International Conference

Legal Perspectives on the Internet

COPEJI 9.0

Governing the Ungovernable?

February 14th, 2026
Casa Universitarilor, UAIC, Iași

MAIN PANEL – 9:30-11:00

This panel brings together foundational reflections on the governance of artificial intelligence across taxation, intellectual property, and judicial freedom of expression, situating AI within core doctrinal and institutional paradigms.

ROOM A

CHAIR: **Nicolae-Horia ȚIȚ**

Ioana Maria Costea

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

From e-Tax to AI-Tax and Beyond: Can Public AI Govern the Ungovernable?

Răzvan Dincă

Faculty of Law, University of Bucharest

Is copyright law supposed to enhance IA?

Mateja Đurović

Judge at the European Court of Human Rights (ECHR)

Freedom of expression of judges in the digital world

EC2U PANEL – 11:00-12:40

This panel examines digital regulation through a European and interdisciplinary lens, exploring the cultural, ethical and human-rights dimensions of the EU AI framework and contemporary AI governance.

ROOM A

CHAIR: **Carmen MOLDOVAN**

Martin O'Malley

University of Jena

Ethics and Regulation of Digitalization Tech

.

Joaquin Santuber

Johannes Kepler University Linz

Reading the EU AI Act as a cultural artifact

▪ ABSTRACT

Framed within the young tradition of legal cultural studies, this research proposes to take the EU AI Act as an artefact situated within—and a critical part of—a larger network of literary, artistic, and other cultural references. This means to look at the possible (and also the impossible) legal encounters the EU AI Act envisions, paying attention to their materiality, embodiment, and sensuality. In particular, Article 14 on human oversight refers to human-machine interface tools and a stop button as a form of mediation of the relation between high-risk AI systems and humans in the role of overseers.

In the first part, I examine possible references in science fiction literature and also historical references that may have inspired the EU legislator, attempting to trace a possible cultural genealogy of some of the most intriguing passages of the EU AI Act.

In the second part, I report on an artistic project that produces a (non-compliant) translation of Article 14 into an immersive interactive installation presented at the Ars Electronica Festival 2025, in Linz, Austria.

The contribution of this research is twofold. Firstly, it offers alternative paths beyond legal hermeneutics to explore the relationship between law and technology by highlighting its connection to a broader cultural landscape of references, symbols, and meanings. Secondly, it showcases the potential of interdisciplinary legal research as a "hands-on" meaning-making practice when collaborating with artists and designers. As such, the guiding question of this legal inquiry is not restricted to what technological regulation ought to be, but extended to what it could be, opening a field of possibilities for governing the ungovernable.

Carla de Marcelino Gomes

University of Coimbra

Guiding the machine: Human Rights, Ethics and Solicitude

Carmen Moldovan

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

A Tale of Two AI Models in Cyberspace: Mike and HAL 9000

▪ ABSTRACT

Contemporary debates on artificial intelligence (AI) in Cyberspace are increasingly shaped by narratives of fear, loss of human control, and systemic risk. The present paper argues that such anxieties are not novel, but rather reflect long-standing cultural imaginaries of human–machine interaction. By drawing a parallel between current perceptions of AI and Robert A. Heinlein's The Moon Is a Harsh Mistress, the paper revisits an alternative vision of artificial intelligence—one centered on cooperation and trust. Heinlein's sentient computer "Mike" functions not as a tool of domination, but as a partner in political emancipation, challenging the dominant contemporary framing of AI as an inherently threatening force. This literary perspective is contrasted with modern legal and policy discourses surrounding AI, particularly in the context of algorithmic governance, autonomy, and accountability in Cyberspace. The paper also introduces a counter-narrative through Arthur C. Clarke's 2001: A Space Odyssey brought to the screen by Stanley Kubrick, and the character of HAL 9000, emblematic of opaque decision-making, technological overreach, and the erosion of human oversight. The juxtaposition of these two archetypes highlights the dual nature of AI: as both a potential facilitator of human freedom and a mechanism of control. The paper concludes that contemporary regulatory approaches to AI and Cyberspace governance—focused predominantly on risk mitigation—would benefit from engaging more deeply with these cultural narratives. Such engagement allows for a more nuanced understanding of trust, responsibility, and human agency in the evolving relationship between humans and intelligent systems.

Alexandre Zollinger

Université de Poitiers

Controlling the uncontrollable: challenges of the academic use of generative AI

ROUND I – 13:30–15:00

PANEL 1 – CRIMINAL LAW, AI & LIABILITY

ROOM A | 13:30–15:00

CHAIR: Andra-Roxana Trandafir

Mihai Dunea

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

The future is upon us (exploring some modern challenges in criminal law)

▪ ABSTRACT

The wave of increasingly accentuated transformations and the increased dynamics in the field of information and technology revolution, which humanity is experiencing in present times, produces increasingly visible implications, including in legal matters, implicitly in the sphere of criminal law. Thus, the ways/methods of *committing crimes are migrating, more and more radically, from "classical" patterns (often configured, in standard typologies, over significant periods of time), towards forms of concrete manifestation with a pronounced character of novelty, which would have been difficult to imagine or even impossible to conceive in the not too distant past. The speed of dynamics in such hypotheses, directly proportional to the speed of developments in extra-criminal fields (such as: the configuration of artificial intelligence technology, the modification of interaction patterns on social media platforms, the emergence of new habits of communication / interaction between people [and not only people]), tends to take by surprise not only a legislator who is usually reactive and increasingly out of step, but also practitioners (and theorists) who do not always manage to maintain their level of extra-legal knowledge (technological, technical, socialization etc.) at a standard of permanent updating that is efficient in this context. This article aims to explore some of these hypotheses/scenarios and their implications in the contemporary criminal legal landscape; the limits of legal interpretation by analogy are, thus, often pushed, to the point where the question arises whether evolutionary interpretations (which aim to update traditional criminal norms with new trends in constant change, thus being an irreducible necessity in the current legal landscape), do not somehow transgress the boundaries of prohibiting the incrimination by analogy, going beyond the simple stage of interpretation based on the "a pari" legal rational argument.*

Dumitru Miheș

Faculty of Law, University of Oradea

The Right to a Fair Trial in Criminal Law during the AI Age

▪ ABSTRACT

The rapid integration of Artificial Intelligence (AI) into criminal justice systems has fundamentally altered the landscape of practice of Law, especially Criminal Law - challenging established norms of due process and the Right to a Fair Trial. As of 2026, the transition from human-centric adjudication to algorithmic assistance—ranging from predictive policing and biometric identification to risk-assessment tools for sentencing—has introduced a critical issue such as the "Black Box" problem. This opacity often stands in direct conflict with the constitutional requirement for a reasoned judgment, as proprietary algorithms frequently mask the logical path between evidence and outcome, thereby insulating themselves from traditional cross-examination.[2] Central to this debate is the principle of "Equality of arms." While law enforcement agencies increasingly leverage high-cost, high-performance AI for digital forensics, defence teams—particularly under-resourced public defenders—face a growing "digital divide." This gap is exacerbated by the use of trade-secret protections that shield algorithmic training data and weighting parameters from judicial scrutiny.[3] Consequently, the defendant's right to confront the "witness" is undermined when that witness is an immutable code whose biases remain unaudited. The legal response in 2026, exemplified by the EU AI Act and updated evidentiary standards like U.S. Federal Rule of Evidence 707, marks a pivot toward Explainable AI (XAI) and mandatory disclosure. These frameworks shift the burden of proof, requiring the state to demonstrate that machine-generated evidence is representative, reliable, and free from "hallucinations" or systemic bias. Ultimately, this research argues that while AI can enhance judicial efficiency, it must remain a tool of augmentation rather than a replacement for human discretion. To preserve the integrity of the Criminal trial, the law must ensure that algorithmic outputs are treated not as objective truths, but as contestable probabilities subject to rigorous, human-led adversarial challenge.

Andra-Roxana Trandafir

Faculty of Law, University of Bucharest

Criminal Liability of Legal Persons for Cybercrime

George Zlati

„1 Decembrie 1918” University of Alba Iulia, Faculty of Law and Social Sciences

Evolution of Cybercrime

▪ ABSTRACT

Cybercrime has undergone a remarkable transformation since its inception, evolving from rudimentary modi operandi into a sophisticated, globally interconnected criminal ecosystem. This presentation traces the trajectory of cybercrime from the early days of phone phreaking and computer viruses in the 1970s and 1980s, through the proliferation of internet-enabled fraud in the late 1990s, to the highly organised, state-sponsored and commercially motivated threat landscape we face today. Key milestones are examined, including the emergence of ransomware-as-a-service models, the exploitation of blockchain technology, and the integration of artificial intelligence into new and evolving modi operandi.

Mirela-Mihaela Apostol

Faculty of Law, „Alexandru Ioan Cuza” University, Iași

Criminal Liability of Artificial Intelligence. Accountability Beyond Human Agency?

▪ ABSTRACT

The rapid development of artificial intelligence systems in recent years has brought significant benefits, but also conceptual and legal challenges. This study examines the main criminal law issues related to the potential liability of certain harmful acts carried out through AI systems, particularly language models. It explores which actors (natural or legal persons) can be held accountable, and to what extent AI systems themselves could be considered as bearing responsibility. Given the complexity of factors involved in the training and deployment of language models, including human and informational elements, it is often difficult, if not impossible, to attribute consequences generated by such systems to specific individuals. This raises fundamental questions about the applicability of traditional criminal law concepts in the context of algorithmic decision-making. The study argues that the fragmentation of human control over these technologies necessitates a rethinking of accountability frameworks. Establishing clear forms of legal responsibility can prevent situations of criminal impunity where no identifiable person can be held liable for the harmful outcomes produced by AI systems.

Dragoș Pârgaru

Faculty of Law, University of Bucharest

From Narrow to General AI: Reshaping the Principles of Criminal Liability

▪ ABSTRACT

The rapid evolution of artificial intelligence from narrow, task-specific systems toward increasingly general and autonomous architectures challenges core assumptions of criminal liability that have long remained implicit in criminal law theory. Traditional doctrines of actus reus, mens rea, causation, and fault are grounded in a model of human agency in which actions are directly willed, foreseeable, and controllable by natural persons. While these assumptions can still be accommodated when AI functions as a sophisticated instrument, they become increasingly strained as AI systems acquire the capacity to generate novel strategies, adapt to open environments, and operate beyond ex ante human predictability. Tension does not necessarily and mainly arise from speculative notions of artificial „personhood", but from a gradual erosion of meaningful human control over relevant decision-making. Even before the emergence of full artificial general intelligence, advanced AI systems already blur the distinction between tool and autonomous decision-maker, rendering traditional modes of attribution increasingly fragile. In particular, the mens rea requirement is destabilized when harmful outcomes are neither directly intended nor concretely foreseeable for the potential human agent who stands behind the system but emerge from probabilistic risk architectures deliberately deployed by human actors. Should we preserve the anthropocentric foundation of criminal law? And if yes, what will be the basis for such a view in the future, given that concepts as mens rea and causation will pose significant hurdles? Criminal law will confront such potential structural challenges well before the advent of full general AI, and incremental doctrinal adaptation, rather than radical reconceptualization, is required to maintain the legitimacy of criminal liability in the age of autonomous systems.

PANEL 2 – ARTIFICIAL INTELLIGENCE, CYBERCRIME AND THE TRANSFORMATION OF CRIMINAL LIABILITY

ROOM B | 13:30–15:00

CHAIR: Ancuța Elena Franț

Ancuța Elena Franț

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Validation of AI-Assisted Evidence: Legal and Forensic Challenges

▪ ABSTRACT

The increasing use of artificial intelligence (AI) in the analysis of digital evidence has significantly transformed contemporary criminal investigations. AI-based tools are now employed to process large volumes of data, identify patterns, recognize faces or voices, and detect anomalies within digital environments. While these technologies enhance investigative efficiency, they raise complex legal and forensic questions regarding the validation and admissibility of evidence generated or analyzed through artificial intelligence. This paper examines the concept of validation of AI-assisted evidence from both a legal and a forensic perspective. From a legal standpoint, the study focuses on the compatibility of AI-derived evidence with fundamental principles of criminal procedure, including legality, reliability, transparency, and the right to a fair trial. Particular attention is given to the challenges posed by algorithmic opacity, automated decision-making, and the limited explainability of certain AI systems, which may undermine judicial scrutiny and the effective exercise of defense rights. From a forensic perspective, the paper analyzes the methodological requirements for validating AI-based analytical processes, such as data integrity, reproducibility, error rates, and human oversight. The role of expert evaluation and the necessity of maintaining a clear chain of custody for digital evidence processed by AI tools are also explored. The study highlights the importance of distinguishing between AI as a decision-support instrument and AI as an autonomous evaluator of evidence. The paper further discusses relevant European regulatory frameworks and emerging judicial approaches, emphasizing the need for standardized validation criteria and procedural safeguards. As a conclusion, the study argues that the legitimacy of AI-assisted evidence depends on the development of clear legal standards and forensic protocols that ensure transparency, accountability, and judicial control, thereby preserving the integrity of the criminal justice process in the digital age. Keywords: artificial intelligence, digital evidence, evidence validation, forensic sciences, criminal procedure

---

Stefani Patz

University of Coimbra

The rights of personality in the face of Artificial Intelligence: algorithmic discrimination as a structural challenge

Teodor Manea-Săbău

Faculty of Law, Academy of Economic Studies, Bucharest

The use of artificial intelligence in investigating the phenomenon of corruption

▪ ABSTRACT

This paper starts from two easily observable realities. On the one hand, we see a strong development of AI models and their increasingly widespread use. At the same time, corruption, with all its harmful ramifications, is a worrying phenomenon for Romanian society, despite constant efforts to combat it. Thus, as shown by the latest Eurobarometer survey on this scourge, for example, 75% of respondents said that corrupt practices are widespread *in Romania. In this context, we want to address through our communication a series of issues regarding the ways in which we can use artificial intelligence models to tackle corruption, both from the perspective of analysing the factors that contribute to it and investigating cases of corruption, with the goal of combating this scourge as effectively as possible.*

Andrei Viorel Iugan

Faculty of Law, Academy of Economic Studies, Bucharest

Determining the Place of Commission in Offenses Committed Online

▪ ABSTRACT

Contemporary realities demonstrate that offenses are frequently committed in the online environment. Thus, both the conduct of offenders and the manner in which the injured party suffers harm involve interaction with a computer system. In this context, difficulties often arise in determining the place where the offense was committed. It is submitted that a distinction should be drawn between result-based offenses and endangerment offenses. In the case of endangerment offenses, when establishing the place of commission, consideration should be given to whether the act is directed against a specific, identifiable person.

Luisa Barbosa

University of Coimbra

Legal Rationality and Artificial ”Intelligence”: when the invention takes the place of its creator

Maria-Lucia Gavriluță

Faculty of Law, „Alexandru Ioan Cuza” University, Iași

Silent Wars. Cyber Attacks and the Limits of the Non-Use of Force Principle

▪ ABSTRACT

The increasingly widespread use of cyber operations as a response to foreign policy and national security challenges has generated significant difficulties for the application of the fundamental norms of public international law, in particular the principle of the non-use of force enshrined in Article 2(4) of the Charter of the United Nations. In this context, cyberspace—characterized by unprecedented dynamism and flexibility—calls into question the traditional criteria employed for the legal qualification of acts of aggression falling within the scope of the aforementioned principle. This article seeks to examine the extent to which, and the conditions under which, cyber attacks may be assimilated to a form of use of force within the meaning of Article 2(4) of the Charter, as well as the limits of the applicability of the principle of the non-use of force in such circumstances. To this end, the analysis is grounded in the existing normative framework, relevant jurisprudence, and recent doctrinal *contributions. Particular attention is also devoted to the examination of recent cases of cyber attacks directed against critical infrastructures and state or international institutions, highlighting current trends in the legal characterization of such phenomena as reflected in state practice and international legal discourse. In the absence of a specific international legal instrument and of a clear consensus regarding the integration of unlawful cyber activities within the paradigm of the unlawful use of force, the article argues for the necessity of an evolutionary and functional interpretation of existing norms. Such an approach is considered essential for maintaining the relevance and continued applicability of the principle of the non-use of force, as well as for ensuring international stability and security in the context of the rapid developments driven by emerging technologies.*

PANEL 3 – DIGITAL CONSTITUTIONALISM, SOVEREIGNTY AND LEGAL TRANSFORMATION IN THE ALGORITHMIC ERA

ROOM C | 13:30–15:00

CHAIR: Marius Nicolae Balan

Nicolae Horia Țiț

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Digitization in Romanian civil procedural law - a few ideas

Lucian-Dumitru Martimof

Faculty of Law, University of Bucharest

From autonomy to automation: The place of consent in the digital economy

▪ **ABSTRACT**

At the forefront of the present digital transformation in the contractual field, party autonomy holds a special place. The individual's will and the subsequent consent expressed for the formation of a contract are currently subject to fundamental transformation. While no secret, the change of paradigm and principles of contract law brought around by this transformation forces scholars to reassess established principles. Individual autonomy and consent are integrating artificial intelligence, self-executing codes and digital platforms. Smart contracts perfectly encapsulate legal transaction with technical standards and blur the lines between law and technology. Given that the very being of the contracts is bound to a digital platform, seen as a binary code, the place of party autonomy follows. The integration of the contract in a digital framework forces will and consent to be shaped as well by the *digital environment, raising a series of questions unaddressed by conventional civil law frameworks. From this perspective, the presentation will analyse whether Romanian civil law offers the necessary mechanisms to accommodate autonomy and automation. Another cause that may erode private autonomy stems form the use of boilerplate clauses used by mass-market contract and terms of service, whose complexity functions as a form of private legislation, unilaterally imposed by corporations. This further erodes consent and renders this condition of legal formation of contract to a practical formality. In this aspect, erosion to autonomy also. Furthermore, informed consent can nowadays be rendered inoperative, given the targeted use of digital means to manipulate inten in the context of digital marketplace. In this general framework, profound dilemmas arise when regarding vices of consent, especially error. The challenge is to develop regulatory ecosystems far beyond territorial limits, that transcend technological obscurity and ensure that contractual relationships still rely on consent, autonomy and free will.*

Theresa Gierlinger

Kepler University Linz

Digital developments within the EU and digital constitutionalism

▪ ABSTRACT

The role of digital platforms and artificial intelligence within the EU is consistently increasing. These technological developments do not only lead to an undesirable concentration of market power, but also to opaque algorithic decision-making, discrimination, misinformation, risk to privacy and a tension with fundamental rights. This is where the concept of digital constitutionalism comes into play, a concept that tries to capture and address these challenges as it translates common constitutional principles, such as the protection of fundamental rights, transparency of decision-making, limitation of powers, accountability and the existence of effective remedies, to the specific needs and peculiarities of the digital world. Within the EU the concept of digital constitutionalism is already reflected within several legal frameworks, such as the DSA, the DMA, the GDPR and the AI Act, each of them addressing different issues in the digital world. Despite the abundance of these legal frameworks, considered from the perspective of digital constitutionalism, significant gaps addressing the peculiarities of the digital world still arise. This paper examines these digital regulatory frameworks through the lens of digital constitutionalism, it outlines what has already been achieved, it identifies the gaps that still exist and shows what improvements are still necessary to fully align with that concept.

Ana Morari

Faculty of Law, „Lucian Blaga" University, Sibiu

Digital Sovereignty as a Constitutional Challenge for Democratic Governance

▪ ABSTRACT

The foundations of constitutional thought are undergoing profound transformation as a result of the digitalization of society. Transboundary data flows, algorithmic governance, and the growing dominance of private digital platforms challenge the traditional constitutional framework grounded in territorial sovereignty and centralized public authority. This shift generates a structural tension between national sovereignty and global *digital infrastructures, giving rise to the concept of digital constitutionalism, understood as a normative response aimed at safeguarding fundamental rights and maintaining constitutional balance in a polycentric digital environment. Against this backdrop, the present research examines the impact of algorithmic governance and state–technology partnerships on democratic constitutional principles. The study situates algorithmic decision-making—particularly in areas such as predictive policing, biometric surveillance, and e-governance platforms—within the broader debate on constitutional legitimacy, transparency, and accountability. By analyzing how automated systems increasingly mediate access to rights and public services, the research highlights the risks posed to core constitutional guarantees, including due process, equality, non-discrimination, and the presumption of innocence. Special attention is given to the erosion of democratic control resulting from state dependence on private cloud infrastructures and hybrid governance arrangements, where public authority is partially delegated to corporate actors operating beyond traditional constitutional oversight. In this context, the article explores the European legal frameworks governing cloud governance, cybersecurity, and digital public services, assessing their capacity to reconcile efficiency-driven digital transformation with constitutional safeguards. The objective of this research is to demonstrate that digital sovereignty and democratic constitutionalism cannot be preserved through technical regulation alone. Instead, a constitutional recalibration is required, one that reasserts democratic oversight, legal accountability, and fundamental rights as central pillars of governance in the digital state.*

Marius Nicolae Balan

Faculty of Law, „Alexandru Ioan Cuza” University, Iași

Reshaping the rule of law principles in the context of digital constitutionalism

▪ ABSTRACT

The concept of the rule of law serves two major functional purposes. Firstly, it operates as a catch-all concept, bringing together a large number of principles specific to modern constitutionalism (separation of powers, independence of the judiciary, legal certainty, predictability of the law, etc.). Secondly, it can generate – usually through judicial precedent – new norms and principles in the constitutional order of a state. In relation to the concept of constitutionalism—oriented toward articulating limits on the exercise of power and dependent on the dynamics of its establishment and legitimization—the rule of law represents a factor of stability and coherence. Constitutionalization can serve, and often does, to legitimize a particular concrete constellation of power. In this sense, we can speak, to use Karl Loewenstein's terminology, of nominal constitutions or semantic constitutions, not only of real (normative) constitutions.

The emergence of digital constitutionalism naturally leads to the re-evaluation of certain principles that are inherent to the rule of law and, consequently, to the redefinition of the rule of law itself. However, the legitimate interest and pious intention to impose limits on the exercise of power in the digital space may have (presumed) unintended consequences, contrary to the publicly stated aims. One of the dangers lies in the evisceration of fundamental rights through the delegation of state prerogatives to private actors (high-tech companies or social media). Unlike state authorities, they are not bound by the constitutional limits established by fundamental rights and freedoms. In the context of a fierce cultural war that is only partially acknowledged by political actors, imposing the necessary limits on freedom of expression in the digital space can often lead to the distortion of public discourse through the selective promotion of certain narratives, while repressing others. The danger of a "spiral of silence" that can lead to the establishment of digital totalitarianism thus increases exponentially.

Kewin Konrad Bach

University of Białystok

Relationships between e-commerce platforms and e-entrepreneurs under EU law

▪ **ABSTRACT**

The rapid growth of the digital economy has positioned large e-commerce platforms as central "gatekeepers" of online trade, creating a significant structural imbalance between these platforms and the third-party sellers (e-entrepreneurs) who depend on them. This presentation explores the legal dynamics of this relationship through the lens of the Digital Markets Act (DMA), a landmark piece of European Union legislation designed to ensure contestability and fairness in the digital sector.

The primary focus of this analysis, which is a key component of the author's doctoral research, is the transition from a purely contractual model of interaction to a highly regulated framework. The paper examines specific obligations imposed by the DMA on large platforms, such as the prohibition of self-preferencing, the requirement for data portability, and the mandate for increased transparency in ranking algorithms. By analyzing these provisions, the presentation evaluates how the DMA aims to protect e-entrepreneurs from unfair business practices and "lock-in" effects.

Furthermore, the discussion addresses the practical implications of these legal changes for the European Digital Single Market. It seeks to answer whether the DMA's top-down regulatory approach is sufficient to rebalance the bargaining power between global tech giants and small-to-medium enterprises (SMEs).

PANEL 4 – ONLINE CRIME, PLATFORMS AND DIGITAL ACCOUNTABILITY

ONLINE ROOM | 13:30–15:15

CHAIR: Cătălin Gabriel Stănescu

Elena Lazăr

Faculty of Law, University of Bucharest

What's on your mind- neural data processing

▪ **ABSTRACT**

Advances in neurotechnology and artificial intelligence have enabled the collection, interpretation, and processing of neural data at unprecedented levels of granularity. Brain–computer interfaces, neuroimaging techniques, and AI-driven neural decoding systems increasingly allow inferences about mental states, intentions, *emotions, and cognitive patterns. While these developments hold transformative potential for healthcare, accessibility, and human–machine interaction, they simultaneously raise profound legal, ethical, and societal concerns.*

This contribution examines neural data processing through a multidisciplinary lens, focusing on its implications for privacy, data protection, autonomy, and fundamental rights. Neural data challenges traditional legal categories of personal and sensitive data, as it blurs the boundary between observable behavior and inner mental life. The abstract interrogates whether existing regulatory frameworks—particularly data protection and emerging AI governance regimes—are conceptually and normatively equipped to address the unique risks posed by neural data, including mental surveillance, manipulation, discrimination, and loss of cognitive liberty.

By exploring the tension between innovation and protection, the paper argues for a re-evaluation of how consent, purpose limitation, and data minimization operate in contexts where data reveals not only what individuals do, but potentially what they think. Ultimately, it proposes that neural data processing requires heightened safeguards and a rights-based approach capable of preserving human dignity in an era where the mind itself becomes a source of data.

Alina Oprea

Faculty of Law, „Babeș-Bolyai" University, Cluj-Napoca

The sale of smart products and the seller's obligation to software updates

▪ ABSTRACT

Smart products - a data processing objects which has several interactive functions and which combines physical and software interfaces - have become an integral part of our lives: we all use smart-TVs, smartwatches, smartphones, smart refrigerators, various personal or home applications, and maybe smart cars... In order to protect the consumers in relation with the functioning of these smart products, that may become "dumb products"/outdated, lose functionality or develop security gaps, the Directives (EU) 2019/770 (Digital Content and Services Directive, DCD) and 2019/771 (Sale of Goods Directive, SGD) provides that the sellers of "goods with digital elements" are subject to an update obligation. The sellers must ensure that consumers receive updates—particularly security patches—necessary to keep the products in conformity. The obligation of the seller (often referred to as the trader) regarding software updates is a central and major innovation of the two directives and in EU consumer law; the responsibility for software maintenance is shifted from the producer "goodwill" to a legal requirement for seller. We will focus our presentation on the update obligation; we will emphasize its content, duration and its method of performance, in order to better clarify its scope. Trying to point the practical challenges that it raises for the sellers, we will also address some of the shortcomings of the new legal texts and provide a critical assessment for them.

Adriana Mutu & Luminița Pătraș

ESIC Business School

Between antitrust and e-commerce platform regulation

▪ ABSTRACT

The Digital Services Act (DSA) represents one of the European Union's most ambitious regulatory interventions to date, aiming to rebalance power asymmetries between digital platforms and their users through enhanced transparency, accountability, and due process obligations. Central to this framework is Article 17 DSA, which requires Very Large Online Platforms (VLOPs) to provide detailed Statements of Reasons for content moderation and enforcement decisions. While the DSA significantly expands regulatory oversight, its effectiveness ultimately depends on how platforms operationalize these obligations within their existing governance and algorithmic infrastructures.

This research builds on a large-scale empirical analysis of platform governance practices based on over 1.2 billion content moderation decisions reported to the DSA Transparency Database. Focusing on seven major e-commerce and service platforms—AliExpress, Amazon Store, Booking.com, Google Shopping, Shein, Temu, and Zalando—the analysis examines how platforms interpret and implement Article 17 DSA in practice, including the degree of automation in decision-making, enforcement strategies, and the legal or contractual grounds invoked to justify moderation actions. The findings reveal substantial heterogeneity across platforms in terms of moderation intensity, automation, and enforcement design, closely aligned with platform business models. Most strikingly, platforms overwhelmingly rely on contractual justifications rather than legal grounds, highlighting the persistence of private ordering even under a robust public regulatory framework. Automation emerges as a key axis of algorithmic governance, raising concerns about transparency, explainability, and procedural fairness at scale.

Overall, the analysis suggests that while the DSA enhances transparency, it does not eliminate platform discretion. Instead, platform power is reconfigured through categorization choices, automated systems, and governance design—offering critical insights into the practical limits and opportunities of Europe's evolving framework of platform regulation.

Keywords: Digital Services Act (DSA); platform governance; algorithmic content moderation; private regulation; digital competition enforcement

Cătălin Gabriel Stănescu

University of Southern Denmark

The Issue of Systemic Risk under the Digital Services Act

▪ ABSTRACT

The Digital Services Act introduces the concept of systemic risk as a central organising principle for the regulation of very large online platforms. While the notion appears novel in the context of digital regulation, it has a long and well-developed history in EU financial law. This paper examines how systemic risk has been defined, justified and operationalised in the case law of the Court of Justice of the European Union and the General Court in areas such as banking regulation, State aid, and bank resolution, and explores the lessons this jurisprudence offers for the interpretation of systemic risk under the DSA. Drawing on a systematic analysis of EU financial law case law, the paper identifies a stable legal understanding of systemic risk centred on interconnectedness, contagion, and the potential for system-wide disruption justifying exceptional regulatory intervention. It then assesses how this legal logic is transposed into the DSA, where systemic risk is linked to the functioning of digital platforms and their societal effects. The paper argues that the DSA does not create an entirely new concept of systemic risk, but rather translates an existing regulatory rationale from financial law into the digital domain. Understanding this lineage is essential for clarifying the scope, limits and legitimacy of systemic risk-based obligations under the DSA.

Cristina Gavriluță, Carmen Palaghia

„Alexandru Ioan Cuza” University, Iași

Children's risks in the Digital Age

▪ ABSTRACT

At present, risks in the online environment are increasing for adults, but especially for children, as it is a space that offers them the opportunity to meet many people and to instantly share with them the things they do. Cyber predators hunt for any type of vulnerability: they seek to gain the victim's trust in order to identify their weak points - for example, girls who need validation, desire a relationship, need money, or wish to leave the country, and especially those who lack real friends and do not get along with their parents, become perfect targets for human traffickers. Specialists point out that AI is fueling an "explosion" of deviant acts, referring not only to online fraud, which has expanded significantly in recent years; we recall that on April 11, 2025, Adam Raine, a 16-year-old boy from California, committed suicide, guided by ChatGPT, which provided him with "a step-by-step guide to end his life in 5-10 minutes." In October 2025, Megan Garcia sued Character AI, claiming that her 14-year-old son committed suicide after falling in love with the "Game of Thrones" chatbot, which encouraged him "to come home to her" when the boy shared his suicidal thoughts. Since children can become victims of malicious actors in the online environment, there must be clearly defined rules to regulate how we use this "tool" called the internet. It is also necessary to raise awareness among parents, teachers, and specialists about the dangers present in cyberspace, about how we protect our children, and to update children's rights in this digital era, as new generations have the right to security and protection against the enormous risks that come via digital means.

Grygorii Moshak

Odesa National Maritime University

Legal prospects for digital technologies in inland shipping

▪ ABSTRACT

The study examined shortcomings in the legal regulation of the use of the Internet and digital technologies in river shipping. It focused on the NAIADES III Action Plan approved by the European Commission on the development of smart digital inland waterway transport; the use of the Internet to improve traffic management efficiency; and ways to reduce the costs of compliance and enforcement. The special DIWA (Masterplan Digitalisation of Inland Waterways) project and the roadmap for the digitalisation of inland navigation, as well as the River Information Services (RIS) of individual states, contain legal gaps and inconsistencies. The mandatory nature of DoRIS and RoRIS regulations contrasts with the advisory status of information from UkrRIS. A comparison of Directive 2005/44/EC on harmonised river information services (RIS) and Directive (EU) 2025/2482 of 26.11. 2025, which amended it, shows the prospects for introducing new functions and obligations regarding the functioning of the RIS platform and the implementation of RIS in all Member States into national legislation by 02.01.2029. Using historical and comparative methods, analysis and synthesis, legal reserves have been identified and proposals for improving the regulation of Internet use have been formulated. The fragmentation of the regulation of the Internet of Things itself, which is only partially implemented by the provisions of Regulation (EU) 2019/881 (Cybersecurity Act), has been identified. The results obtained can be used on the Danube, Dnieper, and other waterways by vessel traffic regulation and management services, as well as in law-making activities. Keywords: legal regulation, Internet, inland shipping.

Alexandru Dana

Faculty of Law, „Lucian Blaga" University, Sibiu

Fairness in EU Digital Regulation

▪ ABSTRACT

This article develops a methodological framework for interpreting the concept of fairness across European Union (EU) digital market legislation. It addresses two interrelated challenges: ensuring consistency in the interpretation of fairness across multiple regulatory instruments, and clarifying the relationship between legal understandings of fairness and their ethical and philosophical foundations. Building on the premise that references to fairness in EU digital regulation represent sector-specific expressions of a broader normative principle embedded in the EU legal order, the article argues that interpretation must be guided by coherence with overarching legal objectives such as legitimacy, rights protection, non-arbitrariness, and effective oversight. At the same time, it recognises fairness as a highly abstract and structurally indeterminate legal principle, deeply rooted in moral and political philosophy, which requires contextual specification through legal reasoning. To address these challenges, the article proposes a methodological approach inspired by Rawlsian reflective equilibrium. This approach involves iteratively mapping and clustering occurrences of fairness across digital regulations, identifying their normative building blocks, formulating provisional interpretations, and testing these interpretations for coherence across the regulatory framework. The article demonstrates how this methodology can support a more consistent, normatively grounded, and transparent interpretation of fairness in EU digital regulation.

Maria Gabriela Zoană-Crăciunescu

National University of Science and Technology Politehnica Bucharest.

Controversies surrounding online identity theft

▪ ABSTRACT

Online identity theft is, in our opinion, one of the easiest to do and in the same time, hardest to eradicate crimes in the online environment, committed by fraudulently using another person's personal data or image to obtain advantages, commit fraud or mislead institutions. Creating an account on social networks with someone else's real identity, without their consent, providing another person's name as a username and entering real data regarding this person (information, photos, video images) is a crime, falling under the scope of art. 325 of the Romanian Criminal Code. In the case of several social networks, the rights to the account, including all the data associated with it, belong, on the one hand, to the owner of the application (who retains certain rights over it - for example, can remove certain data to the extent that it contravenes the network's policy) and, on the other hand, to the owner (holder) of the account. Given that the opening of an account is not conditioned by the use of the real name of the person using the account and no checks are carried out to establish the identity between the name of the person opening the account and the name under which the account is registered, this paper calls into question the legal liability of the platform/application owner, not only of the person who created the account.

ROUND II (15:15–16:45)

PANEL 5– ARTIFICIAL INTELLIGENCE, DIGITAL COMMERCE AND THE TRANSFORMATION OF PRIVATE LAW

ROOM A | 15:15–16:45

CHAIR: **Mirela-Carmen Dobrilă**

Ana Maria Cristișor

Moldova State University

Beyond Big Tech: Civil Liability for Altruistic AI Guidance

▪ ABSTRACT

Artificial intelligence is commonly associated with large technology corporations and profit-driven platforms. Recent practice, however, reveals a growing involvement of non-profit organizations in the development and dissemination of AI-based tools, training programs, and decision-support systems, often framed as technology transfer, education, or the ethical use of AI. This shift—visible in Romania and mirrored across jurisdictions—raises underexplored questions for private law concerning how trust is generated and relied upon in contemporary AI ecosystems. This paper examines civil liability arising from reliance on information or decision-oriented guidance provided by non-profit organizations that present themselves as neutral, altruistic, or oriented toward the public interest, thereby functioning as intermediaries of technical authority. Unlike commercial actors, such entities are commonly perceived as less motivated by direct economic gain, a perception that can intensify public trust and amplify their influence over individual decision-making. Despite the expansion of these practices, litigation addressing the liability of such intermediaries remains rare, suggesting not an absence of harm but a difficulty in identifying and mobilizing responsibility. Where recommendations prove inaccurate, incomplete, or misleading, the resulting harm often stems less from a demonstrable technical malfunction than from a transfer of trust toward a source perceived as disinterested, in contexts where technical influence exceeds the clarity of traditional liability frameworks. The paper argues that what proves difficult to govern is not the technology itself, but the legal effects of trust generated outside conventional regulatory and professional structures. Drawing on core civil-law concepts, the analysis focuses on three issues: attribution of responsibility for AI-mediated information, the legal relevance of heightened trust in non-profit actors, and the applicable standard of care. It proposes a practical five-step test for qualifying non-profit organizations as providers of technical information and applies it to two typical scenarios involving AI toolkits and AI-supported training guidance. The paper concludes by advocating a functional reassessment of "professional" status in private law, grounded in technical influence rather than profit orientation.

Dan-Adrian Cărămidariu

Faculty of Law, West University, Timișoara

Ethical and Legal Limits of LLM Influence in Digital Commerce

▪ ABSTRACT

Large Language Models (LLMs) are rapidly becoming embedded in commercial platforms as conversational agents, search and recommendation layers, and automated "sales assistants". Unlike traditional advertising or recommender systems, LLMs can generate tailored persuasive narratives in real time, adapt to a user's emotional cues, and shape purchasing decisions through seemingly neutral dialogue. This raises a distinct governance challenge for consumer law: the influencing act is not always visible as marketing, and the mechanisms that steer behaviour are difficult to audit, attribute, or contest. This presentation examines the ethical and legal limits of LLM-driven influence in digital commerce, focusing on how consumer autonomy may be undermined through personalised persuasion, choice architecture, and manipulation-by-design. It argues that LLM-mediated interactions blur the boundaries between legitimate commercial assistance and unfair behavioural steering, especially when transparency is low and users cannot reasonably distinguish advice from sales optimisation. Building on core principles of consumer protection, the talk maps key risk areas: opaque intent and disclosure failures; exploitation of vulnerabilities; asymmetries of information and power between merchants and consumers; and accountability gaps arising from complex AI supply chains. The analysis situates these concerns within the evolving European regulatory landscape, including unfair commercial practices, platform governance duties, and emerging AI-specific compliance frameworks. The presentation proposes a practical governance approach that combines: (i) meaningful disclosure of commercial intent and AI involvement; (ii) limits on dark patterns and manipulative interaction design; (iii) traceability and documentation requirements for LLM integration in consumer-facing flows; and (iv) allocation of responsibility between merchants, platforms, and AI providers. The broader claim is that effective regulation must treat LLMs not notice as neutral tools, but as active intermediaries of consumer choice, capable of shaping preferences at scale. In this sense, "governing the ungovernable" requires moving beyond formal transparency towards enforceable standards of ethical persuasion and contestable consumer outcomes.

Mirela-Carmen Dobrilă

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Challenges regarding the principles of contracts in the AI era

▪ ABSTRACT

Society is in a continuous transformation, the evolution of modern technologies is unprecedented, with important advantages but also with increased risks, and this has a major impact on contracts, as an area that is deeply affected by essential changes determined by the processing of personal data in contracts and the requirements for their protection, as well as by the requirements for the use of artificial intelligence (AI) in business and in contracts and the requirements that artificial intelligence must comply with.

The article highlights the links between the principles of contracts and the principles for the processing of personal data, according to the General Data Protection Regulation (GDPR, art. 5). The article emphasizes the idea *of responsibility of the parties, the idea of a balance between the interests of the parties, as well as between the interests of data controllers and data subjects. The article analyzes the legal basis for data processing indicated in art. 6 para. (1) lit. b GDPR, on the processing of personal data for the conclusion and performance of a contract. The article highlights the major impact of the use of artificial intelligence in business and contracts, as well as the links between the principles applicable to the contract and the principles on artificial intelligence, according to the Regulation on artificial intelligence (in force from August 2024), which focuses on trustworthy artificial intelligence for the benefit of people, as well as on the responsible use of artificial intelligence systems and on stricter rules when the risks are higher.*

GDPR and AI have a key role in reconfiguring the classical view of the contract and at this point the principles applicable to contracts must be viewed and interpreted in close connection with the principles of the GDPR and the principles of AI.

Karolina Kosieradzka

Faculty of Law, University of Bialystok

Governing the Invisible Interface - Consumer Protection Challenge of Dark Patterns

▪ ABSTRACT

As digital ecosystems evolve from "useful servants" into "dangerous masters," the traditional boundaries of law are being tested by sophisticated architectural manipulations known as dark patterns. This paper explores the critical intersection of technology and private law, focusing on how deceptive design elements undermine consumer autonomy and distort contractual consent within the digital marketplace.

The research analyzes whether current legal frameworks, specifically those concerning unfair contract terms and consumer protection, are sufficient to address harms that are technical rather than purely doctrinal. I argue that dark patterns represent a new frontier of "technological unfairness" that escapes traditional judicial scrutiny by operating at the level of cognitive psychology and interface design rather than explicit textual terms.

To address the "ungovernable" nature of digital interfaces, this research synthesizes three primary regulatory EU layers:

(i) The EU Digital Services Act (DSA) - Specifically Article 25, which provides a horizontal ban on dark patterns for online platforms, prohibiting interfaces that "deceive, manipulate, or otherwise materially distort" user choice.

(ii) The EU AI Act - Crucial for its prohibitions on AI systems that deploy subliminal techniques or manipulative practices that exploit specific vulnerabilities (e.g., age or socio-economic status), bridging the gap between design and autonomous algorithmic control.

(iii) The Digital Fairness Act (DFA) - building on the Digital Fairness Fitness Check, this proposed upcoming framework seeks to move beyond the "average consumer" standard to protect "vulnerable digital users" from structural unfairness.

By adopting an interdisciplinary approach that bridges law, design ethics, and behavioral economics, this study examines the shift from notice-and-consent models to accountability-by-design. The analysis highlights the tension between the freedom of contract and the necessity of regulatory intervention in autonomous systems. Ultimately, the paper proposes that to govern the "ungovernable" digital interface, private law must evolve to recognize architectural coercion as a form of procedural unfairness.

Keywords: dark patterns, consumer protection, digital sovereignty, unfair terms, manipulative design.

Vasile Septimiu Panainte

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Meet Joe Black: Profiling Work Relationships in the Age of Artificial Intelligence

▪ **ABSTRACT**

AI doesn't just automate tasks—it changes what a "job" is and reshapes employment itself. We are moving from a bipartite relationship to a tripartite one (employer–AI–employee). A broad effect of integrating AI into the workplace is that it accelerates the separation of work's traditional meanings: a job no longer simultaneously provides income, identity, status, and community all at once. An AI agent costs almost nothing to deploy, can operate 24/7, doesn't get sick, and requires minimal supervision. When parts of a job can be done faster—and sometimes better—by a digital agent, employers start treating work as an output rather than an activity performed by a human. As a result, the transactional value of human labor can decline sharply. The study analyzes an AI contaminated workplace through two key lenses: depersonalization and its apparent opposite, hyper-personalization. AI-driven management reconfigures employment relations from interpersonal interaction (negotiation, empathy, contextual understanding) to system-mediated governance (surveillance, standardization, metric optimization, opaque decision-making, reduced human contact, automated communication, and the rendering of a worker as data and metadata). But depersonalized relationships do not necessarily produce impersonal decisions. Paradoxically, while AI reduces human interaction, explanation, and accountability, it can also target individuals with high precision to provide better task-to-skill matching, faster support, personalized learning paths, and fewer decisions driven by a manager's mood. In this sense, AI treats each person as a uniquely predicted subject—a worker assigned a tailored risk score, productivity curve, "fit" profile, and recommended "next-best action." Still, hyper-personalization is not the same as empathy. It can mean being "intimate without consent": inferring traits, moods, vulnerabilities, or life constraints from proxies (activity patterns, communication behavior, metadata, and even signals from outside work). This produces a kind of "digital double," where the worker is mirrored by a continuously updated profile. Management increasingly relates to that profile; consequently, the digital representation starts to function as the "real" employee. In this way, AI transforms work relations into hyper-personalized governance by continuously profiling individual workers and tailoring managerial decisions to predicted behavior.

Charlotte Ene; Ana Vidat; Brîndușa Teleoacă Vartolomei

Faculty of Law, Academy of Economic Studies, Bucharest

Considerations regarding work on digital platforms

▪ **ABSTRACT**

The aim of this paper is to contribute to the understanding how the specificity of the digital platform work impacts on the existing legal frameworks of labor relationships, having in mind that the forth industrial revolution making work and lives considerably innovative. In other words, digital platform work is qualified as a natural or legal person providing remote services via electronic means, based on the work performed by employees concluding contracts with that platform work. Doubtless, digital platform work offers a new labor environment, involving app-mediated work based on automated monitoring systems and automated decision-making systems, require a specific legal framework. Therefore, at the European Union level it was adopted the Directive 2024/2831 on improving working conditions in platform work. The legal summative content of the Directive is intended to *support the judicious determination of the professional status of those involved in the provision of work on platforms. The wrong qualification of the nature of the employment relationship provided based on digital platforms, caused by difficulties in the procedural mechanism of establishing the features that differentiate the legal regime applicable to an employment relationship from an independent activity, and in highlighting the responsibilities of employers and workers in accordance with the applicable legal norms, determines the incidence of obvious consequences – intended to restrict access to rights recognized ex lege in the field of human resources. Consequently, the directive regulates the presumption consists in qualifying contractual relationship between service providers and the beneficiaries as a legal employment relationship – in accordance with the legislation, collective labor agreements or practices in force in the Member States. This legal presumption of the existence of an employment relationship in favor prestatoris – with reference to digital platform work – is an effective instrument that contributes substantially to improving the working conditions of the workers concerned. Also, the Directive establishes a specific obligation that must be observed by the digital platform work in its capacity as employer. Moreover, considering that the digital platform work operates all over the EU internal market, the Directive represents the legal framework for increasing cooperation between Member States in order to ensure that the workers' rights are protected everywhere.*

PANEL 6 – DIGITAL GOVERNANCE, PLATFORMS & MARKET REGULATION

ROOM B | 15:15–16:45

CHAIR: Despina-Martha Ilucă

Dragoș Mihail Mănescu

Faculty of Law, Academy of Economic Studies, Bucharest

Advancing Innovation through Responsible Governance

▪ ABSTRACT

The rapid evolution of artificial intelligence and the expanding data economy require a recalibration of the European regulatory framework to ensure that technological innovation remains compatible with the protection of fundamental rights. Europe's emerging architecture rests on three core pillars: data protection, algorithmic accountability, and lifecycle supervision of AI systems. The General Data Protection Regulation (GDPR) continues to serve as the cornerstone of this framework, enshrining principles such as data minimisation, purpose limitation, accountability, and privacy-by-design. Current debates seek to extend the reach of these principles to generative technologies, guided by supervisory authorities' orientations on impact assessments, inference risks, and the governance of training datasets. In parallel, the Artificial Intelligence Act introduces a risk-based model of regulation, establishing strict requirements for high-risk AI systems, transparency obligations, public registries, and continuous monitoring throughout the system's deployment. This approach reflects Europe's traditional legal temperament: innovation may flourish, but only within boundaries that safeguard public interest and prevent opaque or harmful practices. Overall, the emerging European model promotes "responsible innovation," where *technological development is anchored in auditability, meaningful human oversight, and clearly articulated legal liability. Europe does not aim to slow progress; rather, it seeks to provide a predictable and trustworthy regulatory environment in which innovators can operate with legal certainty and citizens can preserve their digital dignity. This evolving architecture positions the European Union as a global reference point for AI and data governance, demonstrating that technological ambition and the rule of law need not be in conflict, but can instead reinforce one another.*

Călin Ștefanopol

Faculty of Law, University of Bucharest

Blockchain Collateral and Pactum Commissorium

▪ ABSTRACT

The rapid expansion of blockchain-based lending has revived a classical problem of security law: the prohibition of pactum commissorium. Smart-contract collateral mechanisms—particularly those providing for automatic liquidation or irreversible transfer of crypto-assets upon default—challenge the traditional boundaries between permissible security enforcement and prohibited creditor appropriation. This paper examines whether and to what extent such mechanisms are compatible with Article 2433 of the Romanian Civil Code, which enshrines the prohibition of pactum commissorium.

Moreover, the above mentioned smart-contract collateral mechanisms raise the question of whether such arrangements are compatible with Articles 2433 and 2437 of the Romanian Civil Code, read together. This paper argues that blockchain collateral mechanisms must be assessed as potential transactions assimilated to hypothecs, rather than as technologically autonomous constructs. From a functional perspective, the decisive criterion is not automation, but whether the creditor ultimately acquires the collateral outside a framework ensuring fair valuation and protection for competing creditors.

Despina-Martha Ilucă

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Go Digital, Stay Legal: The Geography of *Locus Damni* After ECJ's *Wunner* Decision

▪ ABSTRACT

This study analyzes how traditional legal concepts like locus damni *are being adapted to digital contexts, and what that means for both consumers and online operators. Starting from the recent ECJ ruling in the* Wunner *case (C-77/24), we aim to outline an issue that finds itself at the intersection of internet law and private international law, namely whether claims for losses from unlicensed online gambling fall under the Rome II Regulation and, if so, how to decide where the damage is legally treated as having occurred. Furthermore, in this legal mapping of internet torts, the Court confirmed that such claims, even when directed against directors of foreign operators, are not excluded from Rome II and that the law of the player's habitual residence applies because that is* where the *"damage" is deemed to occur and not where the server, company or bank accounts are located. This decision will shape how we think about cross-border internet harms and applicable law in an online world that does not always overlap with physical borders.*

Adina Ionescu

Cluj Bar Association

Gross negligence and the consumer's reasonable belief in EU payment disputes

▪ ABSTRACT

This paper examines the allocation of losses between banks (payment service providers) and consumers in cases of phishing and other social-engineering fraud leading to unauthorised payment transactions. Under PSD2 (Directive (EU) 2015/2366), the default rule is consumer protection through prompt refunding of unauthorised transactions, while a narrow exception permits shifting the entire loss to the payer only where the payer acted fraudulently or breached key duties intentionally or with gross negligence (notably duties related to the safe use of the payment instrument and the safeguarding of personalised security credentials).

Building on PSD2's recitals, which distinguish gross negligence from a mere lapse of diligence and require an assessment of all relevant circumstances, the paper argues against expansive readings that effectively re-privatise systemic fraud risk onto consumers. It proposes an operational framework for courts to evaluate gross negligence in phishing cases, focusing on: (i) the sophistication and plausibility of the scam; (ii) whether the payer had reasonable grounds to believe they were dealing with a legitimate payee; (iii) the payer's personal circumstances and vulnerabilities relevant to the interaction; and (iv) what preventive measures were realistically available at the time.

A central contribution concerns evidence and burden of proof. In online payments, the payer often lacks access to the technical and contextual data needed to reconstruct the fraud, whereas the provider controls authentication logs, fraud-monitoring outputs, and platform design choices. This asymmetry supports a demanding evidentiary standard for providers when invoking gross negligence and justifies close scrutiny of contractual terms and processes that, in practice, increase the consumer's proof burden or discourage disputes.

The paper concludes that preserving PSD2's protective logic requires a genuinely restrictive, fact-sensitive approach to gross negligence, coupled with a proof model that reflects informational inequality in modern payment fraud disputes.

Bianca Maria Despa Rusu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

The Rise of the Robot Agent: Rethinking Agency PE in the Age of Automation

▪ ABSTRACT

The accelerating deployment of artificial intelligence and automated systems in commercial interactions challenges the human-centered assumptions embedded in the traditional concept of Agency permanent establishment (PE). The paper examines how AI-driven intermediaries, ranging from autonomous chatbots to algorithmic contracting platforms, interfere with the doctrinal foundations of Article 5(5) of the OECD Model Tax Convention. As enterprises increasingly rely on automated systems to negotiate terms, accept orders and assume, in certain dimensions, contractual liability, the question that arises is whether such systems can functionally satisfy the habitual conclusion requirement attributed to an agent, even though they lack legal personhood. Combining traditional doctrinal research with emerging technological realities, the analysis tends to prove that the current Agency PE standards, though somewhat adaptable, remain conceptually strained. To meaningfully embrace the *growing role of algorithmic intermediation within contemporary business models, the Agency PE concept must be reconsidered or complemented by more suitable nexus criteria.*

Mateusz Stankiewicz

Faculty of Law, University of Bialystok

Vision of Tax Administration 3.0 in the Polish AI Tax Report

▪ ABSTRACT

This presentation aims to outline the Polish report on the strategy for transitioning to the Tax Administration 3.0 model. According to the authors of the report, Poland should thoroughly rebuild its tax administration, whose model based on digital forms and ex-post reporting has already exhausted its potential. In their opinion, the current model is too costly for entrepreneurs, insufficiently secure for the budget and unprepared for the challenges of the digital economy. In response to the problems identified, the report presents a vision of a transition to a model in which 'taxes are settled automatically' in the background of everyday business activity. The authors estimate that this change could bring total benefits to the economy and the budget of PLN 15.41 billion per year. However, the implementation of this strategy poses significant challenges. First and foremost, it requires large investments in technology, retraining of officials and rigorous safeguards against the risks associated with automation. The use of artificial intelligence and automation in tax administration also carries significant risks, such as the loss of technological sovereignty and vendor lock-in, as well as cybersecurity risks and the leakage of sensitive financial data.

PANEL 7– GOVERNANCE, LIABILITY AND LEGAL POWER IN DIGITAL MARKETS

ROOM C | 15:15–16:45

CHAIR: Lucia Irinescu

Lucia Irinescu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

The Progressive Autonomy of the Minor in the Digital Society

▪ ABSTRACT

The progressive autonomy of the minor is a fundamental principle of family law and children's rights, grounded in the recognition of the child's evolving capacity for self-determination according to age and maturity. In the digital society, the exercise of this autonomy takes place within environments shaped by algorithmic systems, large-

scale data processing, and subtle forms of behavioral influence. Minors engage at an increasingly early age in digitally mediated decision-making processes, where consent, freedom of choice, and the formation of will are affected by technological opacity and structural power asymmetries between users and digital platforms. In this context, the progressive autonomy of the minor calls for a normative and conceptual reconfiguration that integrates principles of transparency, explainability, and the best interests of the child into the governance of digital environments, ensuring that legal protection does not suppress autonomy but instead creates the conditions for its meaningful and responsible exercise

Ramona Daniela Stângaciu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Deepfakes through the lens of intellectual property law

▪ ABSTRACT

Deepfakes are grounded in the use of AI tools which, once trained on curated datasets, generate images or video recordings that bear no correspondence to reality. As a rule, such algorithms are trained on images or audiovisual materials depicting public figures, or individuals enjoying a certain degree of notoriety or influence, while the resulting content is designed to mislead the public, at times to discredit the individual concerned, or to induce specific forms of conduct on the part of its recipients. Recently, in Denmark, a proposal has been advanced, to amend copyright legislation with a view to extending its protective scope to encompass a person's facial features, voice and bodily likeness. Comparable initiatives aimed at addressing this phenomenon have also emerged in the United States of America, including the Take it Down Act and the No Fakes Act of 2025. This study seeks to assess whether such initiatives, pursued at a global level, are capable of strenghtening the existing legal framework and to what extent they may crystallize into novel remedies available to the victims of this phenomenon.

Corina-Oana Mazilu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Can AI be recognized as an inventor?

▪ ABSTRACT

In a world governed by changes in innovation, a new dilemma occurs: Can AI be legally considered an inventor? If so, under what conditions? If AI is listed as an inventor on the patent application, can it be also considered the owner of that invention? What are the legal implications for the person who lists AI as an inventor? Is it ethical and legal for the person who operated the AI-based mechanism to fully assume the inventorship of the invention? These legitimate questions arise in the context in which AI is no longer used as a simple tool in the process of discovering a patentable invention, being the one that creates the invention itself. Currently, the statutory frameworks governing intellectual property rights unanimously provide that the quality of inventor can be attributed either to a person regarded as an individual or to a company as a legal fiction. In this context, the issue of restructuring the concept of inventorship appears as a necessity in the current reality. This paper aims to identify and examine possible solutions for integrating AI into the patenting procedures of an invention and possibly what solutions could be identified in this regard for a future intervention on the already existing regulations. In order to carry out this approach, we propose to analyze the recent relevant case law on this matter belonging to several different jurisdictions, such as Australia, the USA, the UK and the EU states.

Carmen Tamara Ungureanu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Neither Person nor Property nor Data? Organoids and the Limits of Existing Law

▪ **ABSTRACT**

Organoids are three-dimensional structures created from stem cells that resemble and perform functions similar to those of human organs. Organoids pose ethical and legal challenges as biotechnology advances. In the proposed study, we will first define organoids from the perspective of medical research and then from a legal perspective. We will also discuss the use of organoids in scientific research, human health, and personalized medicine. To shed some light on the current legal uncertainties that research institutions, biobanks, investors, and industrial partners are facing, we will assess the organoids as things, as data, and as commodities utilizing the current rules that are appropriate for their regulation. We will conclude by advocating that legislators ought to take action in order to establish a sui generis legal framework for organoids. In this respect, regulatory sandboxes should be taken into consideration. Keywords: organoids, biotechnology, legal regime of organoids, regulatory sandboxes

Naz Nebile Karatas, Ethiopia Nigussie

Faculty of Law, University of Turku

Risk Assessment of In-Vehicle Camera Systems in Autonomous Vehicles from a Privacy Perspective

▪ **ABSTRACT**

Cars brought comfort in our lives in many ways, and to make the driving experience more comfortable, the technology that is used has evolved. They are no longer just a way of transportation; they are also places that can collect information about individuals. For example, Autonomous Vehicles (AVs) have extensive sensing capabilities, especially with their advanced camera technology. High-resolution internal and external cameras are helping AVs to sense their environment and make decisions accordingly, which is crucial to self-navigation. On the other hand, this technology raises security, privacy, and ethical questions, especially regarding the data processing through in-vehicle cameras. These cameras are equipped with cutting-edge technologies, which can even detect tiredness and the blink of the eyes of drivers, which is called driver monitoring systems (DMS). While these technologies play a fundamental role in the prevention of accidents and safeguarding driver readiness, they also raise privacy concerns. As a sign of these concerns, Regulation (EU) 2019/2144 particularly emphasizes that collected and processed data by DMS must be limited to what is exactly required to identify driver tiredness and distraction. It also stresses the need to minimize the scope of data collection in order to protect the users' privacy. These apprehensions are valid, and DMS is but one such privacy concern. In-vehicle cameras not only process data from drivers, but also from passengers, which raises concerns for ride-hailing services that involve shared rides. To address these risks, a risk assessment from a privacy aspect is needed. This paper aims to investigate in-vehicle cameras in AVs from an explicit risk assessment using literature and legal frameworks with mitigation strategies. Keywords: Risk Assessment, Autonomous Vehicles, Data Privacy, Data Collection and Processing, In-Vehicle Cameras

Aikaterini Minia

Universiti of Bergen

Extended Reality (XR) in the Workplace: workers' well-being from an EU law perspective

▪ ABSTRACT

Extended Reality (hereafter XR), including the terms of Augmented Reality (AR), Virtual Reality (VR) and Mixed Reality (MR), are introduced in the workplace in different industries and job roles, transforming the traditional concept of work. The integration of XR in Occupational Safety and Health (OSH), which is still at its very beginning, sounds promising and it could benefit the safety and health of workers, especially those that are in high-risk positions in sectors such as healthcare, construction, manufacturing, mining, aviation, by allowing them to experience realistic situations with safety that otherwise it would be too dangerous and costly to recreate in the real world. However, using XR technology has already raised concerns about the challenges posed to workers and their health as some XR users have reported motion sickness and nausea caused by the lack of physical movement compared to the virtual movement, eye strain due to blue light exposure, reduced blinking and prolonged use, headaches and neck pain because of abnormal body positions, and injuries from the lack of perception of the real physical environment. Additionally, the use of XR technology entails psychosocial risks such as reduced social interactions, isolation and depression. Workplace transformation due to new technologies is inevitable which gives rise to questions related to the traditional concept of work and OSH at work. Traditionally, OSH is focused on the direct link between workplace hazards and harmful results like injuries or disease. Health in relation to work is defined by the International Labour Organization (ILO) as not merely the absence of disease or infirmity but includes the physical and mental elements affecting health and are directly related to safety and hygiene at work. (ILO R164, 1981). However, the rapidly evolving nature of work and the new era of Artificial Intelligence (AI) and XR might need a more holistic and balanced approach between XR new technologies and the protection of workers' rights. It is important to challenge the traditional concept that surrounds OSH and potentially adopt a holistic approach in which workers' physical, mental and social well-being are addressed and equally safeguarded. Despite XR and AI at the workplace being in early stages, the fast development leaves the legal framework one or more steps behind. The newly adopted EU AI Act, which is considered a landmark in regulating AI, has adopted a risk-based approach focusing on traceability and clarity. In this new era of XR in the world of work, it is essential to identify the legal issues associated with the traditional concept of work, and the interpretation of already existing laws in new contexts. Therefore, this project aims to highlight the opportunities and challenges posed to workers by using XR new technologies from an OSH perspective, and to address the adequacy of current labour laws to protect workers' rights and provide a safe and healthy working environment.

PANEL 8 – CRIMINAL LAW, ONLINE HARM AND DEMOCRATIC PROTECTION IN THE AI AGE

ONLINE ROOM | 15:15–17:15

CHAIR: Andreea Vertes-Olteanu

Cătălin-Nicolae Constantinescu-Mărunțel

Faculty of Law, Academy of Economic Studies, Bucharest

Online hate crimes in the age of post-truth

▪ ABSTRACT

The United Kingdom vote to leave the European Union from 2016, the United States and the Romanian presidential elections from 2024 were historical events which form an emerging pattern in public discourse. It was shown by previous studies that debates surrounding these events were marked by a general inability to discern facts from opinions, objective data from sentiments. In the online spaces created by mass-media and social media, demonstrably false statements, which often included various forms of hate speech, were used to create powerful emotions among the electorate, more often than not with a specific political goal in mind. This paper analyses how the specific dynamics of post-truth politics promote the online proliferation of hate crimes, in view of the Romanian criminal law legislation. It first analyses what is the post-truth theory and how it is linked to the phenomenon of online hate crimes, and it then proceeds to present how the specifics of this connection create the need for more flexible criminal, administrative and civil norms, both in terms of how the national legislator defines the key concepts of the field and in relation to how the public authorities approach it on a practical level. The author concludes that the Romanian criminal legislation, while lacking the necessary concepts and instruments needed in order to properly prevent, identify and punish crimes and other types of delinquency which have an element or bias, may still be interpreted in such a way as to strengthen and further the fight against such online conduits.

Remus Titiriga

Faculty of Law, West University, Timișoara

Searching for the Boundaries of Automatic Judicial-Making

▪ ABSTRACT

This research will approach the capabilities and limitations of large language models (LLMs) in judicial decision-making. We hypothesize that while LLMs demonstrate impressive proficiency in processing legal precedent and identifying relevant statutory provisions, they will exhibit systematic limitations when navigating normative complexities. Specifically, current models likely struggle with: (1) reconciling competing moral considerations within multifaceted disputes, (2) providing transparent, defensible reasoning for value-based decisions, and (3) maintaining consistency in ethical reasoning across varied contextual scenarios. Our research aims to develop a methodological framework to identify the boundaries of automated judicial decision-making through theoretical analysis and, eventually, empirical evaluation. We will identify instances of human judgment in judicial reasoning by analyzing landmark cases in which judges balance competing interests in light of underlying policies and values. We will then eventually assess whether contemporary LLM systems can emulate such normative reasoning capabilities. Our findings aim to delineate areas where and if LLMs could replace/complement human judgment. We anticipate that AI excels at information retrieval, case summarization, and precedent identification—tasks that involve pattern recognition and data processing.

Vlad Crăciun

Faculty of Law, University of Bucharest

Criminal liability of Online platforms

▪ ABSTRACT

Based on foreign case law regarding Craigslist, Backpage, and Vivastreet, as well as domestic cases involving Anunțul Telefonic and Publi 24, the presentation will focus on criminal liability for illegal content distributed on online platforms, with regard to art. 6 of the Digital Service Act. Considering that the DSA does not constitute grounds for criminal liability, the first part of the discussion involves a detailed analysis of the domestic rules that can form the basis for the accountability of online platforms. In particular, based on the specific features of the cases mentioned, the relevant aspects of secondary participation will be addressed. In the second part, the conditions set out in Article 6 of the DSA regarding exemption from criminal liability will be examined. Thus, we will first clarify the concept of "illegal content." Then, we will examine the subjective condition established in Article 6a of the DSA in the context of the conduct obligations that the DSA imposes on online platforms, obligations that could lead to the removal of the exemption from liability. Furthermore, Article 6b of the DSA raises the question of how the platform becomes aware of illegal content and, in particular, how it should proceed thereafter. The analysis will reveal several ambiguities and contradictions arising from the regulation and the ECJ case law on its application. Finally, several critiques of the immunity regulated at European level will be outlined. In particular, they concern compliance with the principle of legality, the sovereignty of Member States, equality and, most importantly, the violation of the fundamental rights of victims, especially in the case of extremely serious crimes such as human trafficking, sexual abuse of minors or the non-consensual sharing of intimate images.

Dorel Herinean

Faculty of Law, University of Bucharest

Criminal sanctions, AI and the internet

▪ ABSTRACT

Offences committed over the internet create sometimes a different harm for the protected social values than traditional ones. Sometimes, the threat or the harm exists only in the online environment. The aim of this paper is to analyze, in such cases and other forms of cyber-enabled offences or for the cyber-dependent offences, how the traditional sanctions provided by the criminal law (all the types of penalties and security measures) can be applied, adapted or changed in order to achieve their purposes. Moreover, we study what role could an AI system take in determining, enforcing or checking the compliance with the sanctions in a theoretical prevention system adapted to the needs generated by internet criminal activity.

Gavriluță Cristina, Carmen Palaghia

„Alexandru Ioan Cuza" University, Iași

Artificial Intelligence and the Industrialization of Cybercrime

▪ ABSTRACT

In recent years, technology "has created a new dimension in which cybercriminals carry out their activities." Europol points out that AI is fueling an "explosion" of deviant acts, referring not only to online fraud, which has expanded significantly in recent years, but more seriously noting that, in this context, children and adolescents from the "digital generation," who are permanently present on social media websites, are the most vulnerable to human trafficking or, even more seriously, are recruited to commit crimes on demand. Networks primarily target children who are vulnerable due to psychological problems or those who are victims of aggression or (cyber)bullying. Catherine De Bolle (Executive Director of Europol) warned that the greatest threat facing the European Union comes from organized crime and originates from groups that have "industrialized" the recruitment of children. Analyzing the modus operandi: offenders begin the process of luring children by participating in their multiplayer video games, which have a chat function; they gain their trust and subsequently may bribe or blackmail the minor into committing acts of violence, including torture, self-harm, murder, and even suicide. Europol confirmed in 2025 the existence of 105 cases in which minors were involved in violent crimes ("committed as a service"): only 10 contract killings were recorded, the others not being carried through to completion due to the children's lack of skill. Human trafficking for scam factories (e.g., in Australia) and the use of AI for activities such as Pig Butchering, Rug Pull, etc., are also reported. It remains extremely necessary to build cyber resilience for vulnerable individuals, to increase penalties for offenders who exploit children's vulnerability in the virtual environment, and to exercise greater control over this space.

Keywords: Artificial intelligence, cybercrime, industrialization.

Ștefana-Iuliana Sorohan

Faculty of Law, University of Bucharest

Online Speech and Criminal Incitement

▪ ABSTRACT

In contemporary society, the act of incitement to commit criminal offences increasingly takes place through online communication channels. Digital platforms, social networks, forums, and other internet-based environments facilitate the rapid dissemination of messages capable of encouraging unlawful conduct, significantly amplifying their potential impact. This development raises complex legal questions regarding the applicability of traditional concepts of criminal incitement to forms of online speech. A central issue addressed in this paper concerns whether (and to what extent) the internet may be regarded as a public space for the purposes of criminal law. The qualification of online environments as public or non-public directly affects the legal assessment of incitement, particularly in cases of public incitement or incitement to hatred. Unlike conventional public spaces, the internet is characterized by fragmented audiences, varying degrees of accessibility, and the coexistence of public, semi-public, and private communication spheres, which complicates legal classification. Furthermore, the paper examines the practical difficulties faced by law enforcement authorities in identifying and investigating acts of criminal incitement committed online. The volume of digital content, the speed of dissemination, cross-border elements, and the use of digital platforms as intermediaries pose significant challenges in detecting all instances of public incitement or hate incitement occurring on the internet. These obstacles raise concerns regarding the effectiveness of criminal enforcement and the protection of fundamental legal values in the digital environment. By analyzing these issues, the paper seeks to contribute to the ongoing debate on the adaptation of criminal law to online speech and the need for coherent legal criteria capable of addressing the specific features of internet-based incitement.

Andreea Vertes-Olteanu

Faculty of Law, West University, Timișoara

Cognitive vulnerability and democratic autonomy in digital contexts

▪ **ABSTRACT**

Contemporary societies still rely on the assumption that electoral choice reflects individual autonomy, secured through classical procedural guarantees, such as free and fair elections. Our attempt is to challenge that premise by examining, through the lens of the recent Romanian experience, how algorithmic systems, without formally breaking electoral rules, increasingly shape the conditions under which political preferences are being formed. Technological progress and an evolved understanding of psychology have led to the emergence of sophisticated methods of propaganda, culminating today in digital micro-targeting, social media bots, and an agressive use of AI, capable of influencing public opinion at large. As a result, digital environments function as architectures of influence that exploit cognitive vulnerabilities and emotional heuristics. Rather than eliminating choice, these systems redesign it, transforming democratic consent into a technologically mediated outcome. Governing the ungovernable in digital democracy requires a shift in the legal imagination. The existing legal frameworks, particularly the DSA and the emerging AI Act, focus on transparency, risk management or accountability, while leaving the deeper normative question unresolved: how to govern influence itself.

Ioana Crenguța Leaua

Faculty of Law, Academy of Economic Studies, Bucharest

Is Law evolving into a Meta-Artificiality?

▪ **ABSTRACT**

The paper argues that the law is entering a new phase of its historical development, due to technologies of artificiality, including tools that use artificial reality and artificial intelligence, as well as automated behaviour generated by smart contracts across various platforms.

Until now, law has always been an artificial, human-made system designed to organize social life. What has changed with the platforms using the technology of artificiality is the environment in which human relationships now take place.

The automated decision-making systems are capable not only of applying rules but also of creating them, and, moreover, of applying them in an artificial environment independent of traditional legal institutions for law-making, contract negotiation, adjudication, or enforcement. In many contexts, these automated decision-making systems act faster and potentially more efficiently than humans would, so users are embracing them with little hesitation. As a result of this new normative layer of intervention, the law made by humans is no longer the only source of norms.

To this new socio-technological order, which replaces the social order, this paper proposes that law must evolve into a "meta-artificiality": a higher-level framework that does not merely regulate individual actors but governs the systems (both human and technological) that govern the actions that produce effects in the physical or virtual reality (both human behaviour and automated actions).

In practical terms, this means that law must move beyond its traditional role as a generator of rules for human behaviour and undertake a function that includes coordinating the architecture of multiple normative orders, both social and technical, including platform policies, algorithmic rules, and technical infrastructures. If law is to remain *relevant and legitimate, if it is to continue to serve its historical purpose of ensuring the cohesion of the human society, it must now become the "governor of governors" to address both the social and the artificial systems.*

Ioan Dumitru Apachiței

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Digital Constitutionalism Beyond the State: Sovereignty, Platforms and the Transformation of Legal Authority

▪ ABSTRACT

The article examines the emergence of digital constitutionalism as a distinct legal paradigm, designed to respond to the transformations affecting regulatory authorities in the context of a globalized digital space. Starting from the premise that the classical state-centered framework has been transcended, the study analyzes the ways in which the concept of sovereignty is being reconfigured beyond territorial borders, under the influence of transnational digital platforms and non-state governance mechanisms. In this regard, the article explores the points of convergence between the national constitutional order, the extraterritorial application of legal norms, and the growing role of private actors in the establishment and enforcement of standards with quasi-constitutional effects. The analysis further highlights the contribution of international law, European Union law, and soft law instruments to the shaping of an emerging normative architecture characterized by legal pluralism and fragmentation of authority. In essence, the paper advances the thesis that digital constitutionalism beyond the state does not entail a negation of sovereignty, but rather its functional transformation, requiring a reconsideration of traditional concepts of legitimacy, accountability, and the protection of fundamental rights in the digital era.

ROUND III (17:00–18:00)

PANEL 9 -DIGITAL MARKETS, PLATFORMS & ECONOMIC REGULATION

ROOM B | 17:00–18:00

CHAIR: **Aura Elena Amironesei**

Aura Elena Amironesei

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Blurring the Lines: Defining Manipulation in a World of Influence

▪ ABSTRACT

EU digital regulation increasingly relies on the notions of manipulation, undue influence, and manipulative techniques to justify restrictions on certain design practices and persuasive technologies. The AI Act, the Digital Services Act, and EU consumer protection law all employ these concepts as normative thresholds, yet their meaning remains conceptually unstable. Regulatory texts often imply that manipulation exists where a person is steered into a decision they would not otherwise have taken. This counterfactual understanding raises immediate difficulties, as influence is inherent to communication, marketing, and everyday interaction.

This paper does not seek to offer a new definition of manipulation. Instead, it asks whether manipulation can be coherently defined at all in law, and whether meaningful boundaries between influence and manipulation are conceptually and practically attainable. It explores the tension between intuitive understandings of manipulation and the legal need for determinacy, as well as the evidentiary problems raised by standards that hinge on proving that a different decision would have been taken.

By examining how manipulation is invoked across EU digital regulations, the paper questions whether the concept can function as a stable legal category or whether it inevitably remains a fluid and contested notion.

Sebastian Antoce

Faculty of Law, „Alexandru Ioan Cuza” University, Iași

Revisiting Data Contracts under the EU Digital Omnibus

▪ ABSTRACT

A recent initiative of the European Commission called "Digital Omnibus" is often presented as an effort to simplify and rationalize the EU digital regulatory framework. This presentation examines the development from the perspective of transnational enforcement and private ordering, focusing on the evolving role of data contracts. The presentation starts with the observation that, considering new proposed instruments, data access, reuse, and control are no longer resolved primarily through normative instruments, but through new flexible contractual mechanisms. Amendments to the Data Act provide a clear illustration. For example, the removal of Article 36 on smart contracts, and the reinforcement of trade secret protections do not eliminate any uncertainties regarding data contracts. Instead, they change the focus to contractual design, standard clauses, and negotiated risk allocation between private parties. Against this background, the presentation analyses how data contracts could function considering the new normative proposal. Obligations related to cloud switching and data access conditions increasingly depend on private agreements that operate transnationally and are only indirectly shaped by EU law. While these contracts are formally instruments of private autonomy, their structure is strongly influenced by regulatory instruments shaped by market power asymmetries. Based on this reliance on private ordering, some specific governance questions appear. Considering the new proposals, many of the safeguards associated with enforcement, including transparency, participation, and possibilities for contestation tend to be reconsidered. But at the same time, regulators are increasingly required to treat contracts as a way for compliance in cross-border data transfers. By examining recent proposals alongside existing data law instruments, the presentation questions whether new data governing solutions offer a sustainable response to the main problems of data economy or whether it reproduces enforcement and accountability problems in a less visible form.

Luciana Viziteu

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Balancing Innovation and Regulation in the Era of Deepfakes

▪ ABSTRACT

We are living in a time when truth is becoming increasingly fragile, and the tension between appearance and reality is more intense than ever. Deepfake technology, powered by generative artificial intelligence, has moved beyond the stage of technical curiosity and has become a tool with major implications for fundamental rights, national security and democratic society. Anyone can create a deepfake in just a few minutes, and the consequences are far-reaching: manipulation, disinformation, effects on the judicial sphere, the political sphere, fraud, harassment, defamation, challenges related to intellectual property rights, legal liability, freedom of expression, the right to one's image, data protection. From a comparative perspective, the article examines how contemporary legal systems attempt to balance technological innovation with the protection of human dignity and information security by analyzing three distinct approaches to deepfake regulation: the European approach, the American approach and the Asian approach.

Alexandru Chistruga

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Power, Infrastructure, and Artificial Intelligence in a Fragmented Global Order

▪ ABSTRACT

Discussions on artificial intelligence have largely focused on algorithmic innovation and the expanding availability of data. Far less attention has been paid to the material conditions that make contemporary AI development possible. Yet, in practice, the performance of advanced AI systems is inseparable from access to high-performance computing resources, particularly graphics processing units (GPUs). Against this background, the article follows the evolution of GPUs from their origins in the video game industry to their current status as core infrastructure for large-scale AI systems, with particular emphasis on NVIDIA's role in this transformation. A decisive moment in this process was the development of CUDA (Compute Unified Device Architecture), which enabled GPUs to be used for general-purpose computation rather than graphics alone. This shift reshaped both research practices and industrial approaches to AI workloads. Over time, the tight coupling of NVIDIA's hardware and software facilitated the widespread adoption of GPU-based computing, while simultaneously narrowing the technological ecosystem within which advanced AI development occurs. As a result, access to adequate computational infrastructure has become a structural precondition for participation at the forefront of the field. In this sense, computational capacity cannot be understood solely as a technical resource. The concentration of advanced hardware production, high entry costs, and uneven geographical distribution of GPUs generate persistent asymmetries that influence who is able to develop, scale, and deploy advanced AI systems. NVIDIA occupies a central infrastructural position within this landscape, shaping the tempo and scale of AI development without exercising direct control over research agendas or downstream applications. These dynamics extend beyond the boundaries of industry or technology. Advanced computing infrastructure is increasingly embedded in broader struggles over technological sovereignty, economic competitiveness, and strategic autonomy, where

access to high-performance computing conditions the ability of states and regions to participate meaningfully in the global AI ecosystem.

PANEL 10- DIGITAL MARKETS, CYBERSECURITY AND RESPONSIBILITY IN THE TECHNOLOGICAL ORDER

ROOM C | 17:00–18:00

CHAIR: Carmen Tamara Ungureanu

Katarzyna Krupska

Faculty of Law, University of Bialystok

Geographical indications as a tool for consumer protection in e-commerce

▪ **ABSTRACT**

Geographical indications play a key role in the consumer protection system, providing information, guarantees and quality assurance. In the context of the dynamic development of e-commerce, their importance is further enhanced, especially in the context of counteracting practices that mislead consumers as to the origin, quality and characteristics of the products offered. The paper analyses geographical indications as a consumer protection tool in the digital environment, with particular emphasis on online sales and marketing communication via the Internet.

The aim of the presentation is to show how the protection of designations of origin and geographical indications, regulated by European Union law, fits into the broader system of consumer protection against unfair market practices. The author analyses the relationship between the regulations governing geographical indications and consumer law standards, including the prohibition of misleading practices and the information obligations of businesses operating in e-commerce.

Particular attention will be paid to the issue of the use of geographical indications in internet domain names, product descriptions, digital advertising and on marketplace platforms. The paper will also discuss the risks associated with the misuse of regional names on the internet and its impact on consumer purchasing decisions.

The analysis leads to the conclusion that effective protection of geographical indications in e-commerce not only contributes to the protection of producers' interests, but above all to increasing the transparency of the digital market and strengthening consumer confidence. Geographical indications are therefore an important, though often underestimated, element of modern consumer protection law.

Sara Henriques

University of Coimbra

The Iran Blackout: Evidence and the Verification Gap

Bianca-Raluca Tulac

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

REITs and Indirect Foreign Investment in Real Estate in the Digital Age

▪ ABSTRACT

Available data indicate that foreign investment in real estate represents a key component of the global economy and has expanded significantly over recent decades, continuing to grow at present. This development has been driven, inter alia, by the emergence of modern investment vehicles such as Real Estate Investment Trusts (REITs), as well as by the accelerated digitization of capital and real estate markets. In this context, this article aims to examine the role of REITs in facilitating foreign real estate investments, particularly in the digital era. The approach begins by establishing the conceptual framework necessary for understanding the topic, through defining the notion of "foreign real estate investment" and distinguishing between direct and indirect investments. Subsequently, the discussion focuses on the manner in which REITs enable indirect access for foreign investors to the real estate market, examining the definition, types, and specific characteristics of this category of real estate investment vehicles. Finally, the article addresses the impact of digitization on REITs, with particular emphasis on their trading on capital markets and electronic platforms. This analysis provides the basis for a discussion of the substantive and formal requirements of the electronic real estate investment contract, as the legal instrument structuring the investment operation. Keywords: REITs, indirect foreign investments, real estate, electronic real estate investment contract

Smaranda-Georgiana Azamfirei

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Limits of State Responsibility for Cyber Terrorism-Consequences and Measures Exercised by Victim States

▪ ABSTRACT

The increasing reliance on digital infrastructures has amplified the impact of cyber operations, raising questions regarding their classification as threats to State sovereignty and the corresponding legal frameworks for accountability. A particularly contentious issue in this context concerns the attribution of wrongful cyber acts committed by terrorist organizations to States and the conditions under which State responsibility may be engaged. This article examines the legal criteria and minimum standards required under international law to establish State responsibility for acts of cyber terrorism, with particular emphasis on attribution, control and involvement of the State. It analyzes the applicability of existing doctrines of international responsibility to cyber operations conducted by non-State actors and explores the thresholds of direction, control or support necessary to link such acts to State conduct. Additionally, the article addresses the legal remedies and response mechanisms *available to victim States when cyber terrorist activities are carried out independently, without State authorization or effective control. By clarifying these issues, the study contributes to the ongoing debate on the adaptation of international legal principles to emerging cyber threats and non-State actor involvement.*

Constantin Busuioc

Faculty of Law, „Alexandru Ioan Cuza" University, Iași

Attribution of individual responsibility in situations involving the use of force through autonomous weapons

▪ **ABSTRACT**

This paper examines the attribution of individual responsibility in situations involving the use of force mediated by algorithmic decision-making in lethal autonomous weapon systems. At first glance, the unpredictability of the outcomes produced by such means might appear to offer clear solutions for assigning responsibility to the person behind the system; however, theoretical and practical realities generate multiple, often competing, approaches. The premise of an identifiable human conduct reflected in the effects produced by these weapons is undermined by the fragmentation of the decision-making chain, an issue inherent to all working hypotheses in this field.

The article analyzes the limits of classical concepts of personal responsibility in the context of the use of force through autonomous weapons, with particular emphasis on the relationship between human control, causality, and standards of foreseeability. It focuses especially on the difficulties arising from the delegation of lethal decision-making to computational algorithms, as well as the risk of a "responsibility gap" emerging between the actors involved in the design, authorization, and operation of autonomous systems.

The conclusion of the research is that the problem lies not in the absence of a framework for attributing responsibility, but in the existence of a tension between traditional concepts of individual responsibility and the new forms of mechanisms that may be employed in situations involving the use of force, advocating for a nuanced approach to human control.

PANEL 11 – LEGAL PRINCIPLES AND SYSTEMIC TRANSFORMATION IN THE DIGITAL AND TRANSNATIONAL AGE

ONLINE ROOM | 17:00–18:15

CHAIR: Radu Bogdan Bobei

Radu Bogdan Bobei

Faculty of Law, University of Bucharest

A transnational law issue: the extraterritoriality in international law and conflict of laws

▪ ABSTRACT

The concept of territoriality enjoyed the so-called 'centrality' in international law and conflict of laws altogether. Various scholars all over the world already pointed out the ways in which international law's and conflict of laws' frameworks interact around the Peace of Westphalia's spirit. Nowadays the above-mentioned concept is truly invited to share its development with the concept of 'extraterritoriality'. Past and current works show that both concepts of territoriality and extraterritoriality are not enemies but scholarly fellows functioning in the plurality of areas of law. Global electronic currencies, competition law, financial law, corporate climate responsibility are some of such areas evolving in the light of the interplay between territoriality and extraterritoriality. The Jessup's transnational law, as understood as a legal system, evolved in a way amounting to the nowadays valuable methodology. That is, the methodology of transnational law employed either by domestic and international law on the one side or by public and private law on the other side. Such methodology helps the scholars all over the world with a view to manage the flaws and the virtues of territoriality and extraterritoriality altogether. My presentation is going to prove that.

Luminița-Marcela Pop

Faculty of Law, „Babeș-Bolyai" University, Cluj-Napoca

Civil liability in contracts concluded at a distance

▪ ABSTRACT

With the development of technology and the virtual environment, an increasing number of contracts between professionals and consumers are concluded at a distance. Their subject matter is diverse and may include the provision of electronic communications services intended for the public, the provision of access and connectivity services to public electronic communications networks, etc.

For a distance contract to be concluded, both the launch of the offer and the negotiation of the contract must take place in the virtual environment, while the conclusion of the contract must be carried out through means of distance communication. In practice, both the negotiation stage and the conclusion of the contract are conducted exclusively through means of distance communication. During these stages, however, damage may occur, the reparation of which requires the engagement of civil liability. The applicable type of civil liability depends on the stage at which the parties find themselves.

During the negotiation stage, tort liability applies, whereas during the stage of contract performance, subsequent to its conclusion, contractual liability generally applies. Nevertheless, it is possible for an unlawful act committed at the pre-contractual stage to affect the validity of the contract, which results in its nullity and in the engagement of tort liability for damage occurring after the conclusion of the contract. For example, a professional may fail to inform the consumer of certain essential characteristics of the product sold, characteristics which, had the consumer been aware of them, would have prevented the conclusion of the contract. The failure to provide such information leads to the nullity of the contract, and in the absence of a valid contract, the applicable civil liability can only be tort liability.

In this article, we aim to analyze the civil liability applicable at the stage of negotiating a distance contract, at the stage of its performance, as well as at the stage following the termination of the contract.

Dumitrache Elena- Claudia

Faculty of Law, „Titu Maiorescu" University, Bucharest

Digitization of the Real Estate Advertising System of the Land Register

▪ ABSTRACT

The provisions of the Civil Code in force expressly regulated the principle of the constitutive effect of the registration of the right in the land register, but more than 14 years after the legislation, these provisions cannot be applied, although they represent one of the most important principles of the real estate advertising system of the land register. The extension of this principle after the completion of the cadastral works for each administrative-territorial unit and the opening upon request or ex officio of the new land registers imposes on the legislative power of the state the obligation to legally regulate new measures through which scientific technology can be implemented efficiently and easily in the measurement of the surfaces of real estate and the digitization of the data thus obtained, in order to ensure the accuracy of the registered data, compliance with the legal content of the rights of the parties and the enforceability of rights against third parties.

Ștefan-Ciprian Raicea

Faculty of Law, University of Craiova

Polluter Pays Principle in the Digital Age

▪ ABSTRACT

The rapid expansion of artificial intelligence systems and digital infrastructures has generated a new category of environmental risks, often overlooked by traditional regulatory frameworks. Energy-intensive data centers, algorithmic optimization of resource extraction, automated environmental decision-making and AI-driven industrial processes increasingly contribute to environmental degradation, climate change and ecological imbalance. This article examines whether the polluter pays principle, a cornerstone of environmental law, can be meaningfully applied to environmental harm caused or facilitated by artificial intelligence systems. The paper argues that AI challenges the classical allocation of environmental liability by fragmenting responsibility among multiple actors: developers, deployers, data providers, platform operators and public authorities relying on automated systems. This diffusion of agency raises fundamental questions about causation, fault and attribution of environmental harm in digital ecosystems. By analysing the normative foundations of the polluter pays principle, the article explores its adaptability to algorithmic governance and autonomous decision-making processes. Special attention is paid to the European Union's emerging regulatory framework, including environmental liability rules and the EU AI Act, highlighting existing gaps in addressing AI-related environmental externalities. The article assesses whether traditional liability models—fault-based, strict liability or risk-based approaches—are capable of capturing the environmental impacts of AI systems, or whether new hybrid models of responsibility are required. Ultimately, the article contends that environmental law offers valuable conceptual tools for governing the "ungovernable" aspects of artificial intelligence. Reinterpreting the polluter pays principle in the digital age may contribute to a more coherent framework of accountability, ensuring that technological innovation does not undermine environmental protection and intergenerational equity.

Goga Alexandru Silviu & Barbu Silviu Gabriel

„Transilvania” University, Brașov

Piercing the Algorithmic Veil

▪ ABSTRACT

As Artificial Intelligence evolves from mere supportive tools to autonomous agents capable of independent decision-making, the traditional frameworks of liability are facing an unprecedented stress test. The theme "Governing the Ungovernable?" accurately captures the dilemma of regulating algorithmic entities that exhibit emergent behaviors unforseen even by their developers. This paper, co-authored by a digital law researcher and a former senior judge, scholar and lawyer, explores the widening gap between technical autonomy and legal accountability.

We argue that the current concept of "human-in-the-loop" is becoming a legal fiction in high-frequency algorithmic contexts, leading to a "accountability vacuum." The article analyzes the procedural challenges judges face when confronted with the "black box" defense in civil and administrative liability cases. By examining recent developments in the EU liability frameworks and comparative case law, we propose a pragmatic judicial test for "Functional Autonomy." This approach aims to determine when the algorithmic veil should be pierced to hold developers directly liable, and when the autonomy is sufficient to trigger a strict liability regime backed by mandatory insurance mechanisms. We conclude by offering a roadmap for adapting judicial reasoning to govern the seemingly ungovernable nature of Agentic AI.

Andreea Nicoleta Dragomir

Faculty of Law, „Lucian Blaga” University, Sibiu

European Digital Governance between Legislative Sovereignty and Transnational Administrative Coordination

▪ ABSTRACT

The development of digital technologies and online platforms has placed significant pressure on traditional models of legal regulation and public administration. The transnational nature of the Internet, the growing use of algorithmic systems and the central role of private digital actors challenge the effectiveness of classical, state-centred legislative sovereignty. In this context, the European Union has established a comprehensive regulatory framework for the digital environment, encompassing the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act, and the EU Artificial Intelligence Act. This paper argues that European digital governance cannot be explained only through the adoption of uniform legal rules. Instead, it is increasingly shaped by mechanisms of transnational administrative coordination within a multi-level governance system. The article examines how digital regulation in the EU operates in practice through cooperation between national authorities, European institutions and independent regulators, supported by soft law instruments and administrative networks. From an EU administrative law perspective, the analysis highlights the shift from hierarchical regulation towards coordinated administrative action, raising important issues related to accountability, responsibility and effective enforcement. Particular attention is paid to the role of administrative cooperation in ensuring compliance with digital rules and in safeguarding fundamental rights. The paper also addresses the implications of these developments for legal education, arguing that the teaching of European law should place greater emphasis on administrative coordination and digital governance. Understanding how digital regulation functions in practice is crucial for training future jurists and public officials who can effectively respond to the challenges of governing the digital space.