Eger, Thomas; Scheufen, Marc

The law and economics of the data economy: introduction to the special issue

European Journal of Law and Economics

European Journal of Law and Economics (2024) 57:93–111
https://doi.org/10.1007/s10657-024-09796-x

The law and economics of the data economy: introduction to the special issue

Thomas Eger[1] **· Marc Scheufen**[2]

Accepted: 1 February 2024 / Published online: 4 March 2024

Abstract
This article intends to provide a framework to better understand the economic problems and legal challenges resulting from the transition of the European economy to a data economy. We discuss some policy concerns surrounding the data economy, such as concentration in the data economy, anticompetitive business practices in the data economy, access to data and data sharing, data reliability, distributional effects of the data economy, and cybercrime. Moreover, we provide an overview of some important EU legal initiatives and reforms and clarify how the papers in this special issue contribute to assessing these initiatives from an economic point of view.

Keywords Digital platforms · Data access · Data sharing · Data reliability

JEL Classification K11 · K20 · K21 · L86 · O33 · Y20

1 Features of the data economy

Over the last few decades, the world has changed on an unprecedented scale due to digitization, the advent of the internet, technical innovations such as the Internet of Things (IoT: smart homes, smart factories, autonomous driving etc.) and Artificial Intelligence (AI), as well as new business models such as digital platforms, some of which have already achieved considerable political and economic power.[1] The key ingredient of this new world is all kinds of *data* that can be collected, stored, processed, transferred, and used at much lower cost than in the "old" world without digitization, without the internet and without the technological and institutional

[1] Tirole (2017, chapter 14).

✉ Thomas Eger
thomas.eger@uni-hamburg.de

[1] Faculty of Law (Faculty of Economics), University of Hamburg, Hamburg, Germany

[2] Research Unit Digitalisation and Climate Action, German Economic Institute (IW), Cologne, Germany

follow-up innovations. For example, *Uber* does not own cars, *Airbnb* and *Booking.com* do not own accommodation, *Delivery Hero* does not own restaurants, but each of these companies, apart from selling services, thrives on the data pertaining to the goods and services they deal with. *Parship*, *Tinder* and similar platforms rely on their users' data to provide informed matchings. *Google* collects via its search engine vast amounts of user data to enable third parties targeted advertising. Social media, such as *Facebook* and *X* (previously *Twitter*), provide digital communication channels and rely on advertising and data licensing revenues. *Amazon* not only acts as a kind of mall, selling books and other products, but also collects lots of data and uses them for targeted marketing. "Big data", i.e., the collection and processing of large amounts and varieties of valuable, complex data, is expected to play a decisive role for progress in the health sector, in industry and agriculture, in the energy sector (e.g., smart meters), in research, and so on.[2]

However, besides these (business) opportunities, the transition to the data economy also entails a number of problems, which we will discuss in more detail in Sect. 2. The private and social costs and benefits of that transformation depend on the legal structures, constraints, and conditions, i.e., the law. Precisely how the design of the law affects the costs and benefits (and thereby social welfare) hinges on the *following classifications of data* concerned.

First of all, we must distinguish between personal and non-personal data. *Personal data*, i.e., any information that relates to an identified or identifiable individual, e.g., to their consumption and investment decisions, housing and mobility, health, job performance etc., can be useful for private and public suppliers of goods, services, and jobs, enabling them to customize their offers and thereby make the economy more efficient. Yet most of us value privacy, not wanting our personal data to be recorded, processed, and stored by governments, employers, or other parties without our consent. *Non-personal data*, such as weather data, market prices, and all types of anonymized, aggregate data, is generally less sensitive but may still warrant protection, such as in the case of business secrets. Secondly, some data are collected and processed at *considerable cost* whereas others emerge as a *by-product of other activities*, such as data on consumption patterns and reading or driving behaviour. Thirdly, unorganized raw data can be transformed into two types of information that can be distinguished in accordance with their effect on welfare: *productive information*, which creates not just individual but also social value, such as the formula for a new drug or the location of some valuable raw material, and *redistributive information*, which has individual but no social value, such as insider knowledge of an event which affected the price of some asset. These three classifications will be important to bear in mind throughout this special issue.

Finally, the social welfare effects of different legal rules depend on the companies' ability to cope with the data (*data economy readiness*—or *data readiness* for short).[3] Data readiness refers to the ability to cope with data effectively in data

[2] See also Marciano et al., (2020a,b).

[3] See also the contribution by Jorzik et al. in this volume.

storage, data management, and data use.[4] Without data readiness, the economic potential from data sharing for the data economy will remain untapped.[5]

Recently, the EU generates a huge volume of legislation related to different aspects of the data economy, such as access to personal and non-personal data, cybersecurity, intellectual property rights, regulation of online platforms, use of data generated by the IoT, AI, and many more. This introduction intends to provide a framework to better understand the economic problems and legal challenges resulting from the transition of the European economy to a data economy.

In the following sections, we discuss some policy concerns surrounding the data economy, such as concentration in the data economy, anticompetitive business practices in the data economy, access to data, data reliability, distributional effects of the data economy, and cybercrime. Moreover, we provide an overview of some important EU legal initiatives and reforms. Finally, we clarify how the papers in this special issue contribute to assessing these initiatives from an economic point of view and provide a better understanding of the law and economics in three broad areas of the data economy: (1) Access to data and data sharing (Eckardt/Kerber, Jeon/Menicucci, Rubinfeld), (2) data readiness and data sharing (Jorzik/Kirchhof/Mueller-Langer, Mouton/Rusche) and (3) artificial intelligence and other technologies (Buiten, Mertens/Scheufen).

2 Some policy concerns in the data economy

2.1 Concentration in the data economy

Digital technology markets are highly concentrated for two reasons (Tirole, 2017, 397–400; Belleflamme and Peitz 2021, chapter 1). First, they typically exhibit (positive) *network externalities*: The larger the network, the more beneficial it is to join the network. Secondly, the massive technological investments that this industry requires give rise to *economies of scale and scope*, i.e., the average cost of production declines with the number of users, while the marginal cost is very low.[6] The stronger the impact of network externalities and economies of scale and scope, the higher the probability that "the winner takes it all."

Over the past decades, digital-tech companies such as *Microsoft* (founded in 1975), *Apple* (founded in 1976), *Amazon* (founded in 1994), *Google* (founded in

[4] See Demary (2022); Röhl et al. (2021), Büchel and Engels (2022a; b). For other definitions of data readiness, see Ivers et al. (2016), among others. The German Economic Institute (IW), in co-operation with the Fraunhofer ISST, the Fraunhofer IAO, the ZEW Mannheim and the IIM at TU Dortmund, in the fall of 2022 conducted a survey on data readiness, based on a representative sample of 1,051 German firms. They found that data readiness is achieved by 77 percent of the largest companies (> 250 employees) but by only 58 percent of medium-sized companies (50–249 employees) and 30 percent of small companies (0–49 employees) (Büchel and Engels 2022b).

[5] Büchel and Engels (2023) find that only 42 percent of German companies share data with other companies. See also Sect. 2.5 on access to non-personal data and data sharing.

[6] See also Rifkin (2014).

1998, part of the holding company *Alphabet* since 2015), and *Facebook* (founded in 2004, rebranded as *Meta* in 2021) have acquired hundreds of other digital-tech companies creating an impressive product mix (Gilbert, 2020, 31–3; Kurz, 2023, 332)[7]: They diversified their activities by integrating a large number of substitutive and complementary activities and thus reinforced positive network externalities. Between 2001 and 2020, *Google* and its parent company *Alphabet* made 236 acquisitions, such as the Android operating system, YouTube, Motorola Mobility for smartphones, Zagat for restaurant reviews, Waze for navigation, and several AI firms. Between 2005 and 2020, *Facebook* made 87 acquisitions, such as Instagram and WhatsApp, while *Apple* made more than 127 acquisitions by 2023, such as Beats Electronics for headphones and music streaming, Shazam for music and image recognition, Intel for modems, and several AI start-ups.[8] Between 1987 and 2020, *Microsoft* made 237 acquisitions, including Skype, Nokia, LinkedIn, the open-source software development platform GitHub, the video game holding company ZeniMax Media, and the AI-based technology company Nuance Communications. *Amazon* has been similarly active, with 102 acquisitions between 1998 and 2020, such as online bookstores in Germany and the UK, the internet movie database IMDb, the online music retailer CDNow, the online software retailer Egghead Software, the grocery chain Whole Foods, and the media company Metro-Goldwyn-Mayer. Many of these moves qualify as "killer acquisitions", i.e., "acquisitions of firms or patents with the objective of their suppression" (Kurz, 2023, 349). For many years, these five US digital-tech giants have successively replaced oil and engineering companies among the world's most valuable corporations. Today all of them are among the top ten companies in the world: Microsoft already since the 1990s, Apple since 2010, Alphabet/Google since 2013, and Meta/Facebook as well as Amazon since 2016.[9]

However, the increasing concentration of economic (and political) power has also become apparent in other areas of the data economy.[10]

As of today, five large commercial publishers (Reed Elsevier, Springer, Wiley Blackwell, Taylor&Francis, and Sage) dominate the academic journal market with a market share of more than 50% (Eger and Scheufen 2018, 16–21, and 2021, 1923–25). Over time, *Reed Elsevier*, the biggest academic publisher in the world,

[7] For most recent information see also Andree (2023, 87–92).

[8] https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Apple.

[9] See, for example, https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization. According to Acemoglu and Johnson (2023, 276) the value of these five companies amounts to approximately 20% of US GDP, whereas at the beginning of the twentieth century the value of the then five biggest companies amounted to only about 10% of US GDP. Since 2017, the Chinese digital-tech companies Alibaba and Tencent have ranked among the ten most valuable companies in the world, and recently the Chinese social media company ByteDance, the parent company of TikTok, has found a place among the largest internet companies worldwide.

[10] Regarding US corporations, Zingales (2017) sees "the risk of a 'Medici vicious circle,' in which economic and political power reinforce each other" (114). He offers three explanations for this tendency: (1) "the emergence and diffusion of network externalities"; (2) "the increased role of winner-take-all industries, driven by the proliferation of information-intensive goods that have high fixed and low marginal costs"; (3) "reduced antitrust enforcement" (121).

has acquired or established a number of related business activities, such as, in particular, *LexisNexis*, a commercial host of legal information (Lexis) and press and business information (Nexis), *Scopus,* an abstract and citation database, and a number of preprint platforms (*Mendeley, SSRN, BePress*). Consequently, Reed Elsevier, which in 2015 re-branded itself as *RELX group*, has become an important player in the data economy. During the last decades, the *Thomson Reuters Corporation*, which consists of the Reuters news agency and the Canadian Thomson Corporation, the world's largest information company, also diversified into a number of related activities, such as, in particular, *Westlaw*, one of the "gold standard" research products for the legal profession, and the academic metrics product *Clarivate* (including the *Web of Science*, which was formerly known as Thomson Science and competes with RELX's Scopus). Consequently, today RELX and Thomson Reuters jointly cover a large share of the legal information market and the market for academic metrics and thereby strengthened economies of scope and network externalities.[11]

2.2 Anticompetitive business practices in the data economy

Anticompetitive business practices in the EU by any company, including the data giants, usually fall under Art. 102 TFEU ("abuse of a dominant position"). This ex-post approach requires extensive gathering and processing of information. In the data economy, many services are ostensibly free of charge but the users are obliged to reveal valuable information to the provider, who sells this information to advertisers. These types of markets have been characterized as *two-sided markets* (Rochet and Tirole 2003). More generally, many data companies cross-subsidize the prices of complementary products to strengthen the network externalities from their main product (*multi-sided markets*). Competition authorities often find it difficult to determine when such a business practice is anti-competitive. Since the companies are allowed to continue their practice until the final court decision is valid, since the stakes are high, and since the companies have enough resources to sustain a lengthy legal battle, they have an incentive to delay the procedures as much as they can (Hummel, 2023; Schäfer, 2023).

There are many examples of lengthy legal battles due to the abuse of a dominant position in the data economy. The parallel cases against *Microsoft* in the US and the EU for abusing its dominant position in the market for PC operating systems by "tying and bundling" took more than 14 years in total, from the first investigations in the US until the final decision by the CJEU.[12] The case against *Google* for abusing its dominant position on the market for online general search by placing its own comparison-shopping service more favourably than competing services consumed about 11 years from the first investigations until the final CJEU decision.[13] In 2010,

[11] See for many details Lamdan (2023).

[12] For the US case see, e.g., Rubinfeld (2020), for the EU case see Kühn and Reenen (2009) and van den Bergh (2017, 314–6).

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018XC0112(01). See also Persch (2021).

several national competition authorities began investigating the use of best-price clauses by online travel agencies, such as *Booking* and *Expedia*. While "wide" retail parity clauses prevent participating hotels from offering better room prices or availability on any other sales channel, "narrow" retail parity clauses only prevent them from publishing better prices on their websites. Some national authorities have only banned wide retail parity clauses, others banned both types. The problem was solved in 2022 at the EU level by the adoption of the new Block Exemption Regulation for Vertical Agreements, which only accepts narrow retail price clauses. Consequently, it took 12 years from the first investigations until the final solution.[14]

The long time between the start of the investigations and the final decisions by the Court or by the legislator, which is primarily due to the difficulty for European competition authorities to determine relevant markets, dominant positions, the threat of potential competition, and abusive business practices and to sanction abusive business practices in the data economy, finally led to the EU Digital Markets Act, which we discuss in Sect. 3 below.

2.3 Access to data

2.3.1 General remarks

All modern societies face the question as to who owns the zettabytes of data generated in the data economy.[15] Or, more specifically, what are the rights and obligations of the relevant actors with respect to these data? Data are *non-rival goods*, i.e., their use by one party does not preclude another party's use.[16] Besides non-rivalry, Coyle et al., (2020, 4) list several other economic characteristics of data that affect their social value: excludability, externalities, increasing or decreasing returns, the large option value of data, the high up-front and low marginal cost of data collection, and complementary investments required for data use. These points raise some follow-up questions: For which types of data should intellectual property rights be defined? How difficult is it to enforce intellectual property rights or other protected data rights and to prevent academic plagiarism, in particular given the rise of generative AI, such as ChatGPT?[17] How is or how should access to data and data sharing be regulated (especially regarding data that are not protected by intellectual property rights)? Who has, or should have, the right to make money from owning certain data? Who is, or should be, liable for a "defective" product that relies on AI,[18] e.g., in autonomous driving – the product manufacturer, the suppliers of components,

[14] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5045.

[15] See also Tirole (2017, 405 ff.), Leyens (2019), Schäfer (2019), and the contribution by Eckardt/Kerber in this volume.

[16] Samuelson (1954) introduced the term 'collective consumption goods' for such goods and proposed conditions for their optimal supply.

[17] In June/July 2023, a California law firm filed class-action law-suits against OpenAI for 'stealing' personal data to train ChatGPT and against Google for 'secretly stealing' vast amounts of data from the web to train its AI technologies, such as 'Bard'; https://mashable.com/article/google-lawsuit-ai-bard.

[18] See also Wagner (2019), Friehe (2019), and the contribution by Buiten in this volume.

the software provider, providers of maintenance and repair, or the operator? Which data are, or should be, portable, and to what extent does portability depend on interoperability?[19]

2.3.2 Access to personal data

An important and controversial question is how much access private and public actors should have to the citizens' personal data, or in other words: how strictly the right to privacy should be protected.[20] More access to personal data means more transparency and, maybe, more efficiency.[21] Knowing more about potential business partners means being in a better position to assess their reliability before entering into a contract; knowing more about a politician means being in a better position to make a well-informed decision on election day; knowing more about suspected terrorists helps the police prevent attacks. However, too much access to personal data by powerful public or private actors might lead to socially inefficient overinvestment in information research (Hirshleifer 1971) and excessive data sharing,[22] and it may facilitate exploitation, blackmail, and oppression. Due to externalities resulting from excessive data sharing, individuals have little incentive to protect their data and privacy (Acemoglu et al., 2022). Consequently, privacy protection and the provision of individual freedom require collective action. Finding the 'right' balance between privacy protection and promoting the benefits of disclosure is clearly a challenge. At one extreme, the EU's General Data Protection Regulation of 2016 apparently provides for strong protection of personal data.[23] At the other extreme, most Western observers would probably agree that China's collection of mass data on individual behaviour by facial recognition software and the introduction of a national social credit system that collects information on the degree to which individuals and businesses comply with social norms constitutes too much (public) access to personal data and too little protection of privacy.[24]

If consumers have little faith in commercial platforms using their personal data confidentially, the result may be an underuse of these platforms, even if they provide

[19] See also the contributions by Jeon/Menicucci and Rubinfeld in this volume.

[20] Cf. Tirole (2021, 2007): "How transparent should our life be to others? Modern societies are struggling with this question as connected objects, social networks, ratings, artificial intelligence, facial recognition, cheap computer power and various other innovations make it increasingly easy to collect, store, and analyze personal data." Tirole also provides a formal model on the calculus of social approval. See also the review article by Acquisti et al. (2016).

[21] This point is stressed by Stigler (1980) and Posner (1981).

[22] Cf. Acemoglu et al., (2022, 219): "when an individual shares her data, she compromises not only on her own privacy but the privacy of other individuals whose information is correlated with hers. This negative externality tends to create excessive data sharing. Moreover, when there is excessive data sharing, each individual will overlook her privacy concerns and part with her own information because others' sharing decisions will have already revealed much about her.".

[23] For a critical assessment, see Hoofnagle et al. (2019) and Cofone (2024).

[24] For more detail, see Acemoglu and Johnson (2023, chapter 10), who stress that digital technologies and the internet can both strengthen and undermine authoritarian regimes (see e.g. the use of Facebook and Twitter during the Arab Spring) – these technologies are neither inherently antidemocratic nor democratic (pp. 353–4).

a benefit to all users (Pareto improvement). Tirole (2017, 408 ff.) discusses the special case of health insurance: On the one hand, the greater availability of personal information allows the insurers to charge lower premiums from those who behave responsibly, which reduces the moral hazard problem. On the other hand, greater availability of information on the genetic background of the insured can cause a breakdown of mutuality and risk sharing, without affecting the risk behaviour of the insured. In this case, "information destroys insurance" (the Hirshleifer effect), since insurance is only possible if there is uncertainty ex ante, when the insurance contract has to be signed. For that reason, most of the world's health care systems are heavily regulated and typically forbid selection based on risk characteristics, especially on those that the insured cannot do anything about.

2.3.3 Access to non-personal data and data sharing

Being non-rival, non-personal data (e.g., machine-generated data on a production process) is a key resource that should be employed by as many actors as possible – at least from a social efficiency point of view. Data sharing is therefore of special significance. Matching external data with a company's own data can yield new business models or facilitate resource optimization, e.g., in production and delivery processes. Yet legal,[25]as well as organizational, technical and economic barriers strongly affect corporate incentives for data sharing.[26]

From an economic point of view, restrictions on access to non-personal data that have *social value* – as opposed to mere *private, redistributive value*—are only justified if the collection of these data and their processing into valuable information causes non-trivial costs to the data holder (Hirshleifer 1971).[27] Free access to such data would undermine the incentive to generate them in the first place, so a paywall may be warranted. The reluctance to share such data in the business-to-business (B2B) sector may be overcome by licensing agreements that offer a means to control data access (Fries and Scheufen 2023).

In practice, there are two reasons for economically unjustified restrictions to the access to non-personal data. First, as already discussed in Sect. 2.1, data markets are typically characterized by market power, network effects and digital platform competition. A few very powerful companies, so-called gatekeepers, often decide on access to and the quality of data. A typical example of a data market where market power can be exploited in this way is "connected cars". In that market, the so-called "extended vehicle" concept allows car manufacturers to control access to the vehicle data through the technical design or storage of sensor data on their own (cloud) server systems (Specht-Riemenschneider and Kerber, 2022). That way, the

[25] See also Röhl and Scheufen (2023).

[26] The recent IW survey (see footnote 4) found that 58 percent of German companies do not engage in any data sharing at all. Larger companies are more likely to participate in data sharing, be it in a recipient or recipient/provider role. Yet the proportion of companies that act purely as data providers is largely independent of company size (Büchel and Engels, 2023).

[27] Restrictions on access to information that is only privately valuable would induce people to invest scarce resources without creating additional social value.

large platforms can extend their power to both upstream and downstream markets. As a result, for example, it is no longer the driver who decides which repair shop she trusts but the vehicle manufacturer who takes over this decision. Proper antitrust law should cope with this problem. Secondly, too little access to anonymized and aggregate data could result from excessive data protection, which tends to misinterpret those data as "personal data." This seems to be the case for example in Germany, where excessive data protection impedes empirical research and forces scholars to conduct comprehensive empirical studies abroad.[28]

2.4 Data reliability

The spread of biased information and "fake news" via social networks affects not only the individuals concerned (e.g., as addressees of online hate speech) but also the efficiency of decision-making. Fake photographs and videos have become an even greater challenge with the advent of generative AI such as ChatGTP. A large share of unreliable but easily accessible information, which we might refer to as "informational pollution," disturb the individual decision-making process. This problem has become more urgent since analogue media such as newspapers, radio and TV that employ professional journalists and whose editors monitor the quality of their information, are increasingly replaced by digital media, such as social media, video-on-demand and search engines that mainly provide user-generated content of not sufficiently monitored quality.[29] In combination with restricted access to reliable information, information pollution leads to the unpleasant result that "the truth is paywalled but the lies are free" (Robinson, 2020). The Digital Services Act (DSA) of 2022 aims to cope with problems like that (see Sect. 3).

2.5 Some distributional effects of the data economy

Massive technological innovations always create both winners and losers.[30] While some people enjoy the benefits of improved products and processes, as well as the returns on their investments in R&D, others are afraid for their jobs, their income and the general quality of their lives. According to Brynjolfsson and McAfee (2014, chapter 10), the top winners of digitization and the rise of the data economy are

[28] See, e.g., Riphahn (2022).

[29] In 2022, the worldwide share of digital advertising spending in total advertising reached 60% and is expected to increase further, undermining the financial basis of the analogue media; https://www.zenithmedia.com/digital-advertising-to-exceed-60-of-global-adspend-in-2022. Digital advertising is dominated by a few big companies. In the first quarter of 2023, 42.4% of global digital advertising spending accrued to Alphabet, 22.7% to Meta and 8.8% to Amazon (Otto 2023). In Germany, the circulation of newspapers declined by 36% between 2010 and 2020, and advertising revenues were reduced by 53%, to the benefit of the digital media, such as social media, video-on-demand, search engines and digital extensions of the analogue media. About 45% of total traffic accrues to the four leading providers (Alphabet, Meta, Apple and Amazon), 71.8% to the top 100 providers – from a total of 131,993 providers. For more information, see Andree (2023, 19–56).

[30] See the recent book by Acemoglu and Johnson (2023).

a small group of stars and superstars.[31] In particular, the founders of four of the five digital-tech giants have achieved top positions on the global rich list: Bill Gates (Microsoft) has been in the top ten of the Forbes List since 1993 and was in the top spot for a total of 18 years. Jeff Bezos (Amazon) has been among the top five since 2016, four times as number one. Mark Zuckerberg (Meta/Facebook) was among the top ten between 2016 and 2021, and Larry Page (Alphabet/Google) was in the top ten in 2019, 2021 and 2022. With respect to employment, Autor (2015) found that over the last thirty years digital technologies have increased jobs at the top of the salary scale (business executives, technicians, managers, and professionals) and at the bottom (nurses, cleaners, restaurant workers, custodians, guards, and social workers), whereas jobs with intermediate pay have declined.[32] However, he expects that "[w]hile some of the *tasks* in many middle-skilled jobs are susceptible to automation, many middle-skilled *jobs* will continue to demand a mixture of tasks from across the skill spectrum." (26).[33]

Digitization and the trend toward a data economy have dramatically changed the asset structure of large companies towards intangible assets, such as patent rights, copyrights and trademark rights.[34] This development poses a challenge to (international) taxation by facilitating tax arbitrage, and it thus affects the distribution between the private and public sector. The large data companies typically establish subsidiaries in low-tax countries. These subsidiaries own the intellectual property rights and collect license fees from the parent companies located in high-tax countries, reducing the latter's profits. As profits are thus shifted from high-tax countries to low-tax countries, we see both a redistribution and an overall reduction of public revenue.[35]

2.6 New types of aggression in the data economy: the emergence of cybercrime

The digital age facilitates existing types of crime and creates ample opportunities for new criminal activities. The global reach of certain types of crime committed via the internet creates additional problems of (international) law enforcement. The German Federal Office of Criminal Investigation (BKA) distinguishes between cybercrime in

[31] Autor et al (2020) found that since the 1980s industries have become increasingly dominated by superstar firms with high markups and a low labor share of value added. This holds for the US and for several OECD countries. As Kurz (2023) has shown, the emergence of innovative general-purpose technologies, protected by intellectual property rights, and the resulting market power, in combination with lenient taxation and anti-trust policies, leads in general "to the emergence of a few dominant firms and results in extreme inequality of income and wealth" (xiii). This already happened in the USA at the turn of the twentieth century with the advent of electricity ("First Gilded Age") and has been happening again with the advent of digitization and the internet since the 1980s ("Second Gilded Age").

[32] See also Tirole (2017, 423–5).

[33] Possible consequences of AI for jobs and wages are discussed by Frey (2019) and Acemoglu (2021).

[34] Among the top 500 US listed companies, the share of the value of intangible assets in the broadest sense in the companies' market value, including special client intangible assets, especially corporate and governance preference rights, increased from 17% in 1975 to 90% in 2020; https://oceantomo.com/intangible-asset-market-value-study.

[35] See Tirole (2017, 427–9) and Zucman (2015, chapter 5).

the *narrow* sense (offences targeted against the internet, data networks, IT systems or their data) and cybercrime in the *broad* sense (all offences committed by means of information technology). Regarding the former, digital identity theft is often the starting point of a cybercrime offence. The most common methods of stealing digital identities are phishing and spam mails, malware, analogue social engineering, data leaks and data breaches. The BKA lists four central forms of cybercrime in the narrow sense: *malware* that is used to spy out and intercept data, manipulate data traffic or extort money, *spam and fishing e-mails* with attachments containing malware, *ransomware attacks* that can lead to massive and expensive interruptions of business, and *denial of service (DDoS) attacks* that aim at overloading the target system.[36] Regarding cybercrimes in the *broad sense*, digital black markets on the darknet cover almost all fields of classical crime phenomena, such as drugs, weapons, child pornography, counterfeit money, and money laundering.[37,38]

3 Regulating the EU data economy

Already in May 2015, the EC issued a Communication on "A digital single market strategy for Europe" [COM(2015) 192 final],[39] with the digital single market being defined in another Commission Staff Working Document [SWD(2015) 100 final].[40] Five years later, on 19.02.2020, the EC issued a communication on "A European strategy for data" [COM(2020) 66 final],[41] which criticized the fragmentation between Member States regarding the regulation of the use and processing of data and the lack of availability of relevant data for potential users. Over the last few years, in particular since 2019, the European Union has initiated massive legislative activity regarding the data economy, starting with legal proposals, followed by intensive discussions, which in many but not all cases have already resulted in new Regulations and Directives. This legislative activity concerns various aspects of the data economy, such as, for example, personal data protection, the free flow of non-personal data, cybersecurity, copyright and related rights, the re-use of public sector information and publicly-held protected data, the fair and transparent treatment of users by online platforms, the regulation of large online platforms, the use of data generated by the IoT, AI, access to financial data, and many more. In the following,

[36] https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html.

[37] https://www.bka.de/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/Cybercrime/nationalSituationReportsOnCybercrime2019.html. For the state of IT security in Germany in 2022 see https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2022.pdf?__blob=publicationFile&v=8.

[38] Regarding the interaction between states, the threats of cyber-attacks and cyber-wars come into play, such as new types of espionage, of sabotage, denial-of-service attacks, cyber propaganda, economic disruption and others. See e.g. Krieger (2017) and Gutmann (2017).

[39] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100.

[41] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

we present the most important of these new laws that are also addressed in the contributions to this special issue:

Already in 2016, the General Data Protection Regulation (GDPR)[42] was enacted, which became effective on 25 May 2018 and ensures the protection of natural persons regarding the processing and free movement of their *personal data*. In particular, the GDPR provides for easier access to an individual's own data, a new right to data portability, a clearer right to be forgotten, and the right to know when an individual's personal data has been breached. Moreover, the GDPR intends to create more legal certainty for the businesses concerned. Despite the positive objectives and the signalling effect of the GDPR as a role model for other countries around the world, the continuing heterogeneity of international data protection efforts with a relatively strong data protection in the EU might be a potential competitive disadvantage for international players from Europe (Engels and Scheufen, 2020). Recent studies show that data protection concerns in particular are seen as the most important obstacle to data sharing (Röhl and Scheufen, 2023; Röhl et al., 2021). Particularly in the case of data, the intended legal certainty of the GDPR may lead to the very opposite for European companies. The lack of technical tools, for example for automatic pseudonymization or automated checks for data protection compliance, leads to this reluctance to share data. This particularly affects small and medium-sized companies with limited financial resources for legal advice (Fries and Scheufen, 2023; Röhl and Scheufen, 2023).

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (*Digital Markets Act, DMA*)[43] of 14 September 2022, which became applicable on 2 May 2023, is restricted to *"large" online platforms* that control one or more "core platform services", such as marketplaces, app stores, search engines, social media, cloud services, and advertising. These platforms are classified as *"gatekeepers"*, a clearly specified concept that replaces the vague concept of "dominant position". On 6 September 2023, the European Commission designated six gatekeepers (with 22 core platform services): Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft.[44] On 15/16 November 2023, Meta (with respect to Messenger and Marketplace platforms), ByteDance (with respect to TikTok) and Apple (with respect to its App Store) appealed against the "gatekeeper" status under the DMA.[45] The regulation lists numerous business practices that gatekeepers must abstain from and specific

[42] Regulation (EU) 2016/679.

[43] Related to the DMA is the Digital Services Act (DSA) of 19 October 2022 (Regulation (EU) 2022/2065). The DSA more generally aims to prevent illegal and harmful online activities and the spread of disinformation, for example, by facilitating combating harmful and illegal online content, by improving transparency on algorithms used in recommending content or products, by strengthening sanctions for rule infringement, and by stating special rules for "very large" online platforms and online search engines.

[44] See https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en.

[45] See https://arstechnica.com/tech-policy/2023/11/meta-tiktok-fight-eu-gatekeeper-status-to-avoid-opening-up-services-to-rivals/.

obligations that they must comply with (see also Schäfer, 2023).[46] The DMA provides for an innovative ex-ante evaluation of gatekeepers to check the market power of large digital companies. It thus promises a faster and more effective solution than the traditional control of an abuse of a dominant market position under European competition law (Kerber, 2022). However, the DMA is but a first step, especially as the per-se rule nature of the obligations requires further development. Other important academic discourses deal with topics such as the relationship between the DMA and other major legislative procedures (e.g. DSA or Data Act), the interplay between competition policy and the DMA (Büchel and Rusche, 2021), data protection and consumer policy (Kerber, 2022). The evaluation of the DMA focuses on the innovative approach of an ex-ante regulation of gatekeepers to combat the market power of large digital companies. The DMA thus provides a faster and more effective solution than the traditional control of an abuse of a dominant market position under European competition law (Kerber, 2022).

The Commission *Proposal for a Data Act* (*DA*) of 23 February 2022[47] aims to ensure fairness by setting up rules regarding the use of data generated by using connected objects (IoT), such as autonomous cars or industrial and agricultural facilities. Overall, the Data Act is intended to ensure a fair distribution of the added value from data among the players in the data economy and promote access to and use of data (Demary 2022). It focuses on four areas: (1) obligation of data controllers to disclose data generated by products and services to users, (2) establishing a balancing negotiating power in data sharing contracts, (3) creating emergency government access to data that are essential for overcoming the existing or impending crisis and, (4) simplifying the switching of cloud providers to prevent lock-in effects and ensure effective competition between providers (Demary 2022). After several years of intense discussions on the efficient allocation of data rights among the parties concerned and on the question which allocation best promotes data sharing and innovation, the final Data Act has been adopted in late November 2023.[48]

With the *Proposal for an Artificial Intelligence Act* of 21 April 2021, the EC for the first time initiated a targeted harmonization of national liability rules for AI.[49] The extensive definitions, prohibitions and complicated compliance regulations in the original proposal drew criticism from industry associations. The preliminary agreement on the AI Act from December 2023, whose final text is expected to be available in 2024, is thus based on a – compared to the proposal—modified

[46] In March 2023, the EC furthermore amended the Article 102 TFEU (abuse of a dominant position) guidance paper. https://competition-policy.ec.europa.eu/system/files/2023-03/kdak23001enn_competition_policy_brief_1_2023_Article102_0.pdf, and https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023XC0331(01).

[47] In July 2023 the Council, the European Parliament, and the Commission agreed in their trilogue proceedings on the final version of the Data Act which was officially enacted in November 2023. See https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/en/pdf.

[48] For a broad discussion of the Data Act (proposal) from a law and economics perspective see e.g. Martens (2023) as well as the contribution by Eckardt/Kerber in this special issue.

[49] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.

risk-based approach, i.e.the higher the risk, the stricter the rules: 1) minimal risk: no additional legal obligations; voluntary codes of conduct possible, (2) limited risk (e.g. Chatbots such as ChatGPT, or certain AI systems): minimal transparency obligations (3) high-risk (e.g. applications that endanger health, security, environment, basic rights and democracy): additional legal obligations (4) unacceptable risks: the technologies concerned are banned (e.g. cognitive behavioural manipulation, untargeted scraping of facial images from the internet, emotion recognition in the workplace and educational institutions, social scoring, biometric categorization to infer sensitive data etc.. There are, however, exceptions for law enforcement purposes). Due to the controversial discussions on General Purpose AI, such as ChatGPT, the preliminary agreed version demands strict regulatory requirements only on those ones that are based on a training with large quantities of data.[50] In addition, the Commission *Proposal for an AI Liability Directive*[51] and the *Proposal for a Revised Product Liability Directive*[52] of 28 September 2022 aim to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies and that victims are compensated for harm caused by defective products, including digital and refurbished products.

Some authors expect that the "Brussels Effect" (Bradford, 2020) will induce other countries in the world to also comply with EU legal norms that govern the data economy in order to sustain or even expand trade with the important Single European Market. In this case, the effects of the pieces of legislation mentioned above would transcend the borders of the European Union.[53] Others stress the risk of overregulation, which could weaken innovation incentives and the competitiveness of the European economy.

The contributions to this special issue discuss some of these European laws from different perspectives:

Eckardt/Kerber in their paper discuss the evolution of the governance of non-personal data generated by using connected objects (IoT) from the status quo ante via the Commission Proposal for a Data Act (February 2022) to the final text of the EU Data Act (enacted in November 2023). They apply property rights theory to analyze how the new legislation will change the bundle of rights regarding non-personal IoT data. For this purpose, they compare three different concepts for the design of this bundle of rights: a data holder-centric IP-like concept, a user-centric concept, and the concept of co-generated data. They conclude that the EU Data Act cannot be expected to contribute much to innovation, competition, and the empowerment of users, since it relies too much on the exclusivity of data and creates too many obstacles to data sharing. Eckardt/Kerber thus address the problems discussed in Sects. 2.1, 2.2, and particularly 2.3.

[50] Recently, Germany, France and Italy had criticized the Proposal for an AI Act and suggested to replace the strict regulation of generative AI by self-regulation via a code of conduct.

[51] https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

[52] https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf.

[53] See Bradford (2020, chapter 5) and Bendiek and Stuerzer (2023).

Referring to the GDPR, the Data Act Proposal and the DMA, *Jeon/Menicucci* formally analyze how data portability affects competition. They distinguish between two opposing effects of data portability on consumer surplus: the rent-dissipation effect and the competition-intensifying effect. An evaluation of data portability must assess the magnitude of the effect after consumer lock-in (the competition intensifying effect) relative to the effect before consumer lock-in (the rent-dissipation effect), which most policy makers seem to neglect. Thus, Jeon/Menicucci contribute to the problems discussed in Sects. 2.2 and 2.5.

Rubinfeld explores the private and social cost and benefits of data portability and interoperability and the case for public intervention. He shows how the EU and the US differ in their approaches to managing portability and interoperability issues. While the EU has chosen a regulatory approach via the GDPR and the DMA, the US rely more heavily on the competition agencies. The author concludes that these differences make sense in light of the two regions' different federal systems. The contribution thus relates relates to Sects. 2.1, 2.2 and 2.5.

Using a simple formal model, *Jorzik/Kirchhof/Mueller-Langer* discuss companies' incentives to invest in data creation, to use the data and to share it with other companies. They compare two regulatory settings, "no data-sharing policy" and "data-sharing policy", taking into account the companies' data economy readiness. For a data-sharing policy to enhance welfare it must not disturb the companies' incentives to create and prepare data. This largely applies to the EU's Proposal for a Data Act. Jorzik/Kirchhof/Mueller-Langer focus on problems discussed in Sects. 2.2 and particularly 2.3.

Rusche/Mouton examine Article 5 (4) of the DMA which targets anti-steering clauses between platforms and business users. These clauses aim to prevent business users of the gatekeepers from "directing acquired consumers to offers other than those provided on the platform, even though such alternative offers may be … more attractive". The authors employ a simple game-theoretic model to show that (a) the anti-steering obligation makes platforms more attractive to business users, (b) the obligation is also attractive to business users, (c) the platform has an incentive to become vertically integrated, (d) the amount of data available for business users and the platform is likely to increase, and (e) the fees are likely to increase if all business users were already using the platform before. As such, concentration in the data economy (Sect. 2.1) and anti-competitive business in the data economy (Sect. 2.2) are important problems discussed by Rusche/Mouton.

Buiten studies the efficient definition of product (manufacturing and design) defects for AI systems with autonomous capabilities and the implications for an efficient allocation of liability for AI between producers and users. In particular, the paper illustrates how AI systems disrupt the traditional balance of control and risk awareness between users and producers. Finally, some policy implications are discussed and the EU proposal for a revised Product Liability Directive (PLD Proposal) is evaluated. There are two critical points with this proposal: First, it retains the consumer-expectation test, which considers whether a product meets the safety expectations the public is entitled to, considering all relevant circumstances. However, this test may lead to the use of unreasonable consumer safety expectations as a benchmark, in particular regarding AI risks. Unfortunately, the proposal does not settle

whether a risk/utility-analysis is allowed. Secondly, even though there is a case for strict liability where risk is significant and risk awareness is low, the PLD Proposal does not follow this track but instead provides for an alleviated burden of proof. To cope with these problems, product liability should be complemented by adequate regulatory and certification standards. Buiten hence contributes to Sects. 2.4 and to some aspects of Sect. 2.6.

Mertens/Scheufen more generally discuss the effects of patent protection on innovation in the data economy while also assessing the impact of the DMA and the Data Act. Most importantly, the authors discuss the effects of patent breadth on the quality and relevance of innovations as measured by the number of forward citations. The authors use data on patents for technologies of the fourth industrial revolution, which are at the core of the data economy (e.g. IoT, AI etc.). Finding an effect of patent breadth on the quality/ relevance of innovations, the authors for the first time show that fourth industrial revolution technologies likely shift the optimal design of the patent system in favour of short and broad patents to stimulate future technological developments. Moreover, the paper finds evidence of path dependencies and differences in the cultural origins of the international patent systems (utilitarianism versus natural rights). In the light of the dominance of the big tech giants from the US and China in terms of the number and relevance of patent applications, the authors stress the importance of the Data Act and the DMA to counteract the increasing market power, especially with respect to access to data (see also Sect. 2.3.3). The paper thus primarily deals with the sort of problems discussed in Sects. 2.2 and 2.3.

Acknowledgements We would like to thank Sönke Häseler, Vera Demary, Manfred Holler, the participants of the research seminar law and economics at the University of Kassel and two anonymous referees for valuable comments.

Author contributions All authors wrote the main manuscript text and reviewed the manuscript.

Funding Open access funding enabled and organized by Projekt DEAL. Marc Scheufen acknowledges funding from the German Federal Ministry of Education and Research (BMBF) within the research project "Incentives and Economics of Data Sharing" (IEDS; funding number IEDS003), seehttps://ieds-projekt.de/for more information.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors have no competing interests to declare that are relevant to the content of this article.

References

Acemoglu, D. (Ed.). (2021). *Redesigning AI. Work, democracy, and justice in the age of automation*. Cambridge: Boston Review.

Acemoglu, D., & Johnson, S. (2023). *Power and progress: our thousand-year struggle over technology and prosperity*. New York: Public Affairs.

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2022). Too much data: Prices and inefficiencies in data markets. *American Economic Journal: Microeconomics, 14*(4), 218–256.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492.

Andree, M. (2023), *Big Tech muss weg! Die Digitalkonzerne zerstören Demokratie und Wirtschaft*. Frankfurt/New York: Campus.

Autor, D. (2015). Why are there still so many jobs? The history and future of workplace automation. *Journal of Economic Perspectives, 29*(3), 3–30.

Autor, D., Dorn, D., Katz, L. F., Patterson, C., & Van Reenen, J. (2020). The fall of the labor share and the rise of superstar firms. *Quarterly Journal of Economics, 135*(2), 645–709.

Belleflamme, P., & Peitz, M. (2021). *The economics of platforms. concepts and strategy*. Cambridge: Cambridge University Press.

Bendiek, A., & Stuerzer, I. (2023). The Brussels effect, European regulatory power and political capital: evidence for mutually reinforcing internal and external dimensions of the Brussels effect from the European digital policy debate. *Digital Society, 2*(5), 4–25.

Bradford, A. (2020). *The Brussels effect. How the European union rules the world*. New York: Oxford University Press.

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age. Work, progress, and prosperity in a time of brilliant technologies*. New York: Norton.

Büchel, J., & Engels, B. (2022a). The Importance of the data economy for Europe's digital atrategic autonomy. In European Liberal Forum (Eds.), *Decoding EU digital strategic autonomy. Sectors, issues, and partners*, Techno-Politics Series, Vol. 1, pp. 13–18.

Büchel, J., & Engels, B. (2022b). *Most companies are not data economy ready*, IW-Kurzbericht, No. 96. https://www.iwkoeln.de/en/studies/jan-buechel-barbara-engels-most-companies-are-not-data-economy-ready.html.

Büchel, J., & Engels, B. (2023). *Data sharing in Deutschland*. IW-Trends, No. 2, Köln.

Büchel, J., & Rusche, C. (2021). On gatekeepers and structural competition problems. *Intereconomics, 56*(4), 205–210.

Cofone, I. (2024). *The privacy fallacy. Harm and power in the information economy*. Cambridge: Cambridge University Press.

Coyle, D., Diepeveen, S., Wdowin, J., Kay, L., & Tennison, J. (2020). *The value of data: How is the value of data created, captured and distributed? Bennett institute for public policy report*. UK: University of Cambridge.

Demary, V. (2022). *Der data act: Welchen rahmen unternehmen für data sharing wirklich brauchen*. IW-Policy-Paper, No. 2, Cologne.

Eger, T., & Scheufen, M. (2018). *The Economics of Open Access. On the Future of Academic Publishing*. Cheltenham: Edward Elgar.

Eger, T., & Scheufen, M. (2021). Economic perspectives on the future of academic publishing: Introduction to the special issue. *Managerial and Decision Economics, 42*(8), 1980–1998. https://doi.org/10.1002/mde.3454

Frey, C. D. (2019). *The technology trap. Capital, labor, and power in the age of automation*. Princeton: Princeton University Press.

Friehe, T. (2019). Korreferat zu Gerhard Wagner: Roboter als Haftungssubjekte? Konturen eines Haftungsrechts für autonome Systeme. In F. Faust & H.-B. Schäfer (Eds.), *Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz* (pp. 41–46). Mohr Siebeck: Tübingen.

Fries, M., & Scheufen, M. (2023). Vertragsgestaltung beim data sharing: Empirie und best practice. *RDI—Recht Digital, 3*(9), 419–425.

Gilbert, R. J. (2020). *Innovation matters. Competition policy for the high-technology economy*. Cambridge: MIT Press.

Gutmann, J. (2017). Comment on Heike Krieger. In Th. Eger, S. Oeter, & S. Voigt (Eds.), *International Law and the Rule of Law under Extreme Conditions* (pp. 213–217). Mohr Siebeck: Tübingen.

Hirshleifer, G. (1971). The Private and Social Value of Information and the Reward to Inventive Activity. *American Economic Review, 61*(4), 561–574.

Hoofnagle, Ch. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hummel, L. M. F. (2023). Innovation as a Competitive Constraint on Online Platforms in European Competition Law: The Industry Life Cycle and Dominant Designs in Digital Markets. In K. Mathis & A. Tor (Eds.), *Law and Economics of the Digital Transformation* (pp. 281–304). Cham: Springer.

Ivers, A. M., Byrne, J., & Byrne, P. J. (2016). Analysis of SME data readiness: A simulation perspective. *Journal of Small Business and Enterprise Development, 23*(1), 163–188.

Kerber, W. (2022), *Stellungnahme: Öffentlichen Anhörung zum Thema "Digital Markets Act"* am 27. April 2022, Ausschussdrucksache 20(9)58, Deutscher Bundestag, https://www.bundestag.de/resource/blob/891306/578dd8a1a09df8a565e269e160f1651f/ADrs-20-9-58_Stellungnahme-Prof-Dr-Kerber-data.pdf

Krieger, H. (2017). Conceptualizing Cyberwar: Changing the Law by Imagining Extreme Conditions? In Th. Eger, S. Oeter, & S. Voigt (Eds.), *International Law and the Rule of Law under Extreme Conditions* (pp. 195–212). Mohr Siebeck: Tübingen.

Kühn, K.-U., & Van Reenen, J. (2009). Interoperability and market foreclosure in the European Microsoft case. In B. Lyons (Ed.), *Cases in European Competition Policy* (pp. 50–71). CUP: The Economic Analysis, Cambridge.

Kurz, M. (2023). *The market power of technology. Understanding the second gilded age*. New York: Columbia University Press.

Lamdan, S. (2023). *Data Cartels. The companies that control and monopolize our information*. Stanford: Stanford University Press.

Leyens, P. C. (2019). Sachenrecht an Daten. In F. Faust & H.-B. Schäfer (Eds.), *Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz* (pp. 47–78). Mohr Siebeck: Tübingen.

Marciano, A., Nicita, A., & Ramello, G. B. (2020a). Puzzles in the big data revolution: an introduction. *European Journal of Law and Economics, 50*(3), 339–344.

Marciano, A., Nicita, A., & Ramello, G. B. (2020b). Big data and big techs: Understanding the value of information in platform capitalism. *European Journal of Law and Economics, 50*(3), 345–358. https://doi.org/10.1007/s10657-020-09675-1

Martens, B. (2023): *Pro- and Anticompetitive Provisions in the Proposed European Union Data Act*, Working Paper 01/2023, Bruegel, https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf (last access: 20/12/2023).

Otto, M. (2023), 'Global digital advertising revenues—A look at the big three: Alphabet (Google), Meta Platforms (META), Amazon.com (AMZN)', *visible alpha*, May 17, https://visiblealpha.com/blog/global-digital-advertising-revenues-a-look-at-the-big-three-alphabet-googl-meta-platforms-meta-amazon-com-amzn.

Persch, J. (2021), Google Shopping: The General Court takes its position, *Kluwer Competition Law Blog*, November 15, https://competitionlawblog.kluwercompetitionlaw.com/2021/11/15/google-shopping-the-general-court-takes-its-position.

Posner, R. A. (1981). The economics of privacy. *American Economic Review, 71*(2), 405–409.

Rifkin, J. (2014). *The zero marginal cost society: the internet of things, the collaborative commons, and the eclipse of capitalism*. New York: Palgrave Macmillan.

Riphahn, R. T. (2022). Wir wissen in Deutschland vieles nicht, was wir wissen sollten. *Perspektiven der Wirtschaftspolitik, 23*(1), 38–46.

Robinson, N. J. (2020), 'The Truth Is Paywalled but the Lies Are Free', *Current Affairs*, August 02, https://www.currentaffairs.org/2020/08/the-truth-is-paywalled-but-the-lies-are-free.

Rochet, J.-C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association, 1*(4), 990–1029.

Röhl, K.-H., & Scheufen, M. (2023). Hemmnisse beim Data Sharing: Empirie und Handlungsempfehlungen. *Perspektiven der Wirtschaftspolitik, 24*(1), 129–144.

Röhl, K.-H., Bolwin, L., & Hüttl, P. (2021). *Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?* https://www.iwkoeln.de/studien/klaus-heiner-roehl-lennart-bolwin-wo-stehen-die-unternehmen-in-der-datennutzung-und-was-sind-ihre-groessten-hemmnisse.html.

Rubinfeld, D. (2020). A retrospective on U.S. v. Microsoft: Why does it resonate today? *Antitrust Bulletin, 65*(4), 579–586.
Samuelson, P. A. (1954). The pure theory of public expenditure. *Review of Economics and Statistics, 36*(4), 387–389.
Schäfer, H.-B. (2019). Korreferat zu Patrick C. Leyens Sachenrecht an Daten. In F. Faust & H.-B. Schäfer (Eds.), *Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz* (pp. 79–85). Tübingen: Mohr Siebeck.
Schäfer, H.-B. (2023). Current legal and economic problems of privacy protection, data sharing and market-opening in the digital economy. *Antitrust Bulletin, 68*(4), 641–656.
Specht-Riemenschneider, L. and Kerber, W. (2022), Datentreuhänder—Gesellschaftlich nützlich, rechtlich größere Anforderungen erforderlich, KAS e.V., *Analysen & Argumente*, Nr. 475, Februar 2022, https://www.kas.de/de/analysen-und-argumente.
Stigler, G. J. (1980). An introduction to privacy in economics and politics. *Journal of Legal Studies, 9*(4), 623–644.
Tirole, J. (2017). *Economics for the common good*. Princeton: Princeton University Press.
Tirole, J. (2021). Digital dystopia. *American Economic Review, 111*(6), 2007–2048.
Van den Bergh, R. (2017). *Comparative competition law and economics*. Cheltenham: Edward Elgar.
Wagner, G. (2019). 'Roboter als Haftungssubjekte? Konturen eines Haftungsrechts für autonome Systeme'. In F. Faust & H.-B. Schäfer (Eds.), *Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz* (pp. 1–39). Mohr Siebeck: Tübingen.
Zingales, L. (2017). Towards a political theory of the firm. *Journal of Economic Perspectives, 31*(3), 113–130.
Zucman, G. (2015). *The hidden wealth of nations. The scourge of tax havens*. Chicago: Chicago University Press.