Summary of the Dissertation „ Cybersecurity Regulation in the European Union – Challenges and Perspectives”

by Margarita Oysolova, PhD student at the Institute for the State and the Law - Bulgarian Academy of Sciences

Information and communication technologies (ICT) constitute the foundation of the complex systems that support everyday social activity, enable the functioning of national economies across essential sectors such as healthcare, energy, finance, and transport, and ensure the operability of both the internal and international market. The use of networks and information systems by citizens, organisations, and businesses throughout the European Union has become ubiquitous. Digitalisation and connectivity are evolving into core features of an ever-increasing number of products and services. With the expansion of the “Internet of Things”, the Union is expected to host an exceptionally large number of interconnected digital devices in the coming decade.

In recent years, and particularly during the Covid-19 pandemic, cyberspace and technological integration advanced rapidly across all spheres of society. Everyday life, fundamental rights, social interactions, and even state economies have become dependent on the flawless and continuous functioning of ICT. Today, complex systems across various sectors—including finance, healthcare, energy, and transport—rely heavily on digital infrastructure. Furthermore, following the Covid-19 pandemic, business continuity has become intrinsically linked to uninterrupted internet access and the reliable operation of information systems.

The increasingly complex nature of cyberattacks aimed at obtaining unauthorised access to systems and networks presents a major challenge for

cybersecurity. Malicious actors continuously develop and deploy sophisticated techniques to breach security mechanisms or exploit existing system vulnerabilities.

In response to these evolving threats, the European Union has taken significant steps to strengthen cybersecurity by adopting comprehensive cybersecurity strategies, regulations, and directives designed to enhance resilience and protect information and communication systems. These risks highlight the need not only for advanced technical safeguards but also for the establishment of ethical standards governing conduct in cyberspace—thus underscoring the importance of cyber ethics.

Cyber ethics represents an interdisciplinary field combining ethical principles, legal norms, and information technology. It addresses issues such as the responsible and fair use of digital resources, the protection of individual autonomy and data privacy, and the delicate balance between freedom of expression and accountability for online content. In a globalised cyber environment, the importance of cyber ethics is amplified, as the absence of physical borders demands universal and shared standards and values.

This study examines key EU legislative acts related to cybersecurity, as well as selected analyses and reports issued by EU institutions. The objective is to provide a comprehensive overview of the Union's legal framework in the area of cybersecurity, contributing to clearer interpretation, more informed policy analysis, and facilitating future legislative amendments. Additionally, the study enhances understanding of the measures undertaken and identifies areas requiring further legislative or policy development in light of emerging technological trends.

Based on the analysis of EU legislation, the paper provides commentary on the practical scope and application of relevant legal provisions.

The research focuses on the period after the year 2000, a limitation justified by the extensive number of legal instruments in the field and the diminished relevance of those issued prior to that period.