Section II.
Cyberspace and Artificial Intelligence Law

Friday – March 22, 2024

ONLINE ON ZOOM

Moderators:

Associate professor **Cristina Elena POPA TACHE,** *„Andrei Şaguna" University of Constanta*

Lecturer **Radu Ștefan PĂTRU,** *Faculty of Law, Bucharest University of Economic Studies*

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

SCIENTIFIC PAPERS

10.00 - 11.00

ELECTRONIZATION OF THE HEALTHCARE SECTOR AND ITS RESPONSIBILITY IN RELATION TO IT AND AI

JUDr. Tereza JONÁKOVÁ
Department of Public Administration, Police Academy of the Czech Republic

Abstract
The modern phenomenon of electronization and digitalization of the contemporary information society affects many areas of human life, and produces, mainly due to the unclear construction of legal liability in relation to AI and its activities, many relevant questions. If AI and the activities and services linked to it are to be responsible to society, they should, above all, be fair, accountable, transparent, confidential and secure to their users, not only with legal implications, but also with moral and ethical ones, all with the aim of mitigating technical and technological risks while maintaining the guarantee of fundamental human rights and freedoms.

EXPLORING THE LANDSCAPE OF ARTIFICIAL INTELLIGENCE LAW IN ALBANIA

Associate professor Rezarta TAHIRAJ
Faculty of Economy/University of Elbasan "Aleksandër Xhuvani", Albania
Director of Scientific Research Centre for Researches and Developments in Law and Economy

Abstract
The advent of artificial intelligence (AI) technologies has brought about significant transformations across various sectors worldwide, prompting governments to adapt legal frameworks to address emerging challenges and opportunities. This paper examines the current state of AI law in Albania, offering a comprehensive analysis of its regulatory landscape, challenges, and potential avenues for advancement. Drawing upon a review of existing legislation, policy documents, and scholarly literature, this study identifies key areas where AI intersects with legal principles and regulatory frameworks in Albania. It explores issues such as data protection, privacy rights, algorithmic transparency, liability, and ethical considerations, highlighting the need for tailored legal frameworks to govern AI deployment and mitigate potential risks. Moreover, the paper discusses the role of international standards and best practices in shaping Albania's approach to AI regulation and underscores the importance of collaboration between government, industry stakeholders, and civil society in fostering responsible AI innovation. By shedding light on the current state of AI law in Albania and proposing strategies for its enhancement, this paper contributes to the ongoing discourse on the global governance of AI technologies and informs future policy developments in the Albanian context.

THE RELATIONSHIP BETWEEN THE VICTIM AND THE PERPETRATOR IN THE ONLINE MEDIATION PROCEDURE

PhD. candidate Fat MUSTAFI
Law Faculty, South East European University of Tetovo, North Macedonia
Professor Ismail ZEJNELI
Law Faculty, South East European University of Tetovo, North Macedonia

Abstract

The victim and the victimizer or the criminal and the victim are often found in interactions and various interactive relationships. The victim and the victimizer in some cases of victimization are always in some relationships and relationships from before, these relationships and relationships can be of various natures, in most cases they are parental relationships, marital relationships, cohabitation or engagement relationships, family or even neighborly love ties. Restorative justice is an approach to justice oriented towards the possible repair of damage caused by a crime or conflict. An essential element of restorative justice is the active involvement of parties, victims, perpetrators, and when appropriate, community members, who voluntarily come together with the help of a mediator to talk about the harm and its consequences, as well as to identify ways to repair them. Restorative justice aims to bring justice to people and considers participation as an important human value that connects people. The focus of restorative justice is on what people perceive as a fair and safe experience in the phase after a crime or conflict has occurred. The purpose of restorative justice is to create a safe environment for sharing feelings (such as fear, anger, sadness) that have arisen as a result of conflict or crime and to talk about possible solutions for repairing the damage.

AI LIABILITY: TOWARDS A EUROPEAN REGULATION

Professor Cristina SEIA
Lusíada University of Porto, Portugal

Abstract

The opening up of the world to new technologies and artificial intelligence poses new challenges in terms of safety and liability. For this reason, the European Union has been working on a European liability regime for damage caused by these new technologies, in particular artificial intelligence systems, with the aim of establishing a legal framework that favors the prevention of damage resulting from the use of artificial intelligence systems and provides legal certainty for their users, equipping them with effective recourse mechanisms in the event of damage suffered. This framework is key to promoting the social acceptance of modern technologies which depend on ensuring a high level of security for their users, and to promote the free movement of goods and services. The aim of this paper is to critically analyze the developments made by the European Union to date with a view to creating a legal regime of this nature, by analyzing the existing legal texts and the main literature on the subject.

11.00 - 12.00

CYBER CHALLENGES AMID THE DIGITAL REVOLUTION IN MARITIME TRANSPORT

Assistant professor Konstantinos KOUROUPIS
Frederick University, Cyprus
PhD. candidate Leonidas SOTIROPOULOS
European University of Nicosia, Cyprus

Abstract

The smart shipping and maritime technology encompasses blockchain and smart contracts technology, information perception technology, autonomous shipping, state monitoring and so on. Nevertheless, these advancements bring with them practical and legal challenges, as well as a new cyber threats. This paper deals with the key challenges and opportunities associated with the integration of digital technologies in shipping transport such as smart contracts and unmanned ships, and how do cyber issues impact the safety, security, and efficiency of maritime operations. Furthermore, its aim is to focus on the new threat that of cybercrime. On this article, the dogmatic legal method is followed, assisted by the socio-legal approach method. The first part examines the technological background into which smart contracts are integrated and operate, i.e. the terms blockchain and technology distributed ledger technology. The concept, the mechanism and the types of smart contracts in maritime industry are further analysed. Also, the aspects of new technologies such as Autonomous Vessels and the challenges they raise are examined. The second part focuses on the legal potential of smart contracts examining their issues and the cyber challenges in maritime industry. The critical remarks and conclusions drawn are listed at the end of the paper.

INFORMATION SUPPORT FOR COMBATING CRIMINAL OFFENCES BY THE STATE BORDER GUARD SERVICE OF UKRAINE (CRIMINOLOGICAL ASPECT)

Associate professor Iryna KUSHNIR
Deputy Chief of Administrative Activities Department,
Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine
Candidate of law, senior researcher Yuliia STEPANOVA
Deputy Chief of the Scientific Research Department,
Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine

Abstract

The article deals with the research of information support for combating criminal offences of the State Border Guard Service of Ukraine taking into account the criminological aspect. This area of information support is directly related to the development of the modern information digital society. The State Border Guard Service of Ukraine (SBGSU) uses modern methods and technologies of criminology to combat criminal offences. The need to improve the organisational and legal instruments (methods) of information support and continuous improvement of information technologies in the field of combating criminal offences determine the relevance of the research topic raised in the article. The purpose of the article is to study, identify the peculiarities and prospects of using information support for combating criminal offences by the SBGSU in the criminological aspect. The methodological basis of the research was formed by a combination of general scientific, sectoral and special scientific methods, which enabled to achieve the research objective when applied in a comprehensive manner. The dialectical method made it possible to consider information support as a complex legal phenomenon in the search for opposites of the essence, elements, and features in their interconnection. The structural and functional method was used to establish the components of information support and the relationship between them. The formal and logical method enabled to formulate concepts and identify areas of information support for combating criminal offences by the SBGSU. To formulate proposals for improving information support for combating criminal offences, the forecasting method was used. Within the article: the essence of information support is clarified;

the information support of criminological monitoring is studied; the possibilities of risk analysis as a component of information support of criminological monitoring are analysed; information support for combating criminal offences based on open data is considered; the prospects for using artificial intelligence are studied, and promising directions for information support for combating criminal offences by the State Border Guard Service of Ukraine are proposed.

CYBERCRIME VICTIMIZATION

PhD. student Dora ARIFI
South East European University of Tetovo, North Macedonia
Professor Besa ARIFI
South East European University of Tetovo, North Macedonia

Abstract

Digitization has taken over the whole world and it's terrifying. The reason behind this is that the Internet offers many options for its users, some of which are very productive. Unfortunately, it also creates a space for hackers to operate freely and achieve their goals. As the number of internet users is increasing, cybercrime victimization is at the highest rate every day. Cybercrime is a new term that defines illegal activity that involves a network, computer, or network device. Cybercrime is a criminal offense committed against individuals or institutions. Anyone can be a victim of cybercrime. As a result, combating this type of crime presents a new challenge for law enforcement. It is crucial to understand the risks and consequences to take appropriate measures to protect the victims of such crimes. The paper is prepared based on other works to finally conclude that cybercrime is a worldwide problem, and no one is immune to it. We must raise awareness of the possible consequences and prevent future cyber victimization before it's too late.

ARTIFICIAL INTELLIGENCE - CURSE OR BLESSING? HISTORICAL ANALYSIS OF DIGITAL DEVELOPMENTS UP TO THE FIRST EUROPEAN LAW ON ARTIFICIAL INTELLIGENCE (AI-ACT)

PhD. candidate Julia KRENN
University of Economics in Bratislava, Slovakia

Abstract

Changes in the way people live and work, driven by digitalization and automation, have always triggered fears. Developments in the field of digitalization and automation, as well as the use of artificial intelligence, which has been the subject of much discussion recently, require people in all areas to have a certain degree of adaptability. Increasing complexity, the loss of jobs and the challenges of data protection are just a few examples of the challenges facing not only society but also legislators. The simplification of daily life and the increasing efficiency gains made possible by AI are some of the arguments in favor of using AI. The EU law on artificial intelligence aims to ensure that AI systems brought to market and deployed in the EU are safe and in line with the EU's fundamental rights and values. The groundbreaking proposal is also intended to promote investment and innovation in the field of AI in Europe.

12.00 - 13.00

CONSUMER PROTECTION SAFEGUARDS AFTER THE AI ACT

Ph.D. student Simos SAMARAS
National and Capodistrian University of Athens, Greece
Assistant professor Dimitrios DEVETZIS
Frederick University, Cyprus,
Visiting Professor at Leibniz University in Hannover, Germany

Abstract

The long awaited introduction of the AI Act, notwithstanding its originality, does not introduce any regulation outside the existing framework. It supplements the safeguards provided in numerous sectors of the EU legislation, inter alia, consumer protection. An examination of the basic EU law along with national legislation of the most influential legal orders, i.e. the French and German one, and model rules of the Draft Common Frame of Reference (DCFR) confirms that the new AI Act sheds light on pre-existing vague legal concepts. In this respect, this novel piece of legislation promotes a better understanding of traditional notions of law applicable to the modern digital reality without introducing totally new rules. Accordingly, certainty of law is reinforced where consumer protection had languished, not because of legislative shortage, but for facts and situations described as necessary conditions of certain rights were contested on the basis of contrary possible interpretations of decisive terms. Ultimately, the very importance of the AI act regarding consumer protection lies not in the introduction of new rights and obligations, but in a multiple practical assistance to the implementation of existing rules adjusting thus the traditional legal concepts with technological development beyond their original scope.

ARTIFICIAL INTELLIGENCE REGULATION: APPROACHES AND IMPLICATIONS

PhD. student Gabriel NIȚĂ
Faculty of Law, „Babeș-Bolyai" University of Cluj-Napoca, Romania

Abstract

The complexity of technological risks and cyber security risks with a major significant impact on fundamental rights and freedoms arising from the adoption of new artificial intelligence technologies calls for the implementation of specific regulations adapted to the rapid pace of technological innovation and the continuous evolution of threats in this area. The proposed study will focus both on the critical analysis of the regulatory and institutional instruments for regulating artificial intelligence as one of the so-called disruptive technologies and on the challenges faced by regulators. Methodologically, the research will involve the identification and analysis of the risks associated with AI technology, followed by a systematic assessment of the mandatory (hardlaw) and non-mandatory (softlaw) legal instruments applicable to the field, as well as proposed governance system proposals, in order to identify similarities and juxtapositions. In addition, synthesising the views expressed in legal doctrine will make an important contribution to analysing and understanding the challenges to regulation and governance posed by new digital technology. By analysing from different perspectives, the proposed regulations to prevent risks associated with artificial intelligence, the scientific contribution brings into question possible directions for the future regulatory framework.

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 4th edition, March 22, 2024 -
www.adjuris.ro/fintech

SCENARIOS ABOUT THE FUTURE OF LEGAL PROFESSIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE?

Professor Verginia VEDINAȘ
Corresponding member of the Romanian Academy of Scientists
President of the "Paul Negulescu" Institute of Administrative Sciences, Romania
Lecturer Ioan Laurențiu VEDINAȘ
Western University "Vasile Goldiș" from Arad, Romania

Abstract

The present study aims to address, succinctly, aspects that concern the future legal professions in the age of digitization. The changes that this period will bring to all professions represent a general concern. It is obvious, however, that the effects to be produced are not similar either as content, or quantitatively. If they are professions "prone" to be replaced, in completeness, computer, equally are professions whose content will be modified, without however, they can be fully transferred from human to computer. Among these, we appreciate that there are also legal professions. Some of the ways in which they are exercised, it will be possible to move into the "competence" of the computer, but man cannot disappear never, entirely, from their exercise.

ARTIFICIAL INTELLIGENCE - THE ERA OF SOCIAL INEQUALITIES. IN REGULATING THE FUTURE, WE NEED TO LOOK AT THE RISKS

Associate professor Carmen Oana MIHĂILĂ
Department of Juridical and Administrative Sciences, Faculty of Law,
University of Oradea, Romania
Lecturer Mircea MIHĂILĂ
Department of Computers and Information Technology,
Faculty of Electrical Engineering and Information Technology, University of Oradea, Romania

Abstract

AI brings with it ethical and legal issues, the discrimination, and workplace safety risks. Decision making through AI techniques is changing the relationships between individuals as we know them today. The development of AI and the integration of these systems into essential services for the population can accentuate imbalances in society and between states. Generating certain predictive models by identifying patterns in the collected data and grouping people in this way can lead to discrimination against certain groups (bias can be encoded in algorithms). Errors or biases may also occur that affect the integrity and confidentiality of information where it is difficult to understand how AI makes data security decisions. In the absence of human supervision and boundary drawing, autonomous AI may hold big surprises. The article will analyse some aspects related to the risks that the use of AI systems involves on fundamental rights, with reference to private life, data protection, non-discrimination regarding and to the effects that the development of AI has in creating new social inequalities.

13.00 - 14.00

ADVANTAGES AND CONSTRAINTS FROM THE PERSPECTIVE OF ADOPTING THE AI ACT FOR THE PUBLIC ADMINISTRATION IN ROMANIA

Associate professor Lucia Flavia GHENCEA
„Ovidius" University of Constanța, Romania

Abstract

The AI Act is a proposal with an exclusively innovative character in the legislative field, being the first law developed by a major regulatory body in the field of artificial intelligence (AI). The law operationalizes AI applications in three risk categories. First, it considers applications and systems that create an unacceptable risk. Second, high-risk applications are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated. If the path of this act was, without a doubt, a particularly difficult one, the practical application will certainly raise several practical problems, depending on the states that will implement it. We propose, in this work, an analysis of the European normative act, from the perspective, on the one hand of the intentions pursued by the European legislator and, on the other hand, of how Romania will implement the AI legislation. We refer to possible situations in which the Romanian public administration will find itself through the prism of the advantages it can obtain, on the one hand, but also, on the other by the prism of the constraints imposed by the regulations in force. We conclude with some proposals to the legislator in the perspective of obtaining concrete advantages following the implementation of this act.

FROM THE INFORMATIC CRIME TO THE INFORMATIC CRIMINALITY

Associate professor Carmen Adriana DOMOCOS
Faculty of Law, University of Oradea, Romania

Abstract

Although the digital world brings enormous benefits, it is also vulnerable. Cyber space incidents, either intentional or accidental, are rising to an alarming level and could disrupt the provision of essential services. State economies are already affected, to a great extent, by cybercrime activities against individuals, public and private sectors. Virtual criminals use more and more complex methods for penetrating into computer systems, such as critical data theft or repositories. Cyber security has become a component of the security of all states, which, according to international conventions and treaties, can be achieved through the knowledge, prevention and counteraction of attacks and threats, as well as by diminishing the vulnerabilities of cyber infrastructures for the effective management of all security risks prevention, and fight against cybercrime and, last but not least, cyber defense. The provision in the new Criminal Code of possible or facilitated offenses by new information and communication technologies, in particular crimes against the security and integrity of systems and computer data, is a necessary action to synchronize our criminal law at the highest level with European law and as well as the necessary response to the exponential growth of this type of crime.

LIABILITY OF NEWS PLATFORMS UNDER THE DIGITAL SERVICES ACT

Assistant professor Sorin-Alexandru VERNEA
Faculty of Law, University of Bucharest, Romania

Abstract

This article analyzes the conditions under which news platforms can be held liable under European Regulation (EU) 2022/2065 of the Parliament and of the Council (Digital Services Act). The first part concerns the object of the DSA regulation, by reference to news platforms, and the second part regards the notion of illegal content and its specific nature in the case of news platforms. The third and fourth parts concern the liability of the online platform both for posted articles and for advertising, in which the author has identified a distinct regime depending on the type of uploaded material. The conclusion of the paper concerns the importance of the European Regulation (EU) 2022/2065 of the Parliament and of the Council for the activity of journalists and news platforms.

THE ROLE OF DIGITAL TECHNOLOGY IN IMPROVING FOOD SECURITY: CHALLENGES AND OPPORTUNITIES

PhD. Geronimo Răducu BRĂNESCU
Transilvania University of Brașov, Romania

Abstract

In the current context, where the widespread use of artificial intelligence and digital technologies has become ubiquitous, this study aims to investigate the impact of these technologies on activities supporting food security. The key role of digital technology in this area is highlighted, in particular in addressing challenges and providing opportunities for safe and affordable food for the whole population. The article highlights how supply chain monitoring and tracking, the implementation of smart agriculture, and the use of data analytics and artificial intelligence can contribute to the sustainability and efficiency of the food system. These can be successfully complemented by communication and awareness through mobile applications and online platforms, used to increase consumer engagement and responsibility. On the other hand, the article also highlights the challenges associated with the intensive use of artificial intelligence and digital technologies in terms of accessibility and data security. In conclusion, it is crucial to make rational use of digital technologies and artificial intelligence to develop a sustainable, safe and crisis-resilient food system.

14.00 - 15.00

THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS AND JUDICIAL PROCESSES: CHALLENGES AND OPPORTUNITIES

Lecturer Mihai ȘTEFĂNOAIA
„Ștefan cel Mare" University of Suceava, Romania

Abstract

The proposed study explores the use of artificial intelligence in criminal investigations and judicial processes, with a focus on the associated challenges and opportunities. The objectives include analyzing the applicability of AI practices in evidence collection and analysis, evaluating the effectiveness of AI algorithms in identifying offenses, and exploring the impact of automated systems in judicial processes. Research methods include literature review, case studies, and critical analysis of existing regulations in the field of AI utilization in justice. The results of the study highlight the effectiveness of AI in accelerating criminal investigations and streamlining judicial processes, as well as the associated risks such as discrimination and algorithmic errors. The implications of the study emphasize the need for clear regulations and guarantees regarding the transparency and correctness of automated decisions, as well as the potential to improve the efficiency of the judicial system through the implementation of AI technologies. These findings provide a critical perspective on the use of artificial intelligence in justice and underscore the importance of a balanced approach between innovation and protection of individual rights.

THE PROCESSING OF PERSONAL DATA IN CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT AND SERVICES

PhD. student Sorana BRISC
Doctoral School, Faculty of Law,
„Babeș-Bolyai" University in Cluj-Napoca, Romania

Abstract

This paper highlights the impact of personal data processing in contracts for the supply of digital content and services. The primary aim of this study is to clarify the role played by the consent given by the data subject to the processing of personal data within the framework of these new-wave digital contracts. In particular, our focus lies on discerning the consequences of the withdrawal of consent on the contract itself. This subject requires a multidisciplinary approach. By using the historical, theoretical and descriptive method of scientific inquiry, we hope to provide a more precise understanding of the complex regulatory framework governing electronic commerce. The paper commences by explaining the socio-economic and regulatory context in which the processing of personal data influences contract law. In the first section of the paper, we underline the distinction between two manifestations of will: the contractual consent, understood as a prerequisite for the validity of a contract, and the GDPR consent, representing an agreement to the processing of personal data. Subsequently, we emphasize the role of GDPR consent in synallagmatic contracts for the supply of digital content and services whereas the third section deals with the effects of GDPR consent withdrawal on the digital contract. Following our research, we concluded that there is a symbiotic relationship between the two legal forms of consent, despite their different nature. It is certain that the extensive processing of data, often referred to as "Big Data", which has been prevalent for at least a decade, claims the need to protect the consumer of digital content and services beyond the non-patrimonial nature of the fundamental rights regulated by Regulation (EU) 2016/679.

HACKING VEHICLES' COMPUTER SYSTEM

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

Abstract

The advent of automotive hacking is a result of the use of electronics in cars. A few years ago, tuning an automobile to produce more power required tuning automotive gear; nowadays, the on-board computer is the new target. For the first time, researchers from Washington and California linked the on-board computer to the OBD-II connector, automatically hacked the system, and installed the Car Shark malware. Aside from other nefarious things, this program could lock the doors, turn off the engine, and force hot air into the cabin. The only solace is that accessing the OBD-II port requires entering the vehicle, and once an attacker is inside, it is simpler for him to take a vehicle than conducting hacking activities. Researchers from the University of South Carolina and Rutgers University had an opposite opinion. They claim that it is possible to remotely hack the car and even control it while it is moving. They use tire pressure sensors to accomplish it. Radio frequencies are used by these sensors to transmit data. Scientists were able to follow the vehicles and tamper with the transmitted data with the use of this signal.

AI IN PUBLIC ADMINISTRATION OR AI AS A PUBLIC SERVANT? A SHORT PREVIEW OF THE RELEVANT PROVISIONS COMPRISED IN THE WORLD'S FIRST MAJOR ACT TO REGULATE AI

Assistant professor Cosmin SOARE-FILATOV
Faculty of Law, University of Bucharest, Romania

Abstract

The European Union's Artificial Intelligence Act is a groundbreaking law that seeks to create a cohesive framework for Artificial Intelligence use across European Union. It's crafted with the future in mind, emphasizing adaptability to keep pace with rapid technological advancements. This regulation sets a global benchmark for responsible AI governance, reflecting a bold commitment to both innovation and fundamental rights. In a fast-changing world, the principles of public administration necessitate flexibility and adaptability. This is why we consider the principle of adaptability as vital. European States considered likewise. This approach allows public administration to remain agile, capable of integrating AI not just as a tool but as a partner in governance. This adaptability encourages a dynamic approach, where AI can enhance public services and decision-making while adhering to stringent safety, transparency, and accountability standards. The vision is clear: AI, within the bounds of this Act, should serve the public good, evolve with societal needs, and uphold the highest ethical standards.

15.00 - 16.00

ARTIFICIAL INTELLIGENCE AND THE FUNDAMENTAL HUMAN RIGHTS

Professor Irina MOROIANU ZLATESCU
National University of Political Studies and Public Administration, Romania

Abstract

Artificial Intelligence, which is developing at an extremely surprising, accelerated pace, has now reached the point of creating systems with cognitive abilities similar to human beings, from perception, understanding, language, reason, even being able to make decisions. Under these circumstances, AI can be perceived from two perspectives, both as a particularly useful tool in many fields, in medicine, contributing to the improvement of the process of diagnosing some diseases, in the economy, by optimizing the management of enterprises, and others, but it can become a threat to the privacy of citizens, for example through the use of personal data in violation of human rights principles. That is why it is necessary to find a balance between the use of AI for the advantages it brings and the protection of citizens' personal data, as it is necessary to establish clear responsibilities and effective control over the way in which Artificial Intelligence is used. A concern, in this sense, has existed in recent years at the global and regional European level. After a series of regulations adopted within the Council of Europe and by the OECD that aim to protect fundamental rights, democracy, and the rule of law, in the face of high-risk AI systems or prohibit certain uses of it that threaten fundamental human rights, these days the European Union came up with an important regulation. Thus, on March 13, 2024, the European Parliament adopted a reference normative act, namely the Legislative Resolution on the proposal for a regulation of the European Parliament and the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union, which we propose to analyze in our study from the perspective of comparative law.

GOOGLE HACKING

PhD. Marius-Vasile BÂRDAN
Faculty of Psychology, Behavioral and Legal Sciences,
„Andrei Șaguna" University of Constanta, Romania

Abstract

This is the method by which an attacker sends a search request to the search engine with the intention of obtaining sensitive information from the web pages indexed by Google or finding vulnerabilities of these web pages. This kind of hacking can be used on any other search engine (it could be called search hacking). Sensitive information on pages stored by Google depends on the ability of the search robot to browse and store the Internet for indexing. The more sophisticated and refined this action, the greater the possibility of sensitive, non-public information being stored by Google. Sensitive information can mean any information related to a card account, for example, up to the folder structure of the server. It can also identify target server vulnerabilities or error messages that may contain valuable information.

ADJURIS
Society of Juridical and Administrative Sciences

INTERNATIONAL CONFERENCE ON FINTECH, CYBERSPACE AND ARTIFICIAL INTELLIGENCE LAW
- 4th edition, March 22, 2024 -
www.adjuris.ro/fintech

LAW IN THE INTERNET OF THINGS ERA. OPPORTUNITIES AND VULNERABILITIES

Assistant professor Tiberiu T. BAN
Faculty of Law, „Bogdan Vodă" University of Cluj Napoca, Romania

Abstract

In the context of computerization and automation of most economic sectors and private life, the increase in the number of attacks on computer systems that expose personal data to unauthorized persons is alarming. It started from a hypothesis already validated in the specialized literature that properly designed security policies and procedures can prevent attacks exploiting known vulnerabilities to a satisfactory extent. However, their simple existence is not enough, these security policies and procedures must be adapted to the specifics of each computer system, with the appropriate legal support. We followed a trans-disciplinary analysis that combines elements of informatics and legal regulations regarding the opportunities and vulnerabilities of smart devices, face to face with the criminal phenomenon of cyber crime aimed at the security and confidentiality of personal data. The main objective of the present study is to identify and extract "lessons learned" regarding vulnerabilities of Internet of Things type information systems. These "good practices" allow the development of procedures and security policies useful in preventing computer attacks criminalized as the crime of unauthorized access to a computer system.

SYNOPTIC APPROACH REGARDING THE IMPLICATIONS GENERATED BY THE USE OF „AI SYSTEMS" IN BUSINESS-TO-CONSUMER CONTRACTS

Associate professor Elise Nicoleta VÂLCU
Pitesti University Center - Faculty of Economic Sciences and Law,
National University of Science and Technology "Politehnica" from Bucharest, Romania

Abstract

The issue of the use of AI in the field of B2C contracts is limited to the objectives assumed by the European Union regarding ensuring the good functioning of the internal market through the stability of the harmonized rules that regulate the use of artificial intelligence in the internal market and ensures, at the same time, a high level of protection. of public interests, such as health, safety and the protection of fundamental rights, as recognized and protected by European Union law. The presence of "digital assistants" in the B2C contract is a "component" area of the European Union's Digital Strategy which aims to regulate artificial intelligence. Topics such as the presence of digital assistants and the implications of their actions in the pre-contractual, conclusion or execution stages of B2C contracts, but also the identification of specific elements of B2C contracts, as a result of their automation through the presence of AI, or the need for legislative adjustments precisely to increase the protection of legal protection of consumers in the context of the presence of AI, will represent topics of reflection advanced by the author of this research.

16.00 - 17.00

THE DECISION ON DISCIPLINARY SANCTIONING OF THE EMPLOYEE WITH SOME REFERENCES TO ITS COMMUNICATION THROUGH ONLINE MEANS OF COMMUNICATION. ELEMENTS OF COMPARATIVE LAW

Lecturer Mihaela MARICA
Faculty of Law, Bucharest University of Economic Studies, Romania

Abstract
Internally, the field of labor discipline is a complex one both from a normative and jurisprudential point of view. In order to ensure a better understanding of the practical implementation of these regulations, this article reviews some theoretical and practical aspects regarding the validity of issuing the decision to sanction the disciplinary of the employee, with an emphasis on doctrinal and jurisprudential issues identified regarding the term in which the sanctioning decision can be issued by the employer, the content elements of the sanctioning decision, the individualization of the disciplinary sanction in relation to the conclusions of the Disciplinary Commission, as well as regarding the communication of sanctioning decisions through online methods . Also, in order to outline a clearer and overall technical-legislative picture of the regulations regarding the issuance of the sanctioning decision, the regulations of other states are also relevant in achieving this objective, the elements of comparative law being aspects that will be closely examined. Thus, the legal systems of France, Cyprus, Great Britain, Georgia are considered.

STUDY ON DIGITAL TRANSFORMATION AND LAW

Professor Carmen Silvia PARASCHIV
Faculty of Law, „Titu Maiorescu" University of Bucharest, Romania

Abstract
The article studies the interaction between digital transformation and the legal field, analyzing the impact of digital technologies on legislation and legal practice. After outlining the basics of digital transformation, it examines how technological evolution affects the rule of law and the legal implications of digital transformation, with a focus on data protection and privacy in the digital age. Emerging legal tools such as smart contracts and blockchain technology present challenges and opportunities. Access to justice in the digital age is analyzed, noting the influence of technology on legal processes and online dispute resolution platforms. The paper also addresses the impact of digital transformation on legal education and the ethical issues associated with the use of technology in legal practice. The paper emphasizes the importance of adapting the legal system and educational practices to the changes generated by the digital transformation.

THE ADVANTAGES OF USING ARTIFICIAL INTELLIGENCE IN INTERNATIONAL ARBITRATION REGARDING DISPUTES RESULTING FROM THE COMMERCIALIZATION OF TOURIST SERVICES IN THE HORECA FIELD

PhD. student Laura Ramona NAE
Doctoral School of Law, Bucharest University of Economic Studies, Romania

Abstract
In the context of the contractual relations resulting from the marketing of tourist services in the HoReCa field, we identify various decisive motivations for which the parties opt for the settlement of a dispute by means of alternative extrajudicial settlement methods (ADR) such as arbitration, through arbitration clause, in order to obtain a solution

favorable to both. These considerations include aspects such as: maintaining and continuing to develop business relationships; rapid resumption of joint business operations; protecting the reputation and notoriety of the parties involved, strategic partners in the specialized profile market; safeguarding the international brand under which the parties operate, in the event of the existence of a franchise agreement, etc. The imminent technological archetype emerging from the use of artificial intelligence (AI) presents a concrete and continuously expanding impact on the entire global socio-economic and geo-political context. It presents an implicit, unavoidable influence on the business environment of the activity of multinational companies, including those in the HoReCa field, which continuously adapt their global practices and policies in order to maintain a single AI development process. The influence exerted by the use of AI also concerns the procedural ways of resolving disputes resulting from the contractual relationships carried out within this field of activity, respectively the matter of international arbitration.

SOME REFLECTIONS ON TWO OF THE MOST VISIBLE DEVELOPMENTS: THE RIGHT TO REFUSE INTERNET USE AND THE 'CHILLING EFFECT'

Associate professor Cristina Elena POPA TACHE
Faculty of Psychology, Behavioral and Legal Sciences, „Andrei Saguna" University, Romania
Lecturer Heliona MIÇO (BELLANI)
Law Department of Epoka University, Tirana, Albania

Abstract

The use of technology brings forth several dilemmas, as does internet usage. Not all individuals possess the necessary skills to master technological capabilities – a challenging feat for most of the world's population. The internet is considered by definition a technology, and in this capacity, it is natural to be attached to a series of rights and obligations. From society's accumulated experience, we have witnessed various metamorphoses of human rights, and one of the precursors to the right not to use the internet is the right to disconnect, increasingly encountered. In what stage is this concept of the individual's right to abstain from participating in the online sphere? Is it an El Dorado for modern human rights? How far can individual autonomy go? Why together with the "chilling effect"? Because the connection between individual autonomy and freedom of expression lies in the fact that freedom of expression is often a way in which people express and affirm their autonomy. Through liberal expression, an individual can express their identity, values, and preferences, contributing to the development and affirmation of their own autonomy. The chilling effect, seen as a modern form of lawfare, stifles the evolution of individual rights, reduces freedom, and diminishes the autonomy of individuals in deciding whether or not to use the internet and to what extent they choose to do so online. This article aims to initiate essential discussions regarding the legal and ethical aspects that may make this option of humanity not to use the internet possible or impossible.