*laws*

MDPI

*Article*

# A Critical Approach to Technofeudalism in EU Law: The Architecture of Big Tech's Influence

**Tamás Dezső Ziegler [1], Thomas Buijnink [2], Reiner Diederik Duvenage [3], Sarolta Szabó [4] and Gergely Gosztonyi [5,6,*]**

[1] Faculty of Social Sciences, Eötvös Loránd University (ELTE), H-1117 Budapest, Hungary; ziegler.tamas@tatk.elte.hu
[2] Doctoral School of Sociology, Eötvös Loránd University (ELTE), H-1117 Budapest, Hungary; thomasbuijnink@gmail.com
[3] Thorbecke Academy, NHL Stenden University of Applied Sciences, 8917 DD Leeuwarden, The Netherlands; reiner.duvenage@nhlstenden.com
[4] Faculty of Law, Pázmány Péter Catholic University, H-1088 Budapest, Hungary; szabo.sarolta@jak.ppke.hu
[5] Digital Authoritarianism Research Lab, Faculty of Law, Eötvös Loránd University (ELTE), H-1053 Budapest, Hungary
[6] Faculty of Law, Széchenyi István University (SZE), H-9026 Győr, Hungary
* Correspondence: gosztonyi@ajk.elte.hu or gosztonyi.gergely@sze.hu

**Abstract**

The article critically examines the emergence of technofeudalism within the European Union's legal framework, drawing on the theoretical contributions of Yanis Varoufakis, Alfred C. Yen, and Katrina Geddes. We argue that the EU's historically market-oriented regulatory architecture contributed to conditions that facilitated the rise of dominant technology companies exercising quasi-governance functions over digital environments, extracting value from users while evading meaningful democratic accountability. Our analysis distinguishes between two categories of enabling legislation: structural rules, which govern corporate status, taxation, and market consolidation; and action-oriented rules, which regulate platform behavior, algorithmic governance, consumer relations, and data protection. We demonstrate how fragmented national tax regimes, ineffective merger control, under-regulated algorithms, asymmetric consumer protections, unclear liability frameworks for online content, exploitable private international law mechanisms, and inadequately enforced data protection standards collectively reinforce Big Tech's dominance. While recent regulatory interventions such as the Digital Services Act and Digital Markets Act represent important steps, they remain embedded in a market-oriented paradigm that insufficiently addresses the broader social, cultural, and democratic implications of platform power. The article concludes by calling for a more coherent, democratically grounded approach to digital regulation—one that moves beyond fragmented, reactive policymaking toward a comprehensive framework capable of strengthening democratic accountability and public oversight within the digital sphere.

**Keywords:** technofeudalism; Digital Services Act; Digital Markets Act; Big Tech; EU single market; platform regulation; algorithmic governance; data protection; content moderation



Academic Editor: Patricia Easteal

Received: 30 April 2026
Revised: 10 June 2026
Accepted: 8 July 2026
Published: 15 July 2026



## 1. Introduction

This article offers a critical mapping of selected elements of the legal framework underlying the emergence of technofeudal tendencies within the European Union (EU). In doing so, it connects general theories on the status of major multinational technology companies (Big Tech) with actual policies and legal provisions. The analysis draws upon more general works, and especially Varoufakis's (2023) book Technofeudalism—What Killed Capitalism, published in 2023. In his analysis, he raised the problem that, as a result of the under-regulation of the internet and the strong position of tech companies, the capitalist system in the western world has become more like a modern feudal system supporting tech companies than competitive capitalism. Very similar statements have also been made by scholars like Yen (2002) and Geddes (2020), and, more recently, by Kapoor (2024).

In Varoufakis's (2023) view, this technofeudalistic system has several features. Major tech companies (like Amazon) do not pay corporate tax in Europe, even though they make great profits there. On the other hand, such companies ask for a tax-like share from sales on their platforms. These companies use free, or very cheap, labour (a modernised, twenty-first-century version of peasants). A good example of this is YouTube, where creators get a very small share of the revenue and most of them work (i.e., create videos) for free. These companies are in a monopolistic position: Amazon, Facebook, Google, Instagram and TikTok do not have competitors, or their competition is very limited. According to Varoufakis, the strong dominance of cloud capital has eliminated the competitive element in capitalism, and created monopolies which function like fiefs. If we are unsatisfied with one cloud fief (like Facebook, Instagram, or Amazon), we can only change to another, and the number of fiefs is very limited. Furthermore, many tech companies also have a very strong effect on our lives. They decide what we find when we search the web using a search engine, and also what we do not find. They set the algorithms which 'help us' in our daily lives, thereby re-shaping our needs to their companies' interests. Many of these companies know our whole life in detail, including many intimate details and metadata about us. For their services, we mostly pay with our data.

Yen (2002, p. 1225) took a similar approach in interpreting technofeudalism in his essays. In his groundbreaking 2002 article, he highlights the general environment of the internet—its architecture and system—along with the control of user data, which together foster a feudal-style dominance over users. As he stated, "some of those favouring minimal regulation take the idea of cyberspace as a separate place so seriously that traditional government cannot effectively intrude". As a consequence of the fragmentation and privatization of state power, so-called "cybermanors" and "cyberlords" have emerged. In his later article, Yen (2020, p. 141) goes even further, emphasizing the ascent of political power concentrated in the hands of these cyberlords.

What distinguishes technofeudalism from capitalism, in Varoufakis's analysis, is the shift from profit through competition to rent through monopoly. Capitalist markets presuppose rivalry among firms and meaningful consumer choice (Bilić 2024); technofeudalism, by contrast, is defined by a stark asymmetry in which billions of users—functioning as digital serfs—create content, generate data, and perform unpaid labor within platforms owned by a handful of cloud lords who capture the resulting value. Yen's framework reinforces this point: what makes the situation feudal is not merely market concentration but the privatization of governance itself, as platforms exercise quasi-sovereign authority over their domains, setting rules, controlling access, and adjudicating disputes without democratic accountability. The parallel to feudalism thus lies in both the extraction of tribute from a dependent population and the displacement of public law by private power.

Geddes (2020, p. 455) approached technofeudalism with a slightly different model, emphasising its legal dimensions. She claimed that "the unlimited power of online platforms to regulate access to user-generated content through antipiracy algorithms leads to three perverse outcomes". These outcomes are, first, that it suppresses lawful free speech. Second, it breaks the traditional foundations of copyright law. And third, the monetisation

https://doi.org/10.3390/laws15040073

of user-generated content by copyright owners exploits users, who use content under copyright protection. In our article, we follow the more holistic model of Varoufakis, but also implement some remarks from the important research of Geddes.

According to critics, the EU's historically market-oriented integration model and its preference for competition-based governance (Bugaric 2023) contributed to periods of regulatory restraint in the digital sphere, thus facilitating the expansion and consolidation of large technology companies before more interventionist forms of digital regulation emerged. The liberal rationale behind this was that "competition is the best and most effective form of regulation" (Ibáñez Colomo 2021, p. 569) and legislative interference was generally seen as more or less undesirable. This became particularly apparent in the tech sector. Added to this is the recent phenomenon of some tech companies and their executives, like Elon Musk, acting like both platform providers and politicians trying to shape policies, which could be interpreted as a sign of the extended power of tech companies and, thereby, the growth of technofeudalistic features in the international and European order (Siebold and Heine 2025).This could put renewed pressure on EU legislation when at the same time there is a US president who is mixing a political role with online business, issues a cryptocurrency the day before his inauguration (Faguy 2025), revokes the executive order of President Biden on the risks of AI (Shepardson 2025), announces Stargate, a $500 billion AI infrastructure investment, in the first days of his presidency (Jacobs 2025), interprets online free speech in a libertarian way (White House 2025), and pardons Ross Ulbricht, the founder of the dark-net platform Silk Road (Raymond 2025). The dangers of gigantic internet corporations were also recognised by Fukuyama (2023, pp. 38–39), who stressed that:

> *The internet itself was not the product of spontaneous order; its underlying technologies were created as a result of US government investment, often done through the Department of Defense, in things like semiconductors, integrated circuits, and the mandating of network protocols like TCP/IP. Once it was privatized by the US government, the internet did not remain a decentralized network, but rapidly became dominated by two or three gigantic corporations whose power could be challenged only by governments—if they could be challenged successfully at all.*

As a result of the regulatory framework in the US and Europe, companies behind messenger services, app stores and search engines have gained the power to act as extremely important gatekeepers. In the EU, institutional recognition of the opportunities and threats posed by the digital world is reflected in policies such as the EU's Digital Decade policy (European Commission 2026a), along with the European Data Strategy (European Commission 2026b). Many related concerns have been addressed in the Digital Markets Act (DMA) (2022/1925, European Parliament and Council of the European Union 2022a) and the Digital Services Act (DSA) (2022/2065, European Parliament and Council of the European Union 2022b), which subject large tech platforms to certain obligations, with financial penalties for non-compliance. For example, according to Article 6(5) DMA, a gatekeeper is no longer allowed to treat services and products offered by the gatekeeper itself more favorably in ranking than similar services or products offered by third parties on the gatekeeper's platform. Gatekeepers are also no longer allowed to prevent consumers from linking up to businesses outside their platforms. Moreover, the DMA includes regulations to ensure the transparent handling of data (Edelson et al. 2023, p. 20). On the other hand, the DSA and the DMA could also be criticised for, in essence, being the continuation of previous regulations that were biased towards market forces. This means that Big Tech companies are not just 'service providers' or 'gatekeepers' but arguably have a much deeper and more profound effect on society and culture. While, without a doubt, the DMA and the DSA include many policy innovations, it is far from certain that a fair market environment can result in fair social circumstances as well. Within such a legal framework, many issues which are not market-related, such as labour practices, a major part of content moderation, the effect of non-regulated algorithms on national culture and many aspects of privacy, might remain unaddressed.

In this article, we highlight how technofeudalism has built up in some selected fields of EU law. Our selection of topics is necessarily selective and illustrative rather than exhaustive: we focus on those fields which, in our view, most clearly demonstrate how different layers of EU law interact with the concentration of digital and platform power. As our intention is to make one of the first sketches of how technofeudalism is represented in the system of EU law, we do not give an all-round analysis in detail, but try to show the most important, policy-forming value choices behind the architecture of rules. The particular issues mentioned below can serve as cornerstones for the creation of the cloud fiefs that Varoufakis writes about. Many of them are seemingly autonomous issues which do not have anything to do with the other fields, and fragmentation is very common, even in individual fields. However, together they can form the vanguard of the protection of technological companies' interests in the EU.

We intentionally write about the role of the EU in creating technofeudalism. Internet regulation cannot be solved solely at the national level, and in most important policy issues in relation to our topic, it is the EU which has the competency to act. At this point, we do not want to give hints about how to solve these issues, as this would be the topic of another article. Our intention is to start a democratic discussion among EU lawyers, practitioners and policy makers on how we could cure the excessive power of Big Tech companies in Europe.

## 2. The Janus-Faced Legal Architecture: Structural and Action-Oriented Rules

To understand how technofeudalism has taken root in the EU, it is necessary to examine the legal architecture that has enabled it. This architecture is not the product of a single legislative choice but rather the cumulative result of decisions across multiple, often fragmented, domains of EU law. In the sections that follow, we map this terrain by distinguishing between two categories of rules. The first category comprises what we term structural rules (SRs): those governing the fundamental status and position of companies within the single market. Here, we focus on two critical areas. The first is corporate taxation, where the combination of fragmented national tax regimes, freedom of establishment, and the persistence of aggressive tax planning opportunities has allowed major technology companies to operate across Europe while contributing minimally to public revenues. The second is merger control, where the EU's existing framework has proven inadequate to address the distinctive dynamics of the digital economy—particularly the proliferation of "killer acquisitions" and the expansion of technology conglomerates into adjacent markets without triggering regulatory scrutiny.

The second category consists of action-oriented rules (AORs): those governing how companies behave within the market and, crucially, in their relationships with users. Here, the picture is one of pervasive under-regulation, over-regulation that misses its target, and regulatory fragmentation. We examine how the governance of algorithms remains largely beyond the reach of binding EU law, leaving consequential decisions about information flows and public discourse to private actors operating according to commercial logics. We analyse consumer protection, where ostensibly robust frameworks conceal significant asymmetries that permit companies to alter products unilaterally, extract free labor and data, and evade accountability for exploitative practices. We consider the evolving and uncertain rules on liability for user-generated content, which have increasingly shifted responsibility toward private adjudication by platforms and, more recently, toward individual users

https://doi.org/10.3390/laws15040073

raising concerns about chilling effects on speech and the privatization of enforcement. We address private international law, where jurisdictional rules intended to provide flexibility in cross-border disputes have instead created opportunities for forum shopping and strategic litigation that powerful actors can exploit to silence critics. And we examine data protection, where the General Data Protection Regulation (GDPR) (2016/679, European Parliament and Council of the European Union 2016) and related instruments, despite their ambitions, have generated compliance burdens that disproportionately affect smaller enterprises while failing to fundamentally disrupt the data monopolies of major platforms.

Throughout this analysis, a common thread emerges: the EU's regulatory approach has been shaped by ordoliberal assumptions that privilege market mechanisms and competition as the primary instruments of governance, while treating legislative intervention as exceptional and potentially distortive. This orientation, embedded in parts of the EU's internal market logic and reflected in decades of jurisprudence and policymaking, has in several respects created favourable structural conditions for the expansion and consolidation of large technology companies, even if more recent legislative developments indicate a partial shift toward stronger public oversight of the digital economy. The result is a legal environment in which Big Tech has been able to consolidate power, extract value, and exercise quasi-governmental authority over digital spaces, while democratic institutions have struggled to assert meaningful control. By mapping the specific legal mechanisms through which this outcome has been produced, we aim to provide the groundwork for a more coherent, democratically accountable approach to the regulation of the digital economy in Europe.

At the same time, it is important not to overstate the continuity of this approach. In recent years, the EU has increasingly moved toward a more interventionist model of digital regulation. These measures reflect a significant shift away from earlier assumptions that market competition and self-regulation alone would be sufficient to govern the digital environment. Accordingly, our argument is that many newer regulatory instruments continue to operate within a broader market-oriented constitutional and institutional framework that has historically facilitated the concentration of digital power in the hands of large technology companies.

Methodologically, the article combines doctrinal legal analysis with a critical regulatory and political-economy perspective on the digital economy. The analysis is primarily qualitative and focuses on the interaction between EU legal frameworks, platform governance, and the concentration of digital power. Rather than providing an exhaustive doctrinal account of each field discussed, the article adopts a critical legal approach that examines how different areas of EU law collectively structure, enable, or fail to counterbalance the growing influence of major technology companies. The aim is not to establish a monocausal explanation for the rise of Big Tech dominance in Europe, but to identify recurring structural and regulatory patterns that may contribute to the consolidation of platform power within the EU legal order.

## 3. Mapping the System Behind Technofeudalism: Structural Versus Action-Oriented Rules

Before giving details about the different fields of legislation, it is important to explain the existing system behind the legal environment of technofeudalism in the EU. When tracking EU laws which enable the excessive power of tech companies, we can easily highlight two distinct groups.

To the first group's aim is to help companies and maintain free competition within the EU in general. These include the foundational freedoms enshrined in the Treaty on the Functioning (TFEU) of the EU which have enabled companies to structure their operations across multiple jurisdictions in tax-efficient ways. They also encompass the EU Merger Regulation, which governs the review of concentrations between undertakings but, as we shall argue, has proven inadequate for the platform economy; directives harmonizing aspects of company law to facilitate corporate mobility; and the patchwork of anti-tax avoidance measures that, despite recent reforms, continue to leave room for aggressive tax planning by well-resourced multinational enterprises. We can call these rules structural rules (SRs): they are structural in the sense that they create the structure, that is, the legal framework of the single market, including the background to companies' actions in the EU's digital market. Structural rules do not regulate individual companies' market actions or the relationship of tech companies with each other or with their customers (i.e., B2B or B2C relationships), but they regulate the actual position and status of companies; they include the rules on taxation, company law and merger control.

To the second group belong all those regulations which set the framework for companies' actions. We can call this group action-oriented rules (AORs). Of course, even among tech companies, these rules can vary greatly, depending on the actual scope of a company's activities. For example, the laws applicable to Amazon may differ from those applicable to Facebook, Instagram, or online news sites. AORs set how companies should function in the market and, especially, in the online environment. They include a fragmented set of consumer legislation, private international law rules, provisions on content moderation and hate speech, and even copyright and trademark regulations.

Of course, these two layers can interact with each other. Consequently, it is not always easy to draw a clear line between them. For example, private international law can interact with company law, or trademarks can also have an effect on a company's status in the market. What is remarkable is that, in the EU, both of these layers (i.e., SRs and AORs) have strengthened the influence of companies. While the first group strengthened their status and income sources, the second, intentionally and sometimes even unintentionally, gave different incentives for their actions. From a legal perspective, this means that, on the one hand, we have many under-regulated areas in which companies received rights to regulate themselves. However, in a number of cases, we can also recognise over-regulation, by which we mean useless forms of seemingly strict regulations, which are unnecessarily complicated to follow in practice (like some of the rules of the GDPR).

In analysing these dynamics, it is important to distinguish between different types of regulatory shortcomings. First, under-regulation refers to situations in which substantive legal rules are absent, minimal, or insufficiently developed, thereby leaving significant discretion to private actors. Second, over-regulation refers to excessively complex, burdensome, or formalistic regulatory frameworks that may generate high compliance costs without effectively addressing underlying structural problems. Third, ineffective regulation refers to situations in which formally existing legal rules are inadequately enforced, circumvented in practice, or structurally incapable of counterbalancing the market power of large technology companies. While these categories often overlap in practice, distinguishing them helps clarify the different ways in which the European regulatory framework may contribute to the consolidation of platform power.

## 4. Structural Rules (SRs)

### *4.1. Making Tax Avoidance Possible*

A first, crucial and controversial element of the operation of Big Tech in the EU is how the European legal system makes potential tax avoidance possible. This is especially true regarding multinational companies which can afford aggressive tax planning. For example, Varoufakis (2023, p. 97) claims that in 2020, "Amazon's best year since its inception, when its pandemic-fuelled sales went through the roof, Bezos's company booked sales worth

€44 billion at its global headquarters in Ireland but paid exactly zero corporate tax because it posted not a cent of profits".

The question of the conditions under which a company can establish itself in another Member State has been raised many times before (O'Shea 2010), and creates a dilemma between freedom of establishment and illicit tax benefits. An important example of this is the textbook Daily Mail case, in which the well-known British newspaper intended to move its headquarters to the Netherlands to operate under a more favourable tax regime, while remaining subject to UK company law (Court of Justice of the European Union 1988). As is well known, the Court of Justice of the European Union (CJEU) ruled that this possibility fell outside the provisions on freedom of establishment of the Treaty establishing the European Economic Community. However, in the crucial Centros case the CJEU ruled that, under the same freedom of establishment rules, a British company could establish a branch in Denmark without meeting certain local capital requirements (Court of Justice of the European Union 1999). Very similar argumentation was later used in other tax law cases, including the Cadbury Schweppes (Court of Justice of the European Union 2006) and Lexel cases (Court of Justice of the European Union 2021b). Arguably, the CJEU's loose interpretation of company rights (i.e., an ordoliberal bias regarding the market) has opened the doors to abuse of the freedom of establishment. An overview of the cases leaves open a relevant question: when would the CJEU consider a company's settlement practices as an abuse of law? Márquez Lasso (2021, p. 401) answers this question as follows:

> *taking into account the jurisprudence of the European Court of Justice already analyzed, we understand that a concept of abuse of law in the practice of the freedom of establishment could be defined as the practice consisting in the creation of purely artificial arrangements, lacking any real economic content, that is destined solely to circumvent the tax regulation, that in normal circumstances would have been a mandatory [sic], with the sole aim of obtaining an illicit tax advantage.*

The problem from a legal practice perspective is that these 'purely artificial arrangements' were never really prohibited by EU law, thereby creating a grey zone which could be used by companies for their own advantage, and the same is true concerning the establishment of offshore companies. The countries on the EU's list of noncooperative countries represent only the tip of the iceberg, and success in eliminating this activity remains limited (European Commission 2018b). However, from the mid-2010s, the EU's corporate tax policy has shifted 'from removing tax obstacles and double taxation, towards more transparency and elimination of abusive tax practices', with the aim of increasing competitiveness and creating a level playing field for all Small and Medium Enterprises (SMEs) (Roland 2018, pp. 17–18), as SMEs often lack the financial means to carry out aggressive tax planning.

The academic literature indicates that multiple dilemmas occur when the EU attempts to counter corporate tax avoidance. Collier et al. (2018) address the Anti-Tax Avoidance Package (ATAP) (MEMO/16/2265, European Commission 2016b) that was proposed by the European Commission (EC) in 2016, which includes tax avoidance measures such as the Anti-Tax Avoidance Directive (2016/1164, Council of the European Union 2016) and Country-by-Country Reporting. While these measures do increase the EU's effectiveness, they still leave plenty of room for tax planning. Also, increasing the complexity of tax law has unintended side effects, such as raising administrative costs and dampening economic activity. Most importantly, the ATAP did not do much to remove the incentives provided by the EU's disjointed national tax systems for companies seeking to relocate their economic operations to low-tax countries. On the other hand, many of such issues were addressed in the Council Directive 2022/2523 (Council of the European Union 2022) on a global minimum tax, especially because it contains an income inclusion rule (IIR) for major global companies. While there could be pitfalls in the application of the directive (e.g., multinational enterprises may create shell entities and hybrid structures, and may shift profits to low-tax non-EU territories, for example, via digital services or intellectual property licensing), it is still an important step in a good direction.

Another tax-related issue concerning technofeudalism is that the DSA and the DMA include provisions to harmonise the market for digital companies operating in the EU by, for example, addressing the gatekeeping positions of services such as the app store and Google play. As a result, the gatekeeping function of these services (i.e., their market position) leaves creators no way to avoid paying a tribute to these companies. This leads to the paradoxical situation in which internet giants levy taxes on the work of unpaid labourers, while paying minimal tax themselves. According to some authors, the DSA and DMA provide a more constitutional approach to the digital environment in the EU, replacing the previously liberal economic approach to the single market (Papp 2024). However, this does not mean that the new e-regulation approaches would spill over to tax law. Thus, even the most recent package, Business in Europe—Framework for Business Taxation (BEFIT), does not address the elephant in the room, which is that companies can continue to make use of letterbox companies. In recent years, the EU has become more committed to a fairer internal market in which everyone pays their fair share, which could be considered a paradigm shift from its previous approach. However, the problem remains that multinational companies, including internet giants, can continue to implement aggressive tax planning if the rules on corporate tax within the EU are not harmonised. This loophole will be hard to close if treaty unanimity is required, and, unfortunately, a more holistic European corporate tax harmonisation does not, right now, seem to be a possible future scenario (Garbarino 2016, p. 277).

### *4.2. Why and How Merger Control Became Obsolete*

Another important structural issue regarding the regulation of Big Tech is that the EU's system of merger control was unable to handle tech companies' spread from one field to the next. Because of this, conglomerates like Google were created. Google owns the most used search engine (with around 81.95% of the market share globally) and the most used internet browser (Chrome, with around 68.38% of the global market share), controls most online advertisements (67.77% of the global market share), and controls YouTube, which has a market share of 97.95% in the streaming platform market. This latter website alone attracts around 25% of global mobile traffic.

In the EU, there are relatively detailed rules on competition policies, and this is also true of merger control. The background rules on mergers and company acquisitions are primarily set out in Council Regulation 139/2004 (Council of the European Union 2004), which forms part of the broader EU competition law framework established under the TFEU. The development of EU merger control cannot be reduced to a single Treaty provision, but is linked more generally to the Union's competition policy architecture, particularly the provisions governing anticompetitive agreements, abuses of dominant position, and the implementation powers of the Council and the Commission within the internal market. Moreover recently, the 2024 Commission Communication on the definition of the relevant market (European Commission 2024b) added some extra rules. From these come the general rules on abusive market dominance and the ban on cartels. However, these rules are behind the times from two major perspectives, and have many other issues (Wörsdörfer 2022, p. 349).

First of all, if a company is active in one field, and starts a new, different field of activity (as, for example, is being done by many tech companies that are moving into Artificial Intelligence (AI), while continuing their original enterprises), European regulations are not able to limit this. If this second activity also grows to the same size as the original one, the company can in this way start to control a major part of the market, without any serious external control. This can have an effect on many other issues, like predatory or below-cost pricing, killer applications, discriminatory business conduct, and immoral and illegal activities as gatekeepers.

Second, if a company acquires another company in a different field from the field of their original market share, this will not, in most cases, raise an alarm with the European authorities. An example could be the fusion, outside the tech world, of Bayer and Monsanto: a leading German pharmaceutical company has acquired a US agrochemical and agricultural biotechnology corporation. Such fusions can have numerous bad effects, and a 'simple' analysis based on their actual market share does not take these into consideration. This is especially true in the online world, where 'killer acquisitions' have become very common. This is how, for example, Amazon bought and abolished an independent online seller of books called Book Depository (which sent books worldwide free of charge). This means that the merger control standard of 'a significant impediment to effective competition' is a relatively low standard, and is unable to operate in practice. As Gautier and Maitry (2024, pp. 246, 259) put it:

> *The five largest firms by market capitalization, Alphabet (Google), Amazon, Apple, Meta (Facebook), and Microsoft, sometimes referred to as the 'big techs' or the 'GAFAM', have massively acquired companies during the last decades, mainly but not exclusively young tech startups. To give an idea, we identify 329 acquisitions by these five companies for the period 2015–2021, which that [sic] is an average of 47 per year. . .*
>
> *. . .We have shown that acquirer massively discontinue the products of the companies they buy. If product discontinuation in itself is not a concern, products fail or are becoming obsolete, the importance of the phenomenon is raising concerns. Building on previous studies, this paper has the ambition to provide more information on the phenomenon. Our analysis shows products of younger firms are more likely to be discontinued. This result does not come as a surprise as a younger firm is less likely to have a well-established brand name and a large customer base. We also show that Apple has a more systematic discontinuation policy than the other big techs. And, regarding killer discontinuation, we observe that they occur mainly in the 'main' segment, where the acquirer holds a stronger market position.*

Thus, killer acquisitions can have a devastating effect on start-ups as well (Kızılay 2024, p. 273) and, thereby, strictly limit competition. We are not saying here that the EU, or, to be more precise, the Commission, did not try to counterbalance the tech companies' power. Many cases prove such efforts, like the case against Intel for anticompetitive practices, which was later overturned (Rankin 2024). One could also mention the case against Microsoft for abuse of market dominance (Court of Justice of the European Union 2007). Several cases were started against Google, because it supposedly manipulated the online advertisement market (European Commission 2017) (in this latter case, the fine was also later revoked (Gerken 2024)) regarding its Android system (European Commission 2018a), and also concerning the functioning of Adsense (Court of Justice of the European Union 2024). A similar case against Apple also raised the problem of abusive app store rules (European Commission 2024a, 2024b), and we could mention many other cases, all of which were based on the existing acquis on free competition. However, under the present rules (and this also true of the provisions of the DMA and the DSA), only extremely 'abusive or anticompetitive practices' can be sanctioned, and there is no analysis of how the position and activity of these companies distort the market even if they are not engaged in abusive or anti-competitive practices in the strict sense of the EU regulations.

https://doi.org/10.3390/laws15040073

## 5. Action-Oriented Rules (AORs)

### *5.1. Under-Regulated Algorithms*

It is probable that at the core of European technofeudal rules lies the problem that, in Europe, binding substantive rules governing algorithmic transparency, recommendation systems, and platform-driven visibility remain comparatively limited and, with some exceptions, this area functions more or less on libertarian (or, at least, ordoliberal) principles. To illustrate, Google's search ranking methodology, YouTube's recommendation engine, Facebook's news feed curation, TikTok's content amplification system, and Amazon's product placement algorithms all operate without legally mandated transparency requirements or substantive public oversight, effectively allowing these companies to shape information flows, consumer behavior, and public discourse according to proprietary commercial logics. By algorithms we mean different types of modus operandi. The term covers the functioning of search engines like Google Search and Yahoo Search and the results these engines show us. It also covers what tech companies show us in our feeds on Facebook or YouTube, and how advertising is organised on the internet. While we find some minor, less important, rules in the EU applying to algorithms, they are the exceptions: in most cases, companies have the right to decide what they show us and how they do it. Our argument is not that Member States or the EU have formally surrendered sovereignty over culture in a legal sense. Rather, the issue concerns the growing private control exercised by major digital platforms over the infrastructures through which culture, information, and public discourse are distributed and consumed. In this context, the problem is closely connected to questions of media pluralism, democratic public discourse, algorithmic visibility, and platform governance. Recommendation systems, search rankings, advertising architectures, and content moderation policies increasingly shape which cultural products, political opinions, news items, and social narratives become visible or marginalised in the digital sphere. The concern, therefore, is that the practical capacity of democratic institutions to influence the communicative environment of national societies has weakened, while private platforms exercising commercially driven forms of algorithmic governance have become central intermediaries of cultural and political life. We agree with Ghosh (2019, p. 76) who notes, regarding Facebook, that:

> *it is not the poor practical implementation of content monetisation that is the cause of the problems, but the very model in which these giant tech companies operate; a model in which they do not distribute content but sell advertising space, and in which content is actually less important. It relies on complex algorithms and the most comprehensive collection of personal data in order to personalise these ads as much as possible and as automatically as possible for its millions of users. As a result, users "are subjected to whatever content the platform believes will maximize profits".*

From a legislative perspective, the great problem with the under-regulation of algorithms is that right now, as Dipayan Ghosh also explained, their primary goal is to serve market interests: they shape and re-shape users without there being social control of what they want to teach to the people. To a certain degree, this creates a situation in which traditional democratic mechanisms for safeguarding media pluralism and structuring public communication become less effective in the digital environment, while major platforms retain broad discretion over the organisation and visibility of online content. The fact that Elon Musk apparently raised the visibility of his posts on X is not just a problem about X or Elon Musk: it shows that we do not have standards for how these websites should function. A very similar issue is raised by Facebook, for which Meta has abolished fact-checking. This shows that private platforms increasingly make decisions with substantial societal and democratic consequences, despite the absence of detailed and democratically legitimised public standards governing many aspects of algorithmic visibility, content prioritisation, and moderation practices. The EU wanted to solve this problem through the 2022 Code of Practice on Disinformation, which is obligatory only to signatories. Comment 31 in the document (European Commission 2022) says that "Relevant Signatories commit to integrate, showcase, or otherwise consistently use fact-checkers' work in their platforms' services, processes, and contents; with full coverage of all Member States and languages". However, this is optional: states may refuse to fulfil their commitment even after they have signed the code of practice, as it does not function like a legally binding, 'proper' legal source with direct effect. According to Article 8 of the DSA there is no general obligation to monitor the information transmitted or stored by providers of intermediary services, and there is no obligation to actively seek out facts or circumstances indicating illegal activity (Lendvai et al. 2025). As a result of this, democratic public discussion on e-regulations is more or less missing, or stuck at a very limited stage. It is also clear that the online Americanisation of the European public may lead to very similar issues to those arising in the US (Shapero 2024). The fact that regulatory approaches to algorithms are mostly stuck on the risks of the profiling of users (Kandov 2024) blocks a more holistic approach, which would ask for transparency regarding the overall content and elements of different types of algorithms.

Furthermore, it is up to these companies to recognise 'systemic risks' (see Articles 34 and 35 DSA), which is applauded by some commentators (Leijten 2026). However, it is rather naïve to ask companies to draw attention to the risks of their own activities, or the risks their platforms raise for society. To a certain degree, it is as if we are asking them to make the rules themselves, and then to apply these rules. In this way, we are adding state jobs to their list of duties, a responsibility far from the original idea of a democratically functioning free market. Companies will never be able to take into account the fact that kids today read less and are prone to depression or to consider whether or not this has something to do with algorithms and the online 'culture' (Twenge 2024). It should be up to the legislator and the public to decide. Furthermore, we do not even explicitly tell companies the basics of all this: what content they should remove, and why (or, in reverse, what content they may not remove). Exceptions, of course, exist, but they only prove the rule. Even detailed online hate speech regulation is hidden behind a code of conduct, instead of hard law (European Commission 2016a; Council of the European Union 2008).

The failure of under-regulation is not just visible in general changes in the cultures of Member States, like the weak results of PISA tests (Colombatto 2024), or students' inability to read and comprehend more complex materials (Shen 2025). It was also visible after the 2024 Romanian elections, when the European Commission started proceedings against TikTok, investigating whether the company had violated the DSA 'by failing to tackle systemic risks'. This investigation was the third against TikTok in a year (European Commission 2024c, 2024d, 2024e). However, it is very clear that the Commission is asking for things the EU should regulate in a more detailed and nuanced way: analysing risks and trying to counter them in the political sphere is the job not of a company, but of the legislator. Whatever Tik Tok did, it is not too different from other platforms: for example, the Hungarian government became the biggest advertiser on Google in the EU (Metodieva 2026). While there are some new EU rules on the transparency of such advertisements, they will probably not change the ecosystem of online advertisements in a more systemic way (Lendvai et al. 2024). This means that, on the one hand, we are delegating state power to companies, and, on the other, we are making the legal landscape uncertain for companies themselves, because we are not explaining what we expect from them in a democratic and open way.

https://doi.org/10.3390/laws15040073

*5.2. Consumer Protection and Malicious Actions of Companies*

Another aspect of technofeudalism is the way in which tech companies have been given the power to extend their decisions on their functioning. How this works can best be explained through the state of consumer law in the EU.

Originally, the online protection of consumers was an extensively, and relatively effectively, regulated area. The Directive on Unfair Clauses in Consumer Contracts (Council of the European Union 1993), together with the Directive on Consumers' Rights (2011/83/EU, European Parliament and Council of the European Union 2011), the Directive on Unfair Commercial Practices (2005/29/EC, European Parliament and Council of the European Union 2005) and the E-Commerce Directive (2000/31/EC, European Parliament and Council of the European Union 2000), gave extended protection to consumers. According to Article 9 of the Directive on Consumers' Rights, consumers in the online space have a right to withdraw from contracts during a 14-day 'cooling off' period. Companies' responsibilities were also regulated (when and how they must repair or change a product, or give the purchase price back to the consumer). On the other hand, after a while some fissures in this good-looking, albeit heavily fragmented, system became visible. As a result, structural asymmetries (Helberger et al. 2021) helping the companies became more apparent.

One of these issues is that companies retain significant discretion to alter or discontinue digital products and services after they have entered the market. However, the legal situation in the EU is more nuanced than a complete absence of regulation. Directive (EU) 2019/770 (European Parliament and Council of the European Union 2019a) on contracts for the supply of digital content and digital services imposes conformity requirements and obliges traders to provide updates, including security updates, that are necessary to keep digital content and services in conformity for the period that consumers may reasonably expect. Similar obligations also arise under Directive (EU) 2019/771 (European Parliament and Council of the European Union 2019b) regarding goods with digital elements. More recently, the Cyber Resilience Act (2024/2847, European Parliament and Council of the European Union 2024b) introduced lifecycle-oriented cybersecurity obligations for products with digital elements, including vulnerability handling and security update requirements.

Nevertheless, these instruments do not fully eliminate the structural asymmetries between consumers and major technology companies. The applicable obligations remain fragmented across different categories of products and services, often focus primarily on cybersecurity and technical conformity rather than long-term functional continuity, and may be difficult for consumers to enforce in practice. In many situations, companies still retain broad discretion to modify platform features, alter business models, rebalance in-game economies, discontinue compatibility, or terminate support after a limited period. This is especially visible in the gaming market, where

> *free-to-play video games bring the majority of the annual revenue to the video game companies, as players are attracted with possibility of playing without paying for the software, but during the game players are seduced with purchases of virtual items with functional (for example, virtual weapon) and without functional assistance (for example, so-called 'skin') to the game.* (Demchenko 2019, p. 194)

If the strategy of the company in such a case is to get the players hooked on the game for half a year and then change the settings (for example, strong characters, who were bought for hundreds of Euros in the game, become weak), there is no remedy. As in the case of other software, withdrawal will not help the consumer, and even if the money spent on the game is given back, the time and effort spent in the game will not be taken into consideration. In such situations, the regulatory framework still leaves companies substantial unilateral discretion over the evolution, modification, and practical lifespan of digital products and platform-based ecosystems.

Finally, even if this is never mentioned in traditional EU or domestic consumer law, we must highlight that consumers very often engage in problematic asymmetric relationships with companies. Varoufakis mentions the problem of free labour on platforms like YouTube: most users receive no compensation for the videos they upload to the platform (and Facebook is even worse, with billions of photos being uploaded without any compensation being given). Moreover, both Varoufakis (2023) and Yen (2002, p. 1251) mention the free transfer of data from consumers to tech companies (for example, on platforms like Facebook or Google). Geddes (2020, p. 477) gives a slightly different meaning to what she calls the 'exploitation of user labour': she adds that copyright owners can take all the revenue of a video, if, for example, a copyrighted song can be heard over the video content. In respect of all three of these aspects of 'exploitation', we can claim that when a private person engages in a consumer relationship with a major platform, they sign a consumer contract, but the free labour and data transfer aspect is handled as if it is a more or less insignificant aspect of this relationship (except for very big channels on YouTube which generate very high user traffic). However, according to conventional wisdom, these consumer contracts could be interpreted as 'manifestly unbalanced (disproportionate) contracts'. As Yen (2002, p. 1256) puts it,

> *the Feudal Society metaphor merely tells us that the present routine acceptance of such provisions is probably unwarranted. In order to curb potentially exploitative methods, courts should therefore seriously consider scrutinizing the provisions of adhesion contracts in cyberspace more closely than they have in the past*.

However, unlike Yen, we do not believe it would necessarily be the courts' role to defend citizens, as this is the role of the legislator, at either the EU or the domestic level.

### *5.3. Liability for Online Comments*

Today's democratic societies are based on a balance between the freedom of the individual and the protection of society. Of course, states have broader discretionary powers concerning crime prevention and enforcement when, for example, user comments are offensive. The three major types of regulatory regime in the world have different approaches to both freedom of expression and the regulatory issues that build on it. US regulation, building on the First Amendment, has contributed to the global expansion and market dominance of large US technology companies (Bradford 2023); the EU's attempts, based on a belief in freedoms and the democratic functioning of the media, have moved from directives to regulations (Monti 2024, pp. 6–9); and Asian-style regulation has sought to convert a belief in the omnipotence of the state and online sovereignty into regulation (Balendra 2024). This also means that, even if there are differences between the US and EU approaches, in most of the western world companies became the primary adjudicators of what content may remain or should be removed from their social media or video platforms, and they also set the most important standards for analysis.

This raises the related legal liability issue of whether, and to what extent, the intermediary service provider, typically the one providing the hosting, is liable and whether the traditional content provider, who created the content about which the comments are made, is liable. In addition to the companies' responsibility, it is, of course, also worth considering the liability of the author of the original comment. Zeno-Zencovich (2014, p. 113) summarises these different liabilities as non-liability, personal liability, and vicarious, third-person liability. It should be pointed out that, while general monitoring seems to be the appropriate way to avoid liability in Australia, this method has been prohibited all along in Europe, under Article 15 of the E-Commerce Directive. Although this prohibition on monitoring remains in Article 8 of DSA, the European supranational judicial fora have already taken subtle steps towards a shift and a clarification (Court of Justice of the European Union 2019). In addition to legal solutions, technical tools (such as word-based, content-based and collaborative filters) can be helpful tools for moderating content (Sorbán 2021). Equally, the position of trusted flaggers under the Article 22 of DSA or the possibility of giving comments a positive (upvote) or negative (downvote) rating, introduced on Reddit in 2020, seems to be an essential step towards enhancing such methods without unacceptable interference in free speech (Peters 2021).

While a unification of European jurisprudence may be unrealistic, the European Court of Human Rights (ECtHR) plays a crucial role in developing a more coherent European approach. The ECtHR has taken a consistent legal position on the subject under consideration, apart from a few minor variations. Therefore, to determine whether content has been lawfully removed or whether there are censorship effects, the following factors need to be examined:

(a) *when it can be declared that the provider has actual knowledge;*
(b) *what is clearly illegal content;*
(c) *what is the timeframe within which the service provider must act; and*
(d) *whether we are talking about an active or passive type of service provider when analysing liability issues* (Oster 2017, pp. 141–42).

In this context, the ECtHR has established a strict liability test, which requires an examination of (A) the context and content of the comments, (B) the possibility of holding the actual author or authors of the comments liable, (C) the measures taken by the service provider to prevent or remove the comments in question, (D) the consequences of the national judgment for the service provider, (E) the conduct of the victim, and (F) the consequences of the comments for the victim (European Court of Human Rights 2015). In addition to this, the ECtHR has, in other decisions, underlined that different types of procedures would be required for different types of content, explicitly highlighting the distinction between content that reaches or falls below the level of hate speech (European Court of Human Rights 2016).

For a long time, it seemed that the ECtHR only imposed liability for comments on large commercial and professionally run portals (European Court of Human Rights 2019, para. 166), but in the Sanchez case of 2023, the ECtHR seems to have chosen a different path: it seems that certain individuals may also be subject to continuous monitoring (European Court of Human Rights 2023). It can be argued that the 2023 decision expands the range of people and entities that need to worry about being held liable as an internet intermediary (Korpisaari 2022). This will indeed have a chilling effect (Gosztonyi and Lendvai 2026), bringing us one step further in the growing digital authoritarianism worldwide (Moldovan 2024; Fuchs 2026). This means that, while we do not have detailed, unified EU rules with direct effect on the problem of when companies may or may not remove comments (i.e., on how to maintain free speech in the EU), the ECtHR precedents will still affect EU law in the future too, and not necessarily in a positive way. Thus, we can see a shift here from company liability to the liability of private persons.

### *5.4. EU Private International Law*

Cases involving cross-border defamation are politically and culturally sensitive, and the internet has multiplied their frequency, complexity, and intensity (Svantesson and Symeonides 2023). The root of the legal tension lies in the fact that different countries place different degrees of emphasis on freedom of expression and access to information on the one hand, and the protection of private life and personal reputation on the other. Libel tourism essentially represents a form of forum shopping, in which a prospective plaintiff files their lawsuit in the jurisdiction where they believe they are most likely to receive a favourable judgment. In essence, jurisdictional rules pave the way for this (Nielsen

2013). The EU's regulations in this regard—unlike conflict of law rules—have been unified by the Brussels Ia Regulation. Previously, under Article 5(3) of the Brussels Convention, then Article 5(3) of the Brussels I Regulation, and currently Article 7(2) of the Brussels Ia Regulation (1215/2012, European Parliament and Council of the European Union 2012), proceedings for tort or delict may be brought before the courts of the Member State 'where the harmful event occurred or may occur' (forum loci delicti). In the Shevill case (Court of Justice of the European Union 1995), a cross-border defamation lawsuit against the printed press, the CJEU interpreted the concept of the 'place where the harmful event occurred' for the first time. According to the judgment, this term refers both to the place where the damage occurred (*forum loci damni infecti*) and to the place of the event which gives rise to the harm (*forum loci delicti commissi*) (Court of Justice of the European Union 1976). Under the Shevill doctrine, the CJEU ruled that the claimant may bring an action for damages against the publisher before the courts of the place where the publisher of the defamatory publication is established, which has jurisdiction to award damages for all the harm caused by the defamation. Alternatively, the claimant could sue in each Member State where the publication was distributed and where they suffered harm. However, these courts can only rule on the harm caused within their own Member State. This approach is known as the mosaic principle (*Mosaikbetrachtung*).

Nearly twenty years later, the issue of online defamation arose in the eDate and Martinez cases. When personality rights are allegedly infringed by content published on a website, what does the 'place where the harmful event occurred' mean? Content published on a website is ubiquitous, as it can be accessed anywhere and instantly downloaded by an indeterminate number of internet users worldwide, regardless of the publisher's intent. As a result, the Court of Justice of the EU (CJEU) 'adjusted' the Shevill precedent by allowing the injured party to bring a claim for compensation for the entirety of the harm caused before the courts of the Member State where the claimant's centre of interests (*Mittelpunkt der Interessen*) is located. The centre of interests is typically the natural person's habitual residence. However, in exceptional circumstances, the centre of interests may be in a Member State where the claimant does not habitually reside, provided other factors—such as the exercise of professional activities—indicate particularly close connections with that state. Additionally, the CJEU upheld the mosaic principle (Court of Justice of the European Union 2011, paras. 46, 48, 51–52).

The 'borderless' nature of online media is difficult to reconcile with jurisdictional rules that are tied to state boundaries. When the centre of interests coincides with the claimant's habitual residence, a forum actoris is created, which enhances the protection of the claimant (Gonçalves 2022) but also broadens the opportunities for forum shopping. Consequently, some argue that the centre of the claimant's interests is not an appropriate solution (Nagy 2012). Instead, they propose either retaining the mosaic principle (but supplementing it with additional conditions) or introducing entirely different jurisdictional criteria (Mankowski 2016). Furthermore, some legal scholars have criticised the continued application of the mosaic principle to the internet (Kyselovská 2019).

The issue of the reputation of legal persons in the Bolagsupplysningen case introduced a new dimension. The CJEU determined that the centre of a legal entity's interests is not tied to its registered office but instead is the location where it conducts its business activities. The centre of interest for such a legal person, therefore, refers to the place where the company's business reputation is most firmly established and where it carries out the main part of its economic activities, and the courts of this Member State have jurisdiction to assess the entire damage (Court of Justice of the European Union 2017, paras. 43–44) This means that the CJEU maintained the mosaic approach, and therefore that the claimant may bring his action before the courts of each Member State in whose territory online content is or has been available. These courts have jurisdiction only in respect of the harm caused in the territory of their particular Member State. The CJEU also clarified that correcting false statements and removing harmful comments cannot be geographically divided (Court of Justice of the European Union 2021a). Therefore, such actions can only be requested before the courts of the Member State that has jurisdiction over the entirety of the harm caused.

The analysis of the CJEU's decisions makes it clear that, as regards cross-border online infringements of personality rights, 'the place where the harmful event occurred' under Article 7(2) of the Brussels Ia Regulation can be interpreted as the centre of interests of the injured party. In line with the eDate case, this is primarily the habitual residence for a natural person. According to the Bolagsupplysningen judgment, it is mainly where a legal entity carries out the main part of its economic activities. The Bolagsupplysningen and Gtflix TV cases (Marongiu Buonaiuti 2022) reinforced the position that requests for rectification and deletion must be filed exclusively with the forum competent to award full compensation. However, maintaining the mosaic principle is questionable, as it does not align with the realities of the online environment in its current form. This raises several issues. Is the jurisdictional multiplicity provided by the mosaic principle compatible with the objectives of the Brussels Ia Regulation? Are plaintiffs genuinely interested in pursuing lawsuits before different national courts? Does this approach facilitate compensation claims, considering the lack of uniformity in conflict of law rules based that there is no EU regulation on the applicable law issue (see Article 1(2)(g) of the Rome II Regulation (864/2007, European Parliament and Council of the European Union 2007))? Some analysts argue that applying the mosaic principle threatens the proper functioning of the judiciary, the predictability of jurisdictional rules, and the consistent adjudication of claims arising from the same situation (Kohler 2021). In cases of the online violation of personality rights, it is technically challenging to allocate damages across multiple countries and assess the extent of damage within a given territory (Gonçalves 2022, p. 138). Does the mosaic principle primarily encourage vexatious litigation strategies? In its current form, does it essentially pave the way for SLAPP (Strategic Lawsuits Against Public Participation) proceedings according to SLAPP Directive (2024/1069, European Parliament and Council of the European Union 2024a)? SLAPP lawsuits are often clearly unfounded or abusive cross-border civil actions initiated against individuals or legal entities, particularly journalists and human rights defenders (Bogrea 2024).

The mosaic principle was originally intended to provide flexibility in cross-border legal disputes, particularly for victims of defamation. However, in the digital age, where harm can be claimed in multiple jurisdictions, it can become a weaponised litigation strategy. Large corporations and powerful individuals can file lawsuits in jurisdictions that are more favourable to their claims (forum shopping), or expensive and slow for defendants to fight cases in, and it is hard to coordinate legal defences across multiple cases, making it easier to pressurise critics into settlement or self-censorship. While tech companies typically avoid direct lawsuits against individuals, they can support or indirectly facilitate SLAPP-like actions by, for example, funding third party litigation against critics, using defamation or data protection rules to justify legal actions that ultimately restrict public discourse, or applying selective content moderation policies.

### *5.5. Data Protection Lost in the System*

From the perspective of Yen (2020) and Varoufakis (2023), if Big Tech companies are to maintain their market position, their monopolisation of the essential digital resource of data is required. In this way, the exclusive control over data by tech companies can be compared to the control exercised over land by landowners in feudal times. Data is indispensable, as it powers the algorithms that determine the content users see, and subsequently influences their decision-making processes in all digitalised areas of life. The control of this data grants tech giants substantial political and economic clout, while allowing them to establish total market dominance in the digital world. An erosion of the privacy and autonomy of users also occurs through the gathering of data, which often occurs unbeknownst to users. These factors lead to an asymmetric power balance between individuals and tech giants, as data (and therefore power) is controlled by the latter (Varoufakis 2023). In the context of the EU, such monopolisation of data poses a threat to the EU's democratic and civic principles, as users have virtually no stake in how their data is being used to generate market dominance by unaccountable cloud fiefs.

On the specific subject of data protection, the EU's regulatory response centres around the GDPR, which is applicable since 2018. The GDPR was designed to unify data protection regulation across the Member States and to enhance the protection of individuals' personal data, whether processed inside or outside the EU. It sets out principles for the processing of data, including fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Rights are also granted to individuals over their personal data, including rights relating to access, rectification, erasure (the right to be forgotten), restricting of processing, data portability, and objections to processing. In order to monitor and enforce compliance, the GDPR mandated the establishment of independent supervisory bodies in all Member States. At the same time, critics have argued that the GDPR illustrates certain features of ineffective regulation: although the framework is formally extensive and compliance-intensive, enforcement asymmetries, uneven institutional capacities among supervisory authorities, and the structural dominance of large platforms have limited its transformative impact on the concentration of data power in the digital economy. Moreover, the GDPR sets out remedies for individuals whose rights have been infringed, and corporate penalties for companies that do not comply with its provisions. This regulation has been bolstered by the European Data Act (2023/2854, European Parliament and Council of the European Union 2023), which is applicable since 2025. It pertains to a broad range of entities conducting business in the EU and sets out wide-ranging data access, sharing, transparency and transfer obligations and requirements. It is also important to connect the transparency rules to the DSA's obligations (Veleva 2024, pp. 155–56). However, as it also applies to non-personal data, it extends even beyond the protection of personal data provided by the GDPR. As a result, entities providing services in which data is collected will have to fulfil the requirements of both the GDPR and the Data Act. Regarding the European Data Act, it is interesting to see that the application of the GDPR has not been without consequence. Fines resulting from GDPR breaches reached a record high in 2023 of €2.055 billion, rising from €841.5 million in 2022 and €1278.4 million in 2021. This trend shows a marked increase from the total fines of €171.6 million in 2020 and €71.8 million in 2019. Most notably, a €1.2 billion fine was imposed on Meta by the Irish Data Protection Commission just two years ago (Armstrong 2024).

Still, there are several challenges related to the EU's regulatory efforts on data protection that align with the central tenets of Varoufakis' theory of technofeudalism. First, a study published in 2023 suggests that small businesses are at a disadvantage compared to large businesses when it comes to GDPR compliance (Data Protection Commission 2023). Second, neither the extensive rules of the GDPR nor those of the Data Act answer the question of what happens in cases when consumers willingly allow companies to store their super-sensitive data, which also raises a moral and legislative dilemma. Third, many of the rules of the GDPR are not enforced in practice. Those who want to bulk delete Facebook posts, or download and erase their data (photos, posts, or videos) from the platform know how difficult it can be to regain control over their personal data, and it is even more complicated in the Google system.

https://doi.org/10.3390/laws15040073

Sunstein (2021), in his book Sludge, describes techniques used by the state and companies to influence users, clients and citizens. For example, it is often complicated to unsubscribe from a newsletter, or to get the necessary document to apply for social aid at state offices. Sunstein's solution to this is to streamline compliance requirements, eliminate redundant regulations and simplify procedures. We see that sludge is extensively used by Big Tech, and this has a strong effect on data protection. First, the state creates sludge through extensive regulations and, second, the companies make sludge to maintain their control over data. We also see that, despite the ever-increasing threat of sanctions, tech giants are able to absorb short-term losses from sanctions because they can still generate long-term gains from the expansion of their total market dominance (Maynor 2025).

## 6. Conclusions—Overcoming Turbulent Fragmentation in the EU's Digital Realm

The structural and action-oriented rules examined in the previous sections demonstrate how under-regulation, over-regulation, and ineffective enforcement may coexist within the EU's fragmented digital regulatory framework. Mapping the different fields of technofeudalism in the EU is extremely important, because these fields are strongly dependent on each other, and actions started in one field can have devastating effects in other areas. On the other hand, the turbulent and growing fragmentation of EU internet legislation is a great barrier in most scholarly analysis (Kelemen 2026). The literature mostly focuses on individual areas, because even then the regulation is overwhelmingly complex. As there is a desire in the EU to regulate the online space (to a certain degree: the aim is to Europeanise and democratise it), it is possible that this phenomenon will become even stronger in the future. As a result, legal fragmentation will also create a need for a holistic understanding of regulation, which can later serve as the basis of policing. However, any complex method must also take into consideration other factors, apart from balancing the excess power of tech companies through legal means, like maintaining or enhancing European competitiveness and enforcing human rights (in the field of free speech regulation, for example). This means that a very rigid regulatory framework can also have negative effects on certain fields, and can backfire.

The analysis undertaken in this article suggests that the emergence of technofeudal tendencies within the EU legal order cannot be attributed to a single legislative failure or policy choice. Rather, it results from the cumulative interaction of multiple legal fields that, taken together, have enabled the concentration of digital and platform power. The structural rules examined in this article have facilitated the economic expansion, market consolidation, and cross-sectoral growth of major technology companies within the single market. At the same time, the action-oriented rules analysed above reveal a fragmented regulatory landscape in which algorithmic governance, platform visibility, consumer relations, online liability, jurisdictional mechanisms, and data protection are often regulated inconsistently, incompletely, or with limited practical effectiveness. While recent EU instruments demonstrate a significant move toward stronger public oversight of the digital sphere, the overall regulatory architecture still struggles to counterbalance the structural asymmetries and quasi-governance functions exercised by dominant digital platforms.

In this article we wanted to do the first groundwork in a democratic discussion on Big Tech companies. Developing such a public discussion is important, as it is the Member States' and the EU's job to regulate Big Tech companies, and if we want to build effective regulations which do not cause harm, we should first set the goals and make the connections clear. Without this, the EU will always lag behind the social reality of the internet, and its actions will only focus on addressing the latest threats in the online space and not on finding the major sources and implications of these threats, from a broader perspective. If

https://doi.org/10.3390/laws15040073

we can talk about technofeudalism; then, we can also talk about techno-democratisation. It is for the Member States and the EU to decide whether they will create a more transparent and democratic internet for the future, or put the power of regulation in the hands of Big Tech companies. Future regulatory debates should therefore focus not only on market efficiency and innovation, but also on the institutional conditions necessary to preserve democratic accountability, media pluralism, meaningful consumer autonomy, and effective public oversight within the digital environment.

**Author Contributions:** Conceptualization, T.D.Z. and G.G.; Methodology, T.D.Z., T.B., R.D.D., S.S. and G.G.; Investigation, T.D.Z., T.B., R.D.D., S.S. and G.G.; Writing—original draft, T.D.Z., T.B., R.D.D., S.S. and G.G.; Writing—review & editing, T.D.Z., T.B., R.D.D., S.S. and G.G.; Supervision, G.G.; Project administration, T.D.Z. and G.G.; Funding acquisition, G.G. All authors have read and agreed to the published version of the manuscript.

**Funding:** The article was supported by the ADVANCED_24 funding scheme of the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

Armstrong, Mark. 2024. EU Data Protection Fines. *Statista*, January 8. Available online: https://www.statista.com/chart/30053/gdpr-data-protection-fines-timeline/ (accessed on 28 April 2026).

Balendra, Soorya. 2024. *Free Speech in the Puzzle of Content Regulation*. Cham: Springer.

Bilić, Paško. 2024. Platforms and the critique of political economy. *Etkileşim* 13: 12–26. [CrossRef]

Bogrea, Ștefan. 2024. The European Union's Proposal for a SLAPPs Directive. *Analele Universității din București—Seria Drept/Forum Juridic* 1: 147–60. [CrossRef]

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. Oxford: Oxford University Press.

Bugaric, Bojan. 2023. The Neo-Liberal Bias of the EU Constitutional Order: A Critical Analysis. In *Research Handbook on the Politics of Constitutional Law*. Edited by Mark Tushnet and Dimitry Kochenov. Cheltenham: Edward Elgar.

Collier, Richard, Seppo Kari, Olli Ropponen, Martin Simmler, and Maximilian Todtenhaupt. 2018. *Dissecting the EU's Recent Anti-Tax Avoidance Measures: Merits and Problems*. EconPol Policy Report No. 08. Munich: ifo Institute. Available online: https://www.ifo.de/DocDL/EconPol_Policy_Report_08_2018.pdf (accessed on 28 April 2026).

Colombatto, Enrico. 2024. PISA Results: Poor Education Is No Recipe for Economic Brilliance. *GIS Reports*, February 22. Available online: https://www.gisreportsonline.com/r/worsening-2022-pisa-tests-results-oecd/ (accessed on 28 April 2026).

Council of the European Union. 1993. Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts. *Official Journal of the European Union* L 95: 29–34.

Council of the European Union. 2004. Regulation (EC) No 139/2004 of 20 January 2004 on the Control of Concentrations between Undertakings (EC Merger Regulation). *Official Journal of the European Union* L 24: 1–22.

Council of the European Union. 2008. Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law. *Official Journal of the European Union* L 328: 55–58.

Council of the European Union. 2016. Directive (EU) 2016/1164 of 12 July 2016 Laying Down Rules against Tax Avoidance Practices That Directly Affect the Functioning of the Internal Market. *Official Journal of the European Union* L 193: 1–14.

Council of the European Union. 2022. Directive (EU) 2022/2523 of 14 December 2022 on Ensuring a Global Minimum Level of Taxation for Multinational Enterprise Groups and Large-Scale Domestic Groups. *Official Journal of the European Union* L 328: 1–5.

Court of Justice of the European Union. 1976. Case 21/76, Bier v Mines de Potasse d'Alsace. Judgment. ECLI:EU:C:1976:16. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61976CJ0021 (accessed on 6 July 2026).

Court of Justice of the European Union. 1988. Case 81/87, the Queen v H.M. Treasury and Commissioners of Inland Revenue, ex Parte Daily Mail and General Trust plc. Judgment. ECLI:EU:C:1988:456. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61987CJ0081 (accessed on 6 July 2026).

Court of Justice of the European Union. 1995. Case C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd. v Presse Alliance SA. Judgment. ECLI:EU:C:1995:61. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61993CJ0068 (accessed on 6 July 2026).

Court of Justice of the European Union. 1999. Case C-212/97, Centros Ltd. v Erhvervs- og Selskabsstyrelsen. Judgment. ECLI:EU:C:1999:126. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61997CJ0212 (accessed on 6 July 2026).

Court of Justice of the European Union. 2006. Case C-196/04, Cadbury Schweppes plc and Cadbury Schweppes Overseas Ltd. v Commissioners of Inland Revenue. Judgment. ECLI:EU:C:2006:544. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62004CJ0196 (accessed on 6 July 2026).

Court of Justice of the European Union. 2007. Case T-201/04, Microsoft Corp. v Commission of the European Communities. Judgment. ECLI:EU:T:2007:289. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62004TJ0201 (accessed on 6 July 2026).

Court of Justice of the European Union. 2011. Joined Cases C-509/09 and C-161/10, eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Ltd. Judgment. ECLI:EU:C:2011:685. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62009CJ0509 (accessed on 6 July 2026).

Court of Justice of the European Union. 2017. Case C-194/16, Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB. Judgment. ECLI:EU:C:2017:766. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0194 (accessed on 6 July 2026).

Court of Justice of the European Union. 2019. Case C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Ltd. Judgment. ECLI:EU:C:2019:821. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0018 (accessed on 6 July 2026).

Court of Justice of the European Union. 2021a. Case C-251/20, Gtflix TV v DR. Judgment. ECLI:EU:C:2021:1036. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0251 (accessed on 6 July 2026).

Court of Justice of the European Union. 2021b. Case C-484/19, Lexel AB v Skatteverket. Judgment. ECLI:EU:C:2021:34. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0484 (accessed on 6 July 2026).

Court of Justice of the European Union. 2024. Case T-334/19, Google LLC and Alphabet Inc. v European Commission. Judgment. ECLI:EU:T:2024:634. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019TJ0334 (accessed on 6 July 2026).

Data Protection Commission. 2023. Decision Pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 GDPR. May 12. Available online: https://www.edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf (accessed on 28 April 2026).

Demchenko, Olena. 2019. Electronic Commerce in Gaming Industry: European Perspective on the Legal Regulation of In-Game Virtual Transactions. In *EU Business Law and Digital Revolution*. Edited by Judit Glavanits, Balázs Horváthy and Lilla Knapp. Győr: Széchenyi István University.

Edelson, Laura, Inge Graef, and Filippo Lancieri. 2023. Access to Data and Algorithms: For an Effective DMA and DSA Implementation. *Centre on Regulation in Europe*. March 16. Available online: https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsa-implementation (accessed on 28 April 2026).

European Commission. 2016a. EU Code of Conduct on Countering Illegal Hate Speech. Available online: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (accessed on 28 April 2026).

European Commission. 2016b. MEMO/16/2265. Available online: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2265 (accessed on 8 April 2024).

European Commission. 2017. Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service. June 27. Available online: https://ec.europa.eu/commission/presscorner/detail/en/memo_17_1785 (accessed on 28 April 2026).

European Commission. 2018a. Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine. *Press Release*. July 18. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_18_4581 (accessed on 28 April 2026).

European Commission. 2018b. Communication from the Commission on New Requirements against Tax Avoidance in EU Legislation Governing Financing and Investment Operations. C(2018) 1756 Final. Available online: https://taxation-customs.ec.europa.eu/system/files/2018-05/i_communication_financing_investment_2018_1756_en.pdf (accessed on 6 July 2026).

European Commission. 2022. The 2022 Code of Practice on Disinformation. Available online: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (accessed on 28 April 2026).

European Commission. 2024a. Commission Fines Apple over €1.8 Billion over Abusive App Store Rules for Music Streaming Providers. *Press Release*. March 4. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161 (accessed on 28 April 2026).

European Commission. 2024b. Commission Notice on the Definition of the Relevant Market for the Purposes of Union Competition Law. C/2023/6789. *Official Journal of the European Union* C 1645: 1–48.

European Commission. 2024c. Commission Opens Formal Proceedings Against TikTok on Election Risks Under the Digital Services Act. Press Release IP/24/6487. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487 (accessed on 28 April 2026).

European Commission. 2024d. Commission Opens Formal Proceedings Against TikTok Under the Digital Services Act. Press Release IP/24/926. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926 (accessed on 28 April 2026).

European Commission. 2024e. Commission Opens Proceedings Against TikTok Under the DSA Regarding TikTok Lite. Press Release IP/24/2227. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227 (accessed on 28 April 2026).

European Commission. 2026a. Europe's Digital Decade. Available online: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade (accessed on 28 April 2026).

European Commission. 2026b. European Data Strategy. Available online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed on 28 April 2026).

European Court of Human Rights. 2015. Delfi AS v Estonia, Application No. 64569/09. Judgment of June 16. Available online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]} (accessed on 6 July 2026).

European Court of Human Rights. 2016. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt. v Hungary, Application No. 22947/13. Judgment of February 2. Available online: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160314%22]} (accessed on 6 July 2026).

European Court of Human Rights. 2019. Høiness v Norway, Application No. 43624/14. Judgment of March 19. Available online: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-191740%22]} (accessed on 6 July 2026).

European Court of Human Rights. 2023. Sanchez v France, Application No. 45581/15. Judgment of May 15. Available online: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-224928%22]} (accessed on 6 July 2026).

European Parliament, and Council of the European Union. 2000. Directive 2000/31/EC of 8 June 2000 on Electronic Commerce. *Official Journal of the European Union* L 178: 1–16.

European Parliament, and Council of the European Union. 2005. Directive 2005/29/EC of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices. *Official Journal of the European Union* L 149: 22–39.

European Parliament, and Council of the European Union. 2007. Regulation (EC) No 864/2007 on the Law Applicable to Non-Contractual Obligations (Rome II). *Official Journal of the European Union* L 199: 40–49.

European Parliament, and Council of the European Union. 2011. Directive 2011/83/EU of 25 October 2011 on Consumer Rights. *Official Journal of the European Union* L 304: 64–88.

European Parliament, and Council of the European Union. 2012. Regulation (EU) No 1215/2012 of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Recast). *Official Journal of the European Union* L 351: 1–32. [CrossRef]

European Parliament, and Council of the European Union. 2016. Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation). *Official Journal of the European Union* L 119: 1–88.

European Parliament, and Council of the European Union. 2019a. Directive (EU) 2019/770 of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services. *Official Journal of the European Union* L 136: 1–27. [CrossRef]

European Parliament, and Council of the European Union. 2019b. Directive (EU) 2019/771 of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and Repealing Directive 1999/44/EC. *Official Journal of the European Union* L 136: 28–50.

European Parliament, and Council of the European Union. 2022a. Regulation (EU) 2022/1925 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). *Official Journal of the European Union* L 265: 1–66.

European Parliament, and Council of the European Union. 2022b. Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union* L 277: 1–102.

European Parliament, and Council of the European Union. 2023. Regulation (EU) 2023/2854 on Harmonised Rules on Fair Access to and Use of Data (Data Act). *Official Journal of the European Union* L 2854: 1–71.

European Parliament, and Council of the European Union. 2024a. Directive (EU) 2024/1069 on Protecting Persons Who Engage in Public Participation from Manifestly Unfounded Claims (SLAPP Directive). *Official Journal of the European Union* L 1069: 1–20.

European Parliament, and Council of the European Union. 2024b. Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. Available online: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (accessed on 28 April 2026).

Faguy, Ana. 2025. Trump Launches Cryptocurrency with Price Rocketing. *BBC News*, January 19. Available online: https://www.bbc.com/news/articles/c9vmym2jvy9o (accessed on 28 April 2026).

Fuchs, Christian. 2026. Digital Fascism and Digital Capitalism. *tripleC: Communication Capitalism & Critique* 1: 90–140. [CrossRef]

Fukuyama, Francis. 2023. *Liberalism and Its Discontents*. London: Profile Books.

Garbarino, Carlo. 2016. Harmonization and Coordination of Corporate Taxes in the European Union. *EC Tax Review* 25: 277–88. [CrossRef]

Gautier, Axel, and Robert Maitry. 2024. Big Tech Acquisitions and Product Discontinuation. *Journal of Competition Law & Economics* 20: 246–59. [CrossRef]

Geddes, Katrina. 2020. How Digital Platforms Sustain Technofeudalism. *Columbia Journal of Law & the Arts* 43: 455–80.

Gerken, Tom. 2024. Google Scores Rare Legal Win as 1.49bn Euro Fine Scrapped. *BBC News*, September 18. Available online: https://www.bbc.com/news/articles/c62rjd363j1o (accessed on 28 April 2026).

Ghosh, Dipayan. 2019. Facebook's Oversight Board Is Not Enough. *Harvard Business Review*, October 16. Available online: https://hbr.org/2019/10/facebooks-oversight-board-is-not-enough/ (accessed on 28 April 2026).

Gonçalves, Anabela Susana de Sousa. 2022. International Jurisdiction in Cross-Border Infringement of Personality Rights in the European Union. *Masaryk University Journal of Law and Technology* 16: 133–60. [CrossRef]

Gosztonyi, Gergely, and Gergely Ferenc Lendvai, eds. 2026. So, What Is Chilling Effect? (Re)Conceptualizing the Phenomenon of Chilling Effect in the Context of Legal Doctrine and Social Perception. In *Legal and Ethical Issues of Chilling Effect*. Cham: Springer, pp. 1–17. [CrossRef]

Helberger, Natali, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marija Sax, and Joanna Strycharz. 2021. *EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets*. Brussels: BEUC. Available online: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf (accessed on 28 April 2026).

Ibáñez Colomo, Pablo. 2021. The Draft Digital Markets Act: A Legal and Institutional Analysis. *Journal of European Competition Law & Practice* 12: 561–75. [CrossRef]

Jacobs, Jennifer. 2025. Trump Announces up to $500 Billion in Private Sector AI Infrastructure Investment. *CBS News*, January 22. Available online: https://www.cbsnews.com/news/trump-announces-private-sector-ai-infrastructure-investment/ (accessed on 28 April 2026).

Kandov, Boris. 2024. Regulatory Approaches for Algorithms on Online Platforms in the Digital Services Act. *ELTE Law Journal* 2: 131–50. [CrossRef]

Kapoor, Ilan. 2024. Musk's Rise Is Symptomatic of Our Neo-Feudal Capitalist Times. *Al Jazeera*, December 26. Available online: https://www.aljazeera.com/opinions/2024/12/26/musks-rise-is-symptomatic-of-our-neo-feudal-capitalist-times (accessed on 28 April 2026).

Kelemen, Roland. 2026. The Cyberfare State: Divergent Models of Digital Governance and Control. *Frontiers in Political Science* 8: 1748562. [CrossRef]

Kızılay, Ahmet Selim. 2024. Lack of Effective Control on Killer Acquisitions in the Big Tech Market under EU Framework: Rethinking EUMR Rules. *Public and Private International Law Bulletin* 44: 273–300. [CrossRef]

Kohler, Christian. 2021. Dismantling the Mosaic Principle. *IPRax* 5: 428–35.

Korpisaari, Päivi. 2022. From Delfi to Sanchez—When Can an Online Communication Platform Be Responsible for Third-Party Comments? An Analysis of the Practice of the ECtHR and Some Reflections on the Digital Services Act. *Journal of Media Law* 14: 352–77. [CrossRef]

Kyselovská, Teresa. 2019. Critical Analysis of the Mosaic Principle. *Prague Monitor of European Law* 1: 39–60.

Leijten, Eline. 2026. An Empirical Critique of the DSA Transparency Database: Mapping Shortcomings and Levers for Improvement. *SSRN*. [CrossRef]

Lendvai, Gergely Ferenc, János Tamás Papp, and Tamás Attila Szikora. 2024. Overview of EU Legislation on Political Campaigning in the Light of the European Court of Human Rights Case Law. *Lawyer Quarterly* 14: 328–42. [CrossRef]

Lendvai, Gergely Ferenc, János Tamás Papp, Tamás Szikora, and Krzysztof Wasilewski. 2025. Can Disinformation Be Regulated? A Comprehensive Overview of the European Union's Pertaining Initiatives. *Central European Journal of Communication* 18: 410–26. [CrossRef] [PubMed]

Mankowski, Peter. 2016. Article 7. In *European Commentaries on Private International Law*. Edited by Ulrich Magnus and Peter Mankowski. Cologne: Verlag Dr. Otto Schmidt, vol. I.

Marongiu Buonaiuti, Fabrizio. 2022. Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet. *European Papers* 7: 360–80.

Maynor, John. 2025. Flood the Zone with Shit: Algorithmic Domination in the Modern Republic. *Social Sciences* 6: 391. [CrossRef]

Márquez Lasso, Daniel E. 2021. The Concept of Abuse in Tax Matters within European Union Law. *Cuadernos de Derecho Transnacional* 13: 362–402. [CrossRef]

Metodieva, Asya. 2026. Digital Sovereignty Contested: Hungary's Strategic Use of EU Platform Regulations. *Journal of Contemporary European Studies* 34: 348–65. [CrossRef]

Moldovan, Carmen. 2024. Mirror, Mirror on the Wall, Who's the Most Authoritative of Them All? Cyber Sovereignty from a Critical Perspective. *ELTE Law Journal* 2: 41–59. [CrossRef]

Monti, Matteo. 2024. *The Unity of Opposites in the Regulation of Social Media Platforms: Content Moderation Between the EU Digital Services Act and the US First Amendment Theories*. European University Institute Law Working Papers No. 7. Fiesole: European University Institute. [CrossRef]

Nagy, Csongor István. 2012. The Word Is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU Law. *Journal of Private International Law* 8: 275–300. [CrossRef]

Nielsen, Peter Arnt. 2013. Libel Tourism: English and EU Private International Law. *Journal of Private International Law* 9: 270–96. [CrossRef]

O'Shea, Tom. 2010. Tax Avoidance and Abuse of EU Law. *EC Tax Journal* 11: 11–33.

Oster, Jan. 2017. *European and International Media Law*. Cambridge: Cambridge University Press.

Papp, János Tamás. 2024. Moving Forward: Charting the Much-Needed Evolution of the Digital Services Act. *Hungarian Yearbook of International Law and European Law* 12: 457–76. [CrossRef]

Peters, Jay. 2021. Reddit Is Adding New Real-Time Features, Including a Live Upvote Count. *The Verge*, December 1. Available online: https://www.theverge.com/2021/12/1/22810850/reddit-real-time-live-upvote-reading-typing-indicator-comment (accessed on 27 May 2024).

Rankin, Jennifer. 2024. Intel Wins Lengthy EU Legal Battle over £880m Competition Fine. *The Guardian*, October 24. Available online: https://www.theguardian.com/technology/2024/oct/24/intel-legal-battle-against-eu-880m-fine-competition (accessed on 28 April 2026).

Raymond, Nate. 2025. Trump Pardons Silk Road Founder Ross Ulbricht for Online Drug Scheme. *Reuters*, January 22. Available online: https://www.reuters.com/world/us/trump-pardons-silk-road-founder-ulbricht-online-drug-scheme-2025-01-22/ (accessed on 28 April 2026).

Roland, Aanor. 2018. *European Corporate Tax Policy Since the Crisis: How the EU Steps Up the Fight Against Corporate Tax Avoidance*. Universität Bielefeld Working Paper No. 3. Bielefeld: Universität Bielefeld.

Shapero, Julia. 2024. Nikki Haley Rips Ramaswamy: 'Nothing Wrong' with American Culture. *The Hill*, December 26. Available online: https://thehill.com/policy/technology/5057033-nikki-haley-rips-ramaswamy-nothing-wrong-with-american-culture/ (accessed on 28 April 2026).

Shen, Yamin. 2025. Distractions in Digital Reading: A Meta-Analysis of Attentional Interference Effects. *Frontiers in Psychology* 16: 1671214. [CrossRef] [PubMed]

Shepardson, David. 2025. Trump Revokes Biden Executive Order on Addressing AI Risks. *Reuters*, January 21. Available online: https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/ (accessed on 28 April 2026).

Siebold, Sabine, and Friederike Heine. 2025. German Ambassador Warns of Trump Plan to Redefine Constitutional Order. *Reuters*, January 19. Available online: https://www.reuters.com/world/us/german-ambassador-warns-trump-plan-redefine-constitutional-order-document-shows-2025-01-18/ (accessed on 28 April 2026).

Sorbán, Kinga. 2021. Ethical and Legal Implications of Using AI-Powered Recommendation Systems in Streaming Services. *Információs Társadalom* 21: 65–67. [CrossRef]

Sunstein, Cass R. 2021. *Sludge: What Stops Us from Getting Things Done and What to Do About It*. Cambridge, MA: MIT Press.

Svantesson, Dan Jerker B., and Symeon C. Symeonides. 2023. Cross-Border Internet Defamation Conflicts and What to Do about Them: Two Proposals. *Journal of Private International Law* 19: 137–65. [CrossRef]

Twenge, Jean M. 2024. Are Books Dead? Why Gen Z Doesn't Read. *Generation Tech*, March 5. Available online: https://www.generationtechblog.com/p/are-books-dead-why-gen-z-doesnt-read (accessed on 28 April 2026).

Varoufakis, Yanis. 2023. *Technofeudalism: What Killed Capitalism*. London: The Bodley Head.

Veleva, Simona. 2024. Digital Services Act: Anticipating Challenges in Regulatory Implementation. *ELTE Law Journal* 2: 143–59. [CrossRef]

White House. 2025. Executive Order 14149: Restoring Freedom of Speech and Ending Federal Censorship. January 20. Available online: https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/ (accessed on 28 April 2026).

Wörsdörfer, Manuel. 2022. What Happened to 'Big Tech' and Antitrust? And How to Fix Them. *Philosophy of Management* 21: 345–69. [CrossRef]

Yen, Alfred C. 2002. Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace. *Berkeley Technology Law Journal* 17: 1207–58. [CrossRef]

Yen, Alfred C. 2020. Revisiting the Western Frontier. *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 60: 134–68.

Zeno-Zencovich, Vincenzo. 2014. Anonymous Speech on the Internet. In *Media Freedom and Regulation in the New Media World*. Edited by András Koltay. Alphen aan den Rijn: Wolters Kluwer.