BRATISLAVA LAW REVIEW

PUBLISHED BY
THE FACULTY OF LAW,
COMENIUS UNIVERSITY
BRATISLAVA

ISSN (print): 2585-7088
ISSN (electronic): 2644-6359

ŠIŠKOVÁ, NADĚŽDA (ED.): LEGAL ISSUES OF DIGITALISATION, ROBOTIZATION AND CYBER SECURITY IN THE LIGHT OF EU LAW. KLUWER LAW INTERNATIONAL, 2024 / Igor Sloboda

Mgr. Igor Sloboda
PhD. Student
Comenius University Bratislava
Faculty of Law
Institute of European Law
Šafárikovo námestie č. 6
810 00 Bratislava, Slovakia
igor.sloboda@flaw.uniba.sk
ORCID: 0009-0005-9408-1618

Submitted: 16 December 2024
Published: 31 December 2024

Suggested citation:
Sloboda, I. (2024). Šišková, Naděžda (Ed.): Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law. Kluwer Law International, 2024. *Bratislava Law Review*, 8(2), 277-282. https://doi.org/10.46282/blr.2024.8.2.957

The issue of the challenges arising from the development of information technologies in the context of EU law has been a relatively extensively researched and discussed area, particularly over the past decade. This is due in part to the rapid development and integration of modern technologies into practice, which has created a vast field of research across a diverse range of legal sectors into which EU law extends.

The collective monograph compiled by professor Šišková, entitled "Legal Issues of Digitalisation, Robotisation and Cyber Security in the Light of EU Law", provides an ideal introduction for readers to current trends and challenges reflecting the development of modern technologies and their impact on both EU citizens and companies operating in the EU through EU Law.

From a systematic perspective, the publication is divided into four parts, which guide the reader through the subject matter in a step-by-step manner. The initial section of the publication is comprised of four chapters, each addressing the implications of digitalisation and robotisation on human rights from a distinct perspective. The second part of the publication addresses the topic of consumer protection in the context of the digital economy. The third part focuses on competition law in the digital age. The fourth and final part of the publication covers the crucial issues of cyber security, cyber crime and the effective legal tools that can be employed to combat these threats and ensure compliance with relevant legal norms.

The initial chapter, authored by Soňa Matochová, provides a comprehensive overview of the evolution of personal data protection in the context of technological advancement, elucidating the intricate balancing act between the utilisation of personal

data and the safeguarding of its confidentiality. In the concluding section, the author assesses the present framework of data protection, emphasising its beneficial impact on the safeguarding of personal data. Conversely, however, she observes that the implementation of these regulations remains a challenge, particularly due to the existence of disparate procedural rules at the national level, and advocates for the harmonisation of these standards (Matochová, 2024).

In the second chapter, Naděžda Šišková presents a discussion of the right to be forgotten from the perspective of the general concept of fundamental rights. Her findings indicate that the 'right to be forgotten' is not currently an effective instrument. This is primarily attributable to the concealment of personal data exclusively within the EU through geo-blocking, the restriction of the territorial scope to the EU alone, the intrinsic nature of the Internet, which precludes the absolute deletion of data, and the Streisand effect. In light of these considerations, the author proposes the establishment of a global digital registry of individual claims as a potential solution (Šišková, 2024).

In the following third chapter, Martin Mach picks up the same theme of the right to be forgotten, but this time from the perspective of the so-called "watchdogs search engines", which are subject to the same obligations as internet search engines. The issue here, however, focuses on the fact that the source of these search engines is data originating from public administrations. Therefore, these search engines cannot arbitrarily decide on the availability of this data. The author sees a solution to this through internal control mechanisms (Mach, 2024).

In the last chapter of the initial section of the publication, the trio of authors Luisine Vardanyan, Hovsep Kocharyan and Ondrej Hamuľák address the question of the right to the Internet. Throughout the chapter, they inquire as to whether this is a new fundamental right or, conversely, whether the Internet is a new platform for fundamental rights. (Vardanyan, Kocharyan and Hamuľák, 2024, pp. 76-79). Their findings suggest that we cannot speak of a platform in this case, but neither can we speak of a separate human right. According to their conclusions, it can be considered as an integral part of the right to digital integrity. Securing the right of access to the Internet can also be seen as a means by which it will not be necessary to adopt a new legal framework guaranteeing fundamental rights for the Internet. In conclusion, however, they perceive some practical and technical problems (Vardanyan, Kocharyan and Hamuľák, 2024).

The following part of the publication is devoted to consumer protection issues. Although it is the shortest part of the publication, it offers in its two chapters a comprehensive selection of contemporary issues, challenges but also opportunities and suggestions on how to improve consumer protection in the light of modern technologies. In the fifth chapter, Blanka Vítová addresses the issue of consumer protection in the light of the digital era. In her chapter, she will gradually present us with the challenges but also the opportunities that consumer protection faces today, among which are, for example, the lack of transparency (Vítová, 2024).

In chapter six, the authors Zsolt Hajnal and Rita Simon discuss the main challenges in the implementation of the Digital Content Directive in the Czech Republic and Hungary. Their findings show that the specificities related to both countries have not been fully eliminated and practical problems can be expected in the future when it comes to the consumers data performance as reward for digital services and in the case of collision with data protection principles (Hajnal and Simon 2024).

The third part of the publication deals with the intersection of competition law in the digital economy, opening with a chapter by Michal Petr in which he discusses the parallel application of competition law, the DMA and sectoral regulation. He points out their different characteristics as well as the instruments through which they achieve their

objectives. The chapter also raises the issue of compliance with the ne bis in idem principle in the case of parallel investigations of undertakings by competition authorities and national regulators (Petr, 2024).

In chapter eight, Ondrej Blažo presents a detailed analysis of the issue of private enforcement of the DMA, including its extent, limitations and challenges. Within the chapter, the author identifies provisions where private law enforcement is allowed by the regulation, but where no procedural regulation for its enforcement is provided (Blažo, 2024, pp. 147–156). Furthermore, the chapter presents a comparative analysis of the competition rules and the proceedings for damages. In light of these considerations, the author concludes in the chapter that, with respect to private law enforcement, the objective of the DMA has not been met, although there is potential for conflict between the laws of the Member States (Blažo, 2024).

In chapter nine, Marika T. Patakyová addresses the topic of pricing algorithms. In the course of the article, the author examines the issue from two distinct perspectives: firstly, through the lens of the substantive regulation contained in Article 101 TFEU; and secondly, from a procedural point of view. To ascertain how the competition authority might assess the situation at the substantive level, the author proceeded to conduct a theoretical experiment utilising a model situation. (Patakyová, 2024, pp. 168–173) The findings demonstrated that some of the traditionally employed evidence is not applicable in this case. Additionally, based on the findings of the experiment, the author presents, in the penultimate subsection, her three de lege ferenda proposals (Patakyová, 2024, pp. 174–179) to enhance the enforcement of concerted practices by the competition authorities (Patakyová, 2024).

In the final chapter of the third part of the publication, Kseniia Smyrnova discusses the changes that e-commerce brings to competition and illustrates these findings with selected cases. Throughout the chapter, she takes us step by step through examples of anti-competitive behaviour that can be found in e-commerce, such as geo-blocking, most-favoured-nation clauses, discriminatory practices in internet search, and vertical restraints in e-commerce. The author also discusses the current legal framework and the chapter examines the recent case law of the Court of Justice, illustrating these practices with selected cases (Smyrnova, 2024).

This is followed by the fourth and final part of the publication - chapters eleven to eighteen, which take us through the issues of cybersecurity, cybercrime, civil liability and the instruments for effective resilience. In the opening eleventh chapter, the author duo Agnes Kasper and Anett Mádi-Nátor provide an introduction to the EU legal framework in relation to digital vulnerability. The chapter presents a comprehensive overview of the theoretical background of digital vulnerability, along with an examination of the current and proposed legislation within the EU context. Additionally, it addresses cross-cutting links to prominent examples of vulnerability, such as Spectre and Meltdown. (Kasper and Mádí-Nátor, 2024).

In Chapter twelve, the authors Pablo Martínez-Ramil and Tanel Kerikmäe raise the question of algorithmic responsibility in the context of artificial intelligence. As EU Law is evolving in parallel, it is not straightforward to determine the answer. Despite the best efforts of those involved in the creation of AI, it is possible that a situation may arise in which wrongful conduct occurs. Nevertheless, if the prevailing standards are applied, it remains unclear who should be held accountable for the algorithm in this instance. The answer to this question is more challenging to ascertain due to the lack of a definitive method for enforcing criminal liability. In light of the aforementioned considerations, it can be posited that the answer may lie in the realm of non-contractual civil liability. However, it is imperative to note that three conditions must be met for this to be the case.

DOI: 10.46282/blr.2024.8.2.957

An alternative avenue for consideration could be the Product Liability Directive. In such a scenario, the outcome would also be contingent upon the competent authority, given the necessity for an individual assessment of the degree of faultiness of the AI system, as outlined in Article 6 of the Directive (Martínez-Ramil and Kerikmäe, 2024).

In the thirteenth chapter, Jozef Andraško addresses the issue of cyber security of automated and fully automated vehicles in the context of the current legislative framework. The necessity for effective legislation is demonstrated by the author in the introductory section of the chapter with several security incidents that have taken place in the recent past. The core of the chapter consists mainly of an analysis of the existing legislation adopted at international and EU level. (Andraško, 2024, pp. 252–262) The legislation is evaluated and its practical impact is highlighted, while also comparing the adopted acts and differences between them (Andraško, 2024).

In chapter fourteen, the author, Peter-Christian Müller-Graff, addresses the issue of the EU's strategic sovereignty in relation to the modern threats currently facing the Union. Within the chapter, the author seeks to answer whether strategic sovereignty is one of the EU's objectives directly deriving from primary law. Furthermore, the chapter seeks to ascertain the options available to the EU in terms of securing this sovereignty, given the powers currently defined by primary law in this regard. The author's findings lead to the formulation of four key conclusions in relation to defence policy, energy security, strategic sovereignty and unification around EU values (Müller-Graff, 2024).

In the following fifteenth chapter, Ondřej Filipec analyses the nature of EU-NATO cooperation in the field of cyber security and cyber defence. The author defines this cooperation in the context of both EU and NATO policies. Within the last subchapter, author focuses on the cooperation between the two organisations, on the basis of documents through which cooperation occurs in specific areas and within specific bodies. Nevertheless, in addition to theese areas, the author also identifies the differences and limitations of the policies of the two organisations (Filipec, 2024).

In the sixteenth chapter, Volodymyr Denysov and Liudmyla Falalieieva examine the present challenges and future prospects for the evolution of EU cybersecurity legislation. The authors start by introducing the basic theoretical background, gradually moving into the specific legal and institutional framework in relation to both the private and public sectors. The authors identify the issues and challenges that arise from the current EU legislation in both areas under study. In this way, the authors also put forward a concrete proposal for the creation of a unified EU cybersecurity system, taking into account the current challenges (Denysov and Falalieieva, 2024).

Within the seventeenth chapter, the author Yuliia Vashchenko focuses on the cybersecurity of the energy sector in the EU and Ukraine. The author defines the cybersecurity of the energy sector and the relevant authorities in the conditions of the EU, the Member States and Ukraine. (Vashchenko, 2024, pp. 318–332) In light of her findings, author formulates a comprehensive conclusion, underscoring a multitude of necessities. (Vashchenko, 2024, pp. 332–334) These include the establishment of effective control mechanisms, the fostering of collaboration between public administration entities, the cultivation of inter-sectoral cooperation between the private and public spheres, and numerous other factors pertaining to the cybersecurity of critical infrastructure (Vashchenko, 2024).

Within the last, eighteenth chapter of the publication, the author Bohdan Strilets discusses cybersecurity rules for cryptoasset markets. As the popularity of cryptoassets continues to grow, the necessity for robust cybersecurity measures also increases. The author therefore analyses the current legislation in force in the EU context in this respect. Furthermore, he conducts an analysis of the underlying theoretical background and the

protection of consumer and investor rights. In conclusion, the author presents a proposal for improvement, which includes, for example, strengthening the powers of ENISA (Strilets, 2024).

The publication concludes with a comprehensive fifteen-page-long conclusion. This represents the collective effort of the authors to synthesise the findings of the individual chapters into a unified conclusion that conveys a coherent message.

The reviewed publication is a very enriching reading, which is not just a simple introduction to the issue of legal regulation of information technologies by EU Law, but represents a comprehensive output of several years of research mapping several selected areas. Despite the apparent interconnectedness of these areas at first glance, are linked precisely by the intersection of EU Law and modern technologies. Although the publication is not exactly timed to coincide with the 10th anniversary of the launch of the Digital Single Market strategy in May 2025, it offers valuable insights and ideas. This encompasses not only an overview of the achievements made thus far, but especially in relation to what we can expect in the future, even after the impact of practical experience, but especially where EU legislation might be evolving in the future.

BIBLIOGRAPHY:

Andraško, J. (2024). Cyber Security of Automated and Fully Automated Vehicles – New Legal Instruments. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 249 – 263). Alphen aan den Rijn: Kluwer Law International.

Blažo, O. (2024). Private Enforcement of the Digital Markets Act: Filling Holes and Creating New Ones in Harmonized Enforcement. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 145 – 161). Alphen aan den Rijn: Kluwer Law International.

Denysov, V. and Falalieieva, L. (2024). Legal Regulation of Cybersecurity in the European Union: New Challenges and Prospects Development. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 292– 314). Alphen aan den Rijn: Kluwer Law International.

Filipec, O. (2024). EU-NATO Cooperation in Cyber Security and Cyber Defense. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 276 – 291). Alphen aan den Rijn: Kluwer Law International.

Hajnal, Z. and Simon, R. (2024). Key Challenges to the Implementation of the Digital Content Directive in Hungary and Czech Republic. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 113 – 126). Alphen aan den Rijn: Kluwer Law International.

Kasper, A. and Mádí-Nátor, A. (2024). EU legal framework of digital security vulnerabilities. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 211 – 231). Alphen aan den Rijn: Kluwer Law International.

Mach, M. (2024). The „Right to Be Forgotten" – by Watchdogs and Open-Source Search Engines. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 60 – 69). Alphen aan den Rijn: Kluwer Law International.

Martínez-Ramil, P. and Kerikmäe, T. (2024). Who is accountable for the algorithm ? Assessing the effectiveness of the EU's approach towards AI liability. In: Naděžda

Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 232 – 248). Alphen aan den Rijn: Kluwer Law International.

Matochová, S. (2024). GDPR and the Right to Personal Data and Privacy in Modern Society in Digital Age. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 21 – 42). Alphen aan den Rijn: Kluwer Law International.

Müller-Graff, P.-Ch. (2024). The European Union's Strategic Sovereignty – Legal Implications in the Light of Modern Threats. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 264 – 275). Alphen aan den Rijn: Kluwer Law International.

Patakyová, M. T. (2024). Pricing Algorithms and Anticompetetive Agreements. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 162 – 180). Alphen aan den Rijn: Kluwer Law International.

Petr, M. (2024). EU Regulation of On-Line Platforms: between Competition Law and Digital Markets Act. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 129 – 144). Alphen aan den Rijn: Kluwer Law International.

Smyrnova, K. (2024). Does e-commerce change the ordinary competitive conditions ? Current investigations of geo-blacking and geo-filtering in EU practice. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 181 – 207). Alphen aan den Rijn: Kluwer Law International.

Strilets, B. (2024). New Cybersecurity Rules for Markets in Crypto-Assets in the EU Law. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 335 – 355). Alphen aan den Rijn: Kluwer Law International.

Šišková, N. (2024). The „Right to Be Forgotten" – Some Considerations on a General Concept in the Light of Fundamental Rights. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 43 – 59). Alphen aan den Rijn: Kluwer Law International.

Vardanyan, L., Kocharyan, H. and Hamuľák, O. (2024). The Right to Internet Acces: A New Fundamental Right or a New „Platform" for Fundamental Rights ? In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 70 – 92). Alphen aan den Rijn: Kluwer Law International.

Vashchenko, Y. (2024). Energy Sector Digitalization: Issues of Cybersecurity in the EU and Ukraine. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 315 – 334). Alphen aan den Rijn: Kluwer Law International.

Vítová, B. (2024). Future Challenges and Opportunities In European Consumer Law Protection In the Digital Era. In: Naděžda Šišková (Ed.), *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law* (pp. 95 – 112). Alphen aan den Rijn: Kluwer Law International.