REVIEWS AND ANNOTATIONS

Naděžda Šišková (ed.) Legal Issues of Digitalisation, Robotisation and Cyber Security in the Light of EU Law. Alphen aan den Rijn and Prague: Kluwer Law International BV and Wolters Kluwer CZ, 2024, 392 pages.

The collective monograph with a long title, which reflects the multiple impacts of IT, the Internet and artificial intelligence on the EU legal framework and through it on the lives of Europeans and their societies, is a useful contribution of 24 authors from 8 institutions in the Czech Republic, Slovakia, Germany, Hungary, Estonia and Ukraine. Published by linked publishing houses in the Czech Republic and the Netherlands, it has a good chance of reaching readers far beyond the Czech Republic, where Palacký University in Olomouc and the editor of the publication, Naděžda Šišková, were the main drivers of this research and publication.

The book contains 18 chapters, 2 prefaces (by the editor and also by CJEU judge J. Passer), extensive joint Conclusions (16 pages, to be further mentioned) and a very useful list of cited case law of the CJEU and the ECHR. One third of the contributions are devoted to cybersecurity issues. Equally represented (4 contributions in each Part) are the protection of human rights on the internet (personal data, right to be forgotten, right to internet access) and the protection of competition in the online environment (practical application of the Digital Markets Act – DMA, use of pricing algorithms, practices of geo-blocking and geo-filtering). Two papers focus on consumer protection on the Internet and one paper on the responsibility for the use of artificial intelligence and another one on the assertion of EU strategic sovereignty amidst modern threats.

This thematic opulence, in some cases ambiguity, is of course an understandable price for attempting to connect a diverse multinational author collective. It is, to some extent, also an inevitability if the connecting element is EU law and the Internet - because today it is almost impossible to find a topic that could not be related to this connecting element in one way or another. However, the greater dispersion and variety of contributions may undoubtedly be sympathetic to a reader who is looking for lessons in only a particular aspect (e.g. EU law on cybersecurity *de lege lata* and *de lege ferenda*, right to be forgotten or legal aspects of the use of smart algorithms) and will not read the publication from the first to the last page.

The more practical are then the rather extensive joint Conclusions at the end of the book, because there is an attempt to combine the conclusions of the partial contributions into one whole. Partly, of course, it is a summary, but partly it is a list of important issues that digitalisation and artificial intelligence pose for EU law and that EU law will have to address in one way or another in the coming period. Personally, I find these Conclusions very valuable for orienting myself to the current issues under examination, and also practically useful for any reader who wants to choose from the menu of contributions outlined above with more knowledge of their matter than is offered by the Table of Content in the introductory part of the book.

In terms of the actual content and quality of the individual contributions, the authors and the editor managed to maintain a high level of both interpretation and work with sources, notwithstanding the fact that the authors' approaches differ from each other in terms of content, methods of analysis and interpretation, as well as formal structure of the text. Some contributions provide a theoretical-historical overview of the development of doctrine and legislation (e.g., Chapter 1 on privacy and personal data in the Digital Age, or Chapters 15 and 16 on the international dimension of cybersecurity), others provide an extensive initial review of existing scholarly views and cross-country comparisons (e.g., Chapter 4 on the right to internet access), while others are built on an original experimental model (Chapter 9 on proving cartels formed using pricing algorithms).

Some contributions are devoted to detailed aspects of how a particular piece of legislation works in practice (e.g. Chapter 8 on the possibilities of private enforcement of the DMA) or on the legal assurance of the security of a particular product (Chapter 13 on the cybersecurity of smart vehicles), while others range from law to history to politics (Chapter 15 on EU-NATO cooperation in Cyber Security and Cyber Defence). While some authors have focused on exploring the possibilities provided by current legislation and case law (e.g., Chapter 7 and the issues of parallel application of the DMA, competition law and sectoral regulation), others have not hesitated to overcome existing regulation with far-reaching proposals for change, including the addition of a whole new catalogue of human rights for internet users to the EU Charter of Fundamental Rights (Chapter 2) or the fundamental right to internet access (Chapter 4) or the right to cybersecurity (Chapter 16).

This diversity of approaches guarantees that the reader will find both contributions relevant to legal practice and those that rather stimulate the legal imagination and raise questions whether and to what extent this or that right related to the use of the Internet should be codified at the constitutional level, supported by secondary EU legal harmonisation, or whether the powers of the EU and its agencies relevant to certain aspect of regulation of the digital world should be increased. Here, even the Euro-optimists and techno-optimists among lawyers must agree with the approach of the doyen among the authors of the publication, Peter-Christian Müller-Graff, professor at the University of Heidelberg, that while some of the proposed changes would be useful, and, from a rational point of view, necessary (because legislation is either lacking or differs substantially between Member States), "they are out of touch with the reality of the national willingness...".

The hypertrophy of EU fundamental rights, specialised agencies and, ultimately, EU competences is simply not only a politically sensitive issue, but also a question of practical feasibility in terms of the effectiveness of the law and the cost of its enforcement (as rightly recognised, for example, by the authors of Chapter 4 detailing the possible constitutionalizing of the fundamental right to internal access). However, even with this scepticism about the various *de lege ferenda* solutions proposed in the book, it is valuable and interesting to read what rights are not yet recognised or effectively protected in practice, so that the reader should be on the lookout when he or she enthusiastically starts writing a new post on his or her profile, investing in crypto-currencies, or buying a smart vehicle or other toy from the world of the Internet of Things.

Overall, the work of the author team, supported by the Jean Monnet Network of the EU, is to be highly praised and the reviewed book recommended to readers. Even if those interested in the issues that make up its content will not read it in its entirety and in the order in which the chapters are arranged, they will find a wealth of information, opinions, and suggestions worth knowing and thinking about. The papers in the book were prepared as of September 1, 2023, even so, at the time of writing this review ten months later, it is a timely book, interesting in the variety of its content and usefully thought provoking in the range of its conclusions.

Václav Šmejkal*

* Associate Professor, JUDr. Václav Šmejkal, Ph.D., Faculty of Law, Charles University, Prague, Czech Republic and Škoda Auto University Research Center, Czech Republic. ORCID: 0000-0003-1403-9494.