PROGRAMME

Internet Fragmentation and Censorship

Are we heading to Splinternet and Cyber Sovereignty?

International Scientific Conference
organised by
Eötvös Loránd University (ELTE), Faculty of Law
in cooperation with
University of Bucharest, Faculty of Law
and
University of Zenica, Faculty of Law

March 22-23, 2024
Budapest, Hungary
Faculty Council Room

22 March 2024 (Friday)

8:30 – 8:50	Registration
9:00 – 9:05	Welcome remarks on behalf of the host institution • Krisztina Rozsnyai, Vice-Dean for International Affairs
9:10 – 10:30	Keynote Panel **Chair:** Gergely Gosztonyi (Eötvös Loránd University) • David Frautschy (Internet Society, ISOC) • Gabriella Schittek (Internet Corporation for Assigned Names and Numbers, ICANN) • András Koltay (National Media and Infocommunications Authority / Pázmány Péter Catholic University)
10:30 – 10:45	Keynote Q & A
10:45 – 11:00	Coffee break & Group picture
11:00 – 12:00	Section 1
12:00 – 13:00	Lunch break (all by themselves)
13:00 – 14:30	Section 2
14:45 – 16:15	Section 3
16:15 – 16:30	Coffee break
16:30 – 17:30	Section 4 (Rising Stars Section for PhD Candidates)

23 March 2024 (Saturday)

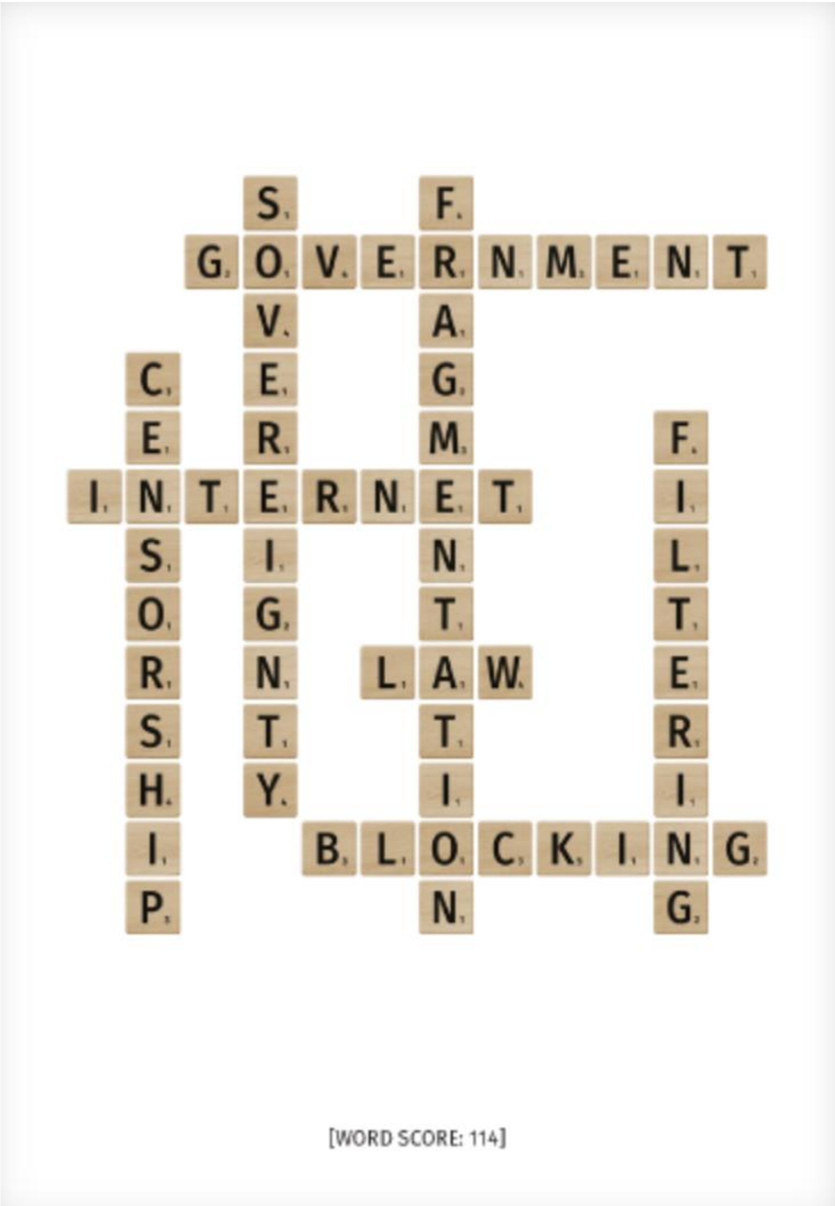
8:30 – 8:50	Registration
9:00 – 9:45	Keynote **Chair:** Gergely Gosztonyi (Eötvös Loránd University) • Joan Barata Mir (Cyber Policy Center, Stanford University / Future of Free Speech, Justitia)
9:45 – 10:00	Keynote Q & A
10:00 – 10:15	Coffee break
10:15 – 11:15	Section 5
11:30 – 12:30	Section 6
12:30 – 13:30	Lunch break (all by themselves)
13:30 – 15:00	Section 7
15:00 – 15:30	Closure

22 March 2024 (Friday)

11:00 – 12:00	**Section 1** **Chair:** Levente Nyakas (National Media and Infocommunications Authority) • Carmen Moldovan (Alexandru Ioan Cuza University of Iași): Mirror, mirror on the wall, who's the most authoritative of them all? Cyber sovereignty from a critical perspective • Zsuzsa Detrekői (Media and Journalism Research Center): Controlling Online Content: Exploring Technical, Legal, and Alternative Methods • Tuba Eldem (Fenerbahce University): Fragmentation and Future: Web3's Role in Redefining Internet Censorship and Governance
13:00 – 14:30	**Section 2** **Chair:** Zoltán Pozsár-Szentmiklósy (Eötvös Loránd University) • Paloma Rocillo (Institute of Reference in Internet and Society) – Paula Bernardi (Internet Society): Fragmentation of the internet in the global south: Instruments of segregation of impoverished populations **(Zoom)** • Shahram Akbarzadeh (Alfred Deakin Institute) – Galib Bashirov (Alfred Deakin Institute) – Ihsan Yilmaz (Alfred Deakin Institute): How does digital authoritarianism spread? The evidence from Muslim-majority nations **(Zoom)** • Elena Sherstoboeva (University of Essex): Navigating silence in the post-truth era: Russian judicial mythmaking, Internet censorship and the war against Ukraine • Zsolt Kokoly (Sapientia University): Filtering and blocking websites by governments – legal aspects in Romania
14:45 – 16:15	**Section 3** **Chair:** János Tamás Papp (Pázmány Péter Catholic University) • Joseph Squillace (Penn State University) – Roland Kelemen (Széchenyi István University) – Justice Cappella (Penn State University) – Richárd Németh (Széchenyi István University): Unveiling the Digital Divide: Internet Access as a Fundamental Human Right and the Persistent Challenge of IT Inequality • Ádám Farkas (Széchenyi István University) – László Vikman (Széchenyi István University): Information Operations as questions of law and cyber sovereignty • Márton Domokos (CMS Cameron McKenna Nabarro Olswang LLP): Navigating National Interests in the Cloud • István Harkai (University of Szeged): Signs of the Internet's territorial fragmentation in end-user license agreements of platforms
16:30 – 17:30	**Section 4 (Rising Stars Section for PhD Candidates)** **Chair:** Péter Báldy (Eötvös Loránd University) • Gergely Ferenc Lendvai (Pázmány Péter Catholic University): Hybrid Regimes and the Right to Access the Internet – comparative case studies from Turkey and Russia before the European Court of Human Rights • Xiaojuan Yang (Hildesheim University): The World Internet Conference and China's Promotion of Cyber Sovereignty • Tina Mizerová (Masaryk University): Disinformation as a symptom of distrust or security threat. Reevaluating legal responses to disinformation

23 March 2024 (Saturday)

10:15 – 11:15	**Section 5** **Chair:** Gergely Gosztonyi (Eötvös Loránd University) • Elena Lazar (University of Bucharest): The digital protectionism measures – a "carte blanche" justifying interference with human rights • Tamás Dezső Ziegler (Eötvös Loránd University): Technofeudalism – How big tech affects the splinternet • Boldizsár Szentgáli-Tóth (Hungarian Centre for Social Sciences) – Orsolya Zita Ferencz (Eötvös Loránd University): Internet as a platform of spreading misinformation during the period of cumulative crises: regulatory challenges and alternative solutions
11:30 – 12:30	**Section 6** **Chair:** Elena Lazar (University of Bucharest) • Simona Veleva (American University in Bulgaria): Transposing the Digital Services Act: Anticipating Challenges in Regulatory Implementation • Boris Kandov (University of Vienna): Regulatory Approaches for Algorithms on Online Platforms in the DSA • János Tamás Papp (Pázmány Péter Catholic University): Pluralism in the Online Space: Can the State Force You to Be More Informed?
13:30 – 15:00	**Section 7** **Chair:** Gergely Gosztonyi (Eötvös Loránd University) • Ivan Garcia Sala (University of Barcelona): The Franco regime's censorship policy in relation to Russian language textbooks • Adelina-Maria Tudurachi (National Institute of Magistracy): Internet access as a basic human right **(Zoom)** • Szabolcs Kéringer (Pázmány Péter Catholic University): Network enforcement: the future of platform regulation or a dead end? • Aneta Fraser (Adam Mickiewicz University): Manipulative Narratives in Post-Election Poland: Balancing Media Freedom and Responsibility • Stefan Bogrea (University of Bucharest): Intermediary liability in the EU: Human Rights and the DSA **(Zoom)**


GOVERNMENT
SOVEREIGNTY
FRAGMENTATION
CENSORSHIP
INTERNET
LAW
FILTERING
BLOCKING
[WORD SCORE: 114]

Keynotes

22 March 2024 (Friday)

David Frautschy
Senior Director for European Government and Regulatory Affairs
Internet Society (ISOC)

Threats to the Internet: getting the Internet Community in action

People around the world -those who have access to it, that is- just give for granted that the Internet will always be available, and fit for purpose. We have to raise awareness that this is just an illusion. The Internet is under threat and might be transformed into something else, something that is not open, globally connected, trustworthy and secure, if we don't stop this trend.

The Internet Society developed a project last year titled "Protecting the Internet from Fragmentation". Among the project deliverables, we created this explainer, that includes a list of identified threats, categorized by typology. It allows filtering by type of threat, by geographical region. Once a threat has been selected, any community member can understand what the risks are, what is ISOC's position and what we have done to work against it, including impact assessments if available. We hope it can be inspirational content for members of the Internet community, to identify, flag and organize a campaign on how to stop a threat – to help them with these tasks, we also created a detailed advocacy toolkit, which is a compilation of techniques to campaign and engage.

We are especially proud of the results of the OurNetcampaign, composed by a set of videos by our Internet Heroes, inspirational stories of people from the global South that are facing Internet threats themselves, encouraging others to take action. These videos have been a great success in social media. The fragmentation simulator is another valuable resource to raise awareness of the threat of fragmentation – the intention of this online game is to explain how it is to live without some of the great advantages that the Internet provides for day-to-day activities.

Finally, on an opposite tone of voice, we have developed the series Internet through the Ages, five short essays that remember all of us how the Internet has transformed our lives in key aspects, like relationships, education and work, entertainment, creativity and health.

Short bio

David is a Government Affairs professional with 22+ years of experience, 15+ of which focusing on telecom and digital regulations, trade policy and Corporate Social Responsibility. Telecommunications Engineer from the University of Alcalá (Madrid), plus master's in business administration from the EOI Business School (Madrid). He's experienced in implementing advocacy campaigns, building coalitions, coordinating cross-border teams, and translating complex technology issues into easily understandable language. David is impassioned about the power of the Internet to transform people's life.

Gabriella Schittek

Stakeholder Engagement Director

Internet Corporation for Assigned Names and Numbers (ICANN)

Internet Fragmentation: Challenges Ahead

The Internet Corporation for Assigned Names and Numbers (ICANN) is a technical organization, coordinating the Internet's unique identifiers, particularly the Domain Name System (DNS). Our mission is to ensure the security, stability, and resiliency of this system of unique identifiers on a single, interoperable Internet. This is done by a multistakeholder, bottoms-up, consensus-driven policy making model. Whilst the Internet today functions technically, a key challenge lies in the growing politicization of the DNS.

ICANN understands that legislation needs to be created to address real world issues, such as fake news, child abuse, human trafficking, arms sales and more. We cannot and should not stop these policy initiatives from being discussed.

However, it is crucial for policymakers engage with the technical community when crafting laws and regulations because the foundational aspects of the Internet inherently transcend national boundaries and must remain globally cohesive. The Internet's global nature can coexist with the rule of law, but ill-considered policies may lead to a fragmented Internet.

Short bio

Gabriella joined the Internet Corporation for Assigned Names and Numbers (ICANN) in 2007, having worked in various positions in the Internet industry since 2001. Her current role is Stakeholder Engagement Director, Nordic & Central Europe, which includes supporting the organization's engagement in the region with all ICANN stakeholders, including governments, private sector, civil society, technical community and academia. Gabriella is originally from Sweden but lives in Poland since 2006. She holds an MA in Political Science from the University of Passau.

András Koltay

President

National Media and Infocommunications Authority

Professor of Law

Pázmány Péter Catholic University

Censorship in the era of social media platforms

Social media platforms have overturned the previously known system of public communication. Now anyone can publish their opinion outside the legacy media, at no significant cost, and can become known and be discussed by others. Due to the technological characteristics of the Internet, it might also be expected that this kind of mass expression, with such an abundance of content, would necessitate the emergence of gatekeepers, similar in function to the ones that existed earlier for conventional media. The newsagent, post office, and cable or satellite services have been replaced by the Internet service provider, the server (host) provider and the like.

However, no one could have foreseen that the new gatekeepers of online communication would not only be neutral transmitters or repositories but also active shapers of the communication process, deciding on which user content on the Internet they deemed undesirable and deciding which content, out of all the theoretically accessible content, is actually displayed to individual users. Content filtering, deleting, blocking, suspending and ranking are all types of active interference with the exercise of users' freedom of speech and practices which also affect the interests of other users in obtaining information. In this way, a new, unexpected obstacle to the exercise of freedom of speech appeared, with the result that the earlier constitutional doctrines could no longer be applied without any change. The crux of the problem is that the platforms are privately owned; in formal terms, they are simply market players which are not bound by the guarantees of freedom of speech imposed on public bodies and which may enjoy the protection of freedom of speech themselves. The presentation addresses the issue of the restriction of freedom of speech by social media platforms in light of the recent EU Regulation in this field.

Short bio

András Koltay is Research Professor at the University of Public Service and Professor of Law at Pázmány Péter Catholic University in Budapest, Hungary. He received LL.M. degree in Public Law at the University College London in 2006, and PhD degree in law at the Pázmány Péter Catholic University in 2008. Between 2018 and 2021, he served as Rector of the University of Public Service He has been the President of the National Media and Infocommunications Authority of Hungary since 2021. His latest monograph, New Media and Freedom of Expression, was published by Hart in 2019. He is the co-editor of Blasphemy and Freedom of Expression (Cambridge University Press, 2017, together with Jeroen Temperman), Comparative Privacy and Defamation (Elgar, 2020, together with Paul Wragg), and Global Perspectives on Press Regulation, Vol. 1 and 2 (Hart, 2023 and 2024, together with Paul Wragg).

Keynote

23 March 2024 (Saturday)

Joan Barata Mir

Fellow, Cyber Policy Center, Stanford University

Senior Fellow, Future of Free Speech, Justitia

Public and private regulation of online speech and the role of online platforms: the Digital Services Act and beyond

Far from being a deregulated space, the Internet is probably the environment where the expression and dissemination of ideas, opinions and information is subject to a greater number of standards, rules and regulations established both by the state and by powerful private subjects.

More particularly, online platforms have been developing a sophisticated set of content governance or moderation policies. This rulemaking process is the consequence of an amalgam of factors including their own civility principles and values, business models, reputational constraints, investors and advertisers' pressures, as well as direct and indirect influence from relevant authorities. In consequence, the biggest current challenge is to guarantee that content moderation processes and interventions are accountable, particularly when it comes to errors and harm. The presentation will consider the nature and implications of private speech governance.

More in particular, it will be analyzed how the notions of illegal and harmful content affect content moderation policies and practices. The presentation will also consider how content is nowadays moderated by online platforms and the potential impact on freedom of expression may have on freedom of expression. Finally, it will focus on how to articulate proper procedural safeguards and human rights obligations to frame and preserve the exercise of freedom of expression under the intermediation of dominant online platforms.

In this context, special attention will be devoted to the adoption of the Digital Services Act (DSA) in the European Union, which has introduced significant changes to the regulation of online intermediaries, although intermediary liability exemptions remain exactly the same. The DSA acknowledges the importance of intermediaries, and particularly very large online platforms (hosting services that store and disseminate information to the public with a significant number of users), in facilitating public debate and the dissemination to the public of information, opinions and ideas, as well as in influencing how recipients obtain and communicate information online. It also warns that they may cause so-called societal risks. Based on these factors, the DSA does not define specific categories of illegal speech online, since this is already covered by the existing rules in the offline environment. Rather, it incorporates new important rights for users and obligations for service providers in areas such as terms and conditions, transparency requirements, statements of reasons in cases of content removals, complaint-handling systems, and out-of-court dispute settlements, among others. Beyond procedural safeguards, the DSA also contains a series of provisions obliging platforms to incorporate fundamental human rights to different aspects related to their content moderation policies.

Besides the importance of the DSA within the European context, it has also started to "inspire" proposals in other part of the world including Brazil, India or Nigeria. It is thus important to reflect on how the "European model" will permeate regulatory approaches in emerging markets and what are the risks associated to this trend.

Short bio

Joan Barata works on freedom of expression, media regulation, access to information and platform regulation issues. He is a Senior Fellow at Justitias Future Free Speech project. He is also a Fellow of the Program on Platform Regulation at the Stanford Cyber Policy Center. He has published a large number of articles and books on these subjects, both in academic and popular press. His work has taken him in most regions of the world, where he has provided legal support and analysed legal and regulatory proposals, trained judges and regulators and supported CSO advocacy efforts. He is regularly involved in projects with international organizations such as UNESCO, the Council of Europe, the Organization of American States or the Organization for Security and Cooperation in Europe, where he was the principal advisor to the Representative on Media Freedom. Joan Barata also has experience as a regulator, as he held the position of Secretary General of the Audiovisual Council of Catalonia in Spain and was member of the Permanent Secretariat of the Mediterranean Network of Regulatory Authorities.

Abstracts

Section 1

Chair: Levente Nyakas (National Media and Infocommunications Authority)

Carmen Moldovan

Mirror, mirror on the wall, who's the most authoritative of them all? Cyber sovereignty from a critical perspective

Freedom of expression does not describe the pattern of an ideal or perfect world; however, it contributes to the dissemination of different ideas and opinions, which is the essential feature of democracy. This function is supported by the use of Internet and the application of the normative equivalence doctrine in Cyberspace. The Internet has had a pervasive effect over communications and technology affecting and developing many levels of human activity and creating the Cyberspace which cannot exist in his absence. The term was coined by William Gibson who gave the best description compatible with the current evolution in Neuromancer.

Cyberspace and Internet are the creation of private actors, they are a global and open environment, constantly expanding and changing the world and human life. They are used by States and non-state actors, yet there is a lack of binding international regulations in this field. However, applicability of general principles and rules of International Law in this environment may not actually be contested or denied. At this point, there is a significant number of results of working groups or group experts (such as Cooperative Cyber Defence Centre of Excellence, UNGGE and OEWG) that analysed different legal concepts and the implications of cyber activities on their content and meaning. Yet there is still legal uncertainty towards the extent to which all the established principles and rules of International Law are applicable in this environment.

There is no legal or widely accepted or recognized definition for the term "cyberspace", "digital space", "online space", "responsible behaviour of States", thus creating an opportunity for States to give their own definition when it suites their interests. Generally, States are ambiguous on the meaning of responsible behaviour in cyberspace, thus leaving room for different interpretations. Trying to regulate aspects on Internet and Cyberspace may seem justified especially due to security reasons and the competences that the State should have on national security and applying the basic principles of International Law. Yet, only the Internet is related to physical infrastructure and may be subject to State sovereignty based on its territorial jurisdiction.

The aim of this presentation is to address one critical issue of the digital sovereignty concept proposed and developed by China and Russian Federation, namely the conflict with the obligation of States to guarantee freedom of expression and access to information. At the same time, this idea and the creation of a national Internet amounts to an authoritarian way to control access to information and the Internet which is contrary to the general obligation of States to protect these fundamental rights in the digital space by applying the general principles in this regard. In order to support this conclusion, the analysis will cover issues related to the features of cyberspace as an unregulated "territory" in International Law and to the status of the recognition of rules that States should apply to ensure a responsible behaviour in cyberspace.

At this point, there is no opinio juris suporting the existence of a State digital sovereignty having the content and meaning used by the China and Russia and in the future, the features and elements of this legal concept should be clarified. Until then, this is in fact a form of State control over information and communication content and means and a fragmentation of Internet and digital space.

Short bio

Carmen Moldovan is Associate Professor of Public International Law at the Law Faculty, Alexandru Ioan Cuza University in Iasi (Romania), Director of the Public Law Department and co-founder of the Centre for International Law at the Faculty. She also teaches courses on Freedom of Expression, and International Law for sustainable development. She holds a PhD in Law since 2012 (Criminal Law limits on the freedom of expression), a Postgraduate studies Diploma in Private International Law and a Bachelor Degree in Law from Alexandru Ioan Cuza University in Iasi. Carmen has carried out a series of teaching mobilities in International Law and human rights at Universities in Spain, the Czech Republic, and Italy. She attended courses at the Hague Academy of International Law, Bonavero Institute of Human Rights, the International Institute of Human Rights (Strasbourg) and has undertaken research visits at the European Court of Human Rights and Orleans University.

Zsuzsa Detrekői

Controlling Online Content: Exploring Technical, Legal, and Alternative Methods

In the last 25 years Internet has spread significantly with its new features (transfer content without borders real-time and sometimes in anonym form) and the world is struggling how to control it, whether to regulate it and if yes how. The purpose of the study is to examine the possible ways to control and regulate online contents and to provide a global picture of the ongoing tendencies.

Another objective of the study is to develop a sort of classified system of methods and means of internet controlling and regulation based on international tendencies. The study explores various technical tools from country level filtering (internet backbone, central ISP) through industry level filtering to end user-level filtering. In another chapter the study also analyses the different regulatory models (mentioning the specialties of the different types of content) from the regulation of content providers to the regulation of ISP including obligatory state-initiated regulation to self-regulation and the efficiency of these models in countries of various cultural backgrounds. In brief, the presentaton examines the influence of internet on the traditional jurisprudential concepts as well as the process of legislation, resulting in light or more severe internet censorship. To show the tendencies and to illustrate the methods the study uses more than 100 famous and less known stories from more than 70 countries from 5 Continents. Hopefully with the help of these stories it is easier to understand the global picture and reading is more entertaining.

Short bio

Zsuzsa Detrekői is a TMT lawyer and a part-time academic. She is a fellow at Media and Journalism Research Center. She was a consultant of OpenNet Initative at Berkman Center for Internet & Society at Harvard University for several months in 2007 and 2008. Zsuzsa was the general counsel of major Hungarian online content provider

origo.hu. She also provides legal support for the Association of Hungarian Content Providers. Her research area is online content and internet related regulations about what she wrote her thesis on and achieved PhD in 2016.

Tuba Eldem

Fragmentation and Future: Web3's Role in Redefining Internet Censorship and Governance

This presentation investigates how Web3 technologies, characterized by decentralized and blockchain-based infrastructures, can counteract internet censorship and influence the paradigms of global internet governance. With the rise of digital authoritarianism, the decentralized nature of Web3 presents an alternative model that may empower users and challenge centralized control. In recent years, decentralized autonomous organizations (DAOs), entities that are building blocks of Web3 using blockchains, digital assets and related technologies to direct resources, coordinate activities and make decisions, have experienced explosive growth. The total value of DAO treasuries has boomed from $380 million in January 2021 to a record $25.1 billion by December 2023, while the number of DAO participants increased by from 13,000 to 6.8 million.

Given the wide-ranging applications and private sector-led innovations of DAOs, it is essential for policy-makers, regulators, and industry leaders to cultivate a sophisticated understanding of these entities and their implications.This study will unpack the concept of Web3 by discussing the key underlying technologies and features, such as blockchain and DAOs, explore Web3's potential to bypass censorship, investigates how it challenges and potentially redefines concept digital sovereignty as self-sovereignty, discuss its likely impacts on the multistakeholder and multilateral governance frameworks of Internet, outline main regulations adopted by global actors and address the challenges that these emerging technologies likely to face. The study adopts a mixed-method approach, combining theoretical analysis with comparative empirical case studies analysing different state responses to blockchain, ranging from restrictive regulatory frameworks to embracing blockchain for governance purposes and synthesizes perspectives from computer science, political science, and legal studies on internet censorship and a distributed ledger-based internet (Web3) to provide a comprehensive understanding of the evolving landscape of internet governance. In doing so, it seeks to contribute to the debates on internet fragmentation and digital sovereignty by offering insights into how emerging technologies could either exacerbate or mitigate these trends, providing a nuanced understanding of the future of global internet governance.

Short bio

Tuba Eldem serves as an Associate Professor of Political Science at Fenerbahçe University in Istanbul and holds the position of Director at the Center for Cyberspace Studies within the same institution. Dr. Eldem earned her PhD in Political Science from the University of Toronto. She subsequently conducted postdoctoral research at the Research College of the Transformative Power of Europe, Freie Universität Berlin, focusing on the emergence and diffusion of security sector reform norms and the democratic control of armed forces.

Dr. Eldem's research interests span the intersection of international relations and comparative politics, particularly examining the interplay between international norms and domestic changes. She has contributed significantly to the academic field with publications on topics including International Cybersecurity Norms, Global Cyberspace Security, Global Cyberspace Governance, Critical Information Infrastructure Protection, and Turkey's

Cybersecurity Strategy and Cyberspace Governance. Furthermore, Dr. Eldem has provided expert analysis for think tank reports on national cyber power capabilities.

Section 2

Chair: Zoltán Pozsár-Szentmiklósy (Eötvös Loránd University)

Paloma Rocillo – Paula Bernardi

Fragmentation of the internet in the global south: Instruments of segregation of impoverished populations

The presentation proposes to investigate the regulatory instruments and economic models that affect internet access, with an emphasis on zero rating and mobile internet franchise. The central objective is to analyze how these practices contribute to network fragmentation, restricting the impoverished population's access to a limited range of online applications and services.

The debate about internet fragmentation is often accompanied by debates about censorship, internet access cuts by authoritarian countries or geopolitical practices. However, perspectives from the global south are still often invisible in this debate. Therefore, this study aims to understand how rights violations occurring in the global south, especially in Brazil, can also be breaches of internet fragmentation.

The research will adopt a multifaceted approach, combining qualitative and quantitative methods. For the quantitative perspective, primary data on mobile internet access will be cross-referenced to verify the potential enclosure of populations and fragmentation of internet access. For the qualitative approach, interviews will be conducted with experts in internet access policies to understand whether there is a collective and academic understanding of digital inequality arising from business models and permissive regulations being valves that increase the fragmentation of the internet.

As an initial hypothesis, theWe anticipate that the results will reveal the existence of a clear trend towards network fragmentation due to zero rating and data allowance limitations. It is expected to identify the prevalence of restricted access to a limited selection of applications, restricting the reach of information and limiting the opportunities available to the most impoverished population.

The presentation aims to contribute to an informed debate on internet access policies, promoting awareness of the challenges faced by the most impoverished populations and defending the importance of open and equal access to the world wide web.

Short bios

Paloma Rocillo is the Director of the Institute of Reference in Internet and Society (IRIS). Bachelor of Laws from the Federal University of Minas Gerais. IRIS Representative in the Working Group on Internet Access and in the Task Force on Elections in the Right on the Networks Coalition. Alternate member of ANATEL's Telecommunications Services Users Defense Committee (CDUST). Author of the books "Digital inclusion as public policy: Brazil and South America in perspective" (2020) and "Transparency in content moderation: National regulatory trends" (2021).

Paula Bernardi is a Senior Policy and Advocacy Advisor at the Internet Society. Experienced professional with a demonstrated history of working with public policy. Skilled in ESG, Political Science, and Public Policies implementation and analysis. Strong project management skills, with a M.Sc. focused on Environmental Governance from Albert-Ludwigs-Universität Freiburg, Germany.

Shahram Akbarzadeh – Galib Bashirov – Ihsan Yilmaz

How does digital authoritarianism spread? The evidence from Muslim-majority nations

In recent years, the optimism of the early 2010s has yielded to heightened concerns about the impact of digital technology on global democracy. Authoritarian regimes have responded to this trend aby heavily investing in advanced tools to monitor, analyze, and suppress dissent, extending their influence beyond restricting online speech and activism to shaping digital landscapes through controlled trolls, bots, and influencers. This transformation has given rise to the concept of digital authoritarianism, denoting the use of information technology by authoritarian regimes to monitor, suppress, and manipulate populations. The dissemination of technological, legal, and political tools globally since 2010 has penetrated countries where such regimes seek to consolidate power. However, existing research predominantly focuses on individual state policies, necessitating further exploration into regional and comparative dynamics.

In the Muslim world, characterized by tumultuous political developments in the twenty-first century, this study examines the diffusion of digital authoritarian practices across four countries—Egypt, Iran, Pakistan, and Turkey. Employing an analytical framework categorizing practices into online censorship, surveillance, deception, and legal restrictions, we identify three diffusion mechanisms: coercion, learning, and emulation within the region. Our findings indicate that since the late 2000s, these countries have implemented similar restrictive legal frameworks mirroring China and Russia's paradigms. The normative frameworks propagated by influential nations have gained traction in the Muslim world, where governments actively adopt practices for digital censorship and surveillance. China's role in advocating urban surveillance practices, utilizing diplomatic ties, loan arrangements, and normative influence, has been particularly influential. The successes of China and Russia have solidified digital deception and manipulation as integral components of digital authoritarian practices, with all countries in the region incorporating tactics such as troll farms and bot networks in recent years.

Short bios

Shahram Akbarzadeh is a Professor and a Deputy Director (International) of Alfred Deakin Institute, Deakin University, Australia and publishes on authoritarianism and foreign policy making in the Middle East.

Galib Bashirov is an Associate Research Fellow at Alfred Deakin Institute for Citizenship and Globalization, Deakin University, Australia. His research examines state-society relations and the impact of digital technologies on political processes in the Middle East and Central Asia. His previous works have been published in Review of International Political Economy, Democratization, and Economy & Society.

Ihsan Yilmaz is a Professor and a Research Chair in Islamic Studies at the Alfred Deakin Institute, Deakin University, Australia and has been doing research on citizenship, authoritarianism and populism in Muslim majority and minority contexts.

Elena Sherstoboeva

Navigating silence in the post-truth era: Russian judicial mythmaking, Internet censorship and the war against Ukraine

Russia's 'special military operation' in Ukraine, portrayed as peace-making by President Vladimir Putin, has reshaped global information flows and accentuated polarisation. This project aims to investigate the impact of Russian 'fake news laws' on the public debate surrounding the war against Ukraine within Russia. The study focuses on the role of domestic law and judiciary in shaping the truth in a climate of Internet censorship and the connections to Soviet Communist ideology and practices.

The research analyses over 500 Russian court decisions made between March 2022 and March 2023 that limit fake news about the war. Applying legal doctrinal methodology and Foucault's discourse analysis, this socio-legal project examines the narrative about the war constructed by Russian courts. A historical approach is used to interpret the Russian approach to limiting 'harmful lies' in the digital era through the lenses of Marxism-Leninism, the official ideology of Soviet Communist Russia.

The study argues that Russian courts make the truth in Russia conditional and loyalty to the government unconditional in a way, actualising Marxist-Leninist principles for guiding Soviet Communist media workers. The presentation shows how conditional truth and unconditional loyalty are used by domestic courts to monopolise public debate on matters of public interest within Russia, including on the war against Ukraine, and to restrict dissent under the labels of 'fake news' or Russia's hatred. The presentation also highlights how judicial mythmaking plays a crucial role in misrepresenting the war as a peace-making operation, using Internet censorship to silence opposing views. The study argues that the Russian approach is not a repetition of Soviet roots but rather an adaptation to modern Russia's government needs to consolidate the tools of state misinformation and Internet censorship during the war.

By using Russia as a case study, this presentation conceptualises conditional truth and unconditional loyalty as distinctive verification tools and explores the global implications of modern fake news laws and court practices for digital authoritarianism and the post-truth era.

Short bio

Elena Sherstoboeva is a Lecturer in Media Law at Essex Law School, the University of Essex. Her recent research and expert projects focus on studying and comparing digital communication laws and policies in post-Soviet and Asia-Pacific contexts from free speech and other perspectives. Since 2011, Elena has collaborated as an independent legal expert with UNESCO, the Council of Europe, and OSCE Representative on Freedom of the Media.

Zsolt Kokoly

Filtering and blocking websites by governments – legal aspects in Romania

The need for filtering and blocking websites by the Romanian government has come to focus in the past years: the need for ensuring a stable legal framework and efficient procedures first presented itself during the Covid-19 pandemia, prompting a review of the collaboration procedures between the different NRAs.

The presidential decree instituting and prolonging the state of emergency during the Covid-19 pandemia has offered the legal basis for filtering and blocking websites by the Romanian government between March 2020 and February 2022, while also investing NRAs with additional competences. However, once the state of emergency was lifted, and almost simultaneously, the need to filter and block websites promoting fake news in light of Russian aggression on the Ukraine has became even more acute, new challenges presented themselves.

Currently, only the Romanian Intelligence Service as NRA in cyber intelligence has competence in blocking websites invoking as legal ground the legislation on terrorism, by requesting ANCOM (the NRA that regulates the Romanian electronic communications sector) to issue block decisions. DNSC as the Romanian national cyber security and incident response team has expertise and assistance attributions and has identified and forwarded to ANCOM in the past lists of websites promoting fake news, eliciting a legal debate on the necessary regulatory framework.

Short bio

Zsolt Kokoly graduated from the Faculty of Law of Law "Babeș-Bolyai" University Cluj-Napoca. He has a PhD in media law (2014). He is a senior lecturer at Department of Law at Sapientia University Cluj-Napoca since 2008. Areas of research: media law and new media, European business law, personality rights.

Section 3

Chair: János Tamás Papp (Pázmány Péter Catholic University)

Joseph Squillace – Roland Kelemen – Justice Cappella – Richárd Németh

Unveiling the Digital Divide: Internet Access as a Fundamental Human Right and the Persistent Challenge of IT Inequality

As a result of the enormous power of data and information technology mediums, it is imperative to better understand the utility in promoting and protecting Internet Access as a Basic Human Right. Due to the ubiquitous nature of how the Internet is now utilized by government, academia, businesses, etc., it is no longer feasible to classify the Internet as a luxury service accessible only to those with the financial means necessary. More importantly, however, is the direct byproduct of limited physical access to the Internet, an additional component of consideration reducing the likelihood of data verification. Individuals without direct access to the Internet will almost certainly be artificially constrained in their educational development and awareness of potential threats they face through the exploitation of media manipulation and misinformation, raising challenges in areas such as voting and political standing.

Technology Inequality is a driving force promoting the acceptance of Internet Access as a Basic Human Right. In academic parlance, the theory of 'Technology Inequality' stems from reduced or limited access to the Internet; a concept that develops over time as users' age. An inaccessibility to get online (Internet) using physical technology and equipment (e.g., computers, tablets, smartphones) is often due to a combination of factors beyond the individual's control, (e.g., economic stature, culture, and education). As the world has moved almost entirely online, users without Internet access are unable to perform basic tasks needed to successfully navigate everyday life, (e.g., civic services, communicating with government representatives, paying bills, ordering medication, receiving emergency news and weather updates, finding a home or place of employment, etc.)

Without adequate Internet access, an individual will accept their surroundings while internally adjusting for truth in the absence of the digital and physical equipment needed to verify the trustworthiness of the data received; a phase colloquially known as "trusted entitlement" where all data received is perceived as true and designated as "trusted," regardless of source, contention, or position. Unfortunately, without Internet access, elimination of "trust but verify," all data will be accepted as true. Thus, creating a unique situation where users with insufficient access to the Internet become more susceptible to media manipulation through Disinformation (typically done intentionally and purposeful with a specific objective; malice to cause harm or provoke violence of action) and Misinformation (unintentional; committed as a mistake without nefarious intent; considered as ignorance); a digital threat scenario known as "campaigns of war."

Failing to protect the Internet as a Basic Human Right, the disadvantage not only reduces users' overall quality of life but also possesses the theoretical possibility to have such a negative adverse effect that could lead to direct harm and even death. This research investigation will use a multiple case study approach to demonstrate the utility of providing Internet Access as a Basic Human Right, while showcasing the societal benefit associated

with providing Internet access to users. Moreover, the research will introduce the Theory of Technology Inequality to highlight the dangers of media manipulation as a byproduct of no Internet access.

Short bios

Joseph Squillace, PhD, is an Assistant Teaching Professor of Cybersecurity at Penn State University. Joseph received a PhD in Information Systems (DISS) with a concentration in Information Security from the College of Engineering and Computing at Nova Southeastern University (NSU), and a NSA Cybersecurity Certification. Joseph's research interests include Cybersecurity, Privacy, Information Privacy, Data Security and Ethics, Incident Response, Disaster Recovery, and Economics of Security Breaches. Joseph's current research includes Cyberbullying, DarkWeb, and Pedagogy of Cyber Education, and collaborating with researchers in Czech Republic and Hungary. Joseph previously published scholarly research in Cybersecurity, Privacy, Information Systems, and Computer Science domains.

Roland Kelemen graduated as a lawyer in 2015. He has been working as a lecturer at Széchenyi István University since 2015, currently as an assistant professor, and since 2017 he has been a part-time research fellow at the National University of Public Service. He obtained his PhD in 2022. My research activities cover the history of military justice, theoretical and historical systems of exceptional power and national security issues of cyberspace security. He has been awarded a Fulbright Scholarship, a PhD Fellowship from the Pallas Athena Geopolitical Foundation, and three times the National Young Talent Scholarship.

Justice Cappella is a Senior attending Penn State University. Justice is a Research Assistant and graduating in May of 2024 with a Bachelor of Science Degree in Business with a focus area in Management and Marketing and a minor in Project Supply Chain Management. Justice's research interests include Climate Change, Sustainability, Cybersecurity, Supply Chain, Project Management, Business. Justice is actively engaged in research examining Cyberbullying and improving the Pedagogy of Cyber Education Pedagogy through collaboration with research teams in the Czech Republic and Hungary. Justice has previously published scholarly research on eWaste, Economics of Security Breaches, and IoT Threats.

Richárd Németh graduated from both the Bachelor's and Master's Degree programmes at Széchenyi István University. He is currently a PhD Candidate and an assistant lecturer at Széchenyi István University. He run his own business as a copyeditor, and he is a proofreader and editor for a scientific journal. He published several papers in various fields and currently working on his first textbook. His research activities cover many fields, including gamification, 3D-visualisation, cybersecurity etc. His current research focuses on the impact of social media on society. He is writing his dissertation entitled "Disinformation and manipulation in social media".

Ádám Farkas – László Vikman

Information Operations as questions of law and cyber sovereignty

The transmission of information content in the digital space, or the restriction, obstruction or distortion of such content, is an extraordinary tool in the information age. States can be targets of information operations, regardless of their political system. For this reason, the ability to counter operations in the information space and the capacity to counter them is a fundamental issue for any state with a modern defence system. Information operations are

therefore a necessary tool for the self-defence of sovereign states in the 21st century. However, the question arises as to what legal and institutional framework can provide an appropriate basis for information operations in such a way that the framework does not react to ad hoc events but ensures a systemic response in the long term while upholding the fundamental values of the state. The presentation aims to contribute to the understanding of this problem by reviewing different nation-state solutions and by providing a conceptual framework that synthesises legal, political, military and intelligence aspects.

Short bios

Major Ádám Farkas was born in Hungary, 1988. He received the Master's Degree in legal and political sciences from Széchenyi István University in 2012 and the PhD in legal and political sciences from his alma mater in 2018. From 2013 to 2018, he was a legal advisor of the Hungarian Ministry of Defence. Since 2014 he is a soldier of Hungarian Defence Forces. From 2012 to 2015 he was assistant lecturer of the Department of Legal History at the Faculty of Legal and Political Sciences of the Széchenyi István University, Győr, Hungary. Since 2015 he is a research fellow of the Department Defence Law and Administration at the Faculty of Military Science and Officer Training in the University of Public Service, Budapest, Hungary. Since 2023 he is senior research fellow of the Department of Public and Private International Law in the Széchenyi István University. Since 2021 he is member of the European Centre of Excellence for Countering Hybrid Threats Expert Pools. Major László Vikman graduated in 2005 at the University of Pécs, Faculty of Law. Started career as a legal counsel at the Mayor's Office in Veszprém, working on procurement, local and EU funded development projects. After that was recruited to a regional level development agency. Later had an opportunity to work in managerial positions at municipal utilities companies, gaining real-life experiences in the topic of resilience. From 2017 is employed in the Hungarian defence sector, as a legal subject matter expert. At the moment researches in topics as cyber- and network security, hybrid warfare, resilience, constitutional and humanitarian law, and is a PhD Candidate at the Széchenyi István University in Győr.

Márton Domokos

Navigating National Interests in the Cloud

Balancing the benefits of cloud computing with the need to adhere to local laws and protect national interests is a complex challenge addressed by the concept of cloud sovereignty. Cloud sovereignty is particularly relevant in a globalized world where organizations and governments increasingly rely on cloud services to store, process, and manage vast amounts of data.

Cloud sovereignty refers to the concept that data and information stored in the cloud should be subject to the laws, regulations, and governance of the country or region where it is physically located. It emphasizes the idea that governments may be concerned about the potential risks associated with storing sensitive data outside their borders. The concept extends beyond technical considerations and has legal, political, and economic implications. Cloud sovereignty may influence decisions related to government contracts, data governance policies, and international agreements. CSPs also recognised the importance of addressing concerns related to cloud sovereignty with certain initiatives.

The purpose of this presentation is to analyse the following considerations:

- Why is determining the legal jurisdiction where data physically resides crucial?
- How can CSPs and users adhere to specific data residency requirements?
- How might the initiatives of CSPs align with existing legal frameworks and regulations governing data sovereignty?
- How can governments maintain control over critical data and enforce data residency requirements?
- What are the economic implications of sovereignty concerns for cross-border data flows?
- How does cloud sovereignty influence decisions related to government contracts and the implementation of data governance policies?

Short bio

Márton Domokos is a Senior Counsel in CMS Cameron McKenna Nabarro Olswang LLP. His areas of expertise: IT law, data protection law, e-commerce law, and cybersecurity law. He is an active participant of the Hungarian AI Coalition. He is a regular contributor to OneTrust DataGuidance, the global privacy compliance service, and is president of the Data Protection Board of the Direct and Interactive Marketing Association. He is a lecturer of the post-graduate IT law course of the University of Pécs and of the Data Science course of Kürt Akadémia. He is a member of the Artificial Intelligence Working Group of IVSZ (Association of IT, Telecommunications and Electronics Enterprises).

István Harkai

Signs of the Internet's territorial fragmentation in end-user license agreements of platforms

The issue of territoriality in copyright law has long been an area of in-depth and thorough research. The territoriality of copyright norms is an established fact, but it is also challenged by technological advances and a long-standing political process. Geographical determinacy is a crucial determinant of the cross-border flow of content enabled by various communication technologies. This is also reflected in the overall legal norms governing the issue. On the one hand, the digital space created by the emergence of the Internet allows for cross-border content delivery, while on the other hand, the free movement of goods and services, one of the four fundamental freedoms of the European Union, also appears to be incompatible with territorial copyright regimes.

There have been many attempts to resolve these contradictions in the European Union, and legal geography, a research method combining the interfaces of geography and law, can help to find a solution. Using this research method, this research takes a new approach to comparing the internal market and territorial fragmentation rules of EU copyright law and the contractual practices of platform providers, in order to answer the question of how geography determines the development of a legal area and how far these geographical and political boundaries can be crossed.

Short bio

István Harkai is a graduated lawyer and a fulltime member of the Institute of Comparative Law and Legal Theory as a senior lecturer. He is a holder of a Ph.D., he wrote his dissertation in the field of international and European copyright law with special regard to the overlap between the right of reproduction and communication to the public and the legal status of intermediaries. He published 62 scientific articles and book chapters in Hungarian and in English. His main research interest covers the questions of copyright and related rights in the age of Internet and digitisation, the legal status of intermediaries, the models of digital content dissemination. He published scientific articles not only in the field of copyright but in the field of International Relations and International Public Law with special regard to the legal status of maritime piracy and peacekeeping missions in Africa. As a senior lecturer he delivers lectures in the field of Comparative Entertainment Law, European and International Copyright Law, Comparative Law, Introduction to Hungarian Civil Law. Beside his research and teaching activity he is the coordinator of two postgraduate programs hosted by the Institute of Comparative Law and Legal Theory.

Section 4

Chair: Péter Báldy (Eötvös Loránd University)

Gergely Ferenc Lendvai

Hybrid Regimes and the Right to Access the Internet – comparative case studies from Turkey and Russia before the European Court of Human Rights

The liaison between authoritarian political governance and the right to access the Internet is anything but a simple question. From blocking access to YouTube and Google to systemically discriminating against a religious group, states such as Turkey and Russia – both often described as hybrid regimes – have been at the forefront of the polemic of the interpretation of access to the Internet as a freedom of expression issue. The presentation aims to delve into a comparative analysis of said hybrid regimes, explicitly focusing on the right to access the Internet as adjudicated before the European Court of Human Rights (ECtHR).

Both countries, exhibiting features of both democratic and authoritarian governance, have faced scrutiny for their policies affecting internet freedom. In the context of Turkey, the government's approach to Internet regulation has undergone significant changes in recent years. From concerns about free speech to restrictions on online content, Turkish cases such as the Ahmet Yıldırım case or the Akdeniz case highlight the delicate balance between political interests disguised as security issues and individual rights. Examining claims brought before the ECtHR, this study investigates how Turkish policies have fared in international human rights law, shedding light on the nuanced challenges posed by hybrid regimes to the right to access information online. Similarly, Russia, with its historical legacy and complex political landscape, presents a compelling case study in the global discourse on internet freedom. By scrutinizing cases before the ECtHR, the study explores the legal dimensions of Russia's approach to internet governance, providing insights into the tension between state authority and individual liberties within the context of a hybrid regime.

The presentation relies on the methodology of comprehensive case comparisons. This implies that the presentation's main objective is to outline the tension between the European understanding of Internet access as a human right and the political-legal measures of hybrid regimes through the principles set forth by the ECtHR. Subsequently, the study analyses twelve landmark cases from the above two countries, allowing for the historical overview of the judgements of the ECtHR and the evolution of the interpretation of Article 10 concerning access and engagement in the digital sphere.

Adding to the findings emerging from the above methodological considerations, the presentation analyses the implications of these cases beyond the immediate legal outcomes. It reflects on the broader impact of ECtHR judgments on shaping the discourse surrounding internet freedom in hybrid regimes and whether these decisions contribute to more robust protection of individual rights in the digital age. The study also explores potential avenues for improving internet governance in hybrid regimes through international legal mechanisms. The latter is of critical importance, specifically in the case of Russia, which ceased to be a party to the European

Convention, envisaging an ambiguous landscape for the protection of freedom of expression, possibly setting up a “system of digital divide” empowered by political means.

Short bio

Gergely Ferenc Lendvai is a PhD Candidate at Pázmány Péter Catholic University, Faculty of Law and a Research Fellow at the Information Society Law Center of the University of Milan. Gergely Lendvai is a visiting lecturer at Károli Gáspár University where he teaches media law and infocommunication law and the assistant coach to the Eötvös Loránd University’s moot team at the Monroe E. Price Media Law Moot Court Competition. His research focuses on the transdisciplinary understanding of media law and new media phenomena. Gergely Lendvai’s work is supported by New National Excellence Program of the Ministry for Culture and Innovation, NAWA Poland and the Rosztoczy Foundation.

Xiaojuan Yang

The World Internet Conference and China’s Promotion of Cyber Sovereignty

Despite ongoing criticism, the Chinese government has relentlessly hosted the World Internet Conference (WIC) for a decade. This research aims to explore the motives behind China’s persistent efforts, particularly focusing on its role in advocating cyber sovereignty. By employing Natural Language Processing to analyze its policy declarations, discussion themes, media coverage, etc. the study seeks to comprehend how China utilizes WIC to propagate its internet governance vision. The research evaluates the potential outcomes of this strategy, emphasizing its importance in understanding the evolving norms and practices of global cyber governance, especially in the context of the developing world. This research is important in decoding China’s influence on shaping the digital landscape, offering insights into the broader implications for international internet policy and governance.

Short bio

Xiaojuan Yang is a PhD Candidate in Hildesheim University in Germany. His research topic is cyber sovereignty, especially China’s cyber sovereignty. He has Master’s Degrese in International Relations from China Foreign Affairs University in Beijing and LUISS university in Rome, as well as Data and Discourse Studies in TU Darmstadt in Germany.

Tina Mizerová

Disinformation as a symptom of distrust or security threat. Reevaluating legal responses to disinformation

Ever since the US presidential election in 2016, the world has been aware of the spread of online disinformation. Most recently, the disruptive nature of online disinformation has been highlighted by the Covid-19 crisis and the Russian invasion of Ukraine. In the EU and its member states, there have been efforts to mitigate the spread of disinformation by using existing legal tools and creating new ones. Examples are The Code of Practice on Disinformation and the Digital Services Act in the EU and the Network Enforcement Act in Germany, which all focus on disinformation shared on the internet or social media platforms. During the COVID-19 crisis, Hungary

took a different approach and criminalised spreading false information that alarms the public or prevents government efforts to protect people in response to the coronavirus crisis. After the Russian invasion of Ukraine, the EU used sanctions to suspend the broadcasting of Russia Today and Sputnik because they were used to spread pro-Kremlin disinformation (Council of the EU, 2022).

Recently, Alcerbi Altai and Berriche (2023) have identified several misconceptions about the previous research on disinformation. Mainly, they claim the previous research focused too much on social media and overestimated their prevalence and circulation as well as impact and reception. To put it simply, not every like and share means that the person is misinformed, disinformation comprises a small part of people's media diet and traffic on trustworthy news sites is much higher than on untrustworthy ones (Alcebi et. al. 2023, 2 - 8). Therefore, they warn that the effects of online disinformation on public discourse are overestimated (Altay & Acerbi, 2023, s. 14) and the tendency to believe disinformation can be fuelled by different factors, such as lack of trust towards institutions or high partisan animosity (Altay, 2023, s. 6), that the relevant actors and measures may not pay attention to. On the contrary, disinformation is being used by foreign propaganda and has been labelled as a security threat by some actors (Mareš & Mlejnková, 2021, s. 76).

In the presentation, I would like to discuss current research as it has put the legal tools that were adopted to mitigate the spread of disinformation into a different perspective. With the perspective given by the current debate, I would like to analyse if the legal tools that were adopted to mitigate the danger of disinformation (and more broadly legal tools in general) are suitable and legitimate tools to prevent the spread of disinformation, as any legal tool aimed at preventing the spread of disinformation can have a chilling effect on the freedom of expression (Kleis Nielsen, 2021).

Short bio

Tina Mizerová is a PhD Candidate at the Institute of Law and Technology, Masaryk University. She holds a Master's Degree in Law, Political Sciences and a Bachelor in Journalism and Media Studies. Her PhD research focuses on the role of Legal Measures in preventing the spread of online disinformation.

Section 5

Chair: Gergely Gosztonyi (Eötvös Loránd University)

Elena Lazar

The digital protectionism measures – a "carte blanche" justifying interference with human rights

Blocking users' access to content with the apparent aim to protect them from illegal content has proved to be an excessive measure in some situations. For example videos from YouTube showing content from the war in Syria or Ukraine, published online with the aim of drawing the worlds' attention on these atrocities, has been removed, being considered as illegal. Furthermore, banning access to certain content to poor populations like indigenous people also has e negative impact on human rights. The flagging of content by social media companies has also led to some drastic responses by governments, around the world, including major disruptions. Another example that we could bring is that of the Nigerian government announcing the indefinite suspension of Twitter after the platform deleted a post from President Buhari's account saying it violated company policies. Nigeria's major telecommunications companies had blocked millions from accessing Twitter, and Nigerian authorities threatened to prosecute anyone who bypassed the ban.

From our point of view, shutdowns or blocking of content like the ones illustrated above matter because they restrict people's ability to access information, also affecting other rights including work, health and education. They also have massive economic costs and undermine development. As such, where should one draw the line on this digital protectionism?

Short bio

Elena Lazar graduated from the Law Faculty of the University of Bucharest and from the Franco-Romanian College, Paris I Panthéon-Sorbonne. She continued with a Master's Degree in International and European Business Law, Paris I Panthéon-Sorbonne and a Master's Degree in Private Law, at the Law Faculty of the University of Bucharest. Since 2015 she is Doctor of Law (magna cum laude) of the Faculty of Law of the University of Bucharest, in the field of Human Rights. In the same field and within the same institution she completed a postdoctoral degree in 2019, also following a postdoctoral internship in New Technologies Law at the University of Paris Panthéon Assas, in the fall of 2020. She is currently a lawyer at the law firm „Lazar Elena", specialized in European human rights law and new technologies law. After completing her studies, she joined the Law Faculty of the University of Bucharest, where she teaches as Associate Professor the courses of Public International Law, International Relations and Organizations, International Law of Minority Protection and European Internet Law. She has also been selected as an expert at the Council of Europe on the issue of Trafficking in Human Beings and on the enforcement of constitutional court decisions in the field of human rights. At the same time, she is executive editor of the Romanian Journal of International Law and executive director of the Centre for International and Transnational Law Studies.

Tamas Dezső Ziegler

Technofeudalism – How big tech affects the splinternet

The presentation connects the concept of technofeudalism, as used by scholars like Yanis Varoufakis, Alfred C. Yen and Katrina Geddes with the legal measures which opened the door for the creation of online fiefs controlled by big tech companies. It claims that splinternet is a necessary effect of internet fragmentation, when companies receive extensive rights to regulate, and as a result, states become powerless. The advantage of using a more comprehensive model to describe internet policies is that it has the potential to put different fields into a bigger picture. The lack of regulations on search engines, the problems of comment regulation and data protection are all connected to a system of rules, which were built to defend companies and enweaken the state.

The first part of the presentation explains how EU law made technofeudalism a reality. Many rules in the EU's legal system cemented big tech into the position it has today. Such rules can be found in EU tax provisions, rules on mergers, consumer law, among more specific, internet related provisions. Second, it explains that in a technofeudal system where tech companies receive extensive rights to censor and manipulate content, many will depend on the good will of these companies. As a result, they reshape our societies according to their own interests.

Short bio

Tamás Dezső Ziegler is associate professor at Eötvös Loránd University (Budapest, Hungary). His major is EU law and European studies (including the interdisciplinary analysis of public policies and political aspects of legislation). Even though he is a lawyer, he finds the social and political science background of law and policy-making by far more interesting than the positivist analysis of actual paragraphs. He started his career at Baker & McKenzie Hungary and Nagy & Trócsányi Attorneys-At-Law. Later, he taught at several Hungarian universities including Corvinus University Budapest, Karoli Gaspar University School of Law, Edutus College (College for Modern Business Studies) as well as at the National University of Public Service, and also worked as a research fellow at the Institute for Legal Studies of the Hungarian Academy of Sciences (Budapest) for more than a decade.

Boldizsár Szentgáli-Tóth – Orsolya Zita Ferencz

Internet as a platform of spreading misinformation during the period of cumulative crises: regulatory challenges and alternative solutions

The development of the online space and social media has an enormous impact on the communication environment. These developments, alongside the extraordinary events of the last few years, such as Brexit, migration crisis, climate change, COVID-19, the Russo-Ukrainian conflict and economic recession, resulted in the exponential growth of fake news. As a response, numerous countries have enacted laws in order to avoid the alleged harm caused by misinformation spred mainly through virtual platforms.

One may identify three waves of recent legislative responses against social media misinformation. Firstly, before the outbreak of the global pandemic, amongst others, China, France, Germany, India, Singapore, Türkiye and the United Kingdom passed laws combatting the accelerated spread of misinformation through the internet platforms. The European Union has also considered the matter during this period several times. However, the number of legislation against fake news has drastically grown with the COVID-19 pandemic, therefore as part

of the second wave, Romania criminalized the spread of fake news about the virus, while Hungary's parliament has also passed a bill that envisages imprisonment for intentionally spreading harmful misinformation during emergencies. Moreover, Armenia, Bosnia and Herzegovina, Greece, Romania and Serbia also adopted similar legislation. The third emerge of anti-disinformation law can be associated with the Russia-Ukraine war. As a result of the conflict, in 2022, Russia implemented a law imposing imprisonment for spreading fake news about the military situation. To fight against Russian propaganda, the Council of the European Union suspended the broadcasting activities of Russian state-owned media outlets in the EU; moreover, around thirty European countries have introduced various restrictions of Russian propaganda channels.

Apart from the legislative steps, landmark judicial rulings are also worth-contemplating. To set three examples, in May 2023, the Supreme Court of the United States of America declined to impose secondary liability on tech companies for allegedly failing to prevent ISIS from spreading misinformation through their platforms. In September, the Supreme Court agreed to decide whether Florida and Texas may prohibit large social media companies from removing posts based on the views they express. In October, the Supreme Court also granted a request from the Biden administration to temporarily block a lower court's order that would limit the ability of government officials to communicate with social media companies about their content moderation policies.

In our presentation, we propose a new model to ensure the effective filtering of fake news with sharing the responsibility between the state, the platform operators and the platform users with the least possible restriction of freedom of expression. Our envisaged model to be detailed at the conference will provide primarily for platform operators the competence to identify fake news, however, this would be subject to judicial review, which could lead in the final instance to the sanctioning of individuals spreading misinformation, but also platform operators who do not comply with judicial rulings.

Short bios

Boldizsár Szentgáli-Tóth is the senior research fellow of the Centre for Social Sciences, Institute for Legal Studies. As a member of the National Laboratory of Artificial Intelligence he has published several contributions from the legal coverage of virtual platforms, especially from the latest challenges on freedom of expression.

Orsolya Zita Ferencz is a law student of the Eötvös Loránd University, she is expected to obtain her law degree in the spring of 2024. She is writing her thesis from the spread of misinformation through virtual platforms and the regulatory instruments to tackle the relevant challenges raised.

Section 6

Chair: Elena Lazar (University of Bucharest)

Simona Veleva

Transposing the Digital Services Act: Anticipating Challenges in Regulatory Implementation

The current study examines the legal aspects and challenges anticipated in the transposition of the Digital Services Act (DSA) into national regulatory frameworks. As the DSA represents a groundbreaking legislative initiative aimed at governing digital services within the European Union, this study explores some practical matters in terms of its implementation, the choices of the Member States countries for a Digital Services Coordinator, as well as potential hurdles faced by regulators in the transposition process.

The research explores the diverse legal landscapes within EU member states, highlighting the need for harmonization and the challenges posed by differing legal traditions and regulatory approaches, emphasizing the mportance of the European Commission in the regulation of the very large online platforms (VLOPS), the current practices and the future tendencies in this regard.

In addition, the study also highlights some complex tasks related to the enforcement the DSA's provisions, considering the technical and logistical challenges faced by regulators in monitoring compliance across a diverse array of digital service providers. The presentation investigates potential conflicts between national legislation and the harmonized rules set forth by the DSA, with a focus on striking a balance between uniformity and flexibility to accommodate national legal traditions.

Short bio

Simona Veleva is a lawyer and a PhD in the field of Constitutional law. The focus of her work is the right to freedom of expression, human rights in the digital sphere, copyright, media law and ethics. Simona is a Member of the Council for electronic media – the Bulgarian media regulator. She is an expert with the Digital Freedom Fund and the Centre for Freedom and Media. Simona teaches Media Law and Ethics, Human Rights in the Digital Sphere and Intellectual Property Law at the American University in Bulgaria. She contributes to the Global Freedom of Expression database at Columbia University and participates in numerous working groups, related to the transposition of the EU legislation in the field of media and media regulation in Bulgaria.

Boris Kandov

Regulatory Approaches for Algorithms on Online Platforms in the DSA

With the seemingly exponential advancement of technology, algorithms are becoming more powerful and intricate, especially with the rise of AI. While the AI Act is still in the proposal stage, existing Union law already governs the use of algorithms on online platforms, addressing potential risks and challenges associated with their

use. The Digital Services Act (DSA) introduces new regulations concerning algorithm-based, automatic filtering systems into EU law. This presentation delves into an analysis of the relevant Articles in the DSA that pertain to these algorithms. These regulations are particularly relevant for online platforms where algorithms, in the form of filtering and recommendation systems, are deployed. While they assist in content moderation and enhance user experience, their use can also lead to potential negative implications. This includes the spread of misinformation, hate speech, and other harmful content on online platforms, which can significantly impact democracy and societal cohesion. The DSA aims to ensure that algorithmic systems are used transparently and responsibly.

In the broader context, these technological advancements and their implications intersect with human rights concerns. The unchecked spread of harmful content can infringe on individuals' rights to safety, dignity, and accurate information. Ensuring that these algorithms operate transparently and responsibly is not just a matter of technological governance but also a fundamental human rights imperative.

Short bio

Boris Kandov has been a research associate at the Institute for Innovation and Digitalization in Law since 2022. After studying law at the University of Vienna, he worked as an associate at a media law firm in Vienna and has completed his Master's Degree in housing and real estate law, where he was specializing in the topic of "tokenization" in real estate law in his master's thesis. His research at the Institute focuses on the current topic of liability for online platforms. The analysis relates in particular to developments in Austria and the European Union.

János Tamás Papp

Pluralism in the Online Space: Can the State Force You to Be More Informed?

Media pluralism, fundamentally, involves a diversity of media sources and perspectives accessible to the public, ensuring representation of various societal groups and preventing dominant narratives. Historically, media sources were limited, often dominated by affluent segments due to high entry barriers. However, the advent of the internet significantly lowered these barriers, democratizing content creation and enhancing media pluralism. This transformation allowed underrepresented voices to be heard, but also introduced new challenges.

One such challenge in digital pluralism is the role of algorithms on platforms like social media, which may create echo chambers by prioritizing content aligning with user preferences, thus limiting exposure to diverse viewpoints. This phenomenon potentially undermines the concept of media pluralism. Moreover, the digital landscape raises concerns about the credibility of these diverse voices, emphasizing the need for differentiating fact from fiction and adhering to journalistic standards in an oversaturated media environment. The role of the state in this context becomes a contentious issue. Some argue for state intervention to ensure exposure to balanced and accurate information, which could include regulating tech giants, establishing digital literacy programs, or creating state-produced content. However, the line between regulation and censorship is thin, and state-defined "truth" might not always be impartial, risking the suppression of legitimate dissent and democratic dialogue.

The diversity of information, a regular debate topic in traditional media, is amplified online. Key questions include measuring diversity, determining indicators for diverse mass media on platforms, defining

online diversity, and verifying measures taken. Personalized technologies in online services make objective verification challenging, as content varies for each user, unlike in traditional media. The algorithmic nature of platforms, while fostering internal pluralism, can ironically limit exposure to diverse views within the platform. Externally, the internet's lowered entry barriers have led to numerous content creators, but the dominance of tech giants can overshadow smaller entities, affecting their visibility. The abundance of online information, a sign of external pluralism, often blurs the lines between credible journalism and misinformation. The challenge lies in not just promoting pluralism but ensuring it is based on accuracy and reliability.

In my presentation, I will review the pluralism rules already applied in media regulation from the perspective of their applicability in the online space. My research methodology is essentially literature review and synthesis, supplemented by analysis and comparison of specific media law rules with EU regulation of online platforms, namely the DSA and EMFA provisions.

Short bio

János Tamás Papp, PhD is an Assistant Professor at Pázmány Péter Catholic University, Hungary, and a researcher of the National Media and Infocommunications Authority of Hungary. He has taught civil and constitutional law since 2015 and became a founding member of the Media Law Research Group of the Department of Private Law. His main research fields are freedom of speech, media law, and issues related to freedom of expression on online platforms. He has a number of publications regarding free speech, social media and media law, including a book titled „Regulation of Social Media Platforms in Protection of Democratic Discourses".

Section 7

Chair: Gergely Gosztonyi (Eötvös Loránd University)

Ivan Garcia Sala

The Franco regime's censorship policy in relation to Russian language textbooks

Like all of the fascist governments in Europe, the Franco regime incorporated the fight against communism and all forms of socialist revolution in its ideological programme. As a consequence, the regime always had an adverse relationship with both Russian and Soviet culture. Especially in the early years of the Franco regime, this animosity led to the banning and repression of books, films and every other form of cultural expression related to Russia and its literature, language and history. In the late 1950s, at the height of the Cold War, the regime emerged from international isolation thanks to its alliance with the United States. Although its anti-communist discourse continued unabated, the Spanish government authorised the teaching of the Russian language in the country's official language schools in 1959. However, the courses and the teaching materials employed were closely monitored by state officials. In the absence of Russian language textbooks, Russian language teachers turned to foreign, especially Soviet, editions.

Although a number of publishers were interested in publishing these books, before publication in Spain, they had to make it past the censors, who, in this case, intervened to prevent the spread of the socialist propaganda allegedly present in some of these texts. In this presentation, we will analyse the censorship reports corresponding to those textbooks, focusing on the personalities of the censors who examined the texts, the changes they made, and the role of the publishers in the censorship process. In contrast to other types of books, from which banned passages were usually removed, in the case of language textbooks, publishers had to propose new versions of the text in order to preserve its pedagogical goals.

Short bio

Ivan Garcia Sala is a researcher into literary translation, professor of Russian literature and literary translator. He has pursued his research and teaching career at the University of Barcelona; from 2002 to 2011 as an associate lecturer, and since 2011, as an associate professor. His research has focused both on the history of translation and on the textual analysis of translations of Russian literature into Spanish and Catalan. He is currently working on a Spanish Ministry project on Francoist censorship and Russian literature. As a translator he has translated the Russian and Polish works into Spanish (Lev Tolstói; Stanisław Wyspiański, Andrei Tarkovski).

Adelina-Maria Tudurachi

Internet access as a basic human right

Ubiquitous, evolving and merely essential. These appear to be a few of the most conspicuous traits of the Internet nowadays. What if suddenly your access to internet was restricted to a limited number of web pages or, even

worse, banned entirely? Taking this dystopic scenario a step further, what if the restriction or the ban impinged on a whole community? For the European space of freedom, security and justice delineated by the borders of the European Union (EU), these hypotheses appear to pertain only to Orwell's or Huxley's writings, yet other parts of the world seem to perceive these challenges as possible and even real. Bearing this assumption in mind, the present presentation aims to verify whether the EU actually provides its nationals a truly safe area as regards internet access, hence deepening the debate revolving around the legal nature of Internet access, an autonomous human right or a means enabling the exercise of others.

Firstly, this contribution outlines the European Court of Human Rights' case-law regarding Internet access, especially the most recent developments in this matter. The analysis focuses on the current legal architecture of the European Convention of Human Rights which does not expressly secure the right to internet access per se. Thus, the presentation puts forth the subtle interference between Internet access and the exercise of other human rights, e.g. the well-known freedom of expression and freedom of assembly, as well as the right to private and family life or the right to education. This presentation strives to underline the recognition and the standard of protection developed by the Strasbourg Court.

Secondly, this analysis aims to emphasize the EU perspective on the matter through the lens of the relevant case-law of the Court of Justice of the European Union (CJEU). Closely linked to the functioning of the single market, from the point of view of the Luxembourg Court, Internet access appears to have a prevalent economical dimension, hence enjoying a rather fade human right legal nature. It is the status of Internet access that the present contribution discusses in accordance with the current legal framework. In this point, the potential overlap between the Strasbourg and the Luxembourg perspectives is under scrutiny, in light of the provisions of Article 52 of the Charter of Fundamental Rights of the European Union (CFR).

Lastly, the limitations of the right to Internet access are assessed. It goes without saying that the geo-political international context nowadays reveals a rather tense configuration of the world scene. This could trigger governments or individuals to resort to restrictive measures that could affect access to Internet to a certain extent. Taking this into account, the presentation discusses the scale of legitimacy that is applicable to Internet access limitations in light of the previously analysed case-law.

Short bio

Adelina-Maria Tudurachi graduated the Faculty of Law, University "Alexandru Ioan Cuza" of Iasi. During her bachelor studies she benefitted from an Erasmus+ mobility of studies in Bordeaux, France, for one semester, at Faculté de droit et sciences politiques, Université de Bordeaux. Then, she pursued her studies with the joint Master's Degree within the Faculty of Law, University of Bucharest and the Faculté de droit, Université Paris 1 – Sorbonne that she graduated with the result "Assez bien". Currently, she is preparing to become a judge at the National Institute of Magistracy, in Bucharest, Romania.

Szabolcs Kéringer

Network enforcement: the future of platform regulation or a dead end?

For long, legislators around the world have been struggling with regulation of unlawful, potentially unlawful or otherwise undesirable user generated content, with special regard to hate speech and misinformation spreading uncontrolled on social media platforms. The 'traditional' notice-and-takedown approach seems unsatisfying in the era of the mass content sharing by users. In recent years, some European states have adopted new laws on the responsibilities and obligations of the service providers, placing them in a sort of simplified prejudicial position, and also threatening with the possibility of great fines.

The first noticeable and most significant act to date is the Network Enforcement Act (NetzDG) of Germany. We go through the main points of the structure of the act, its correlation with the criminal code, and of course the main idea and approach represented in the bill: the share and transfer of responsibilities. Due to the transparency requirements set by the NetzDG, the execution of the law is somewhat accessible based on the data published by the platforms themselves, so we can extract some statistics and conclusions also. The law had been widely criticised already during its codification (not to mention that two tech giants challenged to law before court), and these conclusions might offer some insight whether those fears were fairly grounded or rather just overreacting.

Nevertheless, the NetzDG is not the only network enforcement law in place, it has been followed by copycats, but some interesting versions also appeared, like the short-lived Avia Bill of France or a bill in Poland representing a 'reversed' approach. In this presentation, we also refer to these 'delicacies' to get a broader sense of the issue.

Short bio

Kéringer Szabolcs holds a university degree in law from the Faculty of Law and Political Sciences of Pázmány Péter Catholic University and practicing as an attorney in Budapest. As a lawyer, he provided counsel for media service providers in Hungary for many years, and recently he has been a collaborating expert of Hungary's Digital Strategy for Child Protection. He is currently working on his thesis on the responsibilities for third party content provision on the internet, as a PhD Candidate at Pázmány Péter Catholic University.

Aneta Fraser

Manipulative Narratives in Post-Election Poland: Balancing Media Freedom and Responsibility

The positive news that the democratic opposition had won a majority of seats in both houses of the Polish parliament was overshadowed by the anti-Semitic behaviour of a far-right lawmaker. The footage of him using a fire extinguisher to put out the Hanukkah candles went viral within an hour, both in Poland and around the world. As various newspapers and internet users began to comment on the scandal, the newly appointed speaker of parliament became the target of criticism for failing to control the escalating situation and allowing it to happen under his watch. It has not remained without reaction from the 'third corner of the triangle' (Balkin, 2018), many internet users, Polish citizens, who are polarised on the issue, and online one can find comments ranging from

those criticising the politician to extremist ones praising the politician for ‘his efforts towards a secular state and parliament, free of religious symbols’.

Perhaps unsurprisingly, instead of being inundated with positive news about Poland restoring the rule of law and returning as a significant player in European politics, the press has been awash with scandal, with some editors even going so far as to push the narrative of the Polish parliament as a scene of often racist and shameful behaviour. This leads us to wonder whether measures should not have been taken to counteract the spread of the video of the scandal, which was undoubtedly deliberate to distract public attention from the new government’s inauguration and its efforts to restore the rule of law according to European standards. Although libertarian theories, free media and even the desire to increase public awareness and knowledge could undermine such measures (Mill, 1859) we must also consider the consequences of the viral spread of the video and the ensuing controversies, bearing in mind that public communication requires structured and reasoned discussion (Ward, 2014), rather than harmful and hostile ranting.

Short bio

Aneta Fraser is a first-year PhD Candidate at the Department of Criminal Law at Eötvös Loránd University in Budapest. She has been studying issues related to the digitalisation of criminal proceedings at the Adam Mickiewicz University, Poland. Her current and developing area of research is artificial intelligence and criminal law, and more specifically, the context of ‘risk assessment’ tools used in criminal justice systems. As well as working on her PhD, she also enjoys exploring issues related to hate speech and freedom of expression. Privately, she has a keen interest in both Polish and foreign politics.

Stefan Bogrea

Intermediary liability in the EU: Human Rights and the DSA

The question of liabilities for online intermediaries has become of paramount importance in the European Union in the last decade. While freedom of expression is of paramount importance in a democratic society, it does, however, carry with it special duties and responsibilities. Many voices have called for a greater responsibility for large online service providers who act as intermediaries, while acknowledging the human rights implications of such liability. The recently-adopted Digital Services Act (DSA) is a new landmark in this field, and many provisions will certainly be subject to debate. This presentation will endeavour to approach the DSA from a Human Rights Perspective, acknowledging the global impact of the act.

Short bio

Stefan Bogrea is a collaborating professor at the Faculty of Law, University of Bucharest, where he teaches European Union Law at a BA level and Human Rights at a masters level. He has defended his PhD in European Human Rights Law (2023) and is a practicing lawyer in the Bucharest Bar Association since 2014. He is interested in Media and Tech Law, European Human Rights Law and European Union Law.