

Risks and Resilience in the European Union's Regulation of Online Platforms and Artificial Intelligence: Hungary in Digital Europe



Kitti Mezei and Anikó Träger

Abstract The European Union is taking ambitious steps to strengthen regulation in the digital space as part of the Digital Agenda for Europe. As part of this, the digital services regulatory package (Digital Services Act and Digital Markets Act) has been adopted to define the responsibilities of digital platforms, control online content, protect users' fundamental rights and promote competitiveness in the online space. In addition, an EU regulatory framework for artificial intelligence has been developed (AI Act), which supports a risk-based approach to regulate the technology. One common intersection of these regulations is to maintain transparency. The Digital Services Act aims to fight against filter bubbles and disinformation in social media, where online platforms also use algorithms to provide services. A new challenge in adapting to the accelerating technological development has been the COVID-19 pandemic, which has further increased the penetration of online service providers through mandatory distance and opened up a whole new platform for spreading fake news. The application of the new Digital Europe Regulations raises several questions. Still, these are complemented by application-specific areas for Hungary, such as how Hungarian authorities will act as national authorities or interpret 'illegal content' under the European legislation.

The publication was prepared in the framework of the Hungarian Academy of Sciences' high-risk grant for research on post-COVID phenomena and supported by the European Union project RRF-2.3.1-21-2022-00004 within the framework of the Artificial Intelligence National Laboratory and by the Ministry of Innovation and Technology NRDI Office within the framework of the FK-21 Young Researcher Excellence Program (138965).

K. Mezei (✉) · A. Träger

Institute for Legal Studies, HUN-REN Centre for Social Sciences, Budapest, Hungary

Department of Business Law, Faculty of Economic and Social Sciences, Budapest University of Technology and Economics, Budapest, Hungary

e-mail: mezei.kitti@tk.hun-ren.hu; trager.aniko@tk.hun-ren.hu

© The Author(s) 2025

F. Gárdos-Orosz (ed.), *The Resilience of the Hungarian Legal System since 2010*, European Union and its Neighbours in a Globalized World 16,

https://doi.org/10.1007/978-3-031-70451-2_9

1 Introduction: Digital Europe, Hungary in Digital Europe

Technological progress, giant companies in the digital world and artificial intelligence (AI) are part of our everyday lives; regulating them requires a complex solution from legislators. Digital markets are very different from traditional markets, and so are the regulatory and competition solutions that can be applied to them. Social media service platforms have become the most prominent players of mass communication in expressing opinion. Furthermore, new technologies are emerging, using AI and developing increasingly sophisticated tools and hardware. The EU is responding to the challenges of technology and the digital world by adopting harmonised rules in the areas concerned in the context of the Digital Europe¹ regulatory plan. Given that the European Union (EU) has a dedicated objective of uniform regulation, this directly affects Hungary. As will be presented in detail in this study, EU legislators have opted for proactive regulation in digitalisation and technology. Therefore, these regulations are key parts of the Hungarian regulation and directly apply to the issues they cover which will transform the Hungarian legal system.

The concept of regulation puts European values and people at the centre (human-centred approach). One phase has already taken place between 2010 and 2020. The Decision (EU) 2022/2481 of the European Parliament and of the Council establishing the Digital Decade 2030 Policy Programme (Decision 2022/2481/EU) for the current decade states that the EU should ‘address strategic weaknesses and high-risk dependencies that could lead to supply shortages or cybersecurity risks and promote digital transformation’.² In addition, the resolution also highlights data sharing issues and the protection of personal data in relation to new technologies.³

Specifically on the implementation of the governments, Decision 2022/2481/EU states that ‘Harmonious, inclusive and steady progress towards the digital transformation and towards the achievement of the digital targets in the Union requires a comprehensive, robust, reliable, flexible and transparent form of governance, on the basis of close cooperation and coordination between the European Parliament, the Council, the Commission and the Member States.’⁴

In addition, Decision 2022/2481/EU states that ‘[t]o that end, the Commission should cooperate closely with stakeholders including civil society and private and public actors, such as bodies governed by public laws of the education and training or health sectors, and should consult them about measures to accelerate the digital transformation at Union level’.⁵

¹European Council: A digital future for Europe, <https://bitly.ws/3cARX>; Digital Agenda for Europe, <https://bitly.ws/3cASe>.

²Decision 2022/2481/EU, preamble (5).

³Decision 2022/2481/EU, preamble (16).

⁴Decision 2022/2481/EU, preamble (22).

⁵Decision 2022/2481/EU, preamble (39).

Among the objectives more narrowly related to digital ecosystems, Art. 3 of Decision 2022/2481/EU highlights general objectives which include human-centredness, safety and the use of sustainable ecosystems.⁶

While regulation is usually the first thing we think of in the digital world, it is important to note that Digital Europe does not aim to stifle innovation. It explicitly aims to make businesses use cloud computing, big data, and AI. It just wants to make these technologies more transparent and secure through regulation.

Moreover, the EU has already shown its ability to influence global dynamics, an approach that experts call the *Brussels effect*; it refers to the EU's unilateral power to regulate global matters.⁷ The EU is increasingly aware of its ability to influence policy on digital technologies in other parts of the world, since most new technology and digital services companies are based in the United States or China.⁸

In the Digital Single Market Strategy context, the Commission has issued a Communication stressing the need to ensure that online platforms 'protect core values' and increase 'transparency and fairness to maintain user confidence and protect innovation'. This is due to the role of online platforms in providing social access to information and content and their consequent impact on users' fundamental rights. The Commission stressed that this role comes with wider responsibilities.

It is beyond the scope of this paper to review all the regulations that have been or are being adopted in the framework of the Digital Europe Regulatory Plan. Thus, we will specifically examine regulations which are the most relevant in Hungary's social life and democracy, related to the operational characteristics of digital ecosystems and platforms, with a particular focus on the phenomenon of their increased importance in our daily lives during and after the COVID-19 pandemic, becoming more dominant in the orientation of Hungarian society, in information gathering or even in trapping us in an 'opinion bubble'.⁹

2 Characteristics of Digital Ecosystems and Online Platforms

Digital markets and social networking sites have evolved enormously over the last 20 years, growing from almost nothing to becoming today's dominant players. In commerce, eBay started to take off in the early 2000s, when online shopping was still a speciality. An example of a social media service is Facebook, which was launched in 2004, initially mainly for the leisure activities of the younger generation. From the 2010s onwards, the platforms began to take off and became part of our

⁶Decision 2022/2481/EU, preamble Art. 4(1)(3)(a) and (c).

⁷See Bradford (2020).

⁸De Gregorio (2022a).

⁹Challenges in freedom of information see Bán-Forgács and Szatmári (2023); Bán-Forgács (2023a).

everyday lives.¹⁰ Since then, they have become one of the leading platforms for accessing information. They have proved to be a tool for influencing public opinion, including specific events such as elections.¹¹ The 2020 coronavirus pandemic compounded the rise of online services, as people turned to them more and more. The pandemic created a specific economic situation which benefited some firms and industries, including those dealing in technology, while adversely affecting others. In the final year of the crisis, people and businesses showed an even greater demand for what the tech giants had to offer. Moreover, with the end of the epidemic and the end of restrictions, people recognised the convenience of online services.¹² In addition, there has been no let-up in the spread of misinformation and conspiracy theories, as other events (e.g., Russia's invasion of Ukraine) and issues have been highlighted, and social media has played a significant role in spreading information.¹³

Digital marketplaces have also become dominant as an advertising platform, with a significant number of users visiting these sites continuously. Moreover, their operating model can pre-order or target ads according to users' previous activity. In addition, online platforms have created new professions and occupations, such as influencers, content producers, and even employees managing social media for their explicit employer.¹⁴

With a large number of users and the content they share and upload on online platforms, they can gain a market advantage by processing, exploiting and even selling the vast amount of data¹⁵ that is changing quickly and widely. In addition to the areas already described, the development and use of AI has also accelerated significantly in the 2020s, and its application is also present in digital markets, both in content moderation and in the use of recommendation systems and data analysis.

3 Digital Ecosystems

Firms and state institutions that choose a digital ecosystem-based operating model seek to maximise the benefits of the digital space and digital markets described in the previous paragraph. There is currently no single definition of a digital ecosystem, however, which makes it difficult to define. The term can be traced back to the concept of an ecosystem, as used in biology, which describes the coordinated, interdependent functioning of a system involving all participants. In these areas, the digital ecosystem differs from traditional business models. The digital ecosystem

¹⁰Zódi (2022), p. 66.

¹¹For more on this, see Miró-Llinares and Aguerri (2021); Grinberg et al. (2019).

¹²Affinito et al. (2020), p. 2; Revati Devaki and Dinesh Babu (2021).

¹³Hou et al. (2023), p. 22.

¹⁴For more, see Goanta and Ranchordas (2020).

¹⁵Favaretto et al. (2020), p. 2.

takes advantage of this interaction and builds on the large number of actors and assets involved simultaneously, taking advantage of the network-like structure of this system.¹⁶

The benefits of digital ecosystem-based operations are also demonstrated by the fact that many prominent players in the global economy (e.g., Amazon and Meta-Facebook) have chosen and are currently using this operating model. The operation of these companies and their increasing penetration of digital markets has prompted the EU to develop an effective regulatory model to reduce the vulnerability of users and consumers, mitigate the risks they face and maintain the competitive opportunities of smaller companies. Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA), and Regulation (EU) No 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Market Act, DMA) are the objective of the Regulations.

Issues related to the Internet, technological innovations and, in particular, the vast networks of the digital ecosystem are almost always transnational. To this end, the EU is laying the foundations for regulation, with a view to a uniform approach in its own territory. In our view, the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the repeal of Regulation (EC) No. 95/46/EC (General Data Protection Regulation, GDPR),¹⁷ which is still in force, are already linked to the regulatory background of this problem, which was also based on the realisation that, in particular, companies operating on the international Internet platform process the personal data of vast numbers of users in a way that is difficult to monitor, and also that they can make significant profits of different kinds—which can even have policy-related relevance—in the digital markets by exploiting them directly or indirectly.

4 Key EU Rules Affecting the Operation of Digital Ecosystems and Online Platforms

However, with the rapid development of technology and the increasing use of new technologies, other areas of regulation have come to the fore where the EU has opted for uniform regulation. One step in this direction has been the adoption of the DSA-DMA Regulations, which are currently in the process of entering into force

¹⁶Barykin et al. (2020), p. 1.

¹⁷For GDPR challenges in COVID-19 see Bán-Forgács and Mezei (2023); Bán-Forgács (2023b).

and starting to be applied.¹⁸ In our view, the regulation of AI (AI Act), which also seeks to keep pace with the latest technological changes, can also be linked to this,¹⁹ as companies regularly use AI-based systems in the exploitation of the digital ecosystem and the use of large amounts of data, in the categorisation of individual data.

Although at first glance, one might say that we are talking about different areas of regulation, if you are operating in the online marketplace or using—or planning to use—a digital ecosystem-based operation, all of the above regulations will almost certainly set the framework for your legitimate operations. With this in mind, it is necessary to look at these regulations in context, particularly the regulatory solutions they seek to implement for these service providers.

This approach is supported by the fact that it has already been identified that digital markets have specificities that are difficult to address in a single legal field and that the EU has finally moved towards a coordinated regulatory approach in several areas.²⁰

We can identify a number of similarities in the wording and regulatory solutions of the regulations, which clearly show that they target the same market players and opt for similar measures:

In addition to the provisions focusing on the specificities of the sub-area, each of the regulations clearly responds to the specific nature of digital markets, i.e. each regulation approaches the scope in a way that extends it to all service providers providing services in the EU²¹ and does not link it to the location of the company, thus ensuring that operators outside the EU are obliged to comply with the provisions and that regulations cannot be circumvented by those established in third countries (extraterritorial scope).

Another element common to the regulations' regulatory approach is that they are largely adapted to the size and economic role of the market operator. In some cases, the regulation itself is explicitly based on the role of the market, such as the classification as a gatekeeper²² or the categorisation of service providers in the

¹⁸The DMA entered into force on 1 November 2022 and applied from 2 May 2023. The DSA entered into force on 16 November 2022 and was directly applicable in the EU until 17 February 2024.

¹⁹The AI Act (Regulation of the European Parliament and of the Council—Laying down harmonised rules on artificial intelligence—Artificial Intelligence Act) and amending certain union legislative acts Brussels, 21.4.2021 COM(2021) 206 final 2021/0106(COD) came into effect on August 1, 2024. EU member states must designate the relevant national authorities responsible for overseeing AI systems and conducting market supervision by August 2, 2025. Most of the regulation's provisions will apply starting August 2, 2026. However, bans on AI systems deemed to pose unacceptable risks will be enforced after six months, and provisions related to general-purpose AI models will become applicable 12 months after the regulation's entry into force.

²⁰Pünkösty (2022), p. 175.

²¹DSA Art. 2(1), DMA Art. 2(2), GDPR Art. 3(1), AI Act Art. 2(1).

²²DMA Art. 3.

DSA,²³ but an absolutely common element in the regulations is that the fines are not set at a fixed amount, but are based on the turnover of the infringer.

Risk reduction is also one of the reasons for adopting the regulations and is reflected in the specific rules. In the AI Act, we find an explicitly risk-based approach to the rules to be followed in the application and development of AI.²⁴

Closely related to the foregoing, the regulations aim to protect users and consumers, to reduce the vulnerability of users to giant companies and possibly the lack of information (information asymmetry) and to ensure adequate data protection in this context.²⁵ Although it could be seen as a measure to reduce consumer vulnerability, all regulations pay great attention to the need for operators in the digital market to operate as transparently as possible, to have documented activities and thus to be verifiable.

5 Risk-Based Regulation

A 'risk society',²⁶ as the term is used today, is a society in which risk as a factor plays a dominant role in legal regulation. In the context of technology, this means that the law responds only to the extent necessary to reduce the risks associated with technology and ultimately creates a framework that seeks to strike an appropriate and proportionate balance between different scenarios. Risk in this context means the combination of the probability that a particular harm will occur due to the use of a particular technology and the severity of that harm.

The COVID-19 pandemic has also highlighted the barriers that regulation can pose to response needs if it is inconsistent with a risk-based approach and the regulatory framework is not flexible enough.

Risk-based regulation in Europe was originally developed in response to the risks posed by new technologies and industries to the environment, human health, and safety, and only later extended to other sectors. Since launching the Digital Single Market Strategy, the EU has increasingly relied on this legislative approach to manage digital technologies and has taken a more prominent role in regulating digital markets and society. This is particularly evident in recent legislative efforts in the areas of data, online content and AI.

In examining these regulations, the DSA is also taking a risk-based approach, particularly in the new rules on content moderation practices. In particular, the DSA

²³DSA Art. 33. The Digital Services Act—Ensuring a safe and accountable online environment, <https://bitly.ws/3cASW>.

²⁴Titles 2–3 of the AI Act.

²⁵In the recitals of the regulations referred to, we find recurrent provisions aimed at protecting users, ensuring the protection of fundamental rights, transparency and risk reduction. See also van de Waerdt (2020); Helberger et al. (2021).

²⁶Beck (1992).

defines several categories of service providers according to their role in the digital ecosystem (hosting providers; intermediary service providers and online platforms; and very large online platforms and very large online search engines). Each category is subject to different due diligence obligations in ascending order. The DSA is based on the following simple yet important assumption: the larger an online platform, the greater its impact and, therefore, the greater the risk it poses to users and society. By taking an *asymmetric by-design* approach to ensure a transparent and safe online environment, DSA can be easily identified as a risk-based regulation.²⁷ It is worth noting that the DSA has adopted a size-based criterion instead of an explicit risk-based model, as is the case with the AI Act. In this respect, although the size of the platform may impact the level of risk exposure, it has less influence on other relevant variables in the risk assessment, i.e. the likelihood and severity of adverse consequences. However, the specificities and common characteristics of platforms may justify this size-based approach. This is because platform size is a proxy for risk levels in a network impact-focused context, which may not be true in other domains, such as AI, where AI systems can be applied in various ways.²⁸

However, in contrast to the GDPR, which, following a bottom-up approach, places the onus of risk assessment and mitigation entirely on the controller and/or processor, the DSA significantly reduces the discretion of the recipients of the regulation (in this case, the intermediary service provider) by defining four general risk layers. The DSA does not provide a generic definition of systemic risk, a term best known in regulating financial markets and financial institutions, but instead introduces a novel contextual application of systemic risk primarily by listing three specific systemic risks. These are the dissemination of illegal content, negative impacts on certain fundamental rights (privacy, freedom of expression, non-discrimination and children's rights) and the deliberate manipulation of services. These measures may include the application of content moderation and advertising display schemes or require them to operate under codes of conduct and crisis management protocols. The last few years have provided a number of concrete examples, such as the Facebook-Cambridge Analytica scandal or the use of social media to spread COVID-19-related fake news.²⁹

In the context of risks, it is also necessary to mention the new regulation on AI, which does not set compliance requirements specifically for online platforms but for AI systems in general and their developers.³⁰ At the heart of this regulation is the risk-based approach referred to above, which means that each AI system will be classified into more or less stringent compliance groups according to the risk it poses to users and their fundamental rights, as perceived by the legislator. The shift from a bottom-up to a top-down model in the AI Act is even more evident. As with the DSA, the AI Act sets out four categories of risk that apply to AI systems. The AI Act

²⁷ Efroni (2021).

²⁸ Mantelero (2022).

²⁹ Efroni (2021); Barata et al. (2021).

³⁰ Art. 2(1) of the AI Act.

addresses systemic risks, though its definition is not identical with the DSA, despite similarities. According to Article 3, point 65 of the AI Act, systemic risk refers to the risks associated with the high-impact capabilities of general-purpose AI models. These risks, due to the widespread use of the models or their potential negative impact on public health, safety, public security, fundamental rights, or society as a whole, could significantly affect the EU market and spread extensively across the value chain. Models are considered to have “high-impact capabilities” if the cumulative computational power used to train them exceeds 10^{25} floating-point operations. However, the AI Act only specifies that high-impact capabilities are those that meet or exceed those found in the most advanced general-purpose AI models. This encompasses most models currently available on the market, including OpenAI's GPT-4 and possibly Google's Gemini, which may be regarded as models with systemic risk. Additionally, the AI Act clarifies that AI systems embedded in very large online platforms or search engines fall under the DSA's risk management framework. If AI models meet the DSA's systemic risk obligations, it is presumed that they also comply with the AI Act, unless significant systemic risks arise that the DSA does not cover.

Despite their differences, both pieces of legislation have common features. Together, they mark a new phase in the EU's digital policy history. In particular, these laws illustrate the EU's evolving approach to *digital constitutionalism*.³¹ Both Regulations are based on the organisational principle of risk and seek to balance the economic focus on innovation and the creation of an internationally competitive digital single market with an interest in protecting democratic values, including individual rights and freedoms. Balancing different interests and values through the risk strategy is inherently constitutional. It reflects a shift in the approach of the EU institutions (from the Court of Justice onwards) to digital technologies.³² Furthermore, both the AI Act and the DSA algorithm impose auditing obligations to ensure compliance and transparency. In addition, both pieces of legislation pay particular attention to the risks arising from the design, operation and use of digital services or AI systems, taking into account their adverse effects on fundamental rights, and adopt an ex-ante strategy based on risk assessment, following a common approach to the protection of human rights. The AI Act requires a separate human rights impact assessment to be carried out for high-risk AI systems and should be an integral part of the impact assessment for DSA too.³³

³¹ See De Gregorio (2022b).

³² De Gregorio and Dunn (2023).

³³ Nagy (2023).

6 Digital Ecosystems and the Use of AI and Algorithms

It is worth mentioning the challenges of applying AI on platforms, as this technology is being integrated into the operation of more and more services, among which the first are the recommendation systems and content management algorithms of the platforms mentioned above. Another key area where platforms use algorithms at a systemic level is in the area of content moderation.³⁴ In the case of moderation, the service provider acts with some means to restrict users' fundamental rights (e.g. freedom of expression) or even their dignity (e.g. suspension of a content provider's account, exclusion of monetisation of their content). In Art. 20(6), the DSA refers to the internal complaints handling system, stating that this activity cannot be carried out solely by algorithms but requires the supervision of a qualified person. Apart from this, there is no specific provision for algorithms for content moderation and complaint handling; the regulation refers to referral systems.

In addition, one specific area of application of online platforms and algorithms that has recently received much attention is the problem of fake news. A detailed analysis of the concept and approaches to fake news is beyond the scope of this paper, but in summary, fake news can be referred to as 'a type of online disinformation (1) that (2) consists of misleading and/or false claims that may or may not be related to real events, (3) deliberately intended to mislead and/or manipulate the public (4) specific or imagined, (5) through its appearance, with an opportunistic structure (title, image, content) news format to attract the attention of the reader, to attract more clicks and shares and thereby to attract more advertising revenue and/or ideological gain'.³⁵

With the outbreak of the COVID-19 pandemic, a number of factors have also emerged that have helped to increase the interest in misinformation and fake news and, as a result, to cause more damage. The circumstances surrounding the outbreak itself have also given rise to the spread of dubious news.³⁶

The newly created term *infodemic* (information and pandemic) reflects the significant impact of new information technologies on contemporary health communication. Political scientist David Rothkopf first used the term during the severe acute respiratory syndrome (SARS) pandemic of 2003 to describe how 'some facts, amplified by modern information technologies and rapidly transmitted worldwide, mixed with fear, speculation and rumour, have had an impact on national and international economies, politics and even security that has been totally out of proportion to the underlying realities'.³⁷ The impact cited is that of the COVID-19 pandemic, exacerbated by the fact that by 2020, online media had become much more sophisticated, and the widespread use of smartphones meant that misinformation and theories were spreading at an untraceable speed.

³⁴Zodi (2022), p. 67.

³⁵Baptista and Gradim (2022), p. 633.

³⁶Tomes (2020); WHO Infodemic Summary. https://bitly.ws/3cB86_1.

³⁷Tomes (2020).

Determining the reality basis of information and news is further complicated by the *filter bubble effect*, in which the algorithms used by social media play a prominent role. The role of these algorithms is to prioritise content in a user's news feed that is likely to fit their interests.³⁸ However, the algorithm does not only favour similar content for purchases and hobbies, but for all information. As a result, users can be completely 'bubbled', and on a social networking site, they can almost completely avoid reviews and content that are different from what they have read before or that criticise them. Moreover, the users can further reinforce this lock-in by being able to block users and pages that express opinions he or she does not like.

Social media have become an essential platform for political expression and access to information. In most cases, people are now getting their information there, even to the exclusion of traditional media providers. In addition, political and public actors are trying to maximise this access. We only have to think of the scandals of former US President Donald Trump's use of the Twitter platform (now X).³⁹ Still, a Hungarian example is when election-related advertisements appeared on all the platforms popular in Hungary before the elections, with advertising costs of several hundred million forints.⁴⁰ Furthermore, in Hungary there are several organisations (e.g., Megafon) that, in fact, present messages and topics to users that fit well into government communication and may even create fake user accounts or 'troll profiles' to support their messages.⁴¹

These circumstances, combined with the filter bubble effect of social media sites' algorithms, mean that users, and ultimately voters, are easily cut off from other information (critical information that is contrary to government communication) and thus remain outside the bubble, ultimately preventing access to a wide range of information on public issues.

Moderation and content filtering in Hungary can be hampered by the fact that content (including illegal, hateful content and fake news) is published in Hungarian. In the more minor, less known languages, the algorithms also find it more difficult to filter; making a mistake about a joke, an irony, or an opinion is easier.⁴² This in itself can cause problems even in the proper filtering and moderation of public content.

DSA generally tries to manage the information, news and advertisements that appear on the platforms. While we are still waiting for practices to emerge on its application in general, one of the issues that arises is the problem of over-constraint. There is concern that fearing heavy fines, operators may prefer to remove all dubious content, disproportionately restricting freedom of expression. In Hungary (and Poland), due to the specificities of the political systems in place, there is also concern

³⁸Holone (2016).

³⁹Wells et al. (2020), p. 663.

⁴⁰Bene and Farkas (2022), p. 154.

⁴¹Hidden Agendas: Fake Profiles on Facebook ahead of Hungary's Upcoming Elections. <https://bitly.ws/3cB9C>.

⁴²Duarte et al. (2017), p. 14.

that national authorities will use their powers to exercise their monitoring obligations, even abusively, and effectively censor content they do not want.⁴³

The European Commission's Code of Practice on Disinformation (CoP) which has been in force since 2018, aims to improve the credibility of information and content moderation practices, for example by closing fake accounts, removing bots, investing in technologies that help users to be informed, and voluntarily joining.

It was in 2021, in the wake of the epidemic of fake news and infodemics, that the EU decided to strengthen the CoP,⁴⁴ clarifying its obligations, including the reduction of disinformation linked to advertisements, increased moderation obligations, visibility of information of public interest, the possibility to customise algorithms and the marking of warnings and presumed false information.⁴⁵ This Code already foreshadowed that, with the entry into force of the DSA, which was still in its draft phase, it intended to co-regulate and further harmonise the provisions on moderation, transparency and algorithms, as is currently the case in the process of achieving compliance with the DSA, thus responding to the technological challenges of legal regulation.

7 Implementation Issues Related to Hungary: Conclusion

A common feature of new technologies and online platforms is that they entail significant risks, both in terms of consumer protection and the protection of human rights. This raises the question of how active market players are in adopting codes of conduct and to what extent their content will be able to mitigate the risks identified in the regulations. This leaves a number of additional questions open: in principle, the largest ecosystem users (at least for one of their activities) will be, at the same time, data controllers, gatekeepers, very popular online search engines, intermediary service providers, or users of AI systems, and service providers,⁴⁶ and could therefore be subject to all their Regulations. As a result, they will have a huge 'self-regulatory burden', as all the impact assessments required by the regulation must be carried out and documentation produced.

The way digital ecosystems work, as described in this study, means that these areas are not as sharply separated as the obligation in the various regulations. This raises the question of whether separate regulations should be formally drawn up for each regulatory area or whether it should be sufficient for the content to comply with the requirements of all the regulations, aligning codes and systems with regulations,

⁴³Mchangama et al. (2022), p. 18.

⁴⁴Burri (2022), p. 17.

⁴⁵European Commission, Guidance on Strengthening the Code of Practice on Disinformation Brussels, COM(2021) 262 final, 26 May 2021.

⁴⁶Each of the categories identified is a category defined by one of the Regulations to which a Regulation applies and requires compliance obligations [DSA Arts. 2(1) and 33, DMA Art. 2(2), GDPR Art. 3(1), AI Act Art. 2(1)].

as in many cases regulations have very broad objectives, such as protecting human rights,⁴⁷ or the fight against illegal content.⁴⁸ All of the provisions referred to have relatively general objectives, and it is likely to be difficult to determine whether, in a specific platform policy or a specific case, the person subject to the regulation(s) has acted properly and fully implemented the obligations imposed by the regulation.

These issues are also important because all the regulations provide for heavy fines in case of non-compliance. In relation to fines, there are also uncertainties as to the relationship between infringements of the rules of each regulation and the extent to which the prohibition of double jeopardy applies. As shown above, it is our view that the scope of the regulations in practice, in fact, regulates the same activity of the service provider in several aspects. It also follows that one behaviour (inadequate internal rules or IT systems) may violate several regulations.⁴⁹ However, it is unclear from the current rules whether a penalty for a breach of one of the rules precludes a penalty for the same activity under another regulation.

In recent years, the technological and digital world has been evolving at an accelerating pace, and new challenges and risks have had to be addressed. The EU is taking a complex approach to the issue, seeking to limit the digital ecosystem in several ways, reduce users' vulnerability and improve competition in online markets. However, there are also a number of questions about how the objectives of the regulations will be achieved, which will be answered in practice.

It is important to underline that the EU is thinking of a regulatory model for online platforms and AI, which is a uniform regulatory model across the EU. This desire for uniformity is so decisive that it is expressed in the DSA, the DMA and the AI Act. However, regulations in terms of their legal source are no longer titled 'regulation' but 'act', so the EU legislator aims to achieve complete uniformity. On the one hand, this is a perfectly logical approach, as the platforms and other service providers primarily affected by the regulations provide an international, essentially borderless, global service. They can, therefore, be effectively tackled uniformly across the EU.

However, there are also difficulties with fully harmonised regulation; while regulatory and reporting issues for service providers and their stakeholders can be addressed uniformly, there are several factors (language, cultural differences) that arise when using the platforms which can ultimately lead to different problems across Member States. A regulation, as opposed to a directive, leaves the Member States with little scope for individual solutions. The content of regulations directly applies to national law, and their provisions do not need to be—or should not be—repeated. As stated in the preamble (9) of the DSA, 'Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of the fully harmonised rules

⁴⁷ AI Act preamble, paragraph (13) and (28).

⁴⁸ DSA preamble, paragraph (9).

⁴⁹ The simplest example is when personal data is used to train an AI system in a non-transparent way. In this case, how will it be assessed whether there has been a breach of the GDPR provisions on personal data processing or the impact assessments under the AI Act? Or will a breach of both regulations be established?

applicable to providers of intermediary services in accordance with the objectives of this Regulation.’

In a conflict with national law, EU law also takes precedence. On this basis, the regulations referred to will apply in precisely the same way in all Member States. However, this statement does not stand on its own. An example of this is Art. 3(h) of the DSA, which defines ‘unlawful content’ as any information which, in itself or about an activity, including the sale of products or the provision of services, does not conform with EU law or the law of any Member State which conforms with EU law, irrespective of the precise subject matter or nature of that law.

As can be seen from the quoted text of the DSA, unlawful content may, therefore, not only be content contrary to EU law but also unlawful under Member State law. This is likely to result in differences in each Member State, with differences in what is considered illegal content under the law of a particular State.⁵⁰

However, examining the DSA’s unlawful content under national law, specifically in Hungary, leads to some exciting situations. For example, in Hungary, extremely restrictive content—especially content that is accessible to minors—concerning LMBTQ people is considered illegal.⁵¹ As a result, the assessment of whether content is illegal under EU law and Hungarian law may be markedly different under the DSA. Most social networking sites, such as Facebook, are officially available to users over 13.⁵² Suppose we assume that the child is using the site legally and is indeed at least 13 years old when registering (in the case of social networking sites, this alone is difficult to verify reliably). In that case, he or she is a minor under Hungarian law,⁵³ and thus, content posted on the platform—which is on the LMBTQ topic—may be illegal in Hungary. Still, where this is not the case under EU law, restricting the content under Hungarian law may be considered discriminatory.⁵⁴

Furthermore, in many cases, the DSA also entrusts the competent authorities of the Member State⁵⁵ with the task of dealing with the case, which in itself opens up the possibility of differences between procedures, but—concerning the discussion on fake news—in the case of Hungary, the specificities of the political system raise further concerns about the national process.

Therefore, a seemingly uniform regulatory regime will unlikely result in a perfectly consistent regime. There are also several questions to be answered about the application and effectiveness of the legislation in the EU as a whole.⁵⁶ However, even beyond this, Hungary may still have further questions of application, partly

⁵⁰The Digital Services Act (DSA) and combating disinformation—10 key takeaways. <https://bit.ly/ws/3cB9h>.

⁵¹Act LXXIX of 2021 on tougher action against paedophile offenders and amending certain laws to protect children.

⁵²Facebook Legal Terms 3.1. <https://www.facebook.com/legal/terms>.

⁵³Act V of 2013 on the Civil Code, Book two, Section 2:10 (1).

⁵⁴Mchangama et al. (2022), p. 9.

⁵⁵DSA preamble, paragraph (109).

⁵⁶Husovec (2022).

because content moderation is more difficult to carry out in a minor language less familiar to algorithms and moderators. On the other hand, there may be differences in the Hungarian legal system and official procedures, which may cause difficulties beyond the general application uncertainties.

References

- Affinito A, Botta A, Ventre G (2020) The impact of covid on network utilization: an analysis on domain popularity. In: IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). Pisa, Italy, pp 1–6. <https://doi.org/10.1109/CAMAD50429.2020.9209302>
- Bán-Forgács N (2023a) New data protection challenges in the post-covid area. In: Bratislava Legal Forum 2023: State as a protector and violator of individual rights. Univerzita Komenského v Bratislave, Právnická fakulta, Bratislava, pp 210–221
- Bán-Forgács N (2023b) Freedom of information and Covid-19—the Hungarian case. In: Grajczár I, Laki I (eds) Epidemic and society, trends, consequences, coping strategies. Milton Friedman University, Budapest, pp 35–61
- Bán-Forgács N, Mezei K (2023) Data protection challenges during pandemic: smart phones and other applications during Covid-19. In: Tafaro L, Florek I, Laki I (eds) Digital well-being—a concern for the quality of life. Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie. Milton Friedman University, Józefów, pp 30–40
- Bán-Forgács N, Szatmári P (2023) Challenges in freedom of information. Best practices and worst practices: Hungary. In: Tafaro L, Florek I, Laki I (eds) Digital Well-being—a concern for the quality of life. Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie. Milton Friedman University, Józefów, pp 138–148
- Baptista JP, Gradim A (2022) A working definition of fake news. Encyclopedia 2:632–645. <https://doi.org/10.3390/encyclopedia2010043>
- Barata J, Budzinski O, Cole M, Ledger M, McGonagle T, Pentney K, Rosati E, de Streel A (2021) Unravelling the digital services act package. European Audiovisual Oversight, Strasbourg
- Barykin SY, Kapustina IV, Kirillova TV, Yadykin VK, Konnikov YA (2020) Economics of digital ecosystems. J Open Innov: Technol Mark Complex 4:124. <https://doi.org/10.3390/joitmc6040124>
- Beck U (1992) Risk society – towards a new modernity. SAGE Publications
- Bene M, Farkas X (2022) Ki mint vet, úgy arat? A 2022-es választási kampány a közösségi médiában [Who reaps as he sows? The 2022 election campaign on social media]. Századvég, Budapest
- Bradford A (2020) The Brussels effect: how the European Union rules the world. Columbia Law School
- Burri M (2022) Fake news in times of pandemic and beyond: an enquiry into the rationales for regulating information platforms. In: Mathis K, Tor A (eds) Law and economics of the coronavirus crisis. Springer, Berlin, pp 31–58
- De Gregorio G (2022a) What is digital constitutionalism? A view from Europe. <https://bitly.ws/3cBfM>
- De Gregorio G (2022b) Digital constitutionalism in Europe. University of Oxford, Oxford
- De Gregorio G, Dunn P (2023) The future of digital regulation: a risk-based approach? <https://bitly.ws/3cBgS>
- Duarte N, Llanso E, Loup A (2017) Mixed messages? The limits of automated social media content analysis. <https://bitly.ws/3cBgZ>
- Efroni Z (2021) The digital services act: risk-based regulation of online platforms. <https://bitly.ws/3cBhb>
- Favaretto M, De Clercq E, Schneble C O, Elge B S (2020) What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade. <https://bitly.ws/3cBiN>
- Goanta C, Ranchordas S (eds) (2020) The regulation of social media influencers. Edgar Law, Technology and Society Series

- Grinberg N, Joseph K, Friedland L, Swire-Thompson B, Lazer D (2019) Fake news on Twitter during the 2016 U.S. presidential election. *Science* 25;363(6425):374–378. <https://doi.org/10.1126/science.aau2706>
- Helberger N, Lynskey O, Micklitz H-W, Rott P, Sax M, Strycharz J (2021) EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets. The European Consumer Organisation, Brussels
- Holone H (2016) The filter bubble and its effect on online personal health information. *Croat Med J* 30;57(3):298–301. <https://doi.org/10.3325/cmj.2016.57.298>
- Hou S-M, Fu W-C, Lai S-Y (2023) Exploring information warfare strategies during the Russia–Ukraine war on twitter Korean J Defense Anal 1:19–44. <https://doi.org/10.22883/kjda.2023.35.1.002>
- Husovec M (2022) Will the DSA work? <https://bitly.ws/3cBj4>
- Mantelero A (2022) Fundamental rights impact assessments in the DSA. *Verfassungsblog*. <https://bitly.ws/3cBjj>
- Mchangama J, Alkiviadou N, Mendiratta R (2022) Thought on the DSA: challenges, ideas and the way forward through international human rights law. <https://bitly.ws/3cBju>
- Mir-Llinares F, Aguerri C (2021) Misinformation about fake news: a systematic critical review of empirical studies on the phenomenon and its status as a ‘threat’. *Eur J Criminol* 1:356–374. <https://doi.org/10.1177/1477370821994059>
- Nagy N (2023) ‘Humanity’s new frontier’: human rights implications of artificial intelligence and new technologies. *Hungarian J Legal Stud* 64(2):236–267. <https://doi.org/10.1556/2052.2023.00481>
- Punkosty A (2022) Merre tart az eurpai szint platformszablyozs? ttekints a platformok szablyozsnak versenyjogi sztnzirl, valamint a fzikontroll lehetsges fejlesztsrl [Where is European platform regulation heading? An overview of the incentives for platform regulation and the possible development of merger control]. In: Trk B, Zdi Zs (eds), *Az internetes platformok kora* [The Age of Internet Platforms]. Ludovika, Budapest
- Revati Devaki PC, Dinesh Babu S (2021) The future of over-the-top platforms after Covid-19 pandemic. *Ann Roman Soc Cell Biol* 6:11307–11313
- Tomes N (2020) Managing the modern infodemic. *Can Med Assoc J* 192(43):E1311–E1312. <https://doi.org/10.1503/cmaj.201905>
- van de Waerd P (2020) Information asymmetries: recognizing the limits of GDPR on the data-driven market. *Comput Law Secur Rev*:1–18. <https://doi.org/10.1016/j.clsr.2020.105436>
- Wells C, Shah D, Lukito J, Pelled A, Pevehouse JC, Yang J (2020) Trump, twitter, and news media responsiveness: a media systems approach. *New Media Soc* 22(4):659–682. <https://doi.org/10.1177/1461444819893987>
- Zdi Z (2022) Az eurpai platformszablyozs jellegzetessgei: Platformjog s felhasznlvdelem [Characteristics of European platform regulation: platform law and user protection]. *Medias Res* 1:66–82

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

