Gergely Gosztonyi*

Preface to the Contributions on Digital Authoritarianism, Internet Fragmentation, Splinternet, Censorship and Cyber Sovereignty

The divergence between cyber libertarianism and cyber paternalism characterised discussion related to internet governance in the 1990s. Decisions on content regulation issues were settled in the United States of America (US) with the Communication Decency Act Section 230 and in Europe with the notice-and-takedown system of the E-commerce Directive. However, the era of privatised freedom of expression faced challenges from the mid-twentieth century onwards, from Christchurch and troll farms to the Cambridge Analytica scandal. For a few years now, internet regulation has been a vital issue on the political agenda in all parts of the world, characterised in the US by the need to amend CDA230 and the 'dragging' of giant tech mammoths' leaders before the Senate. In the European Union (EU), the process led to the adoption of the Digital Services Act (DSA) – Digital Markets Act (DMA) – and European Media Freedom Act (EMFA) package of regulations. Meanwhile, for example, in China, the process of change is characterised by the ongoing development of the Golden Shield and the Great Firewall based on the concept of cyber sovereignty, and in Russia, by the wish to disconnect from the international internet network. The increasingly undemocratic practices of these latter rogue states may be attractive to many other countries, and such solutions have started being exported.

Alas, there is a global trend towards governments increasingly resorting to internet restrictions, often for illegitimate purposes and with disproportionate impacts on the public. This shift in international norms towards greater government intervention in the digital sphere is a matter of urgent concern. Technical and legal solutions can range from denying user access through filtering technologies and unlawful bandwidth throttling to collateral and excessive and wholesale blocking by states. This trend necessitates urgent attention and action.

* Dr Gergely Gosztonyi PhD, Habil. Associate Professor, Eötvös Loránd University (ELTE), Faculty of Law. ORCID iD: 0000-0002-6551-1536.
The whole volume on digital authoritarianism, internet fragmentation, splinternet, censorship and cyber sovereignty was supported by the project no. 149657 which has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the ADVANCED_24 funding scheme.

Thus, scholarly articles about cyber sovereignty and its legislation are crucial due to the intricate and evolving nature of internet governance and its profound implications for global politics, security, and individual freedoms. Cyber sovereignty, a concept that refers to a state's right to govern and control internet activity within its borders, is gaining prominence as nations face increasing cyber threats. The Center for Strategic and International Studies (CSIS) reports that the global cost of cybercrime will reach $10.5 trillion annually by 2025. Researching and documenting how different countries enforce cyber sovereignty provides critical data on the effectiveness of various policies.

The legislative landscape of cyber sovereignty varies widely, with over 120 countries having enacted cybersecurity laws by 2023, according to the United Nations Conference on Trade and Development (UNCTAD). These laws range from comprehensive data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), to more fragmented and sector-specific approaches seen in countries around the globe. According to Freedom House's 2023 report, approximately 70% of internet users live in countries where governments impose significant censorship or surveillance. In Asia, countries like China and North Korea enforce strict internet censorship.

Similarly, Russia's Sovereign Internet law aims to route internet traffic through state-controlled infrastructure, increasing the government's ability to control and monitor online activities. Countries like South Korea and Japan have more open internet policies but enforce significant regulations. Examining these practices can provide a nuanced understanding of the trade-offs between national security and individual freedoms, generating data-driven recommendations that support the implementation of balanced approaches.

The role of international human rights courts in dealing with cyber sovereignty and internet restrictions cases is increasingly significant. These courts recognise the implications of such issues on human rights and have ruled on several cases involving state surveillance and internet censorship. For instance, the European Court of Human Rights (ECtHR) has addressed state surveillance and internet censorship, while the Inter-American Court of Human Rights (IACtHR) has highlighted the illegal interception of communications.

Of critical importance is that research on cyber sovereignty and related legislation cannot be accomplished without analysing the technical details and infrastructure behind the internet. This way, addressing the global shortage of cybersecurity professionals would help meet this challenge. In Asia, countries such as Singapore and India invest heavily in cybersecurity education and training to build a workforce capable of addressing emerging threats. Europe is also proactive, with initiatives like the European Cybersecurity Skills Framework (ECSF) intended to enhance cyber education and professional development across the EU. Data shows that countries with solid cybersecurity education programs, such as Israel, have higher employment rates in the cybersecurity sector and better job performance outcomes. Integrating academic research into training and professional development will ensure that the next generation of experts is well-equipped to holistically navigate the complex landscape of cyber sovereignty and internet governance.

Fourteen scholars from ten countries have gathered to discuss those crucial issues concerning modern communication. In the first part of this issue of the ELTE Law Journal, Dorina Gyetván paints a general picture, showing that online private censorship is no longer just a theoretical distant possibility but an everyday reality. Carmen Moldovan highlights the conflict between the idea of state control over the internet and the impact on freedom of expression and access to information, as well as the challenges of the state-driven regulatory model. Adelina-Maria Tudurachi asks if Internet access could or should be seen as a fundamental human right, examining the relevant case law of the European Court of Human Rights and the Court of Justice of the European Union (CJEU). Gergely Ferenc Lendvai focuses on the right to access the Internet (RATI) as seen by the ECtHR and finds it in great danger in Russia and Turkey. Xiaojuan Grace Yang has created a comprehensive overview of World Internet Conferences and China's promotion of cyber sovereignty, giving details about a less well-researched and known topic.

The second part of this ELTE Law Journal issue deals with the European online media legislation processes. Boris Kandov writes about the DSA, clearly underlining that it introduces several new regulations concerning algorithm-based, automatic filtering systems into EU law that are playing a significant role in online platforms, as algorithms are used there in the form of filtering and recommendation systems. Simona Veleva anticipates the challenges with the regulatory implementation of the DSA into national regulatory frameworks; the article focuses on the harmonisation process and the challenges posed by different legal traditions and regulatory approaches.

Readers may swim in the ocean of more technical questions in the third part of this issue of the ELTE Law Journal. Tuba Eldem thoroughly shows how the Internet is increasingly becoming a domain of control, surveillance, and regulation by states and private entities. The article investigates Web3 architecture in relation to countering sovereign controls with a mixed-method approach that synthesises insights from computer science, political science, and legal studies. Roland Kelemen, Joseph Squillace, Richárd Németh and Justice Cappella investigate the relationship between the United Nations Sustainable Development Goals and Internet access, focusing on how digital connectivity influences the achievement of these global objectives and revealing that a robust IT identity enhances digital inclusion and empowerment. In the last article, Ádám Farkas and László Vikman examine information operations as a question of law and cyber sovereignty, reviewing different nation-state solutions and providing a conceptual framework that incorporates legal, political, military and intelligence aspects.

On this basis, the articles in this issue of the ELTE Law Journal examine governmental and other policies and actions that constrain or prevent the use of the Internet to create, distribute, or access information. As a Guest Editor of the ELTE Law Journal, I hope to foster a more comprehensive and detailed understanding of censorship and internet content restrictions by bringing diverse perspectives and expertise together. This is, perhaps, a small contribution to the long fight against digital authoritarianism.