Latent profiles of adolescents’ digital skills across six European countries

Hietajärvi, Lauri

2023-11


http://hdl.handle.net/10138/570051

Downloaded from Helda, University of Helsinki institutional repository.

This is an electronic reprint of the original article.

This reprint may differ from the original in pagination and typographic detail.

Please cite the original version.
# Programme - List of abstracts

## Room 025

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30 - 11:00</td>
<td>Parallel streams</td>
</tr>
<tr>
<td></td>
<td><strong>AI, Data Governance, and Cybersecurity in Financial Services (special track) - Online</strong></td>
</tr>
<tr>
<td></td>
<td>chaired by Alex Ivančo, Joseph Lee</td>
</tr>
<tr>
<td>Alex Ivančo, Joseph Lee</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>Marcus Tsai</td>
<td>AI and Governance in the Financial Market</td>
</tr>
<tr>
<td>Rachel Ntongho, Joseph Lee</td>
<td>Cybersecurity and Corporate Governances</td>
</tr>
<tr>
<td>Vere Marie Khan, Joseph Lee</td>
<td>Open Finance and Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>11:00 - 11:15</td>
</tr>
<tr>
<td>11:15 - 12:45</td>
<td>Parallel streams</td>
</tr>
<tr>
<td></td>
<td><strong>AI, Data Governance, and Cybersecurity in Financial Services (special track) - Online</strong></td>
</tr>
<tr>
<td></td>
<td>chaired by Alex Ivančo, Joseph Lee</td>
</tr>
<tr>
<td>Alessio Azzutti</td>
<td>ComplianceGPT: Legal Implications of Generative AI Models for Financial Regulatory Compliance</td>
</tr>
<tr>
<td>Daniel De Paiva Gomes, Joseph Lee</td>
<td>Lawtech, Access to Justice and Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>Discussion</td>
</tr>
<tr>
<td></td>
<td>12:45 - 13:45</td>
</tr>
<tr>
<td>13:45 - 15:15</td>
<td>Parallel streams</td>
</tr>
</tbody>
</table>

**Partners**

(Images of logos for sponsors)
AI Technologies: generative, destructive - Room 025

Adrienn Lukacs
ChatGPT in the Workplace - Opportunities and Challenges of Using Large Language Models in Labor Law

Technological developments, and among them artificial intelligence (AI), are fundamentally shaping everyday life in the 21st century – and the world of work is no exception. The potential applications of AI in employment seem to be without limits and is constantly evolving. These potential AI solutions include large language models (LLMs), among which ChatGPT – an AI chatbot – recently made headlines and gained considerable attention of the public and of the scientific community. It can be projected that ChatGPT and other LLMs will play a prominent role in information societies in the near future, thus special attention must also be paid to the labor law challenges caused by them. There are a number of possibilities for the use of LLMs both for employers and for employees – of which the presentation focuses on the use of LLMs by employees as a work tool, by addressing the opportunities and challenges that they might introduce and the possible answers given to them. While their use can help to increase employees’ productivity, provide guidance, or relieve them of menial and routine tasks, they also present a number of challenges. Indeed, the use of LLMs by employees may infringe the rules on the protection of personal data and trade secrets and may even question the effective enforcement of the obligation to conduct personal and diligent work. In order to effectively harness LLMs potential, it is crucial that their use in the employment context is addressed and that both employers and employees are aware of the consequences and safeguards related to their application.

Nynke E Vellinga
AI behind the wheel: designing the traffic law of the future

From self-sailing ships to self-driving cars, from drones to automated trains: artificial intelligence (AI) is taking over the wheel. AI increasingly enables vehicles of all modes of transport to be driven without human input. This has significant legal consequences, especially in relation to traffic law. Traffic rules are generally based on the notion of a human handling the steering as well as other driving tasks (assessing the traffic situation, determining speed, etc.). As AI will take the human ‘out-of-the-loop’, AI in employment seems to be without limits and is constantly evolving. These traffic rules no longer apply. The train driver or pilot will therefore lead to lacunae in existing international and national traffic law. This is a challenge that concerns all modes of transport. Therefore, this challenge should be addressed from a cross-modal perspective. This requires the rethinking of key concepts such as responsibility and liability, thus reconsidering to whom traffic rules should be addressed. As this contribution cannot answer all questions arising from this development, it seeks to investigate some specific approaches to developing a new cross-modal legal framework for AI-driven traffic. This includes exploring the incorporation of traffic rules in technical vehicle requirements and the consequences of introducing vicarious liability in this context. Through discussion, this contribution aims to identify key elements for a new cross-modal traffic law framework.

Theodore S Boone
EU and US Regulation of AI: A Comparative Analysis

Presentation will set forth key outcomes of a comparative analysis of US Federal and EU governmental and regulatory initiatives related to AI and discuss the ramifications of such outcomes. Key outcomes: (1) there is general overlap between the US and the EU as to the fundamental importance of building trust in AI and respecting fundamental rights, fostering transparency, preventing bias and promoting economic development, safety and transparency when regulating and using AI; (2) both the US and the EU appear to be driving towards use in guidance and legislation of a definition of ‘AI System’ which is broad and largely tracks the definition of ‘AI System’ used in OECD guidance; (3) the US so far has taken the approach that entities providing and using AI should, with governmental encouragement, voluntarily comply with certain standards and self-regulate whereas the EU appears to be moving towards mandatory and enforceable AI regulations via the EU AI Act and the EU AI Liability Directive (together the “Draft EU AI Regulations”); (4) both the US and the EU are concerned about stifling innovation and economic development as a result of AI regulation; (5) the Draft EU AI Regulations do not give providers of AI Systems the broad shield from responsibility and liability for content which the US provided to internet platforms; (6) because the EU AI Regulations if enacted will apply to any US entities active in the EU and because the EU appears to be ahead of the US in enacting AI related legislation the draft EU AI Regulations if enacted may serve as a model for further development of US AI regulations.
AI Technologies: generative, destructive - Room 025

**Chaired by Herbert Hrachovec, Andreas Kirchner**

**Herbert Hrachovec**

**Cheating by Chatting (GPT)?**

The scene: an academic take-home exam. The questions sent by mail have to be answered in two hours time. The lecturer has repeatedly given the course and knows what responses to expect. One day, however, he is taken aback. The exam’s topics are covered in flawless, intricately nested sentences with surprising epithets and without reference to specifics of the lecture. Is ChatGPT at work here?

Astonishment is followed by shock. It turns out that procedural prescriptions as well as university policy guidelines for this eventuality are missing. Such a case has not yet occurred (or at least has not come to light) in this department. It triggers confused discussions between lawyers, educators and the examination board. The prospective talk documents the quandary between intuition-based expertise of the presenter, professional comments of computer scientists and recommendations of legal experts (who lack IT-knowledge as well as appropriate paragraphs). An attempt is made to give an unbiased account of this unprecedented disturbance. No guidelines can be derived from the diagnosis. But clearly a reassessment of the ritual of academic exams is called for.

**Szymon Skalski**

**Cracking the Code of Generative AI: Legal Implications for Cyber Security and Privacy**

This article examines the dynamic challenges posed by the integration of generative artificial intelligence (AI) in cyber-attacks, and its implications for European private law. As AI technologies continue to advance, cybercriminals are exploiting these innovations to launch attacks with significant financial implications.

The legal issues surrounding cyber attacks carried out by criminals using AI can be categorised into three areas, which will be discussed in this article. The first concerns the entities accountable for the event and those impacted. For private law, it is crucial to tackle the challenge of identifying the liable party, especially when dealing with extensive phishing campaigns executed using AI. Additionally, alterations in cyber-attacks themselves should be noted. The ability to adapt rapidly to changing conditions, thanks to reinforced learning, enables attacker to adjust to the defensive measures taken by the target. This alters the perspective regarding not only the identification of the incident but also the liability of the attacked organisation towards its providers and sub-providers. A crucial matter pertains to the magnitude of destruction inflicted by the specific cyber attack category which surpasses that of typical cyber attacks and provokes concerns in existing practices. In such cases, it is imperative to include discourse that incorporates damages inflicted by AI-induced as well as cyber attacks for identifying their commonalities and disparities.

Overall, this paper provides a comprehensive analysis of the implications of the convergence of generative AI and cyberattacks for European private law. It explores issues of civil responsibility in the context of cyberattacks, the liability of AI creators, and the essential adjustments required in cyber insurance policies to address the escalating risks associated with AI-driven cyber threats.
**AI in Alternative Dispute Resolution: Enhancing Efficiency and Access to Justice**

The digital revolution of the 20th century made information available everywhere and anytime. In the age of Artificial Intelligence, this information is used for automating the decision-making process in the hope of better and improved access to justice. The presented paper analyzes the potential use of Artificial Intelligence in alternative dispute resolution and its consequences, considering the evolving regulatory and governance environment for Artificial Intelligence. This paper also explores the potential difficulties of integration, its benefits, and potential implications for future conflict resolution. Artificial Intelligence can reduce the costs of alternative dispute resolution and increase the overall efficiency of the dispute resolution process. Despite these potential benefits, concerns about the use of AI in alternative dispute resolution mainly relate to legal and ethical issues. The findings helped clarify what needs to be considered when implementing Artificial Intelligence in the alternative dispute resolution process de lege ferenda. As AI tools advance rapidly, it will be necessary for alternative dispute resolution practitioners and policymakers to consider the potential benefits and risks of this integration carefully and to take measures to ensure that the use of AI is transparent and impartial.

**ChatGPT: lost without labels**

Generative AI (GenAI) tools can produce poems, articles, source code, or images on demand. All it takes are – apparently - instructions in natural language text. Questions on the social and cultural impact of these tools arise. The public is told that a new era has come. CEOs of AI companies themselves warn of the dangers of this technology and ask to be regulated, not without self-interest: Talking about how AI could lead to doom’s day attracts attention and investors. This talk aims to bring the big question of “AI Apocalypse” down to earth with (1) a ChatGPT experiment from a cybersecurity professional and (2) an investigation on how these tools are built and operated. (1) A cybersecurity professional wants to use ChatGPT to save time on training content for engineers in a corporate context. This experiments surfaces benefits and risks. (2) The investigation deals with an important precondition that GenAI tools need to function: A massive amount of data, annotated mostly by gig workers, coordinated via digital platforms. That work is hardly mentioned by AI companies. Data annotation is mostly outsourced, although most of AI’s “magic” is based on it. Debates on AI legislation, AI company policies, and ethical AI frameworks may benefit from looking right through the big story of artificial “intelligence” and find that AI tools rest upon myriads of micro-decisions made by humans, who receive only little information about how their annotations are used.

**Preserving Data Privacy in Public Cloud-based Machine Learning: Innovative Approaches and Strategies**

Modern machine learning models heavily rely on extensive training data and substantial computing power. The training phase, in particular, demands significant computational resources, prompting many researchers and practitioners to leverage public cloud services. However, this approach poses a critical concern regarding data and algorithm security, as the cloud owners and, by extension, potentially relevant countries gain access to sensitive information. This paper addresses the pressing concern of privacy within the context of machine learning in public cloud environments. Currently, data privacy relies heavily on trust in cloud service providers. We introduce innovative machine learning approaches that don’t involve the use of unencrypted data on the cloud, while still allowing for the utilization of public cloud resources for training machine learning models. These methods are grounded in the principles of secure multi-party computing, which are gaining significant attention from major IT companies, resulting in the development of relevant frameworks.

However, the adoption of these approaches by companies that handle regulated privacy data, particularly in sectors like healthcare and finance in Europe, remains quite limited. Some of these organizations are considering their implementation in the future, but they face significant hurdles. These challenges include a shortage of IT experts and uncertainties regarding data privacy management and compliance with existing regulations.
Viktoriia Rekrutiak

Bias in the Era of Advanced Computing: Challenges and Legal Insights in Quantum AI

Certain limitations of classical AI may be minimised in the future with the use of quantum. However, such an interplay may lead to potential risks. This paper discusses the legal dimensions of bias as a systematic mistake in the model’s predictions caused by its reliance on particular input features. It examines similar cases regarding classical AI (for instance, race bias and gender discrimination indifferent contexts). It also analyzes the probabilistic nature of quantum technologies. Due to this feature bias may be difficult to identify and address. The peculiarities of quantum states could also provide new sources of bias as different data kinds or processing techniques may appear. Existing legal frameworks, such as the proposed Artificial Intelligence Act, are analyzed to discover their applicability to emerging quantum technologies and find gaps or shortcomings. The paper aims to open the discussion regarding the necessity of separate quantum regulation covering the potential risk of bias.

Michal Czerniawski

Exporting EU norms and values outside of the European Union - GDPR case study

In recent years, the European Union emerged as a regulator of the digital markets, not only within but also globally. The challenges ahead of the Union include how to regulate digital markets and how to do it in a legitimate way, in particular as emergence of competing to Brussels regulatory centers seems to be inevitable. EU regulatory model takes into account rights foreseen in the Treaties but also, most notably, Charter of the Fundamental Rights. Therefore, it can be argued via the extraterritorial scope of its laws, the Union is exporting not only laws but also European values. The EU’s task for the years to come is to keep its regulatory power and to “incentivize” non-EU actors to follow the EU policies. This can happen via “hard law” e.g. imposing sanctions, recognition of third-country legal systems as equivalent or “soft law”, in particular via a so-called Brussels effect. The General Data Protection Regulation, serves as a perfect case to illustrate this topic and describe the challenges ahead.

Ioannis Revolidis

Web 3.0 and EU Private International Law: Is there still a place for court litigation?

The regulation on electronic identification (eIDAS), authentication and trust services was created to harmonize the rules on electronic signature and electronic transactions. The aim was to ensure that electronic documents with electronic signatures would be recognized and accepted in all EU Member States. Public entities are required to recognize and accept electronic signatures and seals from all EU Member States.

However, until the entry into force of Regulation 2020/1784 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, the eIDAS Regulation was not directly applicable to civil procedure. Regulation 2020/1784 is therefore the first legal act that relates directly to the provisions of the eIDAS regulation. Such action should be assessed positively as it contributes to the unification of the electronic identification services market and the inclusion of judicial authorities in it.
Therefore, it requires a deeper analysis, to what extent the provisions of the eIDAS regulation can be a direct basis for enabling parties to file pleadings with the court by electronic means and for electronic service of documents as well.

**Jurisdiction in cross-border online infringement of personality rights, in particular in cases of defamation**

Infringement of personality rights are increasing, especially with the development and massive use of electronic media, the internet, social networks and blogs. If the rapid circulation of information brought advantages, as well as its easy accessibility, the truth is that it made the infringement of certain types of personality rights easier and with devastating repercussions, given the worldwide reach of the internet.

The internet has boosted anonymous attacks on a person’s reputation, as it has become easy to create fake profiles on social networks, open email accounts with false names and use systems that change the user’s virtual location. Consequently, cross-border delicts have also increased, as a publication on the internet has a global audience, as it will potentially be accessible for reading and/or downloading in any country and can be accessible for an indefinite period in time, having devastating effects on the right holder. It is true that before the internet there was already a transnational infringement of personality rights by defamation, however, the Internet has made this delict more accessible to anyone, easier and with more devastating repercussions, because all you need is a computer with access to a network like the internet, which has a global reach, and the information placed online is difficult to erase.

The importance of this phenomenon led, on 31 August 2019, at the session held in The Hague, the Institut de droit international to adopt a resolution on jurisdiction, applicable law and recognition of foreign decisions in the context of violations of personality rights through the use of the Internet. Since it is not possible to discuss all the topics that can arise in situations of cross-border defamation, it will be explored the issues regarding jurisdiction in cross-border defamation. To this end, it will be analysed the solutions of the Regulation No 1215/2012, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels 1a).

**An update on data localisation**

‘Data localisation’ refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction. Some forms of this data localisation are highly contentious, and the topic of data localisation has been gaining considerable attention globally over the past couple of years.

Data localisation clearly and directly impacts cross-border data flows with implications both within private international law and public international law. This paper examines these issues with particular emphasis on the latest developments.

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:45 - 13:45</td>
<td>Lunch</td>
</tr>
<tr>
<td>13:45 - 15:15</td>
<td>Parallel streams (in other sections)</td>
</tr>
<tr>
<td>15:15 - 15:30</td>
<td>Coffee break</td>
</tr>
<tr>
<td>15:30 - 17:00</td>
<td>Parallel streams</td>
</tr>
</tbody>
</table>

**Internet and Society - Room 030**

*chaired by Jakub Macek*

Christine W Trueltzsch-Wijnen, Sascha Trützsch-Wijnen, Philip Sinner

**Ban Hate – A quantitative and qualitative analysis of actors and communicative practices of Austria’s No Hate Speech Committee**

Fighting hate speech is a major challenge for mediated societies. The importance of the field is reflected in an extensive state of research: Only for the period from 2014 to 2021, the evidence base of the research network CO:RE (Aroldi et al. 2022) lists 301 publications and 118 studies on the topics of hate speech, cyberhate and bullying for Europe. One focus is on the media usage of hate speech recipients and their respective coping strategies, but also on bullies. Affected
companies such as Facebook and Twitter as well as regulation strategies have been researched. In contrast to this, organized actors in the work against hate speech and structural aspects have so far only been researched to a limited extent.

In our study, we addressed this research gap by examining the political and social communication of the Austrian No Hate Speech Committee and its 30 members. We conducted a quantitative structure analysis as a web screening. This captures the entire overarching media ensemble of all members of the committee and covers 44 semi-automated tools on the one hand and all image, text, and video-based actions and campaigns of the committee and its members on the other. To complement this, we conducted a qualitative content analysis of selected content in order to deepen the research and to reveal the complex interrelationships between structural conditions and the objectives of the members.

We will give an insight in our quantitative results [e.g. activity of actors, kind of content, communicative practices etc.]. In addition, we will illustrate this with examples from our qualitative analysis, which gives a more in-depth picture of the fight against hate speech in Austria. We will discuss this against the background of mediated activism and digital forms of activism that enable counter speech and combatting various kinds of hate speech (often connected to broader social challenges like antisemitism, xenophobia, conspiracy narratives etc.).

Gender differences in public perceptions of the seriousness of offline and online sexual harassment

Although crime seriousness studies have consistently shown that the public perceives sexual offenses as serious offenses, only a few studies examined public perceptions of sexual harassment. Moreover, despite the growth and prevalence of online sexual harassment, public perceptions regarding this phenomenon have not yet been examined. This study aims to explore the perceived harmfulness, wrongfulness, and seriousness of offline and online sexual harassment, and to identify socio-demographic factors associated with those perceptions, focusing specifically on gender differences. Data was collected through an online survey conducted in 2023 among a representative sample of private internet users in Israel (N=525). The results show that: 1. In both spheres, sexual harassment is ranked as a less serious or harmful behavior, and a more wrongful behavior; 2. online sexual harassment is perceived as less serious than offline sexual harassment; 3. gender is a significant predictor of perceived seriousness of both offline and online sexual harassment. Results are contextualized within theoretical frameworks that offer insights as to why online sexual harassment is not viewed as seriously as offline sexual harassment, and a thorough understanding of the gender issue regarding perceptions of sexual harassment, both offline and online. The study will discuss the implications of the findings.

Keywords: Public perception of crime seriousness, online sexual harassment, face-to-face sexual harassment, gender, cybercrime.

Indirect Victimization and Fear of online sexual harassment

Although it is generally acknowledged that the development of the Internet created new criminal opportunities, its perception by the general population, the extent of fear of online victimization, and how perceptions of offline crimes are associated with fear of online crimes has received limited attention (Brands & van Wijlen, 2021).

Fear of crime has become an important research topic because of the understanding that crime can negatively affect not only people’s lives and activities but also the society at large, because of the anxiety and distrust incited by fear of crime among members of the community (Ferraro, 1995; Lewis & Salem, 1986; C. S. Park & Lee, 2010). With the integration of the Internet in everyday activities, the research on fear of crime has been diversified into both offline and online settings-related topics. However, research on online fear of crime is still scarce, except a few studies (Henson et al., 2013; S. Lee et al., 2019). This study aims to fill a gap in the literature and to investigate the extent of fear of online sexual harassment, its relationship with fear from interpersonal sexual harassment and the factors associated with online fear of online sexual harassment.

Our study seeks to explore the extent to which people report fear of a specific online crime, namely, sexual harassment and its correlates. In addition, we study if fear from face-to-face sexual harassment affects fear of online sexual harassment. Data was recently collected from a large survey of Internet users (n=525) in Israel. Results indicate that gender, previous online victimization experiences and high presence in social networking sites are shown to predict fear of online sexual harassment. The implications of the findings are discussed.
Reshaping the Fourth Estate: The algorithmic influence on journalism and its societal implications

Various studies show that our society is polarized to an unprecedented extent, that information bubbles are creating serious social divisions, and that the current functioning of the news media reduces the range of possible interpretations of a given event, which goes hand in hand with a rigid rejection of opposing positions, thus creating patterns of divergent political communication. It is becoming increasingly clear to academics that the cause of this phenomenon is the transformation of journalism rather than the filter-bubbles of platforms.

The operating models and algorithms of online platforms have not locked users in echo chambers, but have radically changed the news media.

As the algorithms running the online space is very different in both content and underlying structure from the traditional news media, the serious social consequences of this for news consumption need to be monitored very closely. This should include the application of new methods for monitoring and understanding journalism, in-depth ethical, ethnographic and social science research into the platforms’ content delivery systems and related processes, and the development of comprehensive media literacy education programmes.

In my presentation and paper, I will explore the impact of algorithm-based content planning on the news media and how it is possible to restore quality journalism and, with it, trust in the media.

I plan to show how social media algorithms affect news consumption habits through various empirical studies of news reader attitudes (e.g. Mukerjee, Yang, Peng 2023; Liao 2023; Klawier, Prochazka, Schweiger 2021), and to parallel this with detectable changes in the media sector (e.g. Rhodes 2021; Vázquez-Herrero, Negreirea-Rey, Lópex-Garcia 2023; Karlsef, Aalberg 2021), and to outline in detail the legal regulatory and societal options that could be used as solutions. The presentation/study is essentially a comparative literature review, with a focus on formulating forward-looking recommendations.

17:00 - 17:15 Coffee break

17:15 - 18:45 Parallel streams

Internet and Society - Room 030

chaired by Jakub Macák

Bounded Ownership: How online platforms reach dominance through limiting (their) ownership rights

In this contribution, I focus on how the concept of ownership is enacted by online platforms. I describe a specific model of intellectual property, which benefits rights holders by abstaining from enforcing their claims on exclusive use of the owned property. This model differs from a conventional model of ownership, which assumes that any unauthorized use of property damages the owner. I argue that bounded ownership is currently the norm for online platforms and their content and as a result, this creates wide availability of cultural goods. At the same time, bounded ownership places platforms into a dominant position of intermediaries for accessing user audiences and securing financial streams. In conclusion, I elaborate current practices of users and cultural producers, which lower their dependence on platforms.

Instances of the first-, second-, and third-level digital divide: Disparities in new media use among different groups of Slovak youth

The potential benefits of effective new media use include broadened opportunities for communication, entertainment, creativity, health and well-being, education, professional development, economic gains, as well as participation, empowerment and civic engagement. However, vulnerability research shows that these opportunities are not equally accessible to everyone, and often, the offline inequalities are mirrored and sometimes multiplied in different social contexts online. Our goal was to better understand the current situation in Slovakia concerning differences in new media access, skills, usage, and outcomes among different youth age groups.
groups (aged 10-25), which were broadly hinted at by existing quantitative research. To this end, we conducted semi-structured interviews with youth from households with average and low socioeconomic status, as well as with youth from the ethnic majority and several ethnic minorities. The research is still ongoing, but preliminary findings include instances of the first-, second-, and third-level digital divide.

Cyberspace for all? Equality, Diversity and the Accessibility Gap in User Security Interactions

Cybersecurity is now a fundamental requirement for all online services and devices. Yet simply making security mechanisms available to users is not enough: they need to be presented in a form that is clear and useable.

Whereas increasingly automated protection and measures exemplify less frequent user involvement, numerous instances still demand regularly explicit user interaction with security. Situations such as website or device authentication, enabling secure connections, malware scanning, and cookie or personal data consent, involve steps that can often be additionally cumbersome or impractical for users with different forms of disability.

Cognitive, motor and visual impairments can make it significantly more difficult to perform common security interactions, not because this is unavoidable, but because of a given system's initial design and implementation. Even ‘accessibility’ features, increasingly available to support and assist general usage, may represent a hindrance in some security interaction contexts.

This may result in disabled users being at an implicit disadvantage compared to other users, becoming less willing to use related mechanisms and thus less protected.

This paper uses illustrative examples to examine how security interactions are inherently more challenging through the lens of disability. It questions the extent to which legal obligations for equality of access have been considered in cybersecurity contexts and what is needed to enable more appropriate attention from designers, developers and platforms.
<table>
<thead>
<tr>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kateřina Kudrlová</td>
<td>Privacy online in 2020 - data from a Czech questionnaire survey on cybercrime related to the misuse of email, social networks and e-banking</td>
</tr>
<tr>
<td></td>
<td>In 2020, the Institute for Criminology and Social Prevention carried out a large-scale questionnaire survey on cybercrime focused on respondents’ experiences with selected online phenomena in 2020. The research sample of nearly 7,000 Czech Internet users aged 16-74 was representative in terms of gender, age, education, region and municipality size. Topics covered included the use of selected devices and applications, online trading, ransomware, phishing, securing and misuse of selected online accounts, use of the darkweb and copyright infringement. A unique feature of the created questionnaire is the parallel wording of some questions answered by respondents in the role of both victim and attacker. This presentation is not about traditional online privacy issues such as cookies, GDPR, etc. Instead, it focuses on the context of privacy within one’s home. This is something commonly protected by legal tools and moral rules in real-world settings. Its online equivalent, on the other hand, also enjoys a degree of legal protection, albeit not entirely appropriate, but on a moral level the difference is clear, as the data from the survey shows. The presentation will introduce the data relating to the misuse of email boxes, social networks and e-banking in 2020 from the perspective of 366/377/199 victims and 169/100/191 attackers. It will focus on the method of misuse of the compromised account and the main actors on both sides, surprisingly mostly partners.</td>
</tr>
<tr>
<td>Tamás Szádeeky, Roland Nagy</td>
<td>Leveraging Artificial Intelligence Models for Computer Incident and Evidence Analysis</td>
</tr>
<tr>
<td></td>
<td>This presentation explores the innovative application of Artificial Intelligence (AI) models to computer incident and digital forensics investigations, adding a robust layer of precision and speed to traditional methods. The central theme discusses how AI can drastically transform the landscape of cybersecurity by enabling more efficient and effective incident response and evidence analysis. Machine Learning (ML) techniques, including neural networks and deep learning, are highlighted as key tools in identifying, categorizing, and analyzing cyber threats, leading to faster incident resolution times. The first segment details how AI-powered anomaly detection systems can spot potential threats and irregular patterns that human analysts might miss, thus enhancing intrusion detection and prevention. The following section delves into the role of AI in automating evidence collection and processing, demonstrating its ability to sift through large volumes of data and extract relevant information, thereby reducing manual labor and increasing the accuracy of investigations. The presentation also discusses how AI models can predict future attacks by learning from historical data, a crucial aspect in proactively maintaining cybersecurity. A case study of AI-based predictive analysis in incident response is shared, emphasizing the value added by this technology. Lastly, the challenges associated with the implementation of AI in cyber forensics, such as data privacy concerns and the risk of AI model manipulation, are examined. Strategies for mitigating these risks are proposed, which involve careful model design, stringent security protocols, and continuous model training and evaluation.</td>
</tr>
<tr>
<td>Hagit Turjeman</td>
<td>Epidemiology of Cybercrime in Encrypted Channels: typology and modes of operation</td>
</tr>
<tr>
<td></td>
<td>Cybercrime is a growing global threat, with the internet’s accessibility and anonymity transforming criminal landscapes. The aim of this study is to map the ecosystem of cybercrime in encrypted channels. Our specific focus centers on mapping Telegram criminal channels. Notably, Telegram offers distinct advantages over other encrypted platforms, such as darknet platforms, due to its accessibility to a broader audience and its recognition as a well-established social networking platform. The current analysis focuses on a specific phase of the study, emphasizing the results of cybercrime profiling. During this phase, we closely monitored numerous encrypted Telegram</td>
</tr>
</tbody>
</table>

**Partners**
communication channels, which serve as conduits for a range of criminal activities. Through content analysis, visual inspection, and network analysis, we've developed two classifications: a cybercrime typology and a mode of operation typology. Additionally, a comparative analysis of Israel and USA data has revealed both similarities reflecting global cybercrime characteristics and differences attributed to distinct societal norms and law enforcement practices.

The creation of these classifications serves as a roadmap for understanding cybercrime, greatly assisting law enforcement and cybersecurity efforts to access the hidden ecosystem of cybercrime and ultimately, contributes to enhancing cyber resilience within society.

### Challenges for LEAs in 5G environment

The advent of 5G network standards is ushering in a new era of unprecedented connectivity advancements, such as increased transmission speed and capacity, decreased latency and enhanced security and privacy. However, this technology also brings forth many challenges for law enforcement agencies worldwide. This research article delves into the critical problems faced by law enforcement agencies in the context of 5G (SA) networks.

The paper aims to examine the unique characteristics of 5G networks. Subsequently, it analyses how these features pose hurdles for law enforcement in terms of surveillance, interception and data collection. These challenges range from enhanced subscriber security and privacy, such as temporal identifiers, and impacts on cell site simulators, timing aspects and t-synchronization between operators and LEAs, to edge computing or private, campus networks.

In addition to challenges, 5G standards can provide some advantages to LEAs, such as enhanced geolocation tracking, however these are not without legal and policy issues surrounding 5G networks interception. The complexities of cross-border data access and privacy protection create jurisdictional dilemmas for law enforcement, requiring innovative approaches to international cooperation.

### 11:00 - 11:15

Coffee break

### 11:15 - 12:45

Parallel streams

<table>
<thead>
<tr>
<th>Law: Cybersecurity, Cyberwarfare - Room 034</th>
<th>chaired by Václav Stupka</th>
</tr>
</thead>
</table>

#### Anna Blechová

**Tech-based versus behaviour-based approaches to advancing space security**

Space security has become an increasingly prominent topic, particularly in light of recent events such as the KA-SAT network cyber-attack in February 2022 and the Russian anti-satellite missile test in December 2021. These incidents have underscored the need for stronger regulation and heightened awareness of outer space threats. Countries such as France, the UK, and the US have taken proactive measures to address these concerns through initiatives like their Space Defence Strategy, National Space Strategy, and Tenets of Responsible Behavior. This trend is further reflected in the German National Security Strategy and the Security Strategy of the Czech Republic, which also emphasizes the importance of space security.

Efforts to enhance space security have not been limited to policy and regulation alone; there is a growing emphasis on technology-based approaches as well. For instance, the Institute of Electrical and Electronics Engineers Standards Association has played a significant role. They have established the Space System Cybersecurity Working Group, which aims to develop a standard that provides technical guidance on cybersecurity for space systems.

The international community has also engaged in discussions on outer space security. The United Nations General Assembly's First Committee on Disarmament and International Security adopted a resolution in November 2021 titled "Reducing space threats through norms, rules, and principles of responsible behaviours (L.52)." This resolution supports a behaviour-based approach to addressing space security concerns and has resulted in the establishment of an Open-Ended Working Group (OEWG) to explore this issue further.

In advancing space security, two distinct approaches have emerged - tech-based and behaviour-based approaches. The aim of this paper is to introduce both approaches and explore their potential implications for the future of space security.

#### Jakub Vostoupal

**Stuxnet vs WannaCry and Albania: The Cyber-Attribution on Trial**

**Partners**

- Rowan
- Zákazky pro lidí
- Wolters Kluwer
- CODEGIS
- PRAVNÍ PROSTOR
- CATERING
- PwC
In the intricate world of cyberspace, cyber-attribution, specifically the procedure of linking cyberattacks, the activities of non-state actors (e.g., hacker groups) and states’ orders and control remains one of the foremost challenges for modern international law. The procedure itself is a complex combination of technical, forensic and intelligence analyses with legal, strategic, geopolitical, and diplomatic requirements and aspects, fundamentally complicated due to the anonymous and often highly sophisticated nature of state-sponsored cyber-attacks. However, despite these challenges, we have witnessed an increase in the public attributions of cyber-attacks (let it be the attribution of WhisperGate and other Russian malicious cyber activities against Ukraine, WannaCry or the highly destructive cyber-attack against the Albanian Government).

But what about Stuxnet? Strikingly, despite its far-reaching implications, the most famous cyber-operation remains officially unattributed. Therefore, in my talk, I shall delve deeper into the procedure of the cyber-attribution of the selected cyber-attacks and analyse and compare the relevant (and publicly available) details to try and identify the emerging state practice in the context of state responsibility and attribution standards. I shall also address the key considerations such as the technical evidence, geopolitical dynamics, intelligence-sharing mechanisms and international cooperation using the Egloff-Smeets Framework for public cyber-attributions.

**Legislative challenges of Active Cyber Protection according to NIS2**

The paper will examine the possible scope of application of Article 57 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2016/1148 (NIS 2 Directive). The aim of the paper is to assess the possibilities of using this article to adapt policies on the promotion of active cyber protection as part of a wider defensive strategy. The boundaries between active cyber protection and active countermeasures (which are explicitly excluded, but in the form of offensive measures, giving some room for discussion) will be explained. And at the same time there is a call for Member States to create and “provide free services or tools to certain entities, including self-service checks, detection tools and takedown services.”

In the course of the speech, I will give a definition of the possible activities under prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner. And appropriate recommendations for implementation within national policies. Also a reflection on the possibilities of providing the mentioned free services.

**The four most common myths about cybersecurity**

Cybersecurity, and in particular its intersection with the law, is shrouded in a number of half-truths and myths, and this talk will look at four of the most common we encounter in practice.

**Myth 1:** We aren’t a big, important company, so we don’t need to worry about cybersecurity. We will discuss that the days when cyber regulation applied only to an elite circle of companies are gone forever. We will present arguments why implementing cybersecurity is a matter of company survival rather than just ticking a box in a compliance checklist.

**Myth 2:** Cybersecurity is the responsibility of IT; other departments don’t need to be involved. We will unveil the multidimensional nature of cybersecurity, where successful implementation and operation require continuous collaboration across company departments.

**Myth 3:** We have a cybersecurity policy / we bought a magic box or a gadget and think it’s enough.

**Myth 4:** Cybersecurity regulations stifle innovation and hinder growth.

---

**12:45 - 13:45**  
Lunch

**13:45 - 15:15**  
Parallel streams

**15:15 - 15:30**  
Coffee break

---

**Partners**

[Images of partner logos]
### New Media and Politics - Room 034

**Semi-homomorphic Cryptography as a Cure for the Inherent Weaknesses of an Envelope-based eVoting Procedure? The German Social Elections 2023**

The Social Elections in Germany are among the largest elections in Europe with some 52 m eligible voters. In 2023 they were also held via eVoting, at least for a significant portion of the electorate, for the first time. The basic eVoting procedure used was Enveloping. The weaknesses of Enveloping are well documented (see for example [1, 2]), they essentially cover reproducibility of the result, independent recount and protection of voting secrecy.

The Social Elections used an Envelope protocol citing the “Estonian model” as an explicit example. To overcome the known issues in Enveloping, the German Federal Office for Information Security (BSI) issued Technical Guideline TR-03162 which introduced (semi-)homomorphic encryption as a remedy. This paper will analyse, whether these amendments by BSI ensure adherence to the general voting principles, particularly conformance with Council of Europe Recommendation CM/Rec(2017)5 on eVoting.

On top of these issues, BSI had to deal with the fact that digital signatures and eID are not very common in Germany (mainly because there are no digital residents’ registers available). The Estonian model, however, heavily relies on digital signatures in their eVoting protocol. BSI devised a workaround, which will also be analysed in the paper.


---

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:30 - 17:00</td>
<td>Parallel streams</td>
</tr>
<tr>
<td>17:00 - 17:15</td>
<td>Coffee break</td>
</tr>
<tr>
<td>17:15 - 18:45</td>
<td>Parallel streams</td>
</tr>
<tr>
<td>19:15</td>
<td>Conference dinner</td>
</tr>
</tbody>
</table>

---

Domenica Bagnato, Robert Müller-Török, Alexander Prosser, Robert Stein

---

**Partners**
The situation of the online press and press publishers in Hungary after the implementation of the press publishers’ right of the CDSM Directive

Digital platforms created the possibility of personalized news consumption, which collects and indexes news produced by press publishers according to the consumption habits of end users. Press publishers, who are also active in the online space are at a competitive disadvantage vis-à-vis platforms that act as news aggregators since the advertising revenue from the sale of online space goes to the platform provider rather than the press publisher.

To redress this imbalance, protection for press publishers aims to promote the interests of publishers in a competitive market where the objectives of competitors intersect at several points. In the online space, the advertising leg of the business has faltered because news consumers do not seek out the news content produced directly on the online interface of the press publication, but through third-party news aggregator sites independent of the publisher. However, news aggregators also have a positive spin-off for publishers, as they make it easier to reach audiences that they could not reach before.

The new neighboring right has also been implemented in Hungary. This fact, together with the difficulties of independent journalism in Hungary, justifies the monitoring of the challenges faced by press publishers through a questionnaire survey. The results of the survey and the status of Hungarian publishers after the implementation of the press publishers’ rights would be presented at the conference.

The Digital Services Act changes everything, or does it? – nine key issues with the Digital Services Act and possible solutions related thereto

The Digital Services Act (DSA), implemented in October 2022, is a novel regulation for digital services and Internet governance. It aims to establish a comprehensive framework for online intermediaries, social media, and other platforms, introducing rigorous obligations to safeguard fundamental rights and democratic values. However, the DSA has sparked debates on its effectiveness, enforceability, and long-term impacts on various platforms.

This study critically evaluates the key issues of the DSA and its implications for the digital environment, online platforms (with a focus on social media), and policy-making. Three research themes guide the study concerning (1) the balancing of freedom of expression and user protection with platform rights, (2) the multi-stakeholder aspect of the effectivity of the DSA and (3) the failed addressing of new media phenomena by the regulation.

The authors adopt a multifaceted methodology, including an exhaustive literature overview of legal documents, opinions, and studies from scholars. Additionally, they employ a comparative and analytical approach to compare the DSA with existing national and international regulations, focusing on countries with previous platform regulation laws.

The study identifies nine key issues concerning the DSA, including the regulatory burden, the ambiguity of risk assessment, the lack of conceptual clarity and inadequate global and platform-specific implications to address digital rights.

The authors propose potential solutions, including enhanced cooperation between platforms and states, harmonization of national regulations, promotion of digital constitutionalism principles, and better protection against illegal content. The research will shed light on broader issues related to digital regulation, policy-making, and the evolving digital landscape, encouraging dialogue and forward thinking regarding the future of the DSA.

A streaming platform as a multi-intermediary services platform

Streaming is a transmission technology in the form of live (e.g., Twitch.tv) or on-demand streaming (e.g., YouTube). The general streaming industry is now worth 106.83 billion USD. The contribution is based on the operating processes of streaming platforms powered by user-generated content. It is necessary to examine how such a large market will be covered by the DSA – “the new Internet constitution”. In practice, there are doubts about the nature of different platforms’ services (e.g.,
advertising) and interpretations to avoid qualifying as an online platform. The results can easily be transferred to other areas of digital services because of a streaming platform characteristic. The contribution determines how to examine whether a web admin is also an intermediary service provider and how to divide the way the platform works, including its interface, between the areas of providing different intermediary services. The qualification depends on the point of view of the process to be qualified. For example, an analysis of whether an online platform service is provided should take place from the point of view of the processes underneath the platform interface, which is displayed to the user viewing the streams ("backdoor approach" subsumption model concept).

The contribution introduces the "multi-intermediary services platform" concept that shall be attributed to platforms that provide several types of intermediary services, which impacts the scope of the obligations to be met.

11:00 - 11:15  Coffee break

11:15 - 12:45  Parallel streams

<table>
<thead>
<tr>
<th>Law: eCommerce, Digital Single Market - Room 038</th>
<th>chaired by Jan Hospes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maciej Bujalski</strong></td>
<td><strong>Online Repair Platforms: Undermining the Consumer Protection and Internal Market Without Contributing to the Circular Economy?</strong></td>
</tr>
</tbody>
</table>

In March 2023 the European Commission proposed a Directive on common rules promoting the repair of goods, COM(2023) 155 final. Its Article 7 requires establishing a national online platform where the repair services will be offered and where the consumers could compare the offers. This paper analyses whether this solution is in conformity with values of consumer protection and internal market and is it needed to meet the environmental goals. Consumers can easily find repair services through the Internet and chances that platforms will be actually used are small. Its promotion may paradoxically discourage unaware consumers from demanding free repair within the Directive 2019/771. Running such a platform requires costs. Professionals will have to pay for registration which will increase the costs of repair for consumers. If the platforms are run by private actors, there will be a risk of monopoly. While setting up platforms at national level denies the internal market, the cross-boarder repair services require transport and contradict the environmental aims. Also, repair is hard to digitalize as it’s difficult to estimate its costs and time without knowing the defect. The aim of the platform, offer comparison, cannot be reached. What’s more, it creates the risk of manipulation: assumption of the simplest defect, which can be repaired quickly and cheaply, when it will finally be longer and more expensive. Unfair practices may occur. Maybe to reach the aims of circular economy it will be better to let the market regulate itself?

| **Matija Damjan**                              | **Mastodon in the room: Applying the EU’s new platform rules to federated social networks** |

The Digital Services Act (DSA) attempts to protect the web from the spread of illegal and harmful content and to safeguard users’ fundamental rights. The regulation of online intermediaries is asymmetric: very large online platforms are subject to stricter rules to protect against the systemic risks connected with their (negative) societal impact.

Federated networks like Mastodon and Bluesky have emerged as alternatives to traditional social networks. They operate as systems of interconnected servers communicating through a decentralised networking protocol. This allows their users to communicate with each other and share data as if on the same platform. Since a federated network has no single owner, the administrator of each local instance sets its rules and enforces them on their server rather than across the network.

The paper will examine how the DSA’s rules apply to federated social networks. If each instance is treated as a separate platform, they must only comply with the minimum obligations for hosting services rather than rules designed for social networks. Yet, the entire federated network could exceed the threshold of 45 million monthly users. The paper will discuss whether this should be seen as a loophole in the DSA’s framework and whether special rules are needed to address specific risks arising from federated networks.

**Partners**
Green transformation of Digital Single Market: adopting consumer protection-by-information model for environmental purposes

Consumers are deemed the driving force of the green transition. It is believed that if informed on the environmental impact of their actions, they shall make environmentally friendly choices. Consequently, the underlying assumption of the European Green Deal is that the model of protection-by-information may be adopted to increase sustainability of the common market.

A drastic increase of pre-contractual information obligations is proposed (Digital Product Passport in Proposal for Ecodesign for Sustainable Products Regulation; requirements regarding environmental claims in Proposal for a Directive on Empowering Consumers and Proposal for a Green Claims Directive; European Repair Information Form under Proposal for a Directive on Repair). This approach seems ill-suited for empowering consumers to make more sustainable choices, especially online. Traditional obstacles to the effective functioning of the protection-by-information model become more severe due to the characteristics of the online environment and the change of subject of protection. Also, new challenges appear: to avoid misleading, a deeper granularity of information is needed.

Using the example of durability-related requirements, the contribution presents possible solutions: differentiating in content and form information that needs to be provided to professionals and consumers; and requiring machine-readability of information so that technology can be used to facilitate understanding consequences of eco-standards.

12:45 - 13:45 Lunch

13:45 - 15:15 Parallel streams

Law: eCommerce, Digital Single Market - Room 038

chaired by Jan Hospes

Joanna Wiszniewska

Influencer marketing – do we need a new law or a new approach?

Facebook, Instagram, TikTok - any social media is full of advertisement. The history of celebrity endorsement of products is nothing really new but Internet brought it to the extreme level. A wide range of global population has been relying on influencers for all sorts of information. It creates the great responsibility as influencer marketing may lead to faulty advertising and misinformation, especially among minors and people with low digital literacy.

Until recently influencers and their activities were not the subject of particular interest. These issues are currently addressed through tailored legislation neither at EU level nor in national regulations. To compensate for it, the last few years have seen a proliferation of soft law and industry self-regulatory measures to provide greater transparency. But is soft law combined with case law enough to provide the desired standard of consumer protection in the Single Market? Considering the fact, that platforms and technologies change at fast pace are we able to create a regulation that will not lag behind the development of the market? The digital environment in which influencer marketing takes place creates additional challenges for legislators.

The aim of the paper is to critically discuss the abovementioned problems on the basis of EU law (including the DSA) and Polish legislation. This will be juxtaposed with the legal solutions and guidelines adopted in selected other EU Member States.

Kitti D Mezei

Balancing Innovation and Accountability: A Meta-Regulatory Framework for Online Platforms in the Age of AI

This paper delves into the intricate realm of technological governance, focusing on the regulation of online platforms and artificial intelligence (AI). In an ever-evolving digital landscape, the exponential growth of online platforms and AI technologies has raised pressing concerns about their impact on user safety, data privacy, and societal well-being. The EU is responding to this problem by enacting the DSA and the AI Act, which form the basis of European legislation.

Partners
This paper introduces the concept of meta-regulation in the context of online platforms and artificial intelligence (AI), providing a comprehensive framework for guiding and overseeing the regulation of these technologies. Meta-regulation involves creating and implementing higher-level regulatory mechanisms that govern the rules and practices of self-regulatory systems. This study explores the challenges and potential benefits of applying meta-regulation to online platforms and AI, focusing on ensuring ethical, responsible, and safe digital environments. Drawing from interdisciplinary research and regulatory analysis, this paper presents a roadmap for integrating meta-regulatory strategies into the governance of these technologies. The findings emphasise the importance of balancing innovation and protecting user rights while empowering stakeholders to collaboratively shape the digital landscape’s future.

**The Challenge of Horizontal Harmonisation: Imbalances of Economic and Institutional Power in Data Regulation**

In this paper we frame an approach to multifaceted and multilateral harmonisation, in order to address power imbalances, both intrinsic and extrinsic to data regulation.

We are developing a twofold argument, first by addressing the role of data as economic tool and its interrelation with economic power. In the EU, the basis for data regulation has plausibly derived from privacy concerns and fundamental rights. However, the resulting regulatory focus does not necessarily address the economic and business importance of data, even where the “economisation” of data is seen in instruments such as the Digital Markets Act.

Second, we follow the global influence of EU regulatory from the GDPR to the Data Governance Act, and from the DMA to the Data Act proposal, leading to a data “Brussels Effect”. To the extent that data protection law has almost become “the law of everything”, the EU has claimed institutional power in relation to data regulation that becomes increasingly problematic, since not only it imposes Eurocentric underlying rationales relating to privacy, but it may also impose economically oriented rationales extraterritorialy.

The paper examines issues of harmonisation laws in general, and of data laws specifically, by exploring key conceptual considerations regarding the notion of “power” and its effects on the nature and scope of harmonisation.

15:15 - 15:30 Coffee break

15:30 - 17:00 Parallel streams

**Law: eHealth and New Technologies in Healthcare - Room 038**

**Assessing pandemic tech: compliance with fundamental rights?**

Mireille M Caruana, Roxanne Meilak Borg

The European Union’s response to the Covid-19 pandemic relied heavily on creating, deploying, and using digital technologies. Our article focuses on three technological measures: contact-tracing, the EU’s expansion of the contact-tracing programme to cross-border notification, and digital vaccination passports. Much of the academic response to these initiatives focused on data protection law, the preservation of privacy, and the reluctance to build surveillance infrastructures that would empower states with tracking capabilities. Our article tackles these digital initiatives from another angle. It explores whether the EU’s desire to get people exercising their right to free movement complied with international obligations to protect human rights, particularly the European Convention of Human Rights and the EU Charter of Fundamental Rights.

This paper examines the deployment of pandemic-related technologies through a human rights lens. We review compliance with the Convention’s three-part test of lawfulness, public interest, and proportionality (‘necessary in a democratic society’). Thus, the paper first examines human rights protection (and limitations) under extraordinary circumstances like public health emergencies. The following section examines Europe’s technological initiatives through the lens of privacy rights. The third part explores whether vaccine mandates are compatible with the EU’s principle of non-discrimination. The paper’s final part assesses the suitability of human rights to protect all citizens during a public health emergency.

**Regulating Neurotechnology: Safe in the Hands of EU Product Safety Standards?**

Ekaterina Hailevich

Quantum technologies are expected to have a significant impact on communication, including electronic transactions. This also applies to advanced electronic signatures which play a key role in ensuring the secure and reliable exchange of information. For this purpose, the signatures use cryptographic algorithms which usually rely on computational complexity resulting, for example,
from prime numbers factorization. Classical computers can theoretically break such encryption. However, this is virtually impossible given the limited time and computing resources. Quantum computers challenge this assumption. Since their computing power is orders of magnitude greater than classical computers, they can eliminate much of the complexity of cryptographic algorithms. Indeed, Peter Shor, a mathematician, created an algorithm for a quantum computer which can quickly factorize prime numbers.

The paper examines standardization as a regulatory tool to mitigate the potential risks which quantum technologies pose to advanced electronic signatures. The analysis is timely as ETSI has already published documents related to quantum cryptography, in particular regarding electronic signatures. Moreover, NIST is also developing similar guidelines. Finally, the European Commission indicated the intention to update Regulation 910/2014 governing electronic signatures in the EU.

17:00 - 17:15 Coffee break

17:15 - 18:45 Parallel streams

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:15 - 18:45</td>
<td>Law: eHealth and New Technologies in Healthcare - Room 038</td>
</tr>
</tbody>
</table>

**Thomir Katulić, Hrvoje Liscic**

**Operation was a success, but the patient died: Data protection compliance and DPO experience in the Croatian health system**

Following the global pandemic and increased efforts by data protection authorities in Europe, the safety and security of health data is once again under the spotlight as the digitalization of health records and telemedicine grow more common. The presentation examines the importance of protection of personal data in the healthcare industry, which entails preventing illegal access to, abuse of, or disclosure of health information for various historically prone to ignoring the care for individuals' privacy.

The research then explores the General Data Protection Regulation (GDPR) regulatory framework with relation to recognized problems in health industry and its role in preventing data breaches and guaranteeing compliance. This research examines instances of data breaches in the healthcare industry to identify frequent gaps and possible legal and patient trust-related consequences of non-compliance.

In the second section, the author analyses the findings of a recent survey with over 80 designated data protection officers of Croatian public health institutions regarding their working conditions, understanding of their obligations, tasks, and competences, and the perceived level of understanding compliance. The author discusses the particular difficulties the health industry faces, such as aging infrastructure, a lack of information technology skills, and increasing cybersecurity threats. Suggestions are given of possible interventions de lege ferenda in the Croatian legal system concerning the status and tasks of public health organizations in Croatia.

**Roxanne Meilak Borg, Mireille M Caruana**

**Alternative legal bases for processing health data for scientific research purposes**

Processing health data for scientific research purposes requires the identification of both a legal basis for processing and a special category exception under Article 9 GDPR. There seems to be a tendency towards opting for consent as the said legal basis; this is also widely advocated for in the literature. Nevertheless, the GDPR sets out an alternative, specific exception to the general prohibition of the processing of special category data, and permits such processing for scientific research purposes where this is (i) based on a Member State or Union law and (ii) subject to 'appropriate safeguards'.

This paper engages in a critical legal analysis of the requirements of Article 9(2)(j) GDPR, referring to selected examples of Member State implementing legislation for illustration purposes, and comparing the requirements and consequences flowing from the choice of this legal basis to those of 'explicit' consent. It argues that the safeguards envisaged by Article 9(2)(j), if implemented faithfully, are more effective at achieving the related goals of enabling researchers, protecting research participants, and promoting the public interest. It thus proposes a shift from the current widespread practice of relying on the legal basis of consent for the concerned data processing, to relying instead on the 'scientific research exemption'. Nevertheless, the uneven implementation of the GDPR by the Member States creates considerable legal uncertainties, resulting in barriers to

**Partners**

![Rowan Legal](rowanlegal.png)  ![Zákoří pro lidi](zakoriziproli.png)  ![Wolters Kluwer](wolterskluer.png)  ![Codexis](codexis.png)  ![Pravni prostor](pravniprostor.png)  ![Catering for You](cateringforyou.png)  ![PwC](pwcc.png)
scientific research. The paper concludes that ultimately what is called for is a harmonised Union law that establishes appropriate safeguards for the protection of the individual.

**Do We Need New Rules of Civil Liability for AI in Health Care?**

There is little doubt that in the near future, artificial intelligence systems will keep increasing their importance in everyday clinical practice. We may anticipate the advent of specialised diagnostic and clinical decision support systems as well as medical robotics, but also the ever more prevalent use of general-purpose chatbots (such as ChatGPT) by individual health professionals. This reshaping of medical practice will inadvertently pose new challenges to the well-established rules and practice of civil liability in health care.

In recent years, a part of the professional discourse has been calling for new rules and principles of tort law to respond to these problems. Nevertheless, a question remains of whether, and to what extent, the more traditional institutes and tools of tort law suffice to address the challenges posed by AI. Using Czech law as a case study, we will ask whether liability for damage caused by a thing and other well-established tort law institutes can be used for AI in health care. Furthermore, we will analyse possible procedural tools such as shifting the burden of proof in well-defined cases. We will also address challenges to the practice of informed consent, such as when the patient needs to be informed about the use of AI in care.

While we cannot provide complex solutions to the outlined issues at this moment in history, they can serve as a framework to set the overall direction for thinking about civil liability for AI, namely to answer the fundamental question: Do we really need brand new rules of civil liability?

---

**Martin Šolc**

---

**19:15 Conference dinner**

---

**Partners**
Room 040

9:30 - 11:00 Parallel streams

New formats of digital legal education (special workshop) - Room 040
casted by **Nikolaus Fogo**

<table>
<thead>
<tr>
<th><strong>Anna Tauber</strong></th>
<th>Remote teaching: opportunity and challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The course ‘Legal Research’ at the Law Faculty of the University of Vienna serves as a mandatory introductory course for first-year law students. Due to roughly 500 course participants per semester, the eLearning platform Moodle serves as the means of knowledge dissemination and communication. While this teaching method allows for great flexibility and self-organisation, it has disadvantages. Motivation, little contact with fellow students leading to isolation, and limited contact with teaching staff over the semester are challenges that must be considered when setting up and structuring remote and non-simultaneous lectures. When extending the digital and asynchronous setting of the course to performance reviews, ensuring that students carry out exams individually and independently is another challenge. Thus, the teaching staff developed several measures to counter possible shortcomings of the setting: learning paths, continuous reviews of learning material, exam simulations and live quizzes, amongst others. Emphasis was put on balancing both personal (e.g. individual, private performance trackers) and external motivators (e.g. internship opportunities; quiz winners). Also, the opportunities of passively listening to and actively interacting with high-profile interviewees, as well as the approachability of the teaching staff during the consultation hours, strive to offer a palette of synchronous contact.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Catherine Liko</strong></th>
<th>Flipped classroom in the age of AI: its potential challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Every year, about 2,000 students start their law studies at the University of Vienna. To pass their first year, they must take the class ‘Legal Research’. The goal of this class is to help students learn how to use the classical legal databases. To address the scaling of the class, the course organizers opted for a flipped classroom. The class is entirely digitalized and available on the platform Moodle. The assessment process is based on multiple-choice question tests which take place in an open-book format. The final grade is then made up of three tests taken throughout the semester and questions at the end of each chapter. One challenge stems from the fact that tests take place online and unsupervised. The students can take the tests wherever and whenever they want during certain time slots. As the tests are open-book, the students can use any material that they wish. However, they cannot take the test with another student as that would fall under cheating. The use of AI-tools would also be a form of cheating. With the recent surge in popularity of AI tools and their easy access to the general public, the teaching staff studied the possibility for students to pass these tests with the help of popular AI tools such as open AI ChatGPT, Microsoft Bing or Google Bard. At first glance, the tools provided seemingly accurate answers. However, we observed several shortcomings and even hallucinations. This indicates that at this stage, the tools remain limited and unreliable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Michael Beier</strong></th>
<th>The Legal Tech Hackathon: An interdisciplinary approach to teaching IT law</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Since 2018, the Legal Tech Hackathon has been taking place as a cooperation between the University of Vienna’s Department of Innovation and Digitalisation in Law and the FH Campus Wien - University of Applied Sciences. Several small interdisciplinary project teams are formed each year consisting of law and computer science students in pursuit of developing and creating a legal tech business idea and prototype. In doing so, the Hackathon does not only aim to deepen the law student’s knowledge of IT law through a practical and hands-on approach, but also actively encourages an inner team knowledge transfer of background information in computer science to the law students, and vice-versa. This hands-on approach allows the students to apply...</td>
</tr>
</tbody>
</table>
IT law in one of the most practical ways possible - on a business idea created by themselves. Given the interdisciplinary nature of the teams and the Hackathon as a whole, this application of IT law is done in a way that is closely focused on the IT aspects utilized by the project team.

In essence, the Hackathon offers a unique opportunity for law students to analyze and answer relevant legal questions in regard to the project their team is developing. As a result, the Legal Tech Hackathon has seen many inspirational business ideas targeting pressing legal issues through the years, some of which have even been continued as startups by the respective project teams after the Hackathon. How the Hackathon is able to achieve this, as well as its goals and methods, will be further examined during the workshop.

**JusProfi: Complementing Traditional Legal Education in the Digital Age**

The digital age is changing how we learn. Legal studies, often taught in classrooms, are now also found online. JusProfi, a legal platform from Austria, is part of this change. This talk will show how JusProfi uses online tools to make legal topics clearer and more interesting, without trying to replace the usual classroom learning.

**YouTube Channel: Making Law Easier to Understand**

JusProfi's YouTube channel offers videos that break down tough legal topics into simpler terms. By using everyday language, adding some humor, and sharing real-life examples, the channel helps viewers understand legal ideas in a friendly way.

**Podcast: Deep Talks About Law**

The "Der JusProfi Podcast" is a place for detailed discussions about law. It invites experts from different legal areas to talk about their work. This gives listeners a chance to hear different views on legal topics and understand how law works in real life.

**Content Creation: Mixing Fun with Learning**

JusProfi believes in making content that's both fun and educational. The content keeps the information accurate but presents it in a fresh and engaging way. This approach helps to cover new legal topics and explore areas that might not be discussed in regular classrooms.

**Reaching More People Online**

Apart from videos and podcasts, JusProfi is active on social media platforms like Facebook, Instagram, and TikTok and has its own website. These platforms offer quick insights into legal topics and build a community of people interested in law. This online community encourages discussions and sharing of ideas. At the same time, JusProfi is not only aimed at law students or lawyers but also a general public which is interested in specific legal topics.

**Adapting to Today's World**

The Covid-19 pandemic showed us the importance of good online learning platforms. JusProfi's ability to offer quality content online makes it a key resource for modern legal studies.

**Helping Today's Learners**

JusProfi gives learners the chance to choose how they learn. They can watch videos, listen to podcasts, or interact with others. This approach makes legal studies more open and flexible for everyone.

**Adding to Traditional Learning**

JusProfi doesn't want to replace classroom learning. Instead, it aims to add to it. By offering a different way to understand tough legal topics, JusProfi supports and enriches the usual classroom experience.

**Conclusion**

JusProfi is helping shape the future of legal studies. By adding to regular teaching methods with the benefits of online tools, JusProfi provides a well-rounded approach to legal education. Their focus on clear explanations and easy-to-understand content makes them a valuable addition to traditional legal studies.

---

**11:00 - 11:15**  
Coffee break

**11:15 - 12:45**  
Parallel streams

<table>
<thead>
<tr>
<th>New formats of digital legal education (special workshop) - Room 040</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annemarie Hofer</td>
</tr>
</tbody>
</table>

**Partners**

[Rowan University]  [Wolters Kluwer]  [CODEXIS]  [PRÁVNÍ PROSTR]  [CATERING]  [PwC]
Adriana Praendl, Hande Özkayagan-Praendl, Faymann

How Should It Be Within Law in the Design and Education of Law Clinics

The Legal Design Sprint is an innovative, interdisciplinary teaching format. It aims at broadening the student’s horizon, bringing a more practical approach into the otherwise often very theoretical education. While the concept of a Design Sprint originates from research and development, we have adapted it to fit into a lecture format.

The underlying theoretical concept assumes, that the difficulties in successfully regulating technology do not stem from unwillingness, but from unknowingness on both the technical and the legal side. Therefore, we are convinced that (future) regulators can highly benefit from an out of the box approach towards techno-legal problem solving.

In my contribution, I will introduce the Legal Design Sprint as a teaching concept, explain the main benefits, and elaborate on the key challenges we faced during the Legal Design Sprints we held so far. This will aid participants in designing their own interdisciplinary teaching concepts to equip their students with the adaptive abilities they need to succeed in an ever more digitized world.

Adriana Winkelmeier

Privacy4Kids: Empowering Children to Protect Their Personal Data

As the digital age continues to evolve, it is crucial to educate children about data protection and privacy. The Privacy4Kids project aims to do just that, by providing children between the ages of 6 and 14 with short videos and games that teach them about the importance of protecting their personal data. Through these resources, children learn more about their rights, how to stay safe on social media, what “cookies” are, and how to protect themselves from online dangers. Videos and card games are produced by students from various fields of study, with the guidance of lecturers and external experts. This interdisciplinary approach ensures that the material is engaging and informative, while being accessible to children from 6 to 14. Nowadays, it is more important than ever to teach children about data protection and privacy, especially as there are various challenges of educating children in the digital age, including the need for appropriate practices and laws to safeguard children’s rights. The question arises of what roles parents and educators play in protecting children’s privacy, and how the Privacy4Kids project can be used in schools but also at home to contribute to empowering children to protect their personal data and how to make learning fun.

Hande Özkayagan Praendl, Lukas Faymann

Experiential learning and legal clinics in the digital age – Art Law Clinic as a case study

Legal clinics as an educational method at universities provide lecturers and students with valuable teaching and learning opportunity. They do not only provide law students the environment to implement theoretical knowledge gathered from their studies into practice and have an interdisciplinary exchange with their advisees, but they also allow the students to receive immediate mentoring and feedback from their clinic instructors through closer cooperation with them. In addition, the clinics make legal consultancy more accessible to groups in the community, who may not have adequate resources to seek help from legal professionals.

However, with the rapidly changing digital and technological landscape and the COVID-19 pandemic as a further added obstacle pushing for a shift to digital education, a necessity has emerged to rethink and adapt legal education provided at universities, including legal clinics. This presentation will discuss and brainstorm together with the participants of the workshop how the work and goals of legal clinics should be adapted to digital education, and how legal clinics can take advantage of the current digital advancements in their work. It will introduce the Art Law Clinic at the faculty of law of the University of Vienna as an example, which was initiated in the first half of the COVID pandemic. It will provide guidance, from the experiences of the Art Law Clinic, to participants from other law faculties who are interested in this teaching format and in setting up legal clinics at their own faculties.

Within the presentation, we will i.a. discuss the following questions:

What are the most fundamental challenges and opportunities of Law Clinics as a format?
Should law clinics play a more prominent role in current law curricula?
How should law faculties readjust the work of legal clinics and the format of experiential learning to the digital environment?

The presentation will be jointly held by Hande Özkayagan-Prändl and Lukas Faymann (both UNIVIE) and will consist of a keynote (20 minutes) and an interactive element (10 minutes).
### AI Special Track: Transforming Information Literacy in the Context of Generative AI Systems: From Prompt Design to Information Evaluation - Room 040

**Chair:** Michal Černý

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:45 - 13:45</td>
<td>Lunch</td>
</tr>
<tr>
<td>13:45 - 15:15</td>
<td>Parallel streams</td>
</tr>
<tr>
<td>15:15 - 15:30</td>
<td>Coffee break</td>
</tr>
<tr>
<td>15:30 - 17:00</td>
<td>Parallel streams</td>
</tr>
</tbody>
</table>

**Laura Grisales Rendón, Mittarvanh Phoomsavarth**

**Exploring Copyright Challenges in the Era of AI: From Language Models to Image and Music Generation**

The increasing use of AI systems, such as ChatGPT for language models, and for image and music generation, has introduced new challenges in the realm of copyright law. This work explores the copyright issues that arise with the use of AI-generated content, including the tension between intellectual property ownership and the use of such content, as well as the difficulties of attribution and fair use. Potential solutions are discussed, such as using Creative Commons licenses and developing new copyright laws and policies that consider the unique nature of AI-generated content. Ultimately, this work aims to contribute to ongoing discussions about how to navigate the complex intersection of AI and copyright in today's rapidly evolving landscape.

**Hagit Turjeman, Ofer Elfassi**

**Telegram Bot as a research tool for social and behavioral sciences**

The 21st-century information era centers on information, its access, and flow as crucial for societal development. Information flow empowers individuals and societies to stay informed on global, regional, and local matters, significantly influenced by mass media and the internet. This shift creates a symbolic virtual environment, with smartphones becoming a routine part of life for many. Interconnected individuals freely share thoughts, values, and ideas across physical, social, and cultural boundaries, transcending physical limitations. In this reality, virtual social networks serve as a central laboratory for studying human society and behavior.

The aim of this project was to explore social phenomena using botnet technology. A Telegram bot was programmed to perform a systematic search over encrypted channels, groups, and bots. One of the significant advantages of the bot was its ability to adapt the search according to the researchers’ search preferences and location. In a pilot study, the bot’s capabilities to explore cybercrime in encrypted channels were compared to human searches with identical keywords. The bot significantly improved the search outcomes, updating its results daily and facilitating efficient organization of data for the analysis phase of the research.

This project offers an open-access research tool and serves as an exemplar for researchers in the social, behavioral, and humanities sciences to leverage technology for systematic and comprehensive understanding of social life in the technological age.

**Andrea K Tóth**

**The European Data Strategy: a reflection on its achievements and the way forward**

In the February of 2020, the Commission adopted its European Data Strategy, in the form of a communication. This adoption coincided with the release of the White Paper on Artificial Intelligence, which acknowledged the importance of data also in the context of AI, and shifted the focus to this fundamental building block of novel digital applications (including AI).
The Commission’s vision enshrined in the strategy was to fulfil an ambitious plan: to create a European single market for data and to make Europe a dominant player in the data economy, specifically when it comes to the utilisation of its rich industrial data.

On one hand, the plan included the creation of a horizontal legal framework around the access and use of data, an unprecedented endeavour even on a global scale. As part of this legal framework, four legislative proposals (Data Governance Act, Data Act, Digital Markets Act, Implementing Act on High Value Datasets) have been foreseen.

On another hand, the strategy has introduced the concept of data spaces and announced the rollout of ten sectoral data spaces in strategically important sectors (such as health, finance, agriculture, among others).

Nearing the end of the mandate of the current Commission, it is worth taking a moment to take stock of and reflect on what has been achieved of these plans, as well as to see what the way forward could be in terms of the European data strategy and the future of the European data economy.

First there was openness. Then interoperability

The public sector in the Member States of the EU collects and produces a wide range of information in many areas of activity and this information represents an extraordinary source of data that can contribute to improving the internal market. The EU institutions are equally responsible for an impressive number of statistics and publications and the European Commission is the institution that produces the highest number of documents, data and software.

In applying the same policies it has proposed for Member States, the EU Commission has integrated legal openness into its own rules. Under the Reuse Decision (Commission Decision 2011/833/EU), documents of the Commission, including research data produced by its Joint Research Centre, is made freely available for reuse without the need for individual applications.

For software, the Commission consolidated its strategy on open source software by adopting the Software Reuse Decision (Commission Decision ([2021] 8759) making open source the preferred distribution for the software it produces and/or holds the intellectual property rights. The European Union Public Licence (EUPL), a 2007 creation of the Commission, has been chosen as the default licence its open source software and code.europa.eu, the code development platform for OS projects shared by EU institutions was set in place in 2022. With these, it was thus once again acknowledged that open source has become an integral part of business models in the software industry, being, without a doubt, largely embraced in the past years by the EU and public institutions.

However, if the intention is to remove barriers to a digital single market, openness and digitalisation alone are not sufficient but it is crucial to achieve the highest level of interoperability with and between public services. The proposal for the Interoperable Europe Act recognizes the role of open source in achieving such interoperability and in enhancing the reuse of (digital) solutions.

Applications such as LEOS, EUSurvey, open e-Prior, open e-TrustEx offered by the Commission to public administrations at European, national and regional level or solutions intended for scientific research in the areas of sustainability and climate; economics, energy and transport such as SMDRM, EJROMOD or Eurogastp are only few examples of open source implementations meant to support reuse and interoperability.

This contribution will tackle the instruments and initiatives adopted by the Commission in applying the concept of openness in its own work and how it further reflects the concept towards the public and public services.

European Copyright Law, Open Science and the European Data Strategy

Recognizing that data has become a valuable asset, the European Union has committed several times to a more open, global data strategy in order to exploit the resources of the European data economy. Many legislative acts, that target the liberation of data for better use, however exclude data protected by intellectual property from their scope and thereby leave the access and distribution rights of a considerable amount of research and other data to the rules of this respective legal domain. Intellectual property – in its theory – monopolizes creative expression in order to incentivize creative work and at the same time seeks to establish a balance between the interest of users (i.e. the public) and the creators of protected content. Copyright – and by its extension neighboring rights – has however evolved into a regime of very broad, technical exclusive rights and very narrow exceptions. This because as a reaction to quick and possibly disruptive technological advancements the CJEU in its jurisprudence and the EU in its legislation have consequently broadened the scope of protection of copyright, in order to give authors the possibility to economically benefit from new forms of uses. This leads to a situation where
Copyright threatens to monopolize data because of its broad scope of protection and thereby leaves the paths originally intended for this area of law. This becomes especially evident with the rise of big data processing and the need to extract large quantities of data in order to foster AI technology through mining processes. The solution envisioned by the European Union is yet another exception integrated in the copyright regime (Art. 3 and 4 of the DSM-Directive pertaining to Text- and Data-Mining) that – while aiming to establish legal certainty especially for researchers – lacks some of the answers such as to the question of how to store works reproduced for mining purposes or the lawful access condition. The presentation will in this context consider how the evolution of copyright to a possible overprotection with a limited catalogue of narrowly interpreted exceptions is detrimental to the aim of liberating data flow, what pitfalls the text and data mining exception poses in this context for OpenScience and what the future of copyright could look like in a society that aims to broadly free the use of data.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:00 - 17:15</td>
<td>Coffee break</td>
</tr>
<tr>
<td>17:15 - 18:45</td>
<td>Parallel streams</td>
</tr>
<tr>
<td>19:15</td>
<td>Conference dinner</td>
</tr>
</tbody>
</table>
Room 133

9:30 - 11:00 Parallel streams

Law: Government 2.0, eJustice - Room 133
chaired by Pavel Loutocký

Liliia Oprysk

The ambiguity of purchasing digital music in the streaming era: EU digital consumer contract law to limited avail?

Consumption of copyright-protected digital content remained on the periphery of regulators’ attention. This was set to change with the adoption of new EU legal instruments, notably the Digital Content Directive 770/2019 ('Digital Content Directive'). The directive aims to safeguard reasonable consumer expectations towards digital content by means of regulating certain aspects of contracts for the supply of such content without being of prejudice to copyright. Following the entry into force of the directive, this chapter aims to reflect on consumers’ experience purchasing digital music in the age of flourishing streaming services with a view to forming reasonable expectations. As the example of music purchased from the iTunes Store shows, consumers are by no means flooded with information that could pre-empt their expectations towards digital content. Moreover, potentially expected uses such as access to different software applications or transfer of copies, despite not being expressly allowed under the terms of purchase, are, in fact, technically enabled. To this end, it is argued that the ambiguity of consumer experience may circumvent the objectives of the directive in the absence of guidance on reasonable consumer expectations.

REMEDIS (Regulatory and other solutions to Mitigate online DISinformation)

The REMEDIS project adopts an interdisciplinary approach (ICT, human-computer interaction, communication science, and law) to address the pervasive issue of disinformation comprehensively. Based on this interdisciplinary expertise, our presentation aims to examine the potential impact of the Digital Services Act (DSA) on combating disinformation.

Our presentation starts with an overview of the way information technology and cybersecurity can inform on the online disinformation phenomenon. Notably, it explores how to measure its diffusion and how this type of assessment could be used as part of the risk assessment obligation of VLOPS under Art. 34 DSA.

The second part centers on the specific legal issues surrounding disinformation encompassed within the framework of the DSA. Particular attention is directed toward the obligations concerning content curation and risk assessments (esp. Art. 16, 22, 34-36 DSA).

The third part leverages insights from information and communication technology and human-computer interaction to comprehend the efficacy of measures aimed at curbing the spread of disinformation on online platforms and which should potentially be part of the mitigation measures that VLOPS should consider (Art. 35 DSA).

Finally, attention turns to extra-legal remedies for addressing disinformation, with an emphasis on the field of communication science. Recognizing the insufficiency of legal responses alone, alternative solutions, including media literacy, are contemplated as effective methods to counteract disinformation.

European data spaces – another puzzle in the mobility data governance?

The EU aims to enhance data exchange in the Single Market. This can improve European mobility by better utilizing car and infrastructure data. Data exchange is crucial for enabling automated cars, making road travel safer and more sustainable, all of which align with the goals of the EC Sustainable and Smart Mobility Strategy. Data sharing and its re-use are essential for achieving smarter transportation and a more data-driven market. The EU addresses data rights in the recently adopted Data Act and other data legislation introduced earlier. Mobility data serves as a particular example: it is mostly non-personal, machine-generated (cars, infrastructure), often a by-product of one's activity, and attains the highest value when processed by various stakeholders (private and public bodies) along the value chain. The automotive sector has recognized the value of mobility data and urges the EC to propose sector-specific rules for accessing car data, which will happen soon. In the non-business sector, efforts are made to

Wojciech Biernacki

Alain Strowel, Marie Dufrasne, Gabriele Lenzini, Anasatasia Sergeeva, Luc Desaunettes, Jean De Meyere, Huiyun Tang, Yuwei Chua, Daphné Chapellier

Partners
Bridging the Gap: Unraveling Lessons from Consumer Dispute Resolution for UGC Disputes on Platforms under the Digital Services Act

The Digital Services Act has introduced novel requirements for the resolution of disputes arising from action taken with respect to user-generated content (UGC) on digital platforms. Articles 20 and 21 DSA mandate the implementation of internal dispute resolution mechanisms by platforms and create a framework for external out-of-court dispute resolution by independent bodies. While these provisions hold great promise for enhancing user protection, their success hinges upon adoption by relevant stakeholders. For both of those mechanisms, the uptake by individuals is crucial, which is notoriously low. Possible reasons for under-assertion include intimidation and a weak prospect of successful redress. This paper seeks to shed light on the potential pitfalls and opportunities for improvement by drawing from the lessons learned from the consumer online dispute resolution (ODR) framework in EU, which includes Directive on consumer ADR, Regulation on consumer ODR and the subsequently created ODR platform.

Consumer ODR in EU provides an insightful case study, as it struggled to reach its full potential due to inadequate stakeholder engagement and practical implementation hurdles. By critically examining the factors that led to its shortcomings, this paper aims to identify key areas for improvement in the context of UGC dispute resolution. The paper shall focus in particular on assessing the factors that hindered active engagement in consumer ODR and proposing methods to foster active involvement from platforms, users, and independent dispute resolution bodies in UGC dispute resolution.

11:00 - 11:15
Coffee break

11:15 - 12:45
Parallel streams

Law: Intellectual Property On-Line - Room 133

chairs by Andreas Wiebe, Matěj Myška

Katarzyna Klafkowska-Wasniowska

‘Unauthorized’ as ‘illegal’? The interrelations between rules on content moderation in the Digital Services Act and the Copyright in the Digital Single Market Directive

The Digital Services Act (DSA) rests on the three pillars: the broad definition of ‘illegal content’, aligning the responsibilities with risks and advancing due diligence of intermediary service providers. The first report the Commission is obliged to deliver by November 2025 includes the question how the DSA interacts with other legal acts. The Copyright in the Digital Single Market Directive (C-DSM) is one of the acts encompassed by the general reference, that the DSA “is without prejudice to the Union law on copyright and related rights”.

The definition of “illegal content” under the DSA is probably the broadest possible: any content that is not in compliance with the Union law, or national law. At the same time this broad definition is based on the objective criterion of incompatibility with the EU/national law. The C-DSM Directive on the other hand at first opened the possibility for a more subjective approach, focusing on the unauthorized content and the claims from the rightholders. The CJEU correctly emphasized the objective of “ensuring users rights” stemming from the art. 17 C-DSM, and underlined the importance of mandatory limitations and exceptions, as well as procedural safeguards for users’ rights. In this context the DSA provisions are sometimes more general, as with the definition of the illegal content, or sometimes more detailed, as for example on the “notices” or out-of-court redress mechanisms. This paper focuses on these interrelations, particularly how the objective approach of the DSA to define “illegal content” that entails moderating activities should be followed in the context of the copyright enforcement and how the normative framework for due diligence calls is the way forward to “ensure user’s rights”, as recognized in the context of fundamental rights.

Peter R. Slowinski

The person skilled in the art of using AI

Partners
How does the increasingly widespread availability of artificial intelligence (AI) for innovative processes change the legal fiction of the person skilled in the art (POSITA) and with it the assessment of novelty and inventive step? This paper argues that across the board of areas of patentable subject matter, the availability of AI to the POSITA drastically changes the latter’s objective ability and therefore should raise the bar for novelty and inventive step.

Current state-of-the-art AI applications are based on predictions of the next step (e.g. GPT systems) or trial-and-error routines (e.g. evolutionary algorithms). Both types are becoming more powerful and therefore capable of solving problems or at least providing answers to questions. Since step-by-step developments and trial and error are essential parts of the inventive process, AI tools play an increasing role in this area. This is true even as current AI systems are far from reaching a level of autonomy to be inventors themselves.

This paper builds on the limited past research regarding novelty and inventive step in times of AI (Słowiński, 2021; Nakayama, 2021; Fabris, 2020; Blok, 2017). It considers the latest developments in AI technologies. It proposes specific guidelines for the evaluation of patent applications and granted patents in fields where AI is now a standard tool for the person skilled in the art, much like the microscope became in the 19th century.

**Do Androids laugh at electric mockeries? - Algorithmic control on uploaded contents and parody exception in EU law**

The EU Directive 2019/790 (art. 17, §4) provided a specific liability of content-sharing service providers, for their unauthorized acts of communication to the public of protected works.

Many Internet providers decided to use automated systems for content filtering, despite of the provision of §8, which explicitly says "the application of this Article shall not lead to any general monitoring obligation".

The rule was extensively debated and was implemented in very different ways in the EU countries, in particular as regards the possibility of excluding systematic preventive checking of contents which were lawfully uploaded on the platform, as covered by copyright limitations and exceptions.

Aim of this study is:

a) To provide a minimum framework for interpreting the rule contained in art. 17, §4;

b) To deepen the study of the difficulties of application of the rule, with respect to the contents covered by exception of parody, given the peculiarity of that expressive register;

c) To examine the solutions adopted by some national legislators in this regard, analyzing in particular the Italian law, compared to the German and Finnish ones;

d) To verify the perspectives opened by the use of next-generation AI in the analysis of the contents uploaded on the platforms.

The hypothesis that I intend to question and prove is the following: despite the great advances in the learning paths of the next-generation AI, at present automated content filtering systems are unable to identify the parodic connotation of content uploaded on platforms; as a result, such automatic protection measures are incompatible with the objective of balancing intellectual property rights and the protection of free use of works covered by author’s rights.

The study concludes with a brief analysis of the forms of protection usable to allow the free upload of parodic content.

**How wide is too wide: Scope of Post-Distribution Control in the Digital Era**

One of the basic theoretical underpinnings of copyright law is to achieve an intricate equilibrium, striking a balance between the interests of the rightsholders and the public-at-large. While the means of dissemination of protected works make it, in fact, much easier for the public-at-large to access and disseminate protected works, European copyright law in the digital era limits even such behavior and acts of the [members of the] public-at-large, which would be perfectly legal in the pre-digital world, in the name of the protection of economic interests of the rightsholders.

The submission discusses the changes in this balance brought about by the digitization of the markets with protected works (and the protected works themselves) and argues, that while the need for protection of the rightsholder is indeed as acute as ever, the European lawmaker needs to consider the public-at-large side of the mentioned balance more diligently, especially in questions of post-distribution rightsholder control.

The submission focuses primarily on the changes in factual scope of the distribution and communication to the public rights due to digitization, illustrating the impact of such changes on CJEU cases such as Tom Kabinet or Renckhoff and puts these changes in context of other tools commonly used for the preservation of interests of the rightsholder, such as private ordering and...
Bohdan Intellectual Property 12:45 - 13:45 Lunch

13:45 - 15:15 Parallel streams

Law: Intellectual Property On-Line - Room 133 chaired by Andreas Wiebe, Matěj Myška

Bohdan Widla

Do we even know what a computer program is? The stakes in C-159/23 Sony v. Datel

Any form of expression of a computer program is protected under copyright according to the Directive 2009/24/EC. The conscious decision not to define the computer program largely stood the test of time, allowing the directive to be largely immune to technological obsolescence. However, it came with a cost. Once we move beyond the obvious forms of expression, i.e. the code of the program (either source or compiled), we enter the penumbra with little guidance available in the normative text of the directive. Important edge cases remain here, as evidenced by the request for a preliminary ruling issued by the German Federal Supreme Court in the case C-159/23 Sony v. Datel. The case concerns software that can be used to cheat in video games by modifying the content of variables stored in the working memory. The plaintiff claims that such alterations amount to unauthorised modifications of the part of the videogames protected as computer programs and therefore infringe the exclusive right from Article 4(1)(b) of Directive 2009/24/EC. This contribution discusses these claims from a broader point of view. Accepting that variables stored in the volatile memory are protected as forms of expression of a computer program would vastly broaden the scope of protection, far beyond the original legislative intent and with far-reaching consequences for the balance of interests in the ICT market.

Vaclav Korckak

ChatGPT, Can I Have Your Autograph? Reevaluating the Concept of Legal Authorship in the Age of Artificial Intelligence

The Copyright Act defines an author as a natural person who creates a work. However, the rapid advancements in generative artificial intelligence (AI) raise critical questions challenging this legal principle. The conventional understanding that computers merely serve as tools for human artists, performing all creative work, is now inadequate.

This paper critically examines current Czech and European legislation concerning authorship in relation to content generated by AI tools. It illuminates the profound paradigm shift in the perception of human creativity demonstrated by generative AI and its implications for existing legal frameworks.

Furthermore, the paper investigates the advantages and risks associated with attributing legal personality to sophisticated AI software. Although discussions on this subject have been relatively muted, some academics, practitioners, and lawmakers advocate for this approach. For instance, in 2016, the European Parliament’s Committee on Legal Affairs proposed a novel legal concept, the "electronic person,” which would grant certain highly autonomous robots a degree of legal capacity. This paper presents arguments supporting the potential efficacy of such frameworks in addressing the issue of non-human authors.

Finally, the paper concludes by reflecting on the future development of copyright law and its implications for authors, considering the evolving landscape shaped by generative AI and its transformative impact on the concept of authorship.

Ondrej Woznica

Property metaphors and property narrative in the value gap: content analysis

The EU Directive on Copyright in the Digital Single Market underwent a tumultuous legislative process. One of the central issues is the problem of the value gap, which stands for difference between the actual value rightsholders receive for their rights and the value they could receive if their rights were not infringed, i.e., the difference in revenue from platforms like Spotify and platforms like YouTube.

Partners
Presentation builds upon empirical research focusing on the issue of value gap. It considers the problem of the propertization of copyright and its reflection in Article 17 CDSM legislative process by content analysis tools. It assesses the application of the recurring property metaphors of free riders, parent-child, agrarian and bad actors, as described by Lemley and Patry to the context of Article 17 CDSM legislative process.

The content analysis reveals that the value gap argument is rooted in the proprietary copyright paradigm that the creative industry wields to advocate for stronger copyright protection. The empirical study reveals resurfacing motives of bad actors and free riding targeted on platforms that cast them in a negative light in combination with the agrarian metaphor that appeals to the moral entitlements of authors. However, the creative market intermediaries benefit from Article 17’s provisions. Study sheds light on the impact of property-based argumentation and the need to consider consequences for creative individuals within the copyright ecosystem.

**Dominika Collett**

**Software developed by AI and its liability**

This contribution aims to focus on software development powered by artificial intelligence (AI). Currently there are several examples where AI is used in different stages of software development from source code generation and testing to GUI code generation. The human software developer can not be fully replaced with the current level of AI abilities; however, AI can assist at several different stages of the development and therefore have a significant impact on the final version of the software and its functionality. Whilst there are fundamental questions regarding the legal protection of such software by copyright, there should also be focus on liability in case of potential defects in software developed by AI. This contribution analyses different approaches to question of the software liability as well as discussion of new EU Proposal Artificial intelligence Act.

**15:15 - 15:30**  
**Coffee break**

**15:30 - 17:00**  
**Parallel streams**

<table>
<thead>
<tr>
<th><strong>Law: Intellectual Property On-Line - Room 133</strong></th>
<th>chaired by Andreas Wiebe, Matěj Myška</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radim Chavrat</strong></td>
<td><strong>Sui Generis Database Rights and data generated by IoT Devices</strong></td>
</tr>
<tr>
<td></td>
<td>The aim of this contribution is to examine the sui generis rights of database makers whether they fulfill their contemplated role. Ramifications of a few judgments of Court of Justice having a major importance with respect to scope of such rights will be briefly outlined (in particular, Ryanair and CV Online Latvia). Another important issue that will be dealt with will be data generated by Internet of Things devices and impact of sui generis rights on such data in connection with Article 35 of the proposed Data Act. Interpretation problems of this provision will also be discussed and a proposal for solving problematic aspects will be presented.</td>
</tr>
<tr>
<td><strong>Lucius Klobucnik</strong></td>
<td><strong>Fragmentation of Rights in European Online Music Licensing and the Ways Out</strong></td>
</tr>
<tr>
<td></td>
<td>Online music services (Spotify, Dezer or Apple Music) offering access to millions of songs by way of streaming or download have become increasingly popular with European end users, who prefer having constant access to large numbers of musical works on any device. However, in order to operate on an EU-wide level, these services face a complex licensing process, resulting in high transaction costs and presenting a substantial barrier to entry for new online music services. This paper suggests that the complex licensing process is due to the threefold fragmentation in the multi-territorial online music licensing market in Europe – territorial fragmentation, rights’ fragmentation, and repertoire fragmentation. Efforts to facilitate multi-territorial licensing benefited mainly rightholders (particularly major music publishers) but have not properly accounted for the interests of online music services as users. While legislative and market-driven initiatives addressed territorial fragmentation, they have neglected other forms of fragmentation (i.e. rights’ fragmentation and repertoire fragmentation) and contributed to the proliferation of individual licensing and the rising number of licensing entities, thus rendering the licensing landscape more complex.</td>
</tr>
<tr>
<td></td>
<td>This paper provides policy recommendations to ameliorate the impact of fragmentation on online music services and facilitate multi-territorial licensing. The past policy options and legislation are analysed in order to determine whether they can inform future solutions. Such future solutions should also be mindful of the technical challenges connected with digital music</td>
</tr>
</tbody>
</table>

**Partners**

![Rowan Legal](image1.png)  
![Ziky pro lidí](image2.png)  
![Wolters Kluwer](image3.png)  
![CODEXIS](image4.png)  
![Právní prostor](image5.png)  
![Catering for You](image6.png)  
![PwC](image7.png)
Civil liability for AI related IPR infringements

Several areas identified in literature where IPR infringements might occur in relation to the use of AI systems are analyzed against the proposed AI Liability Directive to find out who might be held liable for damages in such cases. The research covers situations where infringing IP rights is committed by training an AI system, as well as those where infringement is committed while operating an AI system. The later includes situations where AI systems generate content which is IPR infringing and those where the AI system acts as an intermediary whose services are used to infringe IP rights (for example AI in retail that would either influence the user/consumer to buy a counterfeit or even automatically order such fake products). One hypothetical situation of an AI system created solely for the purpose of infringing IPR rights is going to be investigated, but also situations where otherwise legitimate AI systems are misused in criminal activities as tools for the production and sale of infringing goods. The research will further evaluate if the AI Act will address or might be used to help solving some of the outstanding issues. In particular, the amendments European Parliament made to the initial proposal of the AI Act, such as the obligation to train, design and develop the foundation model and generative AI to ensure safeguards against the generation of content in breach of EU law (which is suggested to include EU IPR legislation) are going to be considered in the research.

Web Scraping and Text and Data Mining Exception for Commercial Purposes under DSM Directive: How the CDSM Directive intended to support reuse of publicly available data and might have achieved the opposite effect?

CDSM Directive introduced new copyright exception allowing to carry out text and data mining on protected content and opened room for permitted use of publicly available data which may be of crucial relevance in times of rising importance of artificial intelligence and massive use of big data. The TDM exception is being criticized namely for the right to opt-out. In practice, such reservation can be expressed via technical restrictions and disallow commands but also via website’s terms of use provided they are in a machine-readable format. At first glance, it might seem that such unilateral reservation can be easily implemented by the rightsholders who could en bloc restrict the reuse of their publicly available data and thus diminish the practical impact of the TDM exception. Many platforms already implement certain technical or contractual restrictions to protect its content. For example, many platforms prohibit TDM via terms of use, but such terms might not be machine-readable (especially considering the unclarity of the requirement of “machine-readability”). Many online platforms also use technical restrictions to impede crawling and scraping (e.g. Robot.txt). Robot.txt brings numerous practical questions – for example applying the disallow command on all users prevents indexing by search engines - which means this step will be out of the question for majority of rights holders. Robot.txt enables to apply different terms on various users or sections of the site (via the “User-agent” and Disallow/Allow line of the Robots.txt), but that requires the rights holders to populate “whitelist” or a “blacklist” of crawlers. The paper aims to explore the role and applicability of TDM exception to legitimize web scraping and re-use of publicly available data for commercial purposes and to identify its main gaps and uncertainty it may bring considering practical implications.

17:00 - 17:15 Coffee break

17:15 - 18:45 Parallel streams

19:15 Conference dinner
Are we in for the twilight of information self—determination?
The concept of information self-determination stood at forefront the right on the protection of personal data. The individual should know what is happening with his or her data and should have a possibility, to a certain extent, to agree or disagree with the processing. GDPR stressed the transparency principle and introduced strict requirements for consent. The trend is, however, reversing. In the case of Österreichische Post (C-300/21), the Post profiled personal data and inferred the applicant’s affinity with a certain Austrian political party from the data. The CJEU held that the data processing caused no harm to the data subject, except frustration. According to CJEU, mere infringement of GDPR does not lead to non-material damage pursuant to Art. 82 GDPR, even if the data belongs to a special category of data (political opinions) and the processing takes place without consent. Unfortunately, the court did not deal with the invasion of the applicant’s privacy, including his right on information self-determination accentuated i.e. by ECHR which the Union recognizes. The contribution will deal with the departure from informational self-determination as an aspect of personal data protection, not only in the case-law of CJEU but in other EU documents and regulations on automatized or algorithmic data processing.

Data pollution: applying property and liability rules
In 1972, Calabresi and Melamed introduced two regulatory approaches, the property rules and the liability rules. These concepts deal with voluntary and involuntary transactions within the field of law and economics, with a particular focus on navigating allocative efficiency. While property rules establish frameworks governing voluntary exchanges, providing individuals with rights to control resources, liability rules serve to regulate the environment where involuntary transactions occur.

Consumers provide data about themselves on every online step they take – sometimes when necessary, sometimes even while compromising their actual preferences (privacy paradox) or disregarding potential consequences of data sharing. These cases cause that nowadays, consumer data are ubiquitous. This phenomenon is referred to as ‘data pollution’.

In my work, I explore the feasibility of applying property and liability rules on this environment. Specifically, I describe where data transactions occur and whether they can be seen as voluntary or involuntary. I introduce different regulatory tools provided by property and liability rules and I discuss implications and challenges associated with applying distinct approaches.

Right to explanation when using AI in schools: the scope and (negative consequences of) limitations of Article 22 GDPR
This contribution explores the scope and (the negative consequences of) limitations of the right to explanation in the General Data Protection Regulation (GDPR) in cases of deploying artificial intelligence (AI) in educational contexts. AI is increasingly having an impact on education, bringing enormous opportunities as well as creating numerous risks to amongst others pupils’ right to privacy and data protection. Children are vulnerable data subjects while using AI requires processing of large amounts of personal data, including personal data that are either legally classified as ‘sensitive’ or at least commonly perceived as such. As one should note, the latest Proposal for Artificial Intelligence Act of May 2023 classifies AI systems in education as high-risk AI systems. From the perspective of data protection, one of the problems raised by the use of AI is (the lack of) transparency and black box phenomenon. In this respect, the GDPR provides for the right to explanation in cases of automated decision-making within the meaning of Article 22 GDPR. Yet, the scope of this is more limited than often assumed. Given that according to GDPR Recital 38 children ‘merit specific protection with regard to their personal data’ and that successful deployment of AI in education depends on trust, this contribution explores the possibilities of broadening the right to explanation, in particular, by analysing Article 22 GDPR, its possible amendments or interpretations.
Driving surveillance: on driver monitoring systems and workers’ privacy

Being a driving worker today comes with important privacy issues. The obligatory driver monitoring equipment in automated vehicles now enables an employer to obtain biometric data or information on the driving behavior, as well as data relating to the mental and physical health of the driver. The systems could show (if and) what the driver is eating during driving, what situations stress him and more. These sensors and cameras are expected to reduce driving accidents significantly. Although this could be applauded from a road safety perspective, the introduction of obligatory driver monitoring systems has its legal drawbacks. Especially where it concerns ‘driving workers’, those behind the wheel to make a living, tensions arise as this triggers a long-standing problem concerning the protection of workers’ data and their fundamental rights at work. Indeed, there have been worldwide reports of delivery drivers often being monitored via systems installed into the van. While monitoring may be optimal from a road safety and a right to life perspective, permanent surveillance of driving workers poses a number of questions considering the ECHR jurisprudence on privacy at work and the protections afforded by GDPR. This contribution aims to untangle this complex web of rights at stake by providing an overview of the legal framework and by exploring a fair balance between road safety and the privacy infringements of monitoring the driving workers.

Real-time bidding, cookies, and EU data protection and ePrivacy law

In the internet age the idea of a person having a control over their privacy became an illusion. Not only we became increasingly inclined to sharing our personal life on social media, but new technology also gave rise to a completely new field – targeted internet advertising. Unlike the ideas of Orwell and Bentham, the advertising companies do not wish to monitor and control our activities. Their goal is much simpler: Making a profit.

This paper attempts to answer the question of how the regulation of both data protection and access to information on terminal equipment of a user should be conceived in order to ensure a high level of protection of fundamental rights and freedoms in the processing of personal data in relation to so-called real-time bidding (a form of targeted internet advertising), while ensuring that the websites financed through targeted advertising face little to no negative effects.

Firstly, the author will discuss the risks of processing personal data in real-time bidding in connection to the human rights and freedoms. After that, the author will analyze the current and proposed data protection and privacy law connected to real time bidding. Lastly the author will propose changes, which the law shall undergo in order to ensure a higher level of protection of fundamental rights while mitigating the negative effects on financing websites through targeted advertisement.

Turning the right of access into a mathematical problem: Personal data in multi-application cloud landscapes from the computer science point of view

The right of access is probably the most important data subject right and often exercised by data subjects. However, to identify, which data under processing by a data controller qualifies as personal data that concerns a specific data subject is not trivial. This becomes even more complex in cloud computing scenarios when various software applications are integrated with each other and when circumstances from one application influence whether data in another application must be considered personal data.

We propose a dynamic, iterative rather than a static, direct approach of identification of personal data within a specific context, such as a cloud software product. We understand by a “dynamic approach” that the set or sets of attributes within a database suitable for uniquely identifying a data subject can vary at different points in time depending on the actual database content, in contrast to a priori fixed parameters. This allows to execute the export of personal data iteratively across multiple applications, so that the knowledge attributable to the controller from one application context can be considered when exporting personal data from another.
application. To our knowledge, this is the most complete approach to exporting personal data, especially in cloud landscapes with standard software applications.

12:45 - 13:45  Lunch

13:45 - 15:15  Parallel streams

<table>
<thead>
<tr>
<th>Law: Privacy and Personal Data - Room 136</th>
<th>chaired by Jakub Mišek, Bettina Bacher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hrvoje Liscar, Tihomir Katulić</td>
<td>Data protection vs. efficacy and public interest - Croatian perspective on data protection in courts and e-justice systems</td>
</tr>
<tr>
<td>Martin Erlebach</td>
<td>Google's AI Ambitions and Privacy Concerns: A Look into Internet-wide Data Scraping</td>
</tr>
<tr>
<td>Jakub Mišek</td>
<td>Balancing Between PSI and Personal Data: EU and National Perspectives</td>
</tr>
</tbody>
</table>

- The primary objective of this paper is to explore the correlation between individuals' right to protection of personal data and the public interest in allowing unrestricted access to public records containing citizens' personal information in its complete form. To achieve this, the authors focus on two crucial components of Croatia's e-justice systems: The Cadastre and Land Registry, and the e-Court Notice Boards. Despite being openly accessible on the internet, these systems hold vast amounts of individuals' personal data that are not anonymized, and justified by efficacy of judicial systems, making it imperative to analyse the regulations and decisions governing them in accordance with the EU's General Data Protection Regulation (GDPR).

- The second part of the paper delves into the implementation of the GDPR within Croatian courts. To accomplish this, the authors conduct a comprehensive analysis of a recent survey administered to key figures within several major courts, including judges and court administration. The primary aim of the survey was to gauge their understanding of data protection responsibilities, assess the level of GDPR compliance among Croatian courts, and identify existing best practices designed to enhance the protection of personal data for all parties involved.

- At the beginning of July, Google changed a part of its privacy policy to read: “For example, we use publicly available information to help train Google’s AI models and build products and features like Google Translate, Bard, and Cloud AI capabilities.” – effectively stating that it will scrape everything that is posted online for its benefit.

- In the current environment of many generative AIs appearing almost daily, the lawful acquisition of training data deserves close attention. This recent change in Google’s privacy policy may offer significant insight into the legality of keeping up with AI’s data-crunching habits.

- Among other legal concerns, issues regarding privacy arise from the aforementioned change to Google’s privacy policy. If the publicly available information from the changed statement is to include personal data, and there is no reason not to believe it does, what is the legal ground for processing this information? In case the processing should be done on the basis of legitimate interest, careful consideration of rights of data subjects will be needed to ensure this is truly possible. Regardless of the evaluation done, issues of transparency and the case of Clearview AI should be considered when thinking about the legality of web scraping of this magnitude.

- Current CJEU case law sets limits on the disclosure and thus re-use of public sector information containing personal data. In particular, in the ruling in joint cases C-37/20 a C-601/20 CJEU decided that the obligation to disclose information on the beneficial owners of companies within the meaning of Article 30 of the amended Directive 2015/849 is in breach of the Charter of Fundamental Rights of the EU, given that, although this regulation is an appropriate tool in the fight against corruption, it is not strictly necessary [there is a less invasive solution] and at the same time it does not offer sufficient guarantees for the effective protection of fundamental rights and therefore disproportionately interferes with them. The discussion contribution takes this decision as its starting point and addresses the question of whether the proportionality test contained therein is binding on all Member States when making national law.
Coffee break

Parallel streams

Legal Informatics - Room 136
chaired by Erich Schweighofer, Jakub Harasta

Pedro D Venâncio

Information and knowledge technologies in law teaching

Law has gone digital.
Legislation and jurisprudence databases were gradually digitized and made available free of charge on the Internet. Judicial and administrative processes were transferred to online platforms. Registrations and corporate acts are now mostly performed digitally. Passports became electronic, the citizen card includes qualified electronic signatures. In addition, most legally relevant acts, public or private, negotiation, contracts and payments are now mostly electronic.

Knowing the technologies that support digital acts and evidence, mastering the electronic platforms of justice, or monitoring the multiple applications of emerging technologies to the justice sector are basic skills for any judge, prosecutor, or lawyer.

It is imperative that higher education institutions know how to equip their law students with:

1. Knowledge necessary to understand the technologies that enable the practice of legally relevant electronic acts.
2. Adequate skills for an efficient use of the technologies of justice, whether in the platforms that support the administrative and judicial processes, or in the databases that gather the relevant legal information (legislation, jurisprudence, etc.).
3. adequate competences for a judicious use of ICT tools, applying them in a safe way to the search and production of legal information useful to their professional practice.

In this presentation we discuss how to introduce these skills in law courses.

In particular, we propose:

- the revision of the curricular programmes of some core subjects of the law course in order to include in the essential subject matter, provision for documents, communications and electronic signatures.
- changes in teaching methodologies to include the pratice of basic skills on how to use justice platforms.
- to include in the learning objectives to be assessed: having the critical sense and basic competences for checking the information and legal knowledge researched and/or produced by ICT.

Štěpán Paulík, Jaromír Frnč

Locating Czech Constitutional Court Decisions in Doctrine Space and Measuring its Caselaw Consistency

Our research explores the estimation of positions of Czech Constitutional Court decisions in a doctrine space using Bayesian statistical model. Traditional methods of estimating ideological positions suffer from limitations, prompting the adoption of new text-as-data approaches empowered by advances in computational technology and statistics. Two research teams have attempted to overcome previous constraints and estimate judicial positions more accurately, one in the SCOTUS context and one in the German lower courts context. Our study implements the method of Clark and Lauderdale of estimating the locations of SCOTUS decisions with positive or negative references to its caselaw: the closer decisions are to each other, the more likely they are to cite themselves positively and vice-versa. We combine our own dataset of all CCC decisions with the data on citations provided to us by Beck. We use the programming language R and the Bayesian engine Stan to estimate the positions employing the Bayesian model of Clark and Lauderdale. Estimating the positions allows us to examine the consistency of the CC's case law across different senates and the plenum. We narrow our analysis to areas of law in common doctrine space that are prone to inconsistency, namely restitution cases and costs of civil proceedings. The research contributes to harnessing the potential of machine learning and quantitative methods in legal research and clarifies the factors influencing caselaw consistency.
Zsolt G Balogh  

**Fuzzy logic in law**

Uncertainty and vagueness of governing concepts is a common phenomenon in legal domain, thus the definition and proper representation of legal concepts means a critical challenge to the legal knowledge-based systems.

The present new wave of AI developments promises more sophisticated approaches to the developers of the intelligent legal expert systems. Beyond the developed Natural Language Processing (NLP) applications the recent advanced machine learning and deep learning methods based on the developments of Big Data technologies facilitates to construct genuine ‘knowledge-based systems’, showing more realistic representation of knowledge. The structure of knowledge representation is about to be more flexible and relates closely to the structure of human thinking. Current legal chatbots, advanced case-law search-engines, virtual assistants may be constructed on the robust Big Data platforms of the leading IT service providers.

The knowledge base of a Big Data related legal expert system must be drafted in a well-tailed legal ontology which can be adapted to the fuzziness of the legal system.

“The law is full of fuzzy thinking. If there is a precise way to think about fuzzy ideas, legal scholars, judges, etc., should use it. .... I do believe that Zadeh has given us important tools for radically better ways of thinking about fuzzy thinking.”

Fuzzy logic, fuzzy sets and fuzzy reasoning are obvious tools for representing and processing vague, arbitrary legal concepts in knowledge-based systems. This presentation seeks to give an example and a demonstration of a legal ontology designed by the combination of fuzzy logic and classical toolkit of semantic systems.

Attila Menyhárd  

**Assistive AI in Legal Services**

It seems that discussions on AI primarily focus on whether and how far technology can replace human resources in different professions or activities. That holds for legal services as well. As in general, also in legal profession, lower emphasis is put on assistive role of AI. In legal profession, automated decision making is possible where legality is controlled in context of regulation. That is the case, e.g. in land registration (UK Land Registration, the new Hungarian land registry system and further jurisdictions are analysed as examples). On the other hand, where law transmits social evaluation of the case, judgments of the courts are the outcome of weighing relevant values of the case (as described by Walter Wilburg as a „bewegliches System“) like in tort law or contract law; or even deciding over priorities between conflicting rights which is typical in constitutional law or in the law of protecting inherent rights of persons. In this latter are of law mostly the freedom of one of the parties conflicts with the human dignity of the other.

If it comes to social evaluation of the case, replacing human resource (the judge) by AI is less realistic, at least in the present structure of our societies. Using AI as assisting human decision, however, shall be considered as a realistic idea. The key is establishing the human – AI interface and the methodology of identifying and weighing conflicting social values via algorithms. Assistive AI can be used as part of a new knowledge management. The chances, challenges and searching for the methodology on this issue is discussed in the contribution.

<table>
<thead>
<tr>
<th>17:00 - 17:15</th>
<th>Coffee break</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:15 - 18:45</td>
<td>Parallel streams</td>
</tr>
<tr>
<td>19:15</td>
<td>Conference dinner</td>
</tr>
</tbody>
</table>

**Partners**

- ROWAN
- Záložky pro lidé
- Wolters Kluwer
- CODEXIS
- PRÁVÍ PROSTOR
- CATERING
- PWC
Fitfluencer effects on body satisfaction and well-being

More and more research shows that the visual imagery of certain social media may affect its users’ well-being and body image (e.g., Jarman et al., 2021; Schmuck, 2021). Social media such as Instagram are highly visualized media on which people tend to picture an idealized version of themselves. When people compare themselves to these idealized versions, they almost necessarily feel worse about themselves, as it seems impossible to live up to these expectations. Yet, social media may also inspire people to feel good about themselves or change their behavior. For example, social media channels about health and food may inspire healthy behavior while movements such as body positivity may help people adopt a more realistic body image (Cohen et al., 2021).

One of the most popular types of social media content is provided by influencers. Influencers are well-known social media users who often gained fame by branding themselves as experts in a certain community and as a result have gathered huge swaths of followers. Influencers who are experts in a certain niche, such as beauty or fashion. Influencers have both reach and impact: They have a large gathering of followers and are able to influence the beliefs, attitudes or even behavior of their followers (Hudders et al., 2021).

A specific type of influencers are so-called fitfluencers, who specialize in health and fitness-related content. Fitfluencers mainly pose health and fitness related content in which they show their muscular bodies, provide instruction videos on training, advice on healthy eating, and upload other content related to physical prowess. People may be differentially affected by fitfluencer content. One the one hand, fitfluencers may inspire people to take up a healthy lifestyle. Fitfluencers often present themselves as ordinary people, next to being experts. They may thus be seen as relatable and achievable role models to their target audience (Eng et al., 2022). On the other hand, fitfluencers often present an idealized body image, near impossible to achieve and unattainable for most people. Their focus on exercise and healthy eating may also cause unhealthy eating behavior in fitfluencers’ followers (Cataldo et al., 2021).

Little research has investigated which factors affect how people are influenced by fitfluencers and when these effects may have positive or negative outcomes for body satisfaction and well-being. Research into the effects of Instagram and general media use shows that this depends on both the type of content and the type of involvement that users have for engaging with certain social media content.

First, relying on audience involvement theory (Brown, 2015), we pose that exposure to fitfluencer content may have both beneficial and adverse consequences, depending on the type of involvement followers experience when engaging with fitfluencer content. Specifically, we expect that body satisfaction and well-being are affected by both wishful identification and perceived similarity with a fitfluencer. Wishful identification occurs when followers wish to become similar to the fitfluencer (i.e., ‘I want to be like this fitfluencer’), which may decrease followers’ self-evaluation, resulting in lower levels of body satisfaction and well-being. Perceived similarity refers to a feeling of being on par with a fitfluencer (i.e., ‘I am like this fitfluencer’), which may reaffirm followers’ self-evaluation, increasing body satisfaction and well-being. People may thus be differentially affected by fitfluencer content depending on whether their involvement is identification or similarity-based.

Second, we expect the effects of exposure to fitfluencer content to depend on the specific content that followers are exposed to. Fitfluencers differ in the type of channel they own and the type of content they share. A first distinction is usually made between influencers with many followers versus influencers with fewer followers: macro vs. micro influencers. Moreover, influencers may also be distinguished based on the influencer’s general motivation. Influencers may be merely passionate enthusiasts, may combine passion with entrepreneurship, or may be influencers who might also be passionate but for whom their niche is not the root cause their online success (e.g.,
a celebrity turned fitfluencer). The specific content posted also depends on the type of influencer. For fitfluencers specifically, there is an important distinction between influencers who solely focus on health and fitness-related outcomes or influencers with a more holistic approach. The first focus mostly on physical fitness, muscularity, and weight loss. The second focuses on integrating physical fitness with a general healthy lifestyle including mental health and a focus on other activities besides fitness.

In sum, the main research question we aim to answer is: To what extent does engagement with fitfluencer content affect followers’ body satisfaction and well-being? This main question is further divided into two sub questions: (1) To what extent do wishful identification and perceived similarity with fitfluencers relate to body satisfaction and well-being? (2) To what extent does specific fitfluencer content affect wishful identification and perceived similarity and the resulting body satisfaction and well-being. As followers of influencers and the general Instagram demographic mostly consists of adolescents and young adults, we investigate these research question in a sample of adolescents and young adults (aged 16-34).

The two sub questions are addressed in two different but related studies, the first of which has been completed, and the second of which is currently being conducted. The first study is a survey study among 1167 Dutch adolescents. The second study combines the outcomes of the survey study with a content analysis of fitfluencer posts.

Study 1: Method and Results

An online survey was conducted among 1,167 Dutch respondents aged 16 to 35. Respondents who did not follow influencers were excluded (N = 420), resulting in 747 respondents (Mage = 19.88; 66% female). Respondents were asked to write down their favorite influencer and to keep this person in mind while answering the questions. Measures included age, gender, well-being (M = 5.39), body satisfaction (M = 60.38), wishful identification (M = 3.94) and perceived similarity (M = 2.95). Body positivity was measured using a slider ranging from 0 to 100. All other constructs were measured with 7-point Likert scales.

Structural equation modeling using Mplus (MLE) was used to test the theoretical assumptions. The structural model provided a good fit to the data: χ²(71): 394.153, p < .001, CFI = .94, RMSEA = .058. Gender was included as a control variable. On average, men reported a significantly higher well-being and body satisfaction than women. All hypothesized paths were significant, with the exception of the direct path between perceived similarity and well-being. Whereas wishful identification (β = -.53, p < .001) was negatively related to body satisfaction, perceived similarity was positively related (β = .40, p < .001). Furthermore, body satisfaction was a significant predictor of well-being (β = .50, p < .001), and indirect effects via bootstrapping analysis (95% CI) confirmed that body satisfaction fully mediated the relationship between perceived similarity and well-being (β indirect = .20, 95% CI [.07, .24]). Finally, body satisfaction only partially mediated the relationship between wishful identification and well-being (β indirect = .40, [.19, .07], given the direct, significant relationship between both concepts (β = -.13, p < .05). The model explained 25% of the variance in body satisfaction and 32% in well-being.

In conclusion, analyses confirm that both identification processes with fitfluencers predict overall body satisfaction, albeit in opposite directions. Additionally, body satisfaction was identified as an underlying mechanism in the relationship between fitfluencer exposure and well-being.

Study 2: Method

For the content analysis, we analyzed the Instagram pages and posts of all influencers who were mentioned at least twice in study 1. This resulted in a list 69 influencers that were mentioned by 378 of the 747 respondents. The content analysis was conducted on two levels: the influencer level and the post level. At the influencer level, we coded the number of followers, time active on Instagram, age, gender, whether the influencer is officially verified by Instagram, and the exact title of the influencer (e.g., athlete, coach, public figure). For each influencer, we coded 20 posts by taking every third post. We analyzed the post as a whole, so if a post consisted of multiple images, these were coded as one. For each post, we coded whether the post displayed physical exercise, nutrition, body aesthetics, motivational statements, and whether the fitfluencer was visible in the post (all Yes/No). We also coded whether the post was focused on passion, performance, enjoyment, positivity, and mental health. We also coded whether the post was sponsored and the number of likes and comments the post had received up to the moment of coding.

Based on the content analysis, we can classify the type of fitfluencer and the type of posts, and relate this to the body satisfaction and well-being of the survey respondents. The content analysis is currently being conducted, and —if accepted— we will present the results at the Cyberspace conference.

**Partners**
Is chatting with friends on social media in the evening harmful for adolescents’ sleep and academic wellbeing? – an experience sampling study with objective sleep measures

Using an intensive longitudinal approach, we examined associations between adolescents’ SMU close to bedtime, same-night sleep and wellbeing at school the next day. In addition, we investigated how social pressure to stay constantly available online and related availability stress associate with sleep and wellbeing. SMU was conceptualized two ways: interactive two-way (i.e. “chatting with friends”) and passive one-way (i.e. “scrolling content”). We collected data during 12 consecutive days from N=143 adolescents (aged 17-18, 68% female) using N=2,590 momentoary measures during the school day and N=1,102 measures during the evening/night. We measured objective bedtimes with activity bracelets. Multilevel models showed that SMU close to bedtime per se was not harmful for adolescents’ sleep or wellbeing at school. On the other hand, results suggested that social pressure to stay constantly available associated with later bedtimes and availability stress associated with poor sleep quality and higher levels of tiredness, stress and anxiety during school days. Based on these results, we conclude that chatting with friends in the evening is not that harmful for adolescents aged 17-18. However, adolescents need socio-emotional and self-regulation skills to tackle the different socio-digital demands and possible stresses arising from SMU. Therefore, also researchers should focus on psychosocial features of SMU rather than only investigating time spent online or the type of use.

Latent profiles of adolescents’ digital skills across six European countries

We report on a large study conducted in six EU-countries that identified latent profiles based on digital skills among adolescents (N=6221; Mage=14.5; SD=1.4) as well as their associations with socio-economic, socio-emotional and digital activity antecedents. Digital skills are considered critical for functioning in contemporary society, yet there are strong differences between adolescents’ skills (so-called digital divides) depending on demographic and socioeconomic variables. Previous research has examined digital skills and their associations with background variables mainly as a set of isolated dimensions. Taking a person-oriented approach and using latent profile analyses followed by tests of similarity across countries, we were able to identify five profiles: 1) All-rounders, 2) Information-oriented, 3) Content-creators, 4) Communication oriented and 5) No high skills. The profiles showed mean and variance similarity across countries but varied in their proportions. The All-rounders reported most high skills and showed overall the best performance across digital knowledge items. Boys were more likely than girls to represent more highly skilled profiles.

Further, support from friends, working with computers (instead of merely mobile phones), using digital media to follow news, to purposefully learn something new, create digital content or communicating with friends increased the odds of belonging to the All-rounders group.

Digital Well-being in Schools: From Data to Practice

"They’re still on those phones! They’re addicted and they don’t care about anything else!” A common phrase heard from schools and parents. The topic of digital technology is new to many adults and is also evolving rapidly. So there is a growing fear that the younger generation will be a generation of digital addicts and that using smartphones will have immeasurable negative effects on wellbeing, relationships and their development.

In response to this issue, Replug me (nonprofit organization) has developed Digital Education, a comprehensive digital well-being programme for schools. It aims to set the foundations for healthy use of digital technology in adolescents. The programme also introduces the digital world of children and adolescents to their teachers and parents. It reduces fear of the negatives, while also showing its positives, which are often overlooked.

The paper will present data collected during the programme mainly from about 700 adolescents (aged 12-15 years) in spring 2023. The presentation will address several questions. First, we will provide evidence on how children themselves evaluate their technology use. Then, we will discuss whether it is really necessary to be afraid of the negative effects of digital technologies. Finally, we will also discuss the overall impact of Digital Education.

11:00 - 11:15 Coffee break

11:15 - 12:45 Parallel streams

Partners
What FUTURE Shows? Understanding The Role Of Digital Technologies In Adolescents' Well-Being - Room 140

Smahel, David, Machackova, Hana, Dedkova, Lenka & IRTIS members

This section is fully devoted to the presentation of a robust five-years long Czech project FUTURE that investigated the role of digital technologies in the well-being of adolescents. The project examined the short- and long-term impacts of technology usage on adolescents' physical, psychological, and social well-being. The purpose of the section is to introduce the main work packages of the project and project’s key findings. Further, as FUTURE applied several methodological approaches, their design and role in answering specific research questions will be described and illustrated more in detail on selected studies. Specifically, the researchers will talk about implementation of and results from these methods: Ecological Momentary Assessment (EMA), longitudinal design, and experimental design. The section will be concluded by a discussion of a new theoretical model (IMEW) developed within the project and also future research directions.

12:45 - 13:45
Lunch

13:45 - 15:15
Parallel streams

Psychology of Cyberspace - Room 140
chaired by David Smahel, Hana Macháčková

Armin Klaps, Daria Kahles, Zuzana Kovacovský, Jan Aden, Birgit Ursula Stetina

Gaming, Internet Gaming Disorder and the specific focus on gender; quality of life and motivation. Gender Equality in Online Gaming?

In our last study on clinical aspects and gender differences in online gaming, no differences regarding clinical scales were found, but clear differences in subjectively perceived quality of life (Klaps et al., 2022). To gain additional insight, a replication study was conducted using similar concepts and adding gaming motivation.

450 gamers filled out an online questionnaire (379 complete datasets) including demographic items and the following test battery: WHOQOL-BREF, IGD-20 and Vees Online Gaming Motivation Scale. 83.1% (n=315) of the total sample identified as male, 13.5% (n=51) indicated female gender; 6 individuals (1.6%) identified as transgender, and 7 participants (1.8%) as non-binary; all aged 16 to 67 (M=27.44, SD=6,83).

No gender differences were found regarding playing time (t(431)=-.053, p=.957) and all IGD-20 scores (eg Withdrawal (F1,1364)=.40, p=.611). But gamers differ significantly with respect to the four domains of quality of life (physical health, mental health, social relationships, environment) (Λ=.93, F(4,361)=6.94, p < .001, η²=.07) with males indicating a higher quality of life. Gender differences are also significant in the three main factors of gaming motivation (Λ=.96, F(3,362)=4.28, p=.005, η²=.03), with females showing higher scores in Immersion.

Gender differences exist in various areas, but the concurrent areas seem to have changed. Are the differences smaller than one would assume? What does that mean for gender equality in Online Gaming?

K-8 Children Know Little about How the Internet Works even after Intensive Tutoring: Preliminary Results from a Mixed-Method Study

Children need to become competent online users. Previous studies suggested that in order to achieve this goal, it helps if children understand basics of how the internet works. This includes notions of how data travels across the internet and that it is semi-permanently stored and analysed on servers. However, two recent reviews showed that knowledge of K-8 children about the internet’s functioning is patchy and frequently incorrect, which is consistent with ‘knowledge in pieces’ theories of knowledge representations. Plus, little is known about how to boost their understanding of this topic. Here, we present preliminary results from a mixed-methods study, in which children (Grade 4/6/8; N=54/57/47): a) were interviewed about how the internet works; b) half of them (random assignment) was explained this topic (50-min-long session; one child: one teacher); c) were interviewed again 5 months later. The interviews are now being analysed through inductive thematic and frequency analyses, which will be completed at the time of

Partners
Cyberspace 2023. As concerns prior knowledge, preliminary findings are consistent with the existent literature. Children understand the internet primarily through their personal experiences and know little about how personal data they upload flows across the internet and where it is stored. Only most knowledgeable children view the internet as a global network with a complex internal, but only vaguely understood, structure. The teaching session promoted understanding in short term, but much less so in a long term. About half of children from the experimental group appeared to forget everything, Most of the second half exhibited in the delayed interview an incoherent amalgam of their prior knowledge and fragments of new information. Our results are important for on-going computing education reforms at K-8 level. They suggest that teaching K-8 children about the internet functioning will be challenging and specific approaches will be needed.

“What is inside a computer?”: preconceptions about computer principles in 6-9-graders - work-in-progress

The new computing curriculum in Czechia for grades 6–9 focuses on, among others, the topic of computer principles, i.e., how computers work internally. There is a lack of teaching materials in Czechia that deal with this topic. When one wants to create teaching materials for children, these materials should be based on children’s preconceptions about the topic so that the materials appropriately target the theme with respect to children’s prior knowledge. However, existing literature has not sufficiently examined children’s preconceptions about computer principles.

Hence, we conducted a mixed-methods study (N = 53, n6+7= 29, n9= 24) in diverse regions of Czechia with the aim of identifying the said preconceptions. Through 45-min-long semi-structured interviews, we investigated children’s understanding of how computers function. Using Atlas.ti, we conducted an inductive thematic analysis and identified around 260 preconceptions, some of which have never been described previously. Based on their occurrence, we performed a non-hierarchical cluster analysis with automatic cluster detection in IBM SPSS 28, identifying three participant groups based on their knowledge level: experts (who comprehend most abstract concepts, e.g., the cooperation between RAM and the processor or the very existence of different types of memory), moderate (who understand some abstract concepts), and naïve (who lack understanding of most abstract concepts; the computer is a magical black box for them). Currently, we are characterizing each group and cataloguing the identified preconceptions. Next, we’ll create educational materials that suit different knowledge levels, guiding children from preconceptions to normative understanding. Our study’s findings could be valuable not only in the Czech context, but also in the process of updating K-9 computing curricula elsewhere.

15:15 - 15:30 Coffee break

15:30 - 17:00 Parallel streams

Psychology of Cyberspace - Room 140

chaired by David Šmahel, Hana Macháčková

Birgit Stetina Ursula, Jan Aden, Zuzana Kovacovsky, Daria Khales, Armin Klaps

Update on Online-Gaming and Mental Health: Quality of Life in Gamers suffering from Internet Gaming Disorder

Gamers with clinically problematic gaming behavior are a small part of the population. However, this conspicuous group is dominating the news and more insight is still needed to create more feasible treatment options and prevention measures.

A quantitative online study was conducted using the WHOQOL-BREF, IGD-20 and Yees Online Gaming Motivation Scale as well as items on gaming patterns and demographics. 459 gamers took part in the study (379 complete), aged 16 to 67 (M=27.44, SD=6.83), with a male majority of 83.2% (n=382), the rest identified as female (13.1%, n=60), transgender (1.3%, n=6) and non-binary (2.0%, n=9).

A small number (n=22, 5.2%) of the sample met all conditions for Internet Gaming Disorder (according to IGD-20), with no significant difference regarding age (t(421)=0.745, p=.455, d=.16). They differ significantly from the rest of the sample regarding the four domains of health-related quality of life (t<.001, d=.93), physiological (t<.001, d=.93), psychological (t<.001, d=1.43), social (t<.001, d=.38) and environmental (t<.001, d=.38) without significant interaction between gender and IGD (t<.001, F<.001).

Partners
The current sample includes a small clinically relevant group of gamers who report problematic gaming behaviors. This group experiences a significant impact on their quality of life in all areas and needs a large variety of evidence-based treatment programs.

“Do we need to know how the Internet works?” Preconceptions and attitudes of novice primary school teachers: Work in progress

Computer science education in the Czech Republic’s primary school curriculum (ISCED 1) is now undergoing a change in order to respond to the needs of the increasingly digitalized world. A newly added content includes teaching the principles of the functioning of the Internet. Little is known about how prepared novice primary school teachers are for teaching this topic and what attitudes they have towards this new educational content. Both of these are important to know for the development of courses for upskilling the teachers. Hence, the present research aims to answer the following questions: 1) What are the preconceptions about the structure and functioning of the Internet novice primary school teachers possess? 2) What attitudes towards this topic do these teachers have? Data were collected through semi-structured interviews (60 min via Zoom) with novice primary school teachers (N = 62) from across the Czech Republic. The data are analyzed using thematic and frequency analyses (software Atlas.ti). Preliminary results suggest that preconceptions of the primary school teachers about how the Internet works are very similar to previously identified children’s preconceptions. For example, they think that cookies help protect our data, satellites are an essential part of any data transmission or that the Internet data are stored in an “immaterial” place. Most of teachers’ preconceptions are scientifically incorrect. Teachers have rather negative attitudes towards teaching the topic in primary school. They mention most often that functioning of the Internet is an interesting but too difficult topic for primary school children. These results raise the question to what extent does a misunderstanding (on the side of the principles) of how the Internet works affect the teaching of Internet safety in primary school.

Examining online fitness-related and appearance-related content exposure in online purchasing of fitness products in adolescents

Background: Using diet pills is prospectively associated with the escalation of eating disorder symptoms. Regular use of muscle-building supplements is identified as a risk factor for subsequent steroid abuse in youth. There is currently limited research on whether exposure to online fitness- and appearance-related content is related to online purchasing of weight loss and muscle-building products in adolescents.

Methods: Czech adolescents (N = 1530; 50% girls) aged 13–18 participated in this study. Quota sampling was used with equal distributions for gender and age. Fitness-related health information seeking, exposure to online body-ideal content (thin-ideal for girls and muscular-ideal for boys), and internalization of beauty ideals were assessed using an online survey. Two separate two-stage hierarchical regression analyses were conducted, controlling for sociodemographic and body image-related characteristics and internet use frequency. The analyses were conducted separately for girls and boys.

Results: Regardless of gender, a higher frequency of seeking online fitness-related health information was associated with online purchasing of weight loss and muscle-building products. Elder adolescents purchased muscle-building products more frequently. Higher exposure to and internalization of muscular body ideals was a significant predictor of purchasing muscle-building products for boys. Girls with a higher BMI were more likely to purchase weight loss products.

Discussion: This is the first study to show the significant role of online fitness-related content seeking in the online purchasing of fitness-related products in adolescents. It newly revealed that exposure to and internalization of muscular-ideal content might be associated with an increased risk for purchasing muscle-building products in boys.

17:00 - 17:15 Coffee break

17:15 - 18:45 Parallel streams

Psychology of Cyberspace - Room 140
chaired by David Šmahel, Hana Macháčková

Partners
DeSHAME CROATIA AND SERBIA COMPARATIVE RESEARCH FINDINGS: HOW EXPOSED ARE HIGH SCHOOL STUDENTS TO SEXUAL CONTENT IN ONLINE COMMUNICATION

Online sexual risky behaviours include situations in which sexual material is exchanged within a virtual environment, with or without interaction with that person in the real world. Self-generated Child Sexual Abuse Material (CSAM) is a form of risky behavior on the Internet implies the production and sharing of sexually explicit content of sexualized images or videos that were created by and featuring children below the age of eighteen, and this type of communication is increasingly present among children and young people. These behaviors can easily result in sexual abuse or harassment via the Internet, regardless of the initial purpose and intent of creating and distributing such material (https://ecpat.org/luxembourg-guidelines/).

Csi.hr conducted representative research in high schools (Croatia: N= 2016, 21 high schools, 53.8% boys, Serbia: N= 2950, 40 high-schools). Aim was to explore sexually risky behaviours of children in online communication regarding sending and receiving sexual content.

Sharing of naked and half-naked photos with other people without their permission is often experienced by 2.8 children in Croatia and 3.8 children in Serbia, while occasionally 2.8% of high school students experience this in Croatia and 2.6 % in Serbia. In Croatia 5.7% and in Serbia 6.6% answered that someone used their photos of sexual content for threaten or blackmail while in Serbia 19.2% and 21.9% from sometimes to often receives unwanted sexual content.

The presentation will also cover the sending of sexual content of themselves that children create, and the quite worrying result is that in both countries, most of the children who do this engage in such communication under the threat of blackmail or against their will.

Keywords: sexually risky online communication, self generated sexual material, high school students, deShame Croatia, deShame Serbia

EXPERIENCE AND PERCEPTION OF PROBLEMATIC GAMING AMONG ADOLESCENTS: RESULTS OF QUALITATIVE RESEARCH WITH CHILDREN AND YOUTH

Adolescents are at the highest risk for problem gaming, considering the neurological, cultural and developmental tasks that occur at this development stage. The characteristics of neurological development in adolescence means that they are more inclined to take risks, experiment and seek excitement, and their motivation is focused on peers, increasing social comparison and sensitivity to social exclusion. Precisely for these reasons, it is important to investigate this topic in the context of Croatian adolescents.

This research aims to gain insight into the experience of playing online video games, with a special focus on problematic gaming, and accordingly find out what adolescents’ recommendations are for creating a safer gaming environment. Research design is based on the qualitative research approach with adolescents (age 14-21) with experience playing online video games who will participate in semi-structured interviews. The research will use Patton’s (1990) intentional sample of maximum diversity (diversity according to gender, age and gaming experience)

This research will enable results to answer the following research questions: 1. How do transgressive behaviors manifest in online video games? 2. How do adolescents perceive transgressive behaviors in online video games?

The research will be conducted in accordance with the Code of Ethics for research with children, and the approval of the Ethics Committee of the Faculty of Law, University of Zagreb was obtained for its implementation.

The participation of adolescents is extremely important in order to gain firsthand insight and draw attention to some of the possible risks of playing online video games.

The Importance of Psychosocial Factors to Adolescents’ Neutral and Problematic Photo Self-disclosure on Instagram

Photo self-disclosure is becoming one of the main activities among adolescents on social networking sites (SNS). However, it’s still unclear how photo disclosure is related to important psychosocial factors on Instagram, which is a popular SNS among adolescents. Thus, this study aims to find out how psychosocial factors are related to adolescents’ neutral and problematic photo self-disclosure. To reach this aim, the quantitative study was organized (N=427; Mage=14.57; SMage=1.39; 57.2% female). Adolescents had to fill in the hard copies of questionnaires, assessing their neutral and problematic photo disclosure on SNS and psychosocial factors (e.g., narcissism, parental mediation). The results of regression analysis show that girls and those adolescents who are older, more narcissistic, and experiencing more

Partners
active parental mediation are more likely to engage in neutral photo self-disclosure ($F = 10.95$, $p < .05$); older adolescents and those who are more narcissistic, and spend more time on SNS are more likely to engage in problematic photo self-disclosure ($F = 6.54$, $p < .05$). Thus, we may state while creating or implementing prevention or intervention programs on adolescents’ photo disclosure on SNS it is important to pay attention on different psychosocial factors depending on a type of disclosure.

19:15 Conference dinner (restaurant Lucullus Brno, Hotel International, Husova 16, Brno, Entry from Veselá Street)