monetary compensation to be paid by the consumer. However, they then finance their business models by other means, which may include offering advertisement services to third parties [25], for example. Nowadays, such types of online advertisement often are personalised using data available about an individual consumer or about groups of persons similar to the individual consumer in question. In such a context, the businesses with access to the biggest and most detailed consumer profile and preference datasets will benefit the most. One might therefore say that consumers do "pay" for these services, but with their personal data and/or with the attention they dedicate to the advertisements shown them based on their profiles [26].

At the same time, Art. 7(4) GDPR is very critical towards practices where the "performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". The provision does not prohibit such business models in general, but emphasises that consent must be voluntary [27]. If this is not the case, the data processing in question is not legitimate [28]. The reason for this rejection lies in the nature of Big Data and possible long-term consequences both for individuals and societies as a whole. Perceiving a product as "free" can have great influence on the consumer's behaviour [29] and impede him from taking a fully self-determined decision regarding his privacy. In this context, one also needs to be aware of the potential danger of the emergence of a "two-class society" regarding data protection – that is, a society consisting of a consumer group that is aware of the risks of disclosing data and that has the financial means to use paying alternatives, and a – potentially much bigger – group of consumers who are not aware or who are aware but cannot afford more privacy-friendly and therefore more expensive products [30]. In practice, many online services continue to tie the use of their services to user consent. It is up to the data protection authorities and courts to increase legal certainty and enforcement.

Example: A consumer would like to read an article of an online newspaper. Before he can access it, the newspaper asks the consumer whether he would like to pay a monetary price of 0,99 EUR for the single article (option A) or of 5,99 EUR for a one-month subscription to the online newspaper (option B) or whether he prefers not to pay any monetary price, but to give his consent to the processing of his personal data for advertisement purposes (option C). He chooses option C.

In this scenario, the consumer's consent can be considered as "freely given", because he had a real choice of whether or not he wanted to give consent in order to read the article by having at least one realistic alternative (option A, option B).

However, even where data processing takes place in perfect compliance with data protection law and where consumers actually are able to make a free and informed choice of whether or not they want to give consent, self-determination regarding personal information is fragile in light of the analytical potential of Big Data. Even if individuals behave in very privacy-protective ways and withhold consent, this does not hinder Big Data applications to reveal probable information about them as soon as a sufficient amount of data is available about other persons who share similar traits or behave in similar ways [31].

2.2. Big Data and Competition Law

After data protection law, it is competition law that is the most concerned with Big Data. On the one hand, the availability of large datasets in almost real-time can stimulate competition by fostering innovative business models and boost the performance of existing businesses [32]. On the other hand, Big Data also poses several risks to competition.

Competition law comprises various tools to protect and foster competition. Long before other areas of private law, competition law scholars already discussed the particular characteristics of multi-sided markets and the platform economy in depth [33]. For example, the question was asked whether a market in the meaning of competition law is established in cases where business models are data-driven and digital products advertised as "free" [34]. Today, the answer to this question is clearly in the affirmative [35]. One of the European member states (Germany) even changed its law to explicitly clarify that such constellations may also be subject to the control of abusive practices [36]. This development is very welcome, as the alternative would be that such businesses might escape certain competition law restrictions despite their real impact on the economy. Considering that businesses offering "free" services to consumers, such as online search engines and social networks, have some of the highest market capitalisations in the world [37], such a result would be absurd.

More importantly, competition law scholars and authorities have examined the impact of data power on the concept of market power, that is, whether access to certain kinds of data helps businesses gain or defend a dominant position in a specific market. While the answer varies from case to case, some general observations can be made. The ability to access large amounts of very granular data in almost real-time clearly has a particularly positive impact on a company's market position in cases where the access

to that kind of data is important to be successful in the specific market, where competitors cannot access these data and where network effects and economies of scale exist and are reinforced by the availability of data [38]. Network effects are particularly important in this context. The term refers to positive feedback effects within networks and multi-sided markets that appear either between users of the same user group or between two or more different user groups [39]. For example, social networks collect vast amounts of data about their users. The more users take part in a social network, the more attractive it becomes for other users (direct network effects). The more members a social network has and the more those make use of it, the more data it creates. And the more exclusive data a social network has at its disposal, the more it can improve its services, for instance, by showing more interesting information to individual users or offer more elaborate product features such as calendar functions. As a result, users are even more attracted by the social network in question and even more data is created [40]. In that case, markets tend to "tip" and only one "winner" takes the whole market, meaning that competition is effectively restricted in that market [41].

Example: An undertaking has a dominant market position in a specific market for search engine services. Because of its dominant market position, the undertaking is subject to particular competition rules to make sure that it does not abuse its dominant market position (Art. 102 AEUV). For example, the undertaking would not be allowed to systematically rank its own products or services (other than the search engine itself) in a higher position than those of its competitors [42].

The importance of access to data has been widely acknowledged over the years. More recently, the European Commission has re-affirmed its intention to foster data access as part of its "European Data Strategy" [43]. Germany, for instance, already adapted its Act against Restraints of Competition (ARC) in order to stress the importance of exclusive access to data relevant for competition [44]. In rare cases, data might even become so important that parallels can be drawn with infrastructure facilities. Refusing access to these kinds of data might be considered as an abuse of market dominance and might lead to access claims granted to other companies [45]. Access to data is an important topic for competition law as a whole, but also for certain sectors in particular – for the automobile [46] and financial services sectors [47], notably.

Example: An independent garage offers repair and maintenance services for cars outside the car manufacturer's own distribution system. Nowadays such a garage can only perform those services, if, among others, it is able to have access to certain vehicle on-board diagnostic information, vehicle repair and maintenance information, as well as the necessary software. In this respect, the access to non-real-time data may not be sufficient in the future anymore. New services, such as predictive maintenance, may require access to full real-time data.

Access to data for competition and economic reasons can never be granted without limits. On the contrary, among others, data sharing always needs to take place within the limits of data protection law in particular [48]. At the same time, data sharing also raises competition law concerns in cases where data are made available that reveal sensitive information that is important for competition [49]. The increasing interaction of

competition law, data protection law and contract law becomes particularly evident in the current Facebook proceedings in Germany. The German competition authority (Federal Cartel Office) had considered Facebook's practice to collect and process data from third party sources as abusive [50], while the Düsseldorf Court of Appeal disagreed and suspended the decision [51].

2.3. Big Data and Contract Law

The "free" goods and services business model has also raised several questions for contract law. In the European Union, the new Digital Content and Digital Services Directive ("DCSD") grants certain rights to consumers in the context of contracts for digital content and digital services [52]. One of the main questions throughout the legislative procedure was whether or not (personal) data could be considered as counter-performance. On the one hand, one needs to be aware of the fundamental rights dimension of personal data and be reluctant towards any commercialisation [53]. On the other hand, we need to make sure that consumers who provide data instead of a monetary price also get to benefit from consumer protection, for example, in cases where a digital service is defective [54]. Contract law and data protection law should thus go hand in hand to provide consumers with protection within their respective scope of application [55].

Other important contract law issues related to data and Big Data in particular concern the questions of security, compatibility, interoperability, updates and potential changes of data-driven products. In the European Union, the DCSD grants consumers and businesses certain rights in this regard for the very first time [56]. For IoT products similar rules exist [57].

Example: A consumer enters into a contract with a provider of music streaming services. To do so, he can choose between a paying option (A) and a non-paying option where the provider processes the consumer's personal data in order to offer personalised advertisement for third parties and create revenues (B). The consumer chooses the non-paying option (B). One year later, the consumer is not happy with the service anymore, for example, because the service does not function properly, is not compatible with the consumer's devices anymore, or because the provider does not offer any necessary security updates (cf. Art. 7(a), (d), Art. 8(1)(b), (2) DCSD).

Under certain circumstances, the consumer has now the right to have the streaming service brought into conformity or to terminate the contract, although he did not pay any monetary price but provided personal data (Art. 14(1)-(4) DCSD). In addition to his contractual rights under the DCSD, the consumer can still exercise his data protection rights under the GDPR, for example, by revoking the consent he gave for processing his data (Art. 3(8), recital 39 DCSD, Art. 7(3) GDPR).

Furthermore, the topic of data sharing that we have already seen in the context of competition law plays an important role in contract law too. Regarding data from the private sector, many data sharing models can be observed [58]. However, no harmonised horizontal rules exist in this regard. So far, the European Commission has elaborated basic principles and a check-list for the sharing of IoT data between businesses, and between

businesses and the public sector [59]. While these are not legally binding, a new "Data Act" is expected to be proposed in 2021 [60].

Example: Company A and company B would like to exchange non-personal data that was created by IoT objects, such as smart machines in a factory. According to the European Commission's guidance, both parties need to comply with certain principles. For example, they should make sure to respect each other's commercial interests and secrets, ensure undistorted competition and minimise data lock-ins.

3. Conclusion

Big Data already falls under the scope of several fields of European law today and more initiatives to adapt existing law or establish new rules are expected within the next few years. Some of the most important areas of law one needs to consider in this context are data protection, competition and contract law. Several data-related topics are addressed by all of these – albeit from different perspectives and in different ways – such as the phenomenon of "free" services and the importance of access to or the protection of certain kinds of data. In many of these data-related cases, data protection law, competition and contract law interact closely and in very complex ways. It is therefore necessary to examine a specific Big Data scenario carefully from all three perspectives and assess how those impact each other.

Of course, other fields of law may also be concerned with Big Data. Public law, for example, has to determine those cases where the processing of data is considered justified under the GDPR because of public interests (Art. 6(1)(e), (3) GDPR) [61]. Criminal law, in turn, will have to deal with an increasing number of data-related crimes, such as data espionage, phishing and providing access to stolen data [62]. IP law, in particular, faces a broad range of challenges concerning the question of whether and to what extent data should be protected by copyright law, as part of databases or trade secrets, and how text and data mining should be treated [63]. Moreover, there has been an intense debate about whether or not new absolute rights are needed, in particular regarding non personal data, such as a "data producer's right" [64].

To fully address Big Data topics, law therefore requires a truly holistic approach. This may include reconsidering carefully the scope of application, the purposes and the means to achieve those purposes of the individual legislative acts.

References

1. For instance, Directive (EU) 2011/83 of 22 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/64.
2. For instance, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.
3. For instance, the buyer of a product may have the right to receive a proportionate reduction in the price where the acquired product is not in conformity with the contract. See 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 L 136/28.
4. Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326/47, arts 101, 102; Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L 24/1.
5. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ("GDPR").
6. Cf Directive (EU) 2019/771 (n 3).
7. Regarding the term "Big Data", see, for instance, Laney, D.: 3-D Data Management: Controlling data volume, velocity, and variety. Application Delivery Strategies, META Group Inc. (2001), http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf, last accessed 2020/06/24; Monopolkommission: Competition policy: The challenge of digital markets. Special Report No 68, (2015), paras 67ff, http://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf, last accessed 2020/06/24; Stucke, M., Grunes A.: Big Data and Competition Policy. OUP, Oxford (2016) paras 2.04ff.
8. For an in-depth overview of the diverse risks and opportunities of Big Data, see, for instance, Tene, O., Polonetsky, J.: Big Data for All: Privacy and User Control in the Age of Analytics. Nw. J. Tech. & Intell. Prop. 11:5 (2013) 239, 243ff, 251ff.
9. Bollier, D.: The Promise and Perils of Big Data. The Aspen Institute, Washington, DC (2010), pp. 20ff.
10. For some examples in practice, see Bartel, J., et al.: Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte. BITKOM e. V., Berlin (2012), pp. 51ff, https://www.bitkom.org/sites/default/files/file/import/BITKOM-LF-big-data-2012-online1.pdf, last accessed 2020/06/24.

11. Minssen, T., Schovsbo J.: Big Data in the Health and Life Sciences: What Are the Challenges for European Competition Law and Where Can They Be Found? In: Seuba, X., Geiger, C., Penin, J. (eds.), Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data. Global Perspectives for the Intellectual Property System, CEIPI and ICTSD, Geneva and Strasbourg (2018), pp. 121, 123; Federal Trade Commission: Big Data – A Tool for Inclusion or Exclusion? (2016) p.5, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf, last accessed 2020/06/24; Bartel, J., et al. (n 10) pp. 70, 76.
12. European Commission: 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 on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. COM(2016) 766 final; OECD: Data-Driven Innovation: Big Data for Growth and Well-Being. OECD Publishing, Paris (2015), pp. 379ff, https://dx.doi.org/10.1787/9789264229358-en; Bartel, J., et al. (n 10) p. 69.
13. OECD (n 12) p. 383; Zhang,Y., Huang, T., Bompard, E.F.: Big Data Analytics in Smart Grids: a Review. Energy Informatics 1:8 (2018) 2, 9f, 12, 15f., https://doi.org/10.1186/s42162-018-0007-5.
14. See, for instance, Federal Trade Commission (n 11) pp. 8ff; Bollier, D. (n 9) pp. 23, 31.
15. Cf European Data Protection Supervisor: Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy. Preliminary Opinion (2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf, last accessed 2020/06/24; cf Crémer, J., de Montjoye, Y.-A., Schweitzer, H.: Competition Policy for the Digital Age: Final Report. Publications Office of the European Union, Luxembourg (2019) pp. 76ff, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf, last accessed 2020/06/24.
16. For an overview see, for instance, Bonneau, V., et al.: Digital Transformation Monitor, Big Data: a complex and evolving regulatory framework. IDATE et al. (eds.), European Union (2017) p. 3, https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Big%20Data%20v1_0.pdf, last accessed 2020/06/24. For privacy breaches in the context of statistical data, see Nissim, K., et al.: Bridging the Gap between Computer Science and Legal Approaches to Privacy. Harvard Journal of Law & Technology 31:2 (2018) 687, 700ff.
17. Cadwalladr, C., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian (17 March 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, last accessed 2020/06/24.
18. See (n 5). For an introduction to US privacy laws, see, for instance, Nissim, K., et al. (n 16) 706ff.
19. For sensitive data, see specific rules in GDPR, art 9(2).

20. GDPR, art 35(3); Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP 248 rev.01 (2017) pp. 8ff, http://ec.europa.eu/newsroom/document.cfm?doc_id=47711, last accessed 2020/06/24; cf Efroni, Z., et al.: Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. EDPL 5:3 (2019) 352, 361ff.
21. See, for instance, Efroni, Z., et al. (n 20) 355f with further references.
22. Efroni, Z., et al. (n 20) 357ff. Cf Hansen, M.: Putting Privacy Pictograms into Practice - a European Perspective. In: Fischer, S., Maehle, E., Reischuk, R. (eds.), Informatik 2009: Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 28.9.-2.10.2009, Lübeck. Gesellschaft für Informatik e.V., Bonn (2009).
23. European Data Protection Supervisor, EDPS Opinion on Personal Information Management Systems: Towards More User Empowerment in Managing and Processing Personal Data. Opinion 9/2016 (2016) paras 5ff, https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf, last accessed 2020/06/24; Horn, N., Riechert, A., Müller, C.: Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Stiftung Datenschutz (2017), pp. 10ff, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftung-datenschutz_broschuere_20170611_01.pdf, last accessed 2020/06/24; Betkier, M.: Privacy Online, Law and the Effective Regulation of Online Services. Intersentia, Cambridge (2019), pp. 79ff.
24. See, for instance, Radlanski, P.: Das Konzept der Einwilligung in der datenschutzrechtlichen Realität. Mohr Siebeck, Tübingen (2016), pp. 97, 204ff, 232f.
25. Monopolkommission (n 7) paras 39f.
26. Weber, R.H.: Information at the Crossroads of Competition and Data Protection Law. ZWeR 12:2 (2014) 169, 175. For the contract law perspective on this topic, see ch 2.3.
27. Metzger, A.: Data as Counter-Performance: What Rights and Duties do Parties Have? JIPITEC 8:1 (2017) 2, para 12.
28. Article 29 Working Party: Guidelines on Consent under Regulation 2016/679. WP259 rev.01 (2017), pp. 5ff, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030, last accessed 2020/06/24.
29. Friedman, D.A.: Free Offers: A New Look. New Mexico L Rev 38:1 (2008) 49ff.
30. Cf Krohm, N., Müller-Peltzer, P.: Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung: Das Aus für das Modell „Service gegen Daten"? ZD 7:12 (2017) 551, 553; Härting, N.: „Dateneigentum" – Schutz durch Immaterialgüterrecht? Was sich aus dem Verständnis von Software für den zivilrechtlichen Umgang mit Daten gewinnen lässt. CR 36:10 (2016) 646, 648.
31. Barocos, S., Nissenbaum, H.: Big Data's End Run around Anonymity and Consent. In: Julia Lane et al. (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement. CUP, Cambridge (2004) pp. 44, 61ff call this phenomenon "the

tyranny of the minority"; Hermstrüwer, Y.: Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data. JIPITEC 8:1 (2017) 9, 12ff, paras 11ff. In the context of statistical data, see Nissim, K., et al. (n 16) 700ff.

32. Federal Cartel Office: Big Data und Wettbewerb. In: Federal Cartel Office (ed.), Schriftenreihe Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft, Bonn (2017), p. 9, http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&hx0026;v=3, last accessed 2020/06/24.
33. For instance, Evans, D.S.: The Antitrust Economics of Multi-Sided Platform Markets. Yale Journal on Regulation 20:2 (2003) 324ff; Evans, D.S., Noel, M.: Defining Antitrust Markets When Firms Operate Two-Sided Platforms. Colum. Bus. L. Rev. 2005:3 (2005) 101ff.
34. Cf text to n 25 in ch 2.1 of this paper.
35. For Germany see, for instance, Federal Cartel Office: Clearance of Merger of Online Real Estate Platforms. Case summary B6-39/15 (2015), p. 3; Federal Cartel Office: Acquisition of the online comparison platform Verivox by ProSiebenSat.1. approved. Case summary B8-76/15 (2015), p. 3; Podszun, R., Franz, B.: Was ist ein Markt? – Unentgeltliche Leistungsbeziehungen im Kartellrecht. NZKart 3:3 (2005) 121ff.
36. Act against Restraints of Competition in the version published on 26 June 2013 (Federal Law Gazette 2013 I, 1750, 3245), as last amended by art 10 of the law of 12 July 2018 (Federal Law Gazette 2018 I, 1151) ("ARC"), § 18(2a). A translation is provided by the Language Service of the Bundeskartellamt and Renate Tietjen, http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html, last accessed 2020/06/24.
37. Forbes: GLOBAL 2000: The World's Largest Public Companies. (2020), www.forbes.com/global2000/list/, last accessed 2020/06/24.
38. Federal Cartel Office (n 32) pp. 7f.
39. OECD: Rethinking Antitrust Tools for Multi-Sided Platforms. (2018) pp. 189f, www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm, last accessed 2020/06/24.
40. These feedback loops can be referred to as "snowball effects"; Federal Cartel Office (n 32) pp. 7f.
41. See, for instance, Barwise, T., Watkins, L.: The Evolution of Digital Dominance: how and why we got to GAFA. In: Moore, M., Tambini, D. (eds.), Digital dominance: The power of Google, Amazon, Facebook, and Apple. OUP, New York (2018), pp. 21, 22ff; Federal Cartel Office: Working Paper – The Market Power of Platforms and Networks, Executive Summary, B6-113/15. (2016), p. 9, www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Think-Tank-Bericht-Zusammenfassung.pdf?__blob=publicationFile&Cv=4, last accessed 2020/06/24.
42. European Commission: AT.39740 Google Search (Shopping); European Commission: Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service –

Factsheet. (2017), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785, last accessed 2020/06/24.

43. European Commission: 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, pp. 12ff.
44. ARC, § 18(3a). A new draft proposal for further amendments to the ACR puts even more emphasis on data access; see Federal Ministry for Economic Affairs and Energy: Referentenentwurf des Bundesministeriums für Wirtschaft und Energie, Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0, GWB-Digitalisierungsgesetz. (2020), https://www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf?__blob=publicationFile&hx0026;v=10, last accessed 2020/06/24. For more details, see Mischau, L.: Market Power Assessment in Digital Markets – a German Perspective. GRUR Int 69:3 (2020) 233, 245ff.
45. Regarding data and the "essential facilities doctrine", see, for instance, Graef, I.: EU competition law, data protection and online platforms: Data as Essential Facility. Kluwer Law International, Alphen aan den Rijn (2016), pp. 249ff; Drexl, J.: Designing Competitive Markets for Industrial Data – Between Propertisation and Access. JIPITEC 8:4 (2017) 257, 278ff; Schweitzer, H. et al.: Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen: Endbericht. DICE Consult (2018), pp. 131ff, https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&hx0026;v=15, last accessed 2020/06/24.
46. Cf Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L 151/1, art 61(1); Kerber, W., Gill, D.: Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation. JIPITEC 10:2 (2019) 244ff.
47. Cf Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35, art 66(1), (4)(b), art 67(1), (3)(b).
48. Crémer, J., de Montjoye, Y.-A., Schweitzer, H. (n 15) pp. 77ff; Bourreau, M., de Streel, A., Graef, I.: Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising: Project Report. CERRE (2017), pp. 15ff, https://www.cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf, last accessed 2020/06/24.

49. Crémer, J., de Montjoye, Y.-A., Schweitzer, H. (n 15) pp. 77ff; Federal Ministry for Economic Affairs and Energy: A new competition framework for the digital economy: Report by the Commission Competition Law 4.0. BMWi, Berlin (2019), pp. 56ff, https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=3, last accessed 2020/06/24.
50. Federal Cartel Office: B6-22/16 Facebook, paras 136ff; Federal Cartel Office: Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding. (2019), p. 5, www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob¼publicationFile&v¼6, last accessed 2020/06/24.
51. Düsseldorf CA, 26 August 2019, Kart 1/19 (V) Facebook.
52. Directive 2019/770/EU of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1 ("DCSD").
53. European Data Protection Supervisor: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. (2017), paras 14ff, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf, last accessed 2020/06/24.
54. DCSD, art 3(1), recital 24. Metzger, A. et al.: Data-Related Aspects of the Digital Content Directive. JIPITEC 9:1 (2018) 90, 93ff, paras 12ff.
55. Langhanke, C., Schmidt-Kessel, M.: Consumer Data as Consideration. EuCML 4:6 (2015) 218, 219f. Regarding the complex interplay between the DCSD and the GDPR, see Metzger, A.: A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services. In Lohsse, S., Schulze, R., Staudenmayer, D. (eds.), Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V, Nomos, Baden-Baden (2020).
56. DCSD, art 7(a), (d), art 8(1)(b), (2), art 19, recitals 42, 47.
57. Directive (EU) 2019/771 (n 3), arts 6(a), (d), 7(1)(d), (3), recitals 28, 30f. In contrast to the DCSD, these rules for IoT products only apply in cases where the consumer has paid a monetary price in exchange for the product.
58. European Commission: Commission Staff Working Document: Guidance on sharing private sector data in the European data economy. SWD(2018) 125 final, pp. 5, 8ff.
59. European Commission (n 58) pp. 3, 6ff.
60. European Commission (n 43) pp. 13, 15.
61. One example is the European eCall regulation, which allows the processing of certain personal data in cases of car accidents in order to accelerate the rescue work of the police and the fire brigarde; see Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC [2015] OJ L 123/77; Klink-Straub, J., Straub,

T.: Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren. NJW 71:44 (2018) 3201, 3203.

62. Cf, for instance, the German Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 19 June 2019 (Federal Law Gazette I, p. 844), §§ 202a-202d. A translation is provided by Prof. Dr Michael Bohlander that is completely revised and regularly updated by Ute Reusch, http://www.gesetze-im-internet.de/englisch_stgb/index.html, last accessed 2020/06/24.
63. These topics are very complex. As a starting point, see 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; see also 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; see also 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 157/1. Cf, for instance, Wiebe, A.: Protection of industrial data – a new property right for the digital economy? GRUR Int 65:10 (2016) 877, 879ff.
64. European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Building a European Data Economy". COM(2017) 9 final, p. 13. Cf, for instance, Zech, H.: Information as Property. JIPITEC 6:3 (2015) 192, 196f, paras 31ff; Wiebe, A. (n 63) 881ff. However, the focus of the debate has in the meantime shifted towards the question of data access, and the introduction of new data property rights has become rather unlikely; see Mischau, L. (n 44) 237f with further references.