European Approaches to the Regulation of Digital Technologies

Martin Müller and Matthias C. Kettemann

Abstract Following years of a liberal approach to digital technologies, platforms, services, and markets, the EU has stepped up its action in recent years. The adoption of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 1) in 2016 can be seen as a starting point for new regulations that are now enacted and proposed under the European Commission's strategy "A Europe fit for the digital age." This article will briefly summarize the contents of the GDPR as well as the Digital Services Act (DSA) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 1), Digital Markets Act (DMA) (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 1), Data Governance Act (DGA) (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 1), and the proposals for the Artificial Intelligence Act (AI Act) (Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21 April 2021, COM(2021) 206 final.) as well as the Data Act (Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), 23 February 2022, COM(2022) 68 final.). We identify the underpinnings of the normative approach and its potential and shortcomings, thus providing an assessment of the role of Europe as a technology regulator more broadly and its relationship to digital humanism.

M. Müller (✉) · M. C. Kettemann
Department for Theory and Future of Law, University of Innsbruck Innsbruck, Innsbruck, Austria
e-mail: martin.mueller@uibk.ac.at; matthias.kettemann@uibk.ac.at

H. Werthner et al. (eds.), *Introduction to Digital Humanism*,
https://doi.org/10.1007/978-3-031-45304-5_39

1 Introduction

In recent years, the European Union (EU) has undergone a significant shift in its approach toward digital tools and technologies, platforms, services, and markets. After years of embracing a more liberal stance, the EU has ramped up its regulatory actions to address the challenges posed by the digital age. A pivotal moment came in 2016 with the adoption of the General Data Protection Regulation (GDPR), marking the beginning of a series of new regulations enacted and proposed under the European Commission's strategy, "A Europe fit for the digital age." This article aims to provide a concise overview of the key regulatory measures introduced by the EU and contextualizes it against the background of an ongoing alignment of EU normative approaches and digital humanism.

2 Overview of EU Platform Regulation

2.1 The Starting Point: GDPR

The General Data Protection Regulation (GDPR) is a great achievement in the field of data protection and one of the toughest privacy and security laws in the world. On 25 May 2018, the regulation entered into force. It is considered a wide-ranging personal data protection regime of greater magnitude than any similar regulation previously in the EU, or elsewhere.[1] The objectives of this Regulation in Article 1 GDPR are to lay down rules relating to the protection of natural persons concerning the processing of personal data and rules relating to the free movement of personal data and to protect fundamental rights and freedom of natural persons.

The Regulation applies to the processing of personal data wholly or partly by automated means. For non-automated means, the GDPR applies as well when personal data is saved in a filing system or is intended to do so. The GDPR sets a low bar, defining "personal data" in Article 4 as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly (. . .)."[2] The territorial requirement for the applicability of the Regulation is that, whether or not the processing takes place in the Union, the processing of personal data must be carried out in the context of the activities of an establishment of a controller or processor in the Union. This means that the GDPR applies to all organizations that process the personal data of EU citizens, regardless of where the organization is based. This includes businesses operating within the EU as well as those outside the EU if they offer goods or services to EU citizens or monitor their behavior. In practice, this means that the GDPR applies to far more data collection activities than its predecessor, the Data

[1] Allen et al. (2019, 785).

[2] Hoofnagle et al. (2019, 72).

Protection Directive, which was based on where the data was processed rather than where the data subject resided.[3] The penalties to be applied by the Supervisory authorities for breaching the Regulation are significant, ranging up to 20 million euros or 4% of global turnover, whichever is higher.

The GDPR seeks to use regulatory powers to create a powerful threatening incentive for companies to behave as the regulators intend. In Article 5, the GDPR lists some principles relating to the processing of personal data. For the regulators, personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject (. . .)"; it shall also be collected for specified, explicit, and legitimate purpose, adequate, relevant, and limited to what is necessary in relation to the object, stored secure for no longer than necessary. Article 13 GDPR lists the information that has to be provided to the data subjects. This includes information about the period of storage of the data, the existence of the subject's right to rectification or erasure of personal data, the existence of the right to withdraw consent at any time, and many more. The data controller and processor must implement appropriate technical and organizational measures to be able to demonstrate that processing is performed in conformity with this Regulation. Article 51 GDPR provides the constitution of one or more independent public authorities in the member states to be responsible for monitoring the application of this Regulation. They should protect the fundamental rights and freedoms of the natural persons in relation to the data. The GDPR sets standards for the authorities which include that the state, while providing the supervisory authority with the human, technical, and financial resources, shall also ensure that such does not affect the independence of the supervisory authority. Article 68 of the GDPR provides the constitution of the European Data Protection Board (EDPB), which shall be composed of the head of one supervisory authority of each member state and the European Data Protection Supervisor.

Five years into the applicability of the GDPR, it is becoming clearer that the GDPR did indeed set a global standard which has been dubbed the *Brussels Effect*[4] and has led to similar data protection laws around the world.[5] However, a few downsides are beginning to show when it comes to clarity and enforcement of the regulation. The provisions of the GDPR are occasionally vaguely worded, so rulings by the European Court of Justice (ECJ) are necessary to remove these ambiguities. Five years after its adoption, 55 cases have had to be decided already or are still awaiting a decision. In view of the approximately 800 cases decided annually by the ECJ for all areas of law,[6] frequent interpretation of the GDPR is necessary. On the enforcement side, civil society organizations showed that procedures under the GDPR take long or may be even not carried out at all. Moreover, as member states

[3] Ibidem, p. 786.

[4] Bradford (2020).

[5] For a comprehensive overview cf. Greenleaf (2021).

[6] ECJ (2023, p. 1).

authorities are responsible for the enforcement, procedure varies and a common approach is hindered by member states-specific procedural issues.[7]

2.2 *Regulating Platforms' Societal Power: Digital Services Act (DSA)*

The Digital Services Act (DSA) is a regulation of the European Union, which came into force in November 2022. The Digital Services Act (DSA) and the Digital Markets Act (DMA) are part of the EU's digital strategy and aim to create a safer digital space in which the fundamental rights of all users of digital services are protected and to create a level playing field to promote innovation, growth, and competitiveness both in the European single market and worldwide. The DSA is a further development of the previous E-Commerce Directive,[8] which will be replaced by the DSA. A significant innovation is the extraterritorial scope of the DSA; this is defined at the outset in the general provisions. The DSA is territorially linked to the establishment of the user. As a result, as long as there is a "substantial connection to the Union," the establishment of the service provider is irrelevant.[9]

The material scope of application of the DSA does not include all digital service providers but is limited to so-called intermediary services, which are further subdivided into "mere conduit," "caching," and "hosting" services. These services include the transmission and storage of user-generated content.[10] The main objective of the E-Commerce Directive was to create a legal framework that facilitates the free movement of intermediaries within the EU in order to promote innovation and e-commerce. The DSA, however, is based on a different approach. It recognizes digital platforms as responsible actors in the fight against illegal content.[11]

Regarding the liability exemptions in its Chapter II, the DSA preserves and upgrades the basic liability rules of the previous E-Commerce Directive. The liability exemptions prevent state actors from incurring any liability for third-party content and obligations to generally monitor third-party content. The liability exemptions cover mere conduit services, caching services, and hosting services.[12]

Based on the idea of acknowledging digital platforms as responsible actors, the DSA sets out due diligence obligations in Chapter III of transparency, accountability, and information for digital services to qualify and contain a variety of obligations

[7] noyb.eu (2023), van Hoboken (2022).

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 1).

[9] Buri and van Hoboken (2021, p. 13).

[10] Wilman (2022, p. 1).

[11] Genç-Gelgeç (2022, pp. 25–60).

[12] Husovec and Roche Laguna (2022, p. 3).

such as specific requirements for terms and conditions, the setting-up of a compliant-management system, or reporting and transparency requirements. The obligations are set depending on the size of the digital service providers and their role in the online world. In doing so, the DSA divides them into four categories: intermediaries, hosting intermediaries including online platforms, online platforms (providers of hosting services that also disseminate information), and very large online platforms (VLOPs) and very large online search engines (VLOSEs) (online platforms with more than 45 million recipients). Each of them is required to perform duties at different levels.[13]

In Chapter IV, the DSA introduces a set of rules regarding the implementation, cooperation, penalties, and enforcement. For example, all providers of intermediary services are bound to report, publicly and at least annually, on how they have dealt with various obligations under the DSA. In addition, not that they are obliged to take certain measures to facilitate public supervision and enforcement. Here, the measures include the appointment of a single point of contact allowing for direct communication with the competent supervisory body. As for very large online platforms and very large online search engines, the DSA aims to ensure adequate internal and external oversight of compliance with the new rules. For this, providers must establish an independent compliance function within the provider's organization. An important innovation of the DSA is the wide-ranging competencies given to the Commission to enforce the rules applicable to very large online platforms and very large online search engines, such as the possibility of investigations and inspections, requiring access to data, and the possibility of imposing heavy fines.[14]

2.3 Regulating Platforms' Economic Power: Digital Markets Act (DMA)

The DMA was enacted at the same time as the DSA; therefore, both acts have to be read together in order to fully understand the overall meaning of the EU's stance to platform regulation. The DMA tries to contain the economic power the "big tech" platforms have in digital markets, which are often monopolistic when it comes to specific online services (think about "the" search engine, "the" online marketplace, or "the" social media platform). Traditional unfair competition law on the EU level (namely, Articles 101, 102 of the Treaty on the Functioning of the European Union (TFEU)) and member states' laws do apply to digital platforms; however, this is understood to be "too little, too late" as proceedings by the European Commission

[13] Genç-Gelgeç (2022, pp. 25–60).

[14] Husovec and Roche Laguna (2022, p. 12) and Wilman (2022, p. 14 et seqq).

against platforms took long and couldn't improve market competition.[15] Moreover, digital markets differ from other markets by some economic characteristics.[16]

The DMA shifts from the so-called ex post approach (i.e., that authorities must first find a violation and can than react with fines or other measures) which is imminent to competition law to an ex ante approach and prohibits or imposes corresponding regulations for a total of 21 practices that are considered harmful to betting in digital markets. These due diligence obligations do not apply to all platforms but only to those that have been designated as *gatekeepers* by the European Commission. In the DMA's understanding, companies are gatekeepers when they meet the following three requirements: (a) having a significant impact on the internal market, (b) providing a so-called core platform service,[17] and (c) enjoying an entrenched and durable position now or in the near future. These rather general requirements are followed by specific thresholds, all of which are met by the known big tech companies.

The due diligence obligations to be followed by platforms can be divided into two groups: Part of the obligations must be complied with by platforms as they stand. This includes, for example, the prohibition for gatekeepers to merge data from different central platform services or the compulsion to have to use a certain payment service. The other part of the obligations, on the other hand, is less specific and can be further narrowed down by the European Commission as supervisory authority. In this group is, for example, a prohibition of self-preference of services or products of the gatekeepers over those of other providers or the possibility for users to simply transfer their own data to another data provider (so-called data portability).

The new regulations are to be enforced almost solely by the European Commission. If obligations are violated regularly, enforcement will be taken in the form of fines. At up to 10% of annual global turnover, these fines are similar to those of the GDPR. However, the DMA also allows the Commission to prohibit mergers of companies and, as a last resort, to break up gatekeeper companies should obligations of the DMA be "systematically violated."

2.4 Regulating Platforms' "Oil" I: Data Governance Act

The DGA is the first piece of legislation at Union level to address data sharing. While the GDPR is concerned with the protection of personal data, the DGA first wants to address data sharing in general, i.e., personal as well as nonpersonal data, and thus represents a realignment of the Union's policy.[18] The goal of the European

[15] Podszun et al. (2021, pp. 60 et seq).

[16] Schweitzer (2021, p. 518).

[17] The DMA lists in Article 2 (2) overall ten *core platform services*. These are, e.g., online search engines, online social networks, video-sharing platforms, or cloud computing services.

[18] Metzger and Schweitzer (2023, p. 43).

Commission within the framework of the proclaimed "data strategy" is to create a "free flow" of data, which is said to have major economic benefits for the Union's common market.[19]

In total, the DGA regulates four different individual areas: first, it creates conditions for the sharing of public sector data; second, it regulates the operation of commercial "data intermediary services"; third, it oversees those that operate altruistically; and finally, it establishes the European Data Innovation Council.

In the context of European platform regulation, these "data intermediaries" are interesting. Unlike in the DSA and DMA, there is (still) no power position by a "big tech" company in data markets. In addition to creating more trust in data markets and, thus, establishing the "free flow of data," the underlying rationale for regulation can be seen in the attempt to prevent precisely such positions of market power from arising.[20]

Once the DGA enters into force, data intermediaries must notify member state authorities. This also applies to companies not residing in the EU, provided they are also active in the European market. Data intermediaries will be bound by 15 different regulations designed to ensure that the objectives of regulation (increasing data sharing, trust in data sharing, and fair competition) are achieved. For example, companies must act neutrally, be interoperable, or provide fair and transparent access (so-called FRAND conditions). Many of the obligations are similar in content to the DMA but may be interpreted differently.[21]

2.5 Regulating Platforms' "Oil" II: Data Act Proposal

The European Commission's Data Act proposal is the centerpiece of the "data strategy." The aim here is to increase the amount of publicly available data. Currently, vast amounts of data are generated by Internet of Things (IoT) devices, which usually remain with the manufacturers and can only be accessed in exceptional cases.[22]

To this end, a so-called horizontal right is created for users vis-à-vis product manufacturers (the "data holders") to access the data generated by the product, i.e., users can demand in any economic sector the data created by "them" through the use of a product (e.g., a connected vehicle, an app-based robotic vacuum cleaner, etc.) to receive it and to have it shared with a third party. With these access rights come various obligations designed to make this right useful in practice. For example, care must be taken in the design and manufacture of the product to ensure that data is

[19] von Ditfurth and Lienemann (2022, p. 272).

[20] von Ditfurth and Lienemann (2022, p. 278).

[21] Baloup et al. (2021, p. 32 et seqq).

[22] Metzger and Schweitzer (2023, p. 43 et seq).

readily available, and the FRAND conditions for disclosure of data also required in the DMA and DGA are also mandatory for data holders in the Data Act.

From a platform regulation perspective, the obligation of so-called data processing services to enable switching between different such services should also be mentioned. Here again, a parallel to the DMA can be seen, except that the data portability obligation goes beyond the "big tech" companies and is extended. Other provisions concerning the interoperability of data, i.e., the technical compatibility of different provider systems, also strike in the same vein.

2.6 Regulating Platforms' "Tools": AI Act Proposal

Widely understood, the European Commission's proposal for the AI Act is a risk-based regulation[23] in which the use of AI systems is classified into different risk categories, with more extensive regulations for higher risk. Besides many innovative areas of application, AI systems also pose risks, particularly for the fundamental rights of users, which made the European Commission now call for the regulation of the technology.

AI systems are classified through the draft AI Act into different risk categories. In the first, certain AI systems are deemed as "unacceptable," such as when they influence the free will of users or contain "social scoring," which is the AI-based assessment of individual citizens' behavior by government agencies. Under the proposed AI Act's scope, their use is then prohibited in the European Union.

The next level includes "high-risk" AI systems, which are listed in the separate Annexes II and III of the proposed regulation. Annex II features a list of existing EU regulations in place that require a "conformity assessment" for products that bear specific risks. If AI is part of these products or the product "itself," it is considered to be a "high-risk" AI system. For the list in Annex III, the context of use is more relevant, i.e., it is not the AI system itself that is considered risky but the area in which it is used. Eight different domains are therefore named in which certain AI systems are "high-risk" AI systems, such as those involved in decisions about access to education or employment. A particularly large number of applications that are considered "high-risk" AI involve those in law enforcement or migration. If an AI system falls into this category, manufacturers and users must adhere to a host of compliance obligations, such as having risk management and quality management systems in place and registering the AI system with the Commission.

The third and final group includes "low-risk" AI systems, for which the AI Act proposal requires "only" transparency obligations and thus significantly fewer requirements than for those in the "high-risk" category. In detail, this means that providers of AI systems that (1) interact with humans, (2) are used for emotion or

[23] Ebers et al. (2021, p. 589) and De Gregorio and Dunn (2022, p. 488 et seqq).

biometrics recognition, or (3) that generate "deepfakes" must notify their users that the content was generated by an AI.

"Risk-free" AI systems are not regulated by the AI act. They include, for example, spam filters for email programs. Here, the risk for users is considered so small that no regulations are envisaged.

3 Digital Humanism in European Platform Regulation

The Vienna Manifesto on Digital Humanism addresses the platforms as the most important actors in digitalization in several places and demands answers regarding the problematic phenomena that have emerged due to their "platform power" (cf. chapter of Samaan). For example, it demands that "Effective regulations, rules and laws, based on a broad public discourse, must be established." The following demand is even clearer: "Regulators need to intervene with tech monopolies."

In addition to these programmatic demands, however, the Vienna Manifesto also contains the normative framework that should underlie digital technology and thus also its regulation. In addition to ethical considerations (cf. chapters by Nida-Rümelin and Staudacher, Werthner, and Prem/Tamburrini when it comes to AI), the reference to human rights explicitly also includes legal considerations. This should be the yardstick for our assessment of platform regulation under European Union law: How does platform regulation under Union law ensure that human rights are protected?

For the European Union, human rights, as found at the level of international law, for example, in the Universal Declaration of Human Rights or the UN human rights covenants,[24] are not the direct connecting factor. As a supranational, European organization, the ECHR as a regional human rights instrument and the Charter of Fundamental Rights (CFR) adopted in 2007 are more relevant and form the constitutional basis for regulation. When it comes to the level of protection for individuals, this is basically on a par with the level under international law in the case of the ECHR and the CFR.

3.1 Fundamental Rights in EU Platform Regulation

In some cases, the various legal acts explicitly refer to fundamental rights in general or also specifically to individual fundamental rights. It starts with the GDPR, which is the concrete formulation of the fundamental rights of Articles 7 and 8 of the CFR, which initially only stipulate that there is a fundamental right to data protection. The

[24] An overview of the different human rights instruments on the UN level can be found here: https://www.un.org/en/global-issues/human-rights (retrieved 24 April 2023).

detailed formulation is then taken over by the GDPR and specifies, for example, the concrete rights of data subjects in Articles 12 et seqq. GDPR or the requirements for data processing. There is no clear mentioning of fundamental rights in the text, but many of the provisions of the GDPR refer to fundamental rights "unconsciously."[25] Not discussed here, but another example for fundamental rights to be respected by platforms can be found in Article 17 DSM Directive, which has been discussed in chapter of Mendis before.

At two provisions, the DSA contains very specific requirements for platforms to take fundamental rights into account. In the legal discussion, this is referred to as a "horizontal binding" of platforms. This is because fundamental rights and human rights historically applied only between citizens and states, thus binding the state "vertically" to rules, giving citizens rights.[26] Now these rules are also applied between private companies and users, who before had been "on the same level" as fundamental rights holders. However, digitalization and the rise of platforms as the most important actors have led to a power imbalance at the expense of users, thus questioning whether equal fundamental rights treatment is still justified or platforms should also be bound to fundamental rights vis-à-vis their users.

First and foremost, there is Article 14 DSA, which deals with the terms and conditions of platforms. These terms and conditions are very relevant in practice as they mainly govern the relationship between users and platforms.[27] So far, platforms have been quite free in their choice of terms and conditions, sometimes called terms of use or terms of service, and are only marginally bound by law. However, users must agree to the terms and conditions if they want to use the platforms' services. Because of the aforementioned tendency of digital markets to monopolize, this then often results in a requirement for consent. Article 14 (4) DSA now requires that the interests of users must be considered when moderating content and for complaints handled by platforms. The fundamental rights of users, such as the fundamental right to freedom of expression, are cited very specifically. Similar to the way in which fundamental rights must be observed in official decisions or court proceedings in democratic states, platforms may not violate any fundamental rights in "their decisions." Article 14 DSA thus undoubtedly represents a horizontal binding of platforms.[28]

Similarly, VLOPs must respect fundamental rights: Because of the "systemic risks" they pose, the DSA requires them to conduct comprehensive risk analyses and take measures on how to deal with the risks. Article 34 (1) DSA again requires users' fundamental rights among other interests to be taken into account when assessing risks.

[25] Celeste and de Gregorio (2022, p. 11 et seq).

[26] This is not an entirely new phenomenon and can be traced back in different legal systems, cf. Frantziou (2015, pp. 670, 674–677) and Quintais et al. (2022, pp. 17 et seqq).

[27] Quintais et al. (2023, pp. 2 et seq).

[28] Quintais et al. (2022, p. 25).

The AI Act proposal mentions fundamental rights in a few places. The recitals, where at the Union level the larger context and rationale for why a particular provision is adopted can often be found, clearly demonstrate how AI can impact fundamental rights. For example, in addition to the certain benefits AI brings, there is also the risk of "manipulative, exploitative and social control practices," so they are to be prohibited because of their contradiction to, inter alia, Union fundamental rights.[29] Examples of those practices are clearly spelled out in Article 5 AI Act proposal that regulates "unacceptable AI systems" and can be the deployment of subliminal techniques to distort a person's behavior or the use of "social scoring" systems.

For new AI systems that have not yet been covered, the AI Act proposal provides that they must be classified as high-risk AI systems if they have an adverse impact on fundamental rights. As briefly mentioned above, the classification then imposes extensive compliance obligations on the providers and users of these AI systems. In concrete terms, these obligations then include fundamental rights at a further point. For example, Article 13 of the AI Act proposal requires providers of high-risk AI systems to transparently describe the risks to fundamental rights when using AI applications. Similarly, human oversight of high-risk AI systems serves to protect fundamental rights (Article 14 (2) AI Act proposal).

3.2 Freedom of Choice/Freedom of Contract

Having already looked at the GDPR, the DSA, and the AI Act, the question arises as to how digital humanism is reflected in the other legal acts from Chapter 2, which concern the factors of the platform economy, i.e., the economic power of the platforms, their "oil," and the tools supporting the work of the platforms. Here, the focal point can be found in the actual safeguarding of freedom of choice and contract, which are protected at various points by fundamental rights such as the right to respect for private and family life in Article 7 CFR, freedom to conduct a business in Article 15 CFR, or the objective of a high level of consumer protection in Article 38 CFR. The human rights of the ECHR, which must be observed by the member states of the European Union, also protect freedom of contract in part through the property guarantee in Article 1 Protocol 1 ECHR.[30] While the DMA thus aims to improve competition among platforms in certain markets, for example, with obligations on interoperability (Article 7 DMA), in areas where there is a monopoly or "quasi" monopoly, "FRAND" conditions (Article 6(6), (12) DMA) are intended to ensure that there is no exploitation of this economic position. Both

[29] Recital 15 AI Act Proposal.

[30] This was pointed out in a variety of cases before the European Court of Human Rights concerning rent-control systems by states which limit the freedom to conclude lease contracts, cf. Pařízek v. the Czech Republic, no. 76286/14, 12 January 2023, § 53 et seq.

approaches are also reflected in the data-related legal acts (DGA and Data Act), as explained above. Especially for the future legal acts related to data, interoperability and FRAND conditions should not be seen independently but are interrelated: In the best case, FRAND conditions allow users access to data not dependent on the "arbitrariness" of data holders, for example, platforms. These can then be used independently of the previously used service through the interoperability obligation. Together, these two factors improve the user's position vis-à-vis platforms as well and allow for an improved exercise of contractual freedom.

4 Conclusions

Our examination of platform regulation and its relationship to digital humanism has shown that binding platforms to fundamental rights is a response by the European Commission to the challenges of digitalization and is in line with the demands of the Vienna Manifesto on Digital Humanism. In order not to go too far, we have not further explored the considerations of other authors on the role of the "rule of law" and "due process," but we do see points of contact in the legal acts of platform regulation that need to be looked at in more detail in the future, for example, through the detailed requirements for complaint management systems in Articles 20 et seqq. DSA.

For the outlook, the exciting question certainly lies in the potential impact of the European draft on the future of platforms: Many of the platforms are located in non-EU countries and the markets of the future for them are not in Europe but in other parts of the world. There is also the question of enforcement: Will it be possible for the various authorities, be it the Commission or even the individual authorities of the member states, to enforce the individual regulations against the platforms? This is not only a financial question but also a question of knowledge, because enforcement in many places requires a deep technical understanding that is unlikely to reside with all authorities. At least, however, the proposed norms provide a solid basis for addressing some of the most challenging issues that individuals and societies are confronted with in times of digitalization.

Discussion Questions for Students and Their Teachers

1. Where can links be drawn between the "Vienna Manifesto on Digital Humanism" and the EU's legal framework for platforms?
2. How does platform regulation ensure that freedom of choice is guaranteed vis-à-vis "big tech" platforms?
3. How are notions of "due process" and "rule of law" as pillars of modern democratic states enshrined in the legal framework for platforms?
4. Is it acceptable to subject platforms to the same requirements as democratic states?
5. How can the EU and its member states learn from the lack of enforcement of the GDPR?

Learning Resources for Students

1. Centre for International Governance Innovation (ed.), The Four Domains of Global Platform Governance, CIGI Essay Series, https://www.cigionline.org/the-four-domains-of-global-platform-governance/ (last retrieved: 26.06.2023).

   The series of 20 essays gives an overview of the different facets of platform regulation, spanning from the content on platforms to the underlying infrastructure.
2. Bietti, E. (2023), A Genealogy of Digital Platform Regulation, 7 Georgetown Law Technology Review (1), 1, available online: https://georgetownlawtechreview.org/a-genealogy-of-digital-platform-regulation/GLTR-01-2023/ (last retrieved: 26.06.2023).

   This paper traces back the history of platform regulation to the 1990s as a part of the discourse on early Internet regulation and suggests to re-invent the rule of law in platform regulation.
3. Richter, H., Straub, M., Tuchtfeld. E. (eds.) (2021), To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package, Max Planck Institute for Innovation and Competition Research Paper No. 21-25, https://pure.mpg.de/rest/items/item_3345402_5/component/file_3345403/content (last retrieved: 26.06.2023).

   This series of originally short blog entries discusses different aspects of the then-proposed DSA/DMA packages. Although the final legal text has changed, certain issues remain relevant.
4. de Gregorio, G. (2022), "Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society".

   This monograph traces back where constitutional fragments and concepts can be found in EU platform regulation and shows that they in fact underline EU digital policy.
5. Persily, N., Tucker, J. (eds.) (2020), Social Media and Democracy, Cambridge, United Kingdom, New York, NY: Cambridge University Press.

   This volume explicitly deals with social media platforms and approaches the issues of disinformation, hate speech, and content moderation from different disciplines.

Acknowledgements The authors are grateful to have received valuable research support by Johanna Erler.

References

Allen, D. et al. (2019). Some economic consequences of the GDPR. *39 Economics Bulletin* (pp. 785–797). Last retrieved: 26.06.2023, from http://www.accessecon.com/Pubs/EB/2019/Volume39/EB-19-V39-I2-P77.pdf

Baloup, J. et al. (2021). *White Paper on the Data Governance Act*. Last retrieved: 14.04.2023, from https://ssrn.com/abstract=3872703

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

Buri, I., & van Hoboken, J. (2021). *The digital services act (DSA) proposal: A critical overview*. Last retrieved: 29.03.2023, from https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf

Celeste, E., & de Gregorio, G. (2022). Digital humanism: The constitutional message of the GDPR. *Global Privacy Law Review, 3*, 4–18.

De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review, 59*, 473–500.

Ebers, et al. (2021). The European Commission's proposal for an artificial intelligence act—A critical assessment by members of the Robotics and AI Law Society (RAILS). *Multidisciplinary Scientific Journal, 4*, 589–603.

ECJ. (2023). *Statistics concerning the judicial activity of the Court of Justice*. Last retrieved: 26.06.2023, from https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-03/stats_cour_2022_en.pdf

Frantziou, E. (2015). The horizontal effect of the charter of fundamental rights of the EU: Rediscovering the reasons for horizontality. *European Law Journal, 21*(5), 657–679.

Genç-Gelgeç, B. (2022). Regulating digital platforms: Will the DSA correct its predecessor's deficiencies? *Croatian Yearbook of European Law and Policy, 18*(1), 25–60.

Greenleaf, G. (2021). *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*. Last retrieved: 23.06.2023, from https://ssrn.com/abstract=3836348

Hoofnagle, C., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law, 28*, 65–78.

Husovec, M., & Roche Laguna, I. (2022). *Digital services act: A short primer*. Last retrieved: 29.03.2023, from https://ssrn.com/abstract=4153796

Metzger, A., & Schweitzer, H. (2023). Shaping markets: A critical evaluation of the draft data act. *Zeitschrift für Europäisches Privatrecht, 31*, 42–82.

noyb.eu (2023). *5 years of the GDPR: National authorities let down European legislator*. Last retrieved: 26.06.2023, from https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator

Podszun, R., Bongartz, P., & Langenstein, S. (2021). The digital markets act: Moving from competition law to regulation for large gatekeepers. *Journal of European Consumer and Market Law, 10*, 60–67.

Quintais, J., Appelman, N. & Fahy, R. (2022). *Using terms and conditions to apply fundamental rights to content moderation*. Last retrieved: 29.03.2023, from https://ssrn.com/abstract=4286147

Quintais, J., de Gregorio, G. & Magalhães, J. (2023). How platforms govern users' copyright-protected content: Exploring the power of private ordering and its implications *Computer Law and Security Review, 48*, 105792, pp. 1–25.

Schweitzer, H. (2021). The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the digital markets act proposal. *Zeitschrift für Europäisches Privatrecht*, 503–544.

van Hoboken, J. (2022). *European lessons in self-experimentation: From the GDPR to European platform regulation*. Last retrieved: 23.06.2023, from https://www.cigionline.org/articles/european-lessons-in-self-experimentation-from-the-gdpr-to-european-platform-regulation/

von Ditfurth, L., & Lienemann, G. (2022). The data governance act: Promoting or restricting data intermediaries? *Competition and Regulation in Network Industries, 23*, 270–295.

Wilman, F. (2022). *The Digital Services Act (DSA) – An overview*. Last retrieved: 29.03.2023, from https://ssrn.com/abstract=4304586