FACULTY OF LAW
Charles University

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW

- 5th edition, March 28, 2025 -

www.adjuris.ro/fintech

Section II.
Cyberspace and Artificial Intelligence Law

Friday – March 28, 2025

ONLINE ON ZOOM

Moderator:

Associate professor **Cristina Elena POPA TACHE,** *„Andrei Şaguna" University of Constanta, President of the International Institute for the Analysis of Legal and Administrative Mutations*

! Each paper will be presented within 15 minutes
! Fiecare lucrare va fi prezentată în maxim 15 minute

SCIENTIFIC PAPERS

THE EU AGENCY FOR THE SPACE PROGRAMME AND THE STRUGGLE AGAINST DIGITAL DIVIDE IN EUROPE

Professor Jakub HANDRLICA
Charles University in Prague, Czech Republic

Abstract

This presentation aims to contribute to the theme of the 5th Conference on FinTech, Cyberspace and AI Law from the viewpoint of the gradual digitalisation of both the public (e-government) and private sectors. Establishing safe connectivity represents a significant precondition for the prospective full digitalisation in Europe. Until now, the connectivity services have been mainly provided by terrestrial transmitters. The fact is, however, that currently, demand is increasing for securing connectivity services for the public administration and private entities in the European Union from satellites. The reason behind this is not only the higher reliability and efficiency of space technologies but also the risks arising for terrestrial transmitters (natural disasters, military conflicts, terrorism). It can be assumed that space technologies, ensuring connectivity, will be an integral part of the European Union of the future. In this context, this presentation aims to briefly introduce to the professional public the project of the European network of communication satellites IRIS2 (Infrastructure for Resilience, Connectivity and Security through Satellites), which aims to provide secure communication under the umbrella of the EU Agency for Space Programme. One of the goals of the IRIS2 project is to prevent or minimise the risk of the so-called digital divide, which consists of the fact that the gradual digitisation of public administration, banking and medicine services can exclude a particular group of people from access to the benefits of e-government. The goal of the IRIS2 project is to minimise this risk by providing connectivity to areas not yet covered by connectivity (so-called dead zones).

THE EUROPEAN CYBERSECURITY FRAMEWORK: CHALLENGES, LEGAL ASPECTS AND REGULATIONS

PhD. candidate Leonidas SOTIROPOULOS
European University of Cyprus

Abstract

*This article analyzes the European Union's cybersecurity evolution, tackling the dual imperatives of fostering technological advancement and ensuring systemic resilience amid rising cyber risks. Centered on the question "How do EU legislative and institutional adaptations safeguard digital sovereignty, critical infrastructure, and cross-border coordination?", it employs **dogmatic legal analysis** to evaluate supranational laws (NIS 1/2, Cyber Resilience Act, DORA), institutional upgrades (ENISA, CERT-EU), and policy innovations. The paper's objectives are: Transitioning from fragmented policies to a unified "cyber shield"; balancing regulatory rigor with adaptive enforcement; identifying gaps in mitigating human-centric threats and cloud vulnerabilities. The article begins with cyberspace's conceptual foundations and EU regulatory milestones. Subsequent parts dissect ENISA's capacity-building initiatives, NIS 2's expanded sectoral coverage, and the Cyber Solidarity Act's crisis-response mechanisms. Case studies on ransomware and election interference highlight systemic vulnerabilities. The conclusion underscores **integration** (unified threat detection), **innovation** (AI defenses, quantum encryption), and **inclusivity** (global partnerships) as pillars for maintaining Europe's leadership in ethical digital governance. By prioritizing workforce development, AI-driven solutions, and transnational collaboration, the EU seeks to establish a global standard for a resilient cybersecurity framework*

FACULTY OF LAW
Charles University

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 5th edition, March 28, 2025 -
www.adjuris.ro/fintech

RETHINKING RESPONSIBILITY: NAVIGATING THE COMPLEXITIES OF CIVIL LIABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Assistant professor Dimitrios DEVETZIS
Frederick University, Cyprus

Abstract

This paper critically examines the complex issue of civil liability arising from the deployment and functioning of artificial intelligence (AI). With the rapid integration of AI-driven technologies into various sectors, including healthcare, transportation, finance, and consumer services, determining civil liability for damage caused by autonomous systems has emerged as a significant legal challenge. The traditional principles of liability, primarily centred on human fault and causation, struggle to adequately address the complexities and opacity inherent in AI systems, leading to legal uncertainties and gaps in consumer protection. This paper explores these key challenges by addressing three central questions: first, whether existing frameworks of fault-based and strict liability under civil law can effectively allocate responsibility in cases involving autonomous AI decisions; second, the problem of transparency and explainability as essential elements in attributing causation and fault; and third, the identification of the appropriate liable parties, such as developers, manufacturers, operators, or users. Additionally, the analysis will consider recent legislative proposals, particularly at the European Union level, such as the proposed AI Liability Directive, evaluating their potential effectiveness in resolving the identified issues. Ultimately, this essay argues for a nuanced approach, suggesting reforms to the current liability regimes that better reflect the unique characteristics of AI, promote legal certainty, and uphold fundamental rights. The findings presented aim to inform ongoing discussions surrounding the establishment of a coherent and balanced legal framework governing civil liability in an AI-driven society.

MAINTAINING TRUST IN THE AI: STRENGTHENING GOVERNANCE AND RIGHTS PROTECTION

Professor Nina GUMZEJ
Faculty of Law, University of Zagreb, Croatia
Professor Marija BOBAN
Faculty of Law, University of Split, Croatia

Abstract

The EU Artificial Intelligence Act (AI Act) establishes a complex and multi-level governance framework, which involves multiple stakeholders at both the EU and national levels, including the AI Office, AI Board, market surveillance authorities and national public authorities protecting fundamental rights. The Act seeks to balance innovation with the protection of fundamental rights, but the division of responsibilities and varying competences among these bodies introduce governance challenges. This paper explores the identified concern of constrained and largely reactive role of national public authorities protecting fundamental rights, which may limit effective oversight and, consequently, undermine public trust in AI systems. The analysis is based on doctrinal legal research approach, which is complemented by comparative analyses and case studies toward evaluating governance challenges and institutional dynamics under the AI Act. While the AI Act provides for a fundamental rights impact assessment mechanism for high-risk AI systems, differences in institutional capacity and technical expertise between the fundamental rights authorities and market surveillance authorities could weaken preventive oversight and lead to inconsistent protection of fundamental rights. Proactive approach of the Croatian Data Protection Authority, despite not (yet) being formally designated as a market surveillance authority, demonstrates the potential for fundamental rights authorities to play a constructive role in supporting the implementation of fundamental rights impact assessments. Its efforts to recommend assessment models and organize practical workshops illustrate how expertise in data protection compliance can enhance AI governance even without formal enforcement powers. At a broader level, however, disparities in institutional capacity between national authorities may result in inconsistent protection of fundamental rights, where better-resourced authorities in some Member States could be more capable at identifying and addressing AI-related risks to fundamental rights, than

those in less well-resourced authorities. Addressing these challenges effectively may ultimately depend on the political and administrative priorities of individual Member States, particularly in building sufficient capacity and oversight. The paper concludes that strengthening coordination and capacity-building among national authorities remains essential for ensuring consistent protection of fundamental rights across the EU, which can enhance public trust, promote regulatory clarity and support sustainable AI innovation.

ENHANCING MARITIME TRANSPORT SAFETY: CRITICAL CONSIDERATION OF AI-BASED SUPPORTING SYSTEMS AND MULTILEVEL COMPUTING SOLUTIONS

Assistant professor Ioannis VOUDOURIS
Frederick University, Cyprus
Lecturer Maria AVTZAKI
Frederick University, Cyprus
Associate professor Soteris THEOCHARIDES
Frederick University, Cyprus

Abstract

In this paper, we explore the implications computer related systems (i.e. multilayer -multilevel computing (MC) and AI) in maritime navigation and safety. Initially, we define cognitive processes as perception, attention, memory, reasoning, and decision-making, highlighting how AI attempts to simulate these human faculties and how AI is juxtaposed to MC. We then discussed this comparison between the two systems and their impact on autonomous navigation, collision avoidance, weather forecasting, predictive maintenance, and crew safety. Subsequently, concerns arose regarding over-reliance on AI, questioning why sophisticated MC methods couldn't suffice without involving "intelligence." We clarify that genuine human intelligence involves consciousness, instinct, and self-awareness—traits machines inherently lack. Using metaphors, we underscored how excessive automation might degrade human abilities, causing skill deterioration, complacency, and diminished decision-making capacity, much like a predator losing hunting instincts due to domestication. Conclusively, we argued for a balanced, restrained AI application ("soft use"), ensuring AI remains a supportive tool rather than a human substitute. Emphasis was placed on maintaining human decision-making authority, intuition, creativity, leadership, and ethical judgment—qualities irreplaceable by AI. Thus, while AI is beneficial in maritime safety as an aid, preserving human skills and responsibility is crucial to prevent harmful dependency and capability erosion.

ARTIFICIAL INTELLIGENCE IN EMPLOYMENT DECISION-MAKING: LEGAL CHALLENGES AND IMPLICATIONS

Lecturer Dana VOLOSEVICI
Petroleum Gas University of Ploiesti, Romania

Abstract

This study explores the legal challenges arising from the use of artificial intelligence in employment decision-making, with particular attention to its implications for employees' rights and managerial accountability. The primary objective is to evaluate whether existing legal frameworks, most notably the General Data Protection Regulation and the Artificial Intelligence Act, offer sufficient protection against the risks associated with automated and algorithmically informed decisions in the workplace. Employing a qualitative methodology, the research is grounded in doctrinal analysis of relevant European legal instruments, supplemented by a review of academic literature in labour law, data protection, and algorithmic governance. The study adopts an interdisciplinary perspective, combining legal analysis with insights from organisational psychology and data science. The findings underscore key concerns, including the risk of indirect discrimination, the opacity of algorithmic decision-making processes, and the potential dilution of managerial responsibility. In response, the paper recommends a series of organisational measures such as targeted training, structured collective bargaining on AI deployment, and the adoption of a sustainable, rights-oriented approach to

managing the workforce. The study concludes that a multidimensional governance model is essential to ensure that technological innovation remains aligned with the protection of workers' fundamental rights and the principles of democratic workplace governance.

HOW TO UNDERMINE DEMOCRACY THROUGH BOTS, ALGORITHMIC MANIPULATION, AND DIGITAL INFLUENCE IN ELECTIONS: LEGAL CHALLENGES – A CASE STUDY ON THE 2024 ROMANIAN PRESIDENTIAL ELECTION

Associate professor Mădălina VOICAN
Faculty of Law, University of Craiova, Romania

Abstract

This research article examines the legal challenges associated with digital election manipulation, focusing on the case of the 2024 Romanian presidential election. First, it outlines the international and European legal framework, including the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights, and the Digital Services Act (DSA). The second part discusses the annulment of the Romanian presidential election results, which was triggered by astroturfing campaigns on TikTok using bot farms, the covert use of influencers, and suspicions of foreign interference. It explores the legal response of the Romanian Constitutional Court and the broader EU implications of such digital manipulation. Additionally, the article examines current legislative gaps, the challenges of regulating digital platforms, and the need for stronger laws ensuring transparency in online election campaigns. In conclusion, the article proposes key legal reforms to safeguard electoral integrity, including stricter accountability measures for digital platforms, sanctions for undisclosed political content promotion, and enhanced mechanisms to combat election disinformation.

AI IN ANTI-CORRUPTION EFFORTS: LEGAL CHALLENGES, ETHICAL CONSIDERATIONS, AND FUTURE IMPLICATIONS

Associate professor Mădălina VOICAN
Faculty of Law, University of Craiova, Romania

Abstract

This research explores the role of Artificial Intelligence (AI) and Generative AI (GenAI) in detecting, preventing, and predicting corruption, addressing both their potential and the legal challenges they present. Traditional anti-corruption mechanisms rely heavily on human intervention, yet they often suffer from inefficiency, limited adaptability. Meanwhile, AI-driven technologies have emerged as powerful tools for enhancing fraud detection, financial monitoring, and procurement oversight. The study further examines how GenAI expands these capabilities by enabling predictive analytics to anticipate corruption risks before they materialize, offering a more proactive approach to combating corruption. However, the deployment of AI in anti-corruption efforts raises legal and ethical concerns, particularly regarding the black-box nature of AI models, data privacy (GDPR compliance), algorithmic bias, and transparency. To mitigate these risks, this study discusses the importance of accountability and regulatory enforcement, emphasizing the need for robust legal frameworks, clear regulatory standards, and ethical guidelines for AI implementation. The research concludes that while AI has the potential to revolutionize anti-corruption efforts, its success depends on strong legal safeguards and responsible governance.

FACULTY OF LAW
Charles University

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 5th edition, March 28, 2025 -
www.adjuris.ro/fintech

ARTIFICIAL INTELLIGENCE: TRANSFORMATION, CHALLENGES AND REGULATION IN A DIGITAL WORLD

Postdoctoral Researcher Nicolae PANĂ
Bucharest University of Economic Studies, Romania
Law graduate Xin Jie ZHU
Las Palmas of Gran Canaria University, Spain
Legalitc International Association researcher

Abstract

The impact of the Fourth Industrial Revolution (Industry 4.0), determining how it has transformed production processes, business models and the integration of manufacturing technologies and information systems. This revolution has not only boosted business efficiency and competitiveness but has also introduced new challenges arising from digitalization and the interdependence of cyber-physical systems, redefining value creation in the industrial sector. In addition, this phenomenon is not limited to technology, but also has a profound impact on economic, social, political and legal structures, generating both obstacles and opportunities in the context of a globalized society. Through this analysis, it seeks to understand how Industry 4.0 is shaping the present and future of organizations and society.

ARTIFICIAL INTELLIGENCE, CYBERSECURITY FACTOR

Associate professor Adriana-Iuliana STANCU
"Dunarea de Jos" University of Galati, Romania

Abstract

Objectives: *The recent cyber-attacks on major European institutions, the exponential increase in threats to cyber structures and the rapid pace of technological change have once again highlighted the importance of greater collaboration and change in the civil-military area, highlighting the fact that there is no hierarchy between civilians and military communities. The EU's cybersecurity policy allows it and its Member States to strengthen their capacity to defend, detect, protect and even prevent, correctly using the full range of security options available in the civilian and military communities to increase the security and protection of the EU, as required by international provisions, including regarding the Charter.* ***Proposals and Methodology:*** *Although, national security of each EU member state is its direct responsibility, including in the sensitive cyber domain, as directly results from the provisions of Article 4(2) TEU, the need to defend European values, to invest in their preservation, has determined that the EU's cooperation structures get involved in the cyber offensive, including with its financial capabilities.* ***Results and Implications:*** *It is necessary that the actions of all European country and European institutions, or organizations and agencies such as EUIBA, be strengthened in the coming period, with a view to defending the EU, its citizens, the EUIBA and their operations and missions in the cyber domain related to the Permanent Security and Defense Policies (PSDP). Furthermore, it underlines the place of cyber resilience at EU level, by increasing the defense capacity in this sensitive, cutting-edge domain, by increasing the possibility of cyber defense and by creating reliable feedback from the Member States. Therefore, joint action is needed to strengthen cybersecurity.*

FACULTY OF LAW
Charles University

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 5th edition, March 28, 2025 -
www.adjuris.ro/fintech

NIS2 DIRECTIVE - LEGAL PREPAREDNESS OF EU HEALTH INFRASTRUCTURE AGAINST LARGE-SCALE CYBERATTACKS

PhD. student Antonia RENGLE
„Babeş- Bolyai" University of Cluj Napoca, Romania

Abstract

This study examines the legal preparedness of European Union health infrastructure under the NIS2 Directive (Directive (EU) 2022/2555) against large-scale cyberattacks, focusing on the health sector as critical infrastructure. Its primary objective is to assess the effectiveness of NIS2's legal mechanisms – risk management, incident reporting, and management accountability – in safeguarding health systems. The research methodology involves a detailed analysis of four recent case studies: Synnovis (2024), NailaoLocker (2024), HSE (2021/2024), and Vastaamo (2020/2024), supplemented by additional research from sources such as ENISA reports and European Commission documents. Findings highlight strengths, including rapid reporting and management accountability, alongside weaknesses such as coordination delays, legacy system vulnerabilities, and uneven transposition. The implications indicate that while NIS2 provides a robust framework, it requires operational and financial support to ensure resilience, proposing reforms like a unified crisis protocol and mandatory system upgrades. This study contributes to the legal discourse on EU cybersecurity, emphasizing the need for harmonization and adequate resources.

ARTIFICIAL INTELLIGENCE ACT AND GDPR: IMPLICATIONS FOR AI SOLUTION DEVELOPERS AND USERS IN ROMANIA

Associate professor Camelia Daciana STOIAN
Faculty of of Humanities and Social Sciences, "Aurel Vlaicu" University of Arad, Romania
Professor Dominic BUCERZAN
Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania
Lecturer **Radu Nicolae STOIAN**
Faculty of of Law, "Vasile Goldiş" University of Arad, Romania
Asistant professor Catalin Raul HALIC
Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania
Associate professor Crina Anina BEJAN
Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania

Abstract

Artificial Intelligence (AI) poses a significant challenge for personal data protection legislation, substantially impacting the way Romanian companies develop and implement AI solutions, as well as affecting human rights. At the European level, the Artificial Intelligence Act (AIA) introduces a regulatory framework for the responsible use of AI, which must be harmonized with the General Data Protection Regulation (GDPR). In this context, Romania faces challenges regarding the compatibility of its national legislation with these European regulations, particularly concerning automated data processing, algorithmic transparency, user rights, and the impact of AI use in judicial and administrative systems. The study examines the extent to which Romanian legislation is prepared to accommodate the new requirements imposed by the AIA, highlighting legal risks and additional obligations for companies developing AI-based solutions. It also evaluates the potential consequences for the Romanian technology market, including impacts on AI-focused startups and institutions utilizing artificial intelligence technologies in their operational processes. The study's conclusions emphasize the need for a proactive and integrated approach to ensure compliance with European standards while simultaneously protecting technological innovation and user rights.

FACULTY OF LAW
Charles University

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 5th edition, March 28, 2025 -
www.adjuris.ro/fintech

DIGITAL RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES AND PERSPECTIVES

Lecturer Aurel Octavian PASAT
Cross-border Faculty, „Dunarea de Jos" University of Galati, Romania

Abstract
As AI technologies become deeply integrated into society, new legal challenges arise related to the collection and use of personal data, as well as risks associated with mass surveillance and digital censorship. The article explores the growing impact of artificial intelligence (AI) on digital rights, focusing on issues such as privacy, access to data, and freedom of expression. It also emphasizes the need to maintain a balance between technological innovation and the protection of citizens' fundamental rights, through a comparative analysis between different legal systems. It provides a look at the data protection legislative framework in the European Union (GDPR) versus that in the United States, examining emerging challenges and opportunities. Relevant case studies are used to illustrate how regulations can be implemented effectively or where they are insufficient, suggesting possible solutions and future directions.

CURRENT CHALLENGES REGARDING TOURISM LAW IN THE METAVERSE

Associate profesor Mădălina BOTINA
Faculty of Law and Administrative Sciences
Ovidius University of Constanta, Romania

Abstract
The synergy between tourism and the metaverse must receive special attention. The metaverse is part of a broader concept known as virtual tourism. This refers to immersive tourism experiences provided through digital technologies such as virtual reality (VR), augmented reality (AR), and artificial intelligence. Virtual tourism allows users to explore destinations, visit museums, or participate in cultural events without being physically present. Thus, the metaverse is a virtual world connected to reality, where users, through a technical prosthesis in the form of a virtual reality headset, progress and evolve in the form of an avatar. A new experience in space and time makes the Metaverse the "instrumentum" of a hybridization of the permanent offer available to industry players, enhancing resources in both virtual and real tourism in a parallel manner. It becomes both the content and the container of a digitalization process, whose impact can be summarized as attracting, enhancing, and reinforcing. Attracting more and better through the construction of a storytelling approach that speaks directly to the target audience while sparking the traveler's desire. The hospitality sector sees this as an opportunity to reinvent itself.