Programme - List of abstracts

Saturday, November 30th, Faculty of Law, Veveri 70, Brno

9:30 - 11:00 Parallel streams

Law: Intellectual Property On-Line (Licensing) - Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Pedro Dias Venâncio

Smart Contracts and Free Use of Copyright Works

The enthusiastic preachers of the Blockchain have proclaimed among the miraculous deeds of this blessed technology the possibility of entering into "smart contracts", self-executing, and thus immune to non-compliance.

Blockchain "is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data" (Wikipedia).

For those who advocate its use, these characteristics make it the ideal technology for the development of so-called smart contracts.

"A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. (...) Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both." (Wikipedia)

Some authors have been advocating these smart contracts as a more effective alternative to technological measures of copyright protection. The technology would allow to bind users and holders copyrights on digital works, with electronic contracts that limit the use of the protected works to the agreed terms.

What I propose to discuss in my presentation is the extent to which these smart contracts are not limited (or in violation) of mandatory statutory rules that grant users / consumers of cultural works certain free and inalienable rights of use.

Christina Kirichenko

Codes in the Clouds: New and Old Approaches to Open Source Software Licensing

The proposed talk is about OSS licensing regimes circulating in the clouds: conventional OSS licenses, the AGPL and source-available licenses (SALs). I will focus on legal risks and issues to consider while using the OSS as SaaS.

In case of SaaS, the copy of the software is usually not transferred to the user but only made available via the computer network. Many OSS licenses tie their obligations to the distribution of the software, whereas making the software available via a network commonly does not constitute distribution. For distribution, a software copy shall generally speaking "change hands".

Thus, many businesses started using OSS in SaaS without contributing upstream. This problem resulted in licenses tailored to the new network reality, e.g. the AGPL that extends the copyleft to making the software available via cloud. However, due to the ambiguity of its copyleft provisions, many businesses have become rather comfortable with applying the AGPLed OSS while successfully circumventing copyleft obligations.

This situation has recently set off a new generation of licenses, the so called SALs. Being different from each other, all SALs have something in common: very far-reaching copyleft obligations imposed on the SaaS use. It is unclear, how SALs would take hold in the OSS world and which effect they would have on the SaaS in the end: the SALs still need to be interpreted, tried and tested.

Lucius Klobucnik

Withdrawal of online rights from collective management organisations in the EU and the US – licensing and regulatory pitfalls

Digital distribution required "innovative" response from the licensing market which lead to changed licensing practices and rise of new licensing entities. Although it had been undisputed that collective management organisations (CMOs) are mandated to license all rightholders' rights regardless of the mode of exploitation (radio, Internet etc), the advent of digital era has witnessed attempts of some rightholders to withdraw their online exploitation rights from the system of collective licensing, while keeping other rights (e. g. for offline exploitation) in the system. Consequently, licensing markets have changed fundamentally – they became more difficult to navigate for digital distribution services and the role of collective licensing has diminished.

The legality of rights' withdrawals has been seen differently by the US and EU authorities. While the US Department of Justice in its recent (2016) antitrust review of the ASCAP and BMI consent decrees advocated the "all or nothing approach", the CJEU (in the Daft Punk case) and the EU legislator (in the 2005 Recommendation and 2014 CRM Directive) favoured the withdrawal of online rights.

This paper aims to analyse the impact of online rights' withdrawals as well as their different understanding in the EU and the US on licensing market, and outline the changing relationship between licensing entities and rightholders.

Law: Privacy and Personal Data (Concepts) - Room 038

chaired by **František Kasl, Jakub Míšek**

Adrienn Lukacs

Job Applicants' Right to Data Protection with Special Regard to the Principle of Data Quality in Social Media

Facebook and other social media platforms have gained considerable importance in everyday life. Their use resulted in the unprecedented share of personal data: individuals from all over the globe share personal data in a quality and quantity never seen before. Employees and prospective employees are amongst users as well, which raises privacy and data protection questions specific to the context of employment.

Arising from the freedom of contract, the parties are free to decide with whom to conclude an employment relationship. In order to enforce this right and choose the most suitable applicant, the employer is entitled to obtain certain information about the candidates. Besides conducting job interviews and professional aptitude tests, nowadays it is a common phenomenon that employers consult the applicant's online profiles in social media as well. However, during such a social media background check the applicant's right to data protection must be respected.

The arising legal issue to be examined is that during such a background check, the principle of data quality, more precisely the principles of relevancy, necessity, accuracy and up-to-datedness – all set out in the GDPR as well – are highly questioned. The presentation will highlight the most important questions relating to the principle of data quality on social media during recruitment. The aim of the presentation is to examine the arising challenges and present the possible solutions that can be given to them.

Tamás Szádeczky, Gergely Szoke

Current challenges of confidentiality and publicity in the view of information security

The paper analyses the issues of confidentiality and publicity, arising from current information security legislation in Hungary. First of all, the information security as state task is analyzed. In Hungary, the information security controls of state and local government entities are regulated. Afterward, on the one hand, the information security as a tool for data protection regulation, state secrets and freedom of information were discussed. On the other hand, information security can be an object of the law, when the protection of security controls is required. One of the main findings of the research was that the information security controls applied at state entities are generally public data (according to freedom of information regulation). Thus it might not stay confidential. We formed proposals to solve this issue.

Erich Schweighofer, Felix Schmautzer

Consent Management and other Legal Aspects regarding „Interactive Radio"

In contrast to a linear broadcast, interactive radio aims to enhance user experience by personalisation of the service and to optimize interaction with listeners. The main objectives are the following:

• Enable the listeners to interact with radio stations in a personalized way through their preferred (social) channel and remain connected;

• Optimise tools and platforms for the radio editorial team to give them a better overview of interaction in order to engage more and better with their audience;

• Build innovative services and platforms to enable automation of user interaction;

To achieve these, a radio station inadvertently processes personal data. The authors argue, that the informed consent of the data subject should be the main legal ground of processing (though there might be other applicable legal grounds). Therefore, a dynamic consent management system has been implemented, enabling the user to control the level of personalisation, the amount of processed data and the purposes for which these can be used. This contribution should provide an overview on the legal aspects and the Privacy-by-Design approach taken within the Horinzon2020 project MARCONI for Interactive Radio Stations.

Jan Tomisek

Cookies and online tracking: future of regulation

Tracking of internet users and use of the acquired data for advertising purposes is a source of significant privacy concerns. Yet the advertising technology industry (AdTech) remains highly opaque to the internet users whose privacy is in question. This submission will tackle the issue of privacy protection with regard to online tracking through cookies and similar technologies and possible future approaches to its regulation.

The current applicable legal framework represented by the GDPR and the ePrivacy directive relies heavily on user consent. However, the requirement for collection of consent remains mostly ignored in majority of online interactions and the relevant authorities are only starting to push toward its enforcement and the AdTech industry is starting to work on consent mechanisms. This is despite the fact that relevant legal rules (or rules similar in principle) are in place for many years.

However, the fact that the consent requirement is currently not enforced may actually be beneficial, because user consent seems to be highly ineffective as a measure to protect users' privacy while it significantly burdens all online interactions.

The submission will further analyze the problems of current consent-based approach and will elaborate on other possible means of achieving privacy protection with regard to online tracking, including changes in liability towards users, requirements on increased transparency of AdTech industry and protective roles of browsers.

Cristina Ponte, Susana Batista

Coping with problematic online situations: the role of the family 'climate' on children' strategies

Regarding family mediation, the new EU Kids Online framework extends the attention from parents to siblings and other relatives (Livingstone, Mascheroni and Staksrud, 2015). The most recent survey (2017-2019) includes specific questions on the family 'climat' (Clark, Kehily, 2003) and its communicative practices. These practices can also be found in the questions on 'enabling mediation' (Livingstone et al., 2017), mediation from the child and in other new questions, such as sharenting.

Research has shown that the level of communicative proximity, trust and reciprocity existing between parent and child is a key component of the parent-child dyad that shape media experiences such as internet practices in families (Fujioka and Austin, 2002; Paus-Hasebrink et al., 2013). Results of a cluster analysis regarding parents' and children's answers identified 'the confident, caring and communicative' family as the most frequent type of parent-child relationship among European families (Paus-Hasebrink et al, 2013). This 'triple C' family was characterized by high levels of active mediation, proximity indicators mostly above the average and children most likely to report harmful experiences. This was the leading family type in Portugal.

Eight years after the previous data collection, and after characterizing the 'family climate' reported by Portuguese children (N=1861), this paper aims to explore its relationship with children's coping with problematic situations. We start by characterizing children who reported having had a bothering situation during the last year (22%, i.e., 342 children) at three levels: 1) their distribution by age, gender, SES; 2) their (re)actions regarding bothering situations; and 3) their family environments regarding communicative proximity, trust and reciprocity.

""Drawn on these backgrounds, our research questions are:

- How do the family communicative practices influence ways of coping with bothering situations? Is there a relation between the levels of communication within the family and social coping (e.g, talk to their parents and siblings; do not talk with anyone)? To what extend are proactive or fatalistic answers related to the communicative family environment?

- Does the family communicative environment add something to the explanation on differences in coping strategies, beyond the already identified differences on coping by age, gender and SES?

Relying on previous studies cited above to identify, the paper considers multiple variables, types of coping strategies and family communicative environment and explores their interrelation.""

Daniela Šincek, Ivana Duvnjak, Marija Milić

Contribution of Sexting Motivation to Explanation of Variance of Sexting

Bianchi, Morelli, Baiocco, & Chirumbolo (2016) propose triple motivation for sexting sexual purpose, body image reinforcement, and instrumental/aggravated reasons. All of them contribute to the explanation of variance of sending sexts, and only instrumental reasons contribute to an explanation of variances of posting sexts and unpermitted sharing. Aim of our study was to explore the contribution of these motivations to sexting and unpermitted sharing in young adults. Data were gathered online from 523 participants (239 (45.7%) males) who fulfilled Socio-demographic, Sexting and Sexting motivation questionnaires. Sexting Motivation questionnaire factors' structure was similar to one found in Bianchi et al. 2016. Hierarchical regressions with following set of predictors: age and gender in the first step, being single/in a relationship in the second step, and motivations for sexting in the third step were conducted for textual sexting, visual sexting and unpermitted sharing of other's sexts. Predictors of textual (38.3% of variance explained) and visual sexting (33.8% of variance explained) were being single/in a relationship (those in a relationships send more sexts), and sexual purpose (those motivated more by sexual purpose, sext more). Predictors of unpermitted sharing were being single/in a relationship (singles shared more), and more pronounced instrumental/aggravated reasons. In this model, only 6% of the variance was explained.

Adrian Abendroth, Hanna Krasnova, Daniel B. le Roux, Doug A. Parry, Jana Gundlach

Technology Use Addiction: Scales, Dimensions, Validity?

In response to concerns about the possibility of technology use addiction, researchers have developed a variety of self-report scales to assess behavioural addictions relating to use of the Internet, smartphones, videogames, or social networking sites. Despite the growth in research attention, or perhaps as a result, conceptions of such addictions are disputed, diverse, and lacking a core set of dimensions. To address this problem, building on a conceptual framework using prominent models of behavioural addiction and the dimensions of addiction described in the DSM-V, we conducted a structured analysis of 50 self-report scales (including 971 individual items) used to assess technology use addictions. From this analysis we found that, while there exists some degree of conformance to established addiction dimensions, there is substantial diversity in the scales. Two dimensions, compulsive use and negative outcomes, were found to account for over 50% of all items considered. The assessment of cognitive absorption was identified as a novel dimension potentially important for technology use addiction. Three questions extend from the study. First, given current debates about technology addiction, what distinguishes behavioural from substance addiction and, which dimensions are needed for its assessment? Third, given the study findings, how valid are the scales assessed as indications of technology use addiction?

Armin Klaps, Jan Aden, Anastasya Bunina, Carolin Griehsler, Zuzana Kovacovsky,

Recreational gaming on the rise: Exploring gender differences in recreational and problematic forms of gaming

Although earlier studies showed that only a very limited number of gamers fulfill the clinical criteria for gaming disorder or other forms of Internet dependency with gaming genres playing a relevant

Reinhard Ohnutek, Birgit Ursula Stetina

role (eg Stetina et al. 2011) the role of gender as relevant factor has not been discussed sufficiently. Therefore, objectives of the presented study were to evaluate a gender balanced sample according to their gaming routine and clinical aspects.

Using several (clinical) scales such as IGD-20 (eg Pontes et al. 2014), SIAS (Matttick & Clarke, 1989) and SPIN (Connor et al., 2000) 147 gamers were surveyed (female:n=66, male:n=81) in a cross-sectional design with an online questionnaire.

In addition to the fact that the sample includes no dependent gamer (cut-off 71) the results show a significant difference between males and females with female gamers (M=33.33,SD=11.28) showing significantly less symptoms (T(145)=-2.561,p=.011) than men (M=38.06,SD=11.01); both groups showing no clinically relevant signs of Internet Gaming Disorder. No gender differences were found in the sum scores of the instruments measuring social anxiety (SIAS:(T(145)=-0.39,p=.694, SPIN:(T(145)=1.18,p=.239).

Once more, data shows that pathologizing is not the answer. However, several factors need more studies, such as the role of gender, and potentially gender-stereotypes, as it was found for gaming motivation, to help identifying risk factors for problematic gaming.

Internet and Society - Room 148

chaired by **Kristian Daneback, Jakub Macek**

Thomas Roessing

The public eye in online communication

The public eye is a metaphor for the social psychological concept of public. This public is a force of social control. The fear to appear negatively in front of the public eye drives processes of public opinion. One of those processes is the spiral of silence: People who fear that their opinion is unpopular fall silent, i.e. they refrain from telling or showing their opinion in public. That makes the opposite camp appear stronger and eventually dominate the public sphere.

The traditional public eye requires proximity, personal contact. Publicly displayed opinions must be heard or seen in order to be judged. However, there is evidence that fear of social isolation is effective in online environments.

The online public eye revives an old question of public opinion research: Is social control effective without face-to-face confrontations with members of the public?

This question became known as the voting booth problem in the early stages of public opinion research: How can public opinion influence votes, given that there is no public present in the voting booth. E. Noelle-Neumann shrugged the critique off by postulating an awareness of the public eye that is effective even in the most private situations.

This paper discusses how the public eye operates in online environments and if results from online research can help to solve the voting booth problem. Online firestorms and opinion formation in Wikipedia serve as examples for public opinion online.

Christine W. Trueltzsch-Wijnen

SES as moderating factor for digital literacy?

In empirical studies evidence is found that young people from milieus with a higher SES appear to be more critical and more self-determined in their approach to media, and often have a more varied media repertoire, than peers who come from lower SES milieus (e.g. Paus-Hasebink et al. 2019; Shala & Grajcevci 2018; Urbančíková et al. 2017; Sowka et al. 2015; Livingstone et al. 2011). Also with regards to adults SES turns out as a clear barrier especially to the access but also to the understanding and creation dimensions of media and digital literacy (Livingstone et al. 2005).

In this presentation we question the reasons for the observed differences by drawing on Bourdieu's (1979) habitus theory and Habermas's (1995a; b) concept of communicative competence. Our focus is on the question if and how observed differences in media performance are connected to the habitus of an individual. We refer to an own empirical study on young people's internet performance in order to illustrate how differences in dealing with media are related to social backgrounds and in how far they relate to differences in media and digital literacy (or not). The aim is to find hints for how young people stemming from lower SES backgrounds can be supported in gaining digital and media literacy in a way that better suits their daily routines and practical sense (cf. Bourdieu) or subjective meaning (cf. Husserl or Schütz & Luckmann) of using media.

Sascha Trueltzsch-Wijnen, Christine W. Trueltzsch-Wijnen

Mobile App Repertoires of Young People and Emerging Adults

'Using a smartphone' is insufficient to describe the media use taking place via this device because it offers various possibilities. Classification is also difficult on the level of content as it is made available via different platforms or media. Various approaches have been developed in media and communication studies since the mid-2000s, seeking to analyse the media habits of individuals from a holistic perspective. One of these is the media repertoire approach on which we draw in our study because it offers connecting points for a theoretical exploration of the social and individual contexts of media activity. It is assumed that people, when constructing their specific media repertoire, take their bearings from principles which apply to all media (e.g. usefulness, involvement, ritualized media use, expansion of cultural capital, legitimate media use etc.), and which make it easier for them to choose specific media.

In our study we explore the mobile app repertoires of young people and emerging adults in Austria and Switzerland (age: 12 to 25 years) by a mixed methods design (1. explorative interviews, 2. quantitative survey). At the time of the conference we will be able to present the results of the explorative interviews and give a first insights into the mobile app repertoires of this age group. We will discuss this with regards to our theoretical assumptions and with respect to the construction of the questionnaire for the quantitative survey."

Rossana Cruz

The child within social media - a parent trap?

The child's presence in social media raises numerous issues related to the exercise and content of parental responsibilities. Those issues have not always been given due attention in the legal field.

It is undeniable that the child's experience today is guided by challenges with different outlines from those that existed in the past. First of all, a whole world is just a click away on a computer, tablet or smartphone. In consequence, the child's security (and 'cyber-protection') begins - in an increasingly evident way - within his or her own room. But if the virtual world (such as the real one) presents dangers, many of these are triggered by the children themselves and / or their parents when they share certain contents in social media. In that scenario, we have to wonder and question: should parents monitor and veto the content of their children's social media shares? And when both parents have a different opinion about the harmlessness or harmfulness of a shared image? And what to say when such disclosure is provided by the parents themselves? Do parents have a right to the act within their child's fundamental rights by exposing them?

Gradually the jurisprudence begins to be confronted with these arising issues and that is why it is pressing to contribute to the discussion in the parents' responsibilities perspective.

Law: Cybercrime, Digital Evidence - Room 208

chaired by **Aleš Završnik, Václav Stupka**

László Dornfeld

Current issues of combatting online child pornography in the European Union

The digital revolution and the spread of ICTs and Internet have caused many changes in everyday life and society. One of those changes was the emergence of a new global threat, cybercrime that encompasses many new and old crimes alike. One of those is online child pornography, which is a very serious offense and targets one of the most vulnerable groups of society.

In time, many theoretical and practical issues emerged regarding this phenomenon. Firstly, even the definition of the term is unclear and differs from country to country. Then, there is virtual child pornography, which depicts not real persons in sexual acts, and is therefore not banned in several legal systems. There is also the problem of self-generated content of underage persons. This means that on the national level and in international instruments, there are several serious differences in persecution.

Among the problems, we can also find many practical ones, like conflicting jurisdictions, encryption, the vulnerability of digital evidence and the lack of efficient legal means of criminal cooperation.

In my lecture, I will present these problems and then the relevant answers given to it on a European and national level.

Felix Emeakpore Eboibi, Muktar Bello

The Economic and Financial Crimes Commission and the Effectiveness of Implementation of Digital Forensics Investigation in the Fight against Cybercrime in Nigeria

Prior to and after the enactment of the Nigerian Cybercrimes Act 2015, the Nigerian Economic and Financial Crimes Commission (EFCC) have been saddled with the responsibility of investigation and prosecution of perpetrators of cybercrimes. The efficiency and the ability of the EFCC in the fight against cybercrimes have been questioned considering the ever increasing and rampant nature of the crime from the Nigerian perspective. The Federal Bureau of Investigation (FBI) yearly published reports (Internet Crime Report) between 2002 and 2017 have consistently placed Nigeria amongst top countries with the greatest impact of cybercrime globally. This paper consequently, highlights the recent development in the role of the EFCC towards the fight against cybercrime and how the deployment of digital forensics investigation have enhanced Nigeria's successes in the curtailment of cybercrime, a fact that is unavailable in the literature. In justification, it shall examine the measures that have been put in place; the increasing total number of cybercrime investigations and convictions of cybercriminals recorded thus far since the implementation of digital forensics. Invariably, this paper would serve as a gap filling in the literature on how the EFCC have risen to the challenge on the fight against cybercrime.

Pedro Miguel Freitas

European Production and Preservation Orders for electronic evidence in criminal matters: impact on Portuguese law

The proposal for the European Production and Preservation Orders for electronic evidence in criminal matters constitutes a step forward towards an effective European criminal law, which is critical in a Europe Union that has no borders and faces common challenges and threats. One of those threats, terrorism, has been one of the leading factors in the appearance of European legal instruments in criminal matters, namely these that are the focus of our paper. Terrorism, as well as other criminal acts, has more than ever taken advantage of all that technology, and especially Internet, has to offer. Real-time communication, anonymization, omnipresence and low cost are some of the key features of technology that can enable the planning and execution of terrorist acts. In face of this, the task of law enforcement agencies has become increasingly difficult. That is reason why instruments such as the European Production and Preservation Orders for electronic evidence in criminal matters are important. In this paper, we will analyze their strengths and weaknesses and evaluate its impact on the Portuguese national law.

Marek Swierczynski, Remigijus Jokubauskas

New Council of Europe Guidelines on electronic evidence in civil and administrative law

On 30 January 2019 the Council of Europe adopted guidelines on electronic evidence in civil and administrative law (hereinafter "the Guidelines"). The authors will explain why its creation is important for the proper administration of justice and how it addresses and reflects technological

developments, new business models and evolving case-law. Several conclusions have been identified regarding how use of the Guidelines will address current practical problems for courts and attorneys while maintaining full compliance with important principles like the right to a fair trial, protection of private life and national laws of the member states. Both authors took active part in the preparatory works and believe it is in the interest of justice that these guidelines are publicly available in the member states and widely disseminated among professionals dealing with electronic evidence.

The Guidelines aim to ensure that specific challenges related to electronic evidence are addressed, such as probative value of metadata, ease of manipulation, distortion and erasure of the electronic evidence, involvement of a third party, such as cloud or trusted services providers in the collection and seizure of electronic evidence.

New trends in combining high security and user experience of mobile applications - Room 211

Workshop

Agáta Kružíková, Petr Doležal, Lenka Knapová

In-Depth User Evaluation of mBanking Authentication Application

Current and novel methods of authentication (hardware tokens, NFC payment card, card-reader, fingerprint and PIN code) were evaluated in the context of mobile banking through an in-depth qualitative user study with multiple rounds. This part of the workshop will introduce the results, especially with respect to the perception of the NFC payment card. We will also describe the iterative process of the conducted user study with regards to changes in test scenarios and applications between rounds based on participants' comments.

Highlights: You will learn the detailed users' accounts of perceived pros and cons of using NFC and payment card for authentication that can be used for designing the most efficient and effective processes and interfaces.

Lenka Knapová, Lenka Dědková, Agáta Kružíková, David Šmahel

NFC Token vs. Card-Reader: A Large-Scale Study of Preferences in Smartphone Authentication

This part will present a large-scale study of authentication methods on smartphones with 500 users (250 of which are 55+ years old). Each person went through two real-life scenarios of activating a digital identity application and paying an invoice in a mobile banking application using various methods. Results on the preference for specific authentication methods (NFC token, card-reader, fingerprint and PIN code) as well as perceptions of their security and usability will be presented. Implications for both researchers and companies, including but not limited to banking institutions, will be discussed.

Highlights: You will learn which authentication method is preferred by different users, which can serve as a starting point for deciding which method should be offered to specific customer segments.

Anežka Pejlová

Visual hash - secure user-friendly transaction authorization

System architects usually need to choose between security and user-friendliness and it is very difficult to find a desirable balance. Often if you want to harden security, you have to lower user experience and vice versa. In this part of the workshop, we'd like to introduce you a visual hash - a new way of transaction authorization which connects the world of security and user-friendliness and emphasizes both of them. The use of visual hash in transaction authorization makes this process faster and significantly easier for the end-user. The technical level of security stays untouched, in fact, the higher rate of attractiveness for the user consequently increases security as well.

Highlights: You will learn the cornerstones of visual hash principle and see how it actually works in live demo presentation.

Law: Government 2.0, eJustice, ODR - Room 214

chaired by **Ludwig Gramlich, Pavel Loutocký**

Maria Dymitruk

Models of AI application in judicial proceedings

There are some serious imperfections of contemporary AI models (such as, but not limited to, the lack of explainability). So, in order to consider the use of AI in legal decision-making, we must come up with a legal framework that takes into account the human being in this process. These frames must ensure that this person does not simply confirm the decision generated by the AI system, because in that case human participation would be fictitious. The point is that we just cannot wait until the AI legal systems will be perfect (fully interpretable, traceable, accountable) because it may not happen soon, but we have to think these issues through right now (in order to enable responsible use of existing AI methods in current justice systems). Taking above into account, I distinguished three models of AI application in judicial proceedings (as described in the abstract: full automated procedure and two types of semi-automated procedure). In semi-automated procedures AI serves as the supporting tool for human judges. The AI-generated support can be based both on suggestions or confrontations. In the first case, the system would provide a judge with a final proposal of the decision or decide on the main factors determining the final decision the judge should make. The system could make only one suggestion (this model is connected with the risk of "rubber-stamping" of the automatically generated advice) or more than one suggestion (this model does not fully remove the risk of approving one of the automatically generated suggestions without proper consideration, but it can partially reduce this threat). In the third model (semi-automated procedure based on confrontation) AI is used not as a decision aid, but as an "adversary". In that

scenario, the machine "attacks"/"critiques" human arguments. In this model there is no risk of rubber-stamping, actually, there is a great chance of enhancing the quality of a decision. But on the other hand, this model would rather slow down the decision-making process instead of speeding it. So, it is very interesting option but could be little impractical (or even unrealistic), but still worth consideration. A clear drawback is that this model does not correspond with the most pressing need in judiciary: the need of efficiency. But what is also interesting, this model eliminates the risk that human intervention in the automatic process will worsen the quality of decision (rather than improve it). This model actually reverses the whole process. Normally, a human tampers with the algorithmic decision-making process, and here it is opposite: the system tampers with the human decision-making process.

Federica Casarosa

The role of courts in shaping social media regulation - The case of Italy

Although not usually understood as part of the regulatory process, courts both at the European and the national level play an influential role in shaping the law affecting the media in the converged environment and its implementation through statutory interpretation. As regards social media in particular, resort to courts by individuals and corporations which claim that respect for their rights has been violated through social media activity has progressively become more pronounced. In interpreting and applying existing laws, national and European courts have engaged in a balancing exercise to reconcile distinct fundamental rights that are seemingly at odds in the digital setting.

The paper will examine the jurisprudence of Italian national courts on social media and convergence in the and investigate the contribution to the development of legal standards that strike an appropriate balance between distinct fundamental rights that are at play in the field. The main questions addressed will be the following:

- Are courts confronted with social media cases?

- What types of cases are brought before domestic courts?

- What regulatory approaches are emerging from this judicature?

- How do national courts balance competing fundamental rights and interests with respect to social media and what is the influence of the jurisprudence of the ECtHR and of the CJEU on national case law?

11:00 - 11:15 Coffee break

11:15 - 12:45 Parallel streams

Law: Intellectual Property On-Line (AI) - Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Jan Zibner

Resystematization of copyright in the age of AI

Within the scope of the author's research "Artificial Intelligence as a Technological Challenge to Copyright" and based on the previous (i) exploratory meta-analysis of an AI and copyright as well as the (ii) descriptive study of status quo, the research is now continuously focused on the resystematization of copyright for the creations of an AI. Author is analyzing the options of how to adapt the current copyright law system of the Czech Republic (while reflecting the EU and necessary international aspects of the copyright) for it to be suitable and flexible enough for the works created with the help or by an AI, while not discriminating the value of traditional works regime. The AI is here understood (based on the previous research) as a quasi-equitable entity able of the creative choices, which is nowadays a valuable part of the creative process and often presented as the "pillar of the modern art". After the assessment of such resystematization, the author is focusing on the possible ways of resystematization of the AI's creations' legal regulation and its consequences and added value either through (i) the transformation of the conceptual features of the copyrighted works and the authorial principle of natural person, (ii) the introduction of the new category of works originating from the AI-included creative process, or (iii) introduction of an exemption from the authorial principle of natural person for such works.

Daria Matvienko

Artificial Intelligence and an Author

Nowadays the question about proper protection of artificial intelligence has a high priority. Due to high economic value and balance of society's and authors' interest generous amount of works, created by artificial intelligence, are worthwhile to be protected by copyright. The following key question is arising: can the artificial intelligence be considered as an author?

By general principle, the author is a natural person. Despite the general principle, an author conception depends on existing system of copyright doctrine in certain country. Nowadays, there are just some provisions on computer-generated works, as well as who is an author in case such works are generated. The question if the artificial intelligence could be an author is explicitly connected to the question if author's rights could belong to the artificial intelligence.

The necessity to change the author conception, conception of originality of works, created by artificial intelligence, ownership allocation possibilities, as well as attribution of author's rights to artificial intelligence are considered in this article. Entitlement the person by whom the arrangements necessary for the work creation are undertaken and, in case there is no such person, the entitlement of rights to a person, who has created the artificial intelligence, which has created the work approached in this article.

Roman Bieda

Do we need a new type of right to protect AI creations?

Artificial Intelligence (AI) has been increasingly applied for the purpose of creating music, graphics, film, computer programs – the works protected traditionally under copyright law.

In a number of cases AI creates works by way of self-perfecting algorithms and provided data, without any direct human involvement. This presentation will scrutinise a thesis that such autonomous creations are not protected by copyrights. It must be noted, however, that making such autonomous creations requires significant investments, including investments to create AI mechanisms and collecting a lot of data.

The main objective of the presentation is to demonstrate a conception of a new type of intellectual property right which will protect investment made to create a work by way of applying AI. The nature of such new right will be analysed (related right, sui generis right?), the subject of the right (the producer of AI, the user of AI?) and the characteristics of the new exclusive right.

European law and Polish law will be taken into consideration.

Law: Privacy and Personal Data (Experience) - Room 038

chaired by **František Kasl, Jakub Míšek**

Tihomir Katulić

A Year in Data Protection: Compliance and Regulatory Response in Croatia

The first year of General Data Protection Regulation application has presented interesting challenges and opportunities for data controllers and processors in Croatia and the EU, as well as national supervisory bodies. Croatian supervisory body in particular is struggling with specific circumstances partly caused by previous neglect of function and development and partly by inadequate currently applicable provisions in the national application law accompanying the General Regulation.

At the same time, an increasing body of research is following the application of the General Regulation revealing the state of compliance, the ongoing efforts and issues stemming from particularities of Croatian economy, workforce education and conditions and relative lack of specialized educational programs in data protection. The paper comments on the current practice, especially application of the Regulation and the national application law, analyzes available and research in progress into state of compliance and awareness of data controllers, processors and data subjects in private and public organisations as well as the supervisory body annual reports.

Finally, the paper outlines required legislative and organisational measures in order to expand and improve the functioning of the national supervisory body and the general state of data protection compliance in Croatia.

Krzysztof Garstka, David Erdos

The "Right to be Forgotten" Online in National Data Protection Frameworks within the G20

The concept of a "right to be forgotten" rose in prominence with the development process of the General Data Protection Regulation and the CJEU decision in Case C-131/12 Google Spain. The idea that individuals should be able to request removal of their personal data, unless there is an acceptable legal basis for the latter's processing, became the subject of broad public and academic coverage. Within this discussion, voices appeared suggesting that the "right to be forgotten" is: 1) limited to the context of online search results and search engines, and 2) a concept exclusively tied to the EU, lacking approval outside of its borders. In this paper, we want to challenge those assumptions, and show that when properly implemented, the "right to be forgotten" is a necessary component of a contemporary data protection framework. It is an element which – if enhanced with flexibility – can provide for the right balance between data subject's interests and the public's freedom of expression. In order to demonstrate the international presence of the right in question, and multiples shapes it can take, we'd like to present the findings of our "right to be forgotten"-oriented study of data protection frameworks of the G20 countries. In doing so, we hope to contribute to the building of international consensus on the matter, which – as an ongoing reference to the CJEU in Case C-507/17 Google v CNIL shows (touching on the issue of extraterritorial reach) – is certainly in demand.

Jakob Zanol, Jonas Pfister

On the "Ibiza Scandal" - Freedom of Speech, Journalism and Data Protection

On 17 May 2019 at 6 pm the German press (Spiegel and Sueddeutsche Zeitung) released video footage of then Austrian vice-chancellor Christian Strache and Club Chairman Johann Gudenus (Freedom Party Austria - FPÖ) from 2017. The videos show how the two politicians, accompanied by Gudenus' wife, meet an alleged niece of a Russian oligarch and her companion in a rented finca on Ibiza. A six-minute excerpt of the seven-hour video was published. In the video, those present talk about potentially corrupt actions, the alleged covert takeover of the biggest Austrian newspaper and the supposed circumvention of the provisions on party financing. In addition, discrediting statements are made about various other politicians. The authenticity of the material was checked several times.

The video footage led to protests outside the chancellors office, the resignation of both Strache and Gudenus and to fresh elections this year.

In the wake of this, a discussion arose if the video footage should have been released since it was obviously taken without the consent of both Strache and Gudenus. Some argued however, that the publication of the footage was a journalistic activity - providing information of public interest to the public.

This contribution will give an overview on the current EU data protection framework for journalistic activities (including investigative journalism) and will evaluate the Ibiza scandal from a data protection perspective.

Jakub Míšek

Open Data Directive and Personal Data Protection

On June 2019 the European legislator approved directive No. 2019/1024, a recast of directive No. 2003/98/EC, on the re-use of public sector information (so-called "PSI Directive"), which will come into force in 2021. The new directive holds a popular name "on open data and the re-use of public sector information" (so-called "Open Data Directive"). One of the traditional areas of conflict surrounding PSI and Open Data is the protection of personal data. This contribution aims to compare, how is this conflict present and solved in the current PSI Directive and the new Open Data Directive. In the first part, the article briefly presents the new Open Data Directive and accents the most important novelties, which it brought. In the second part, the contribution generally focuses on the conflict of PSI (Open Data) in light of the current PSI Directive and personal data protection. In the third part, the contribution presents, how Open Data Directive approaches personal data, and what can be expected from the new legal situation.

Psychology of Cyberspace - Room 133

chaired by **David Šmahel, Hana Macháčková**

Alexander Peter Schouten, Loes Janssen, Emmelyn Croes

Influencer Advertising on Instagram: Product-Endorser Fit and Number of Followers Affect Influencer and Product Evaluations via Credibility and Identification

Companies are increasingly using social influencers to promote their products on Instagram. The goal of this study was to investigate the extent to which influencer popularity and product-influencer fit affect how people like and are persuaded by the influencer. Furthermore, we examine credibility and identification as possible underlying processes in the relation between product-influencer fit, influencer popularity, and product and endorser evaluations. We tested our hypotheses in an experiment among Instagram users (N=435), using a 2 (product-influencer fit: good fit vs. poor fit) x 2 (number of followers: moderate vs. high) between-subjects design. Participants were presented with a mock-up Instagram page of a fitness influencer, with either 5037 or 537k followers, promoting either a protein shake (good fit) or ice cream (poor fit). Analyses showed that influencers were liked more when they endorsed a fitting product, mediated by trust, identification, and similarity perceptions, but only when the influencer had a high number of followers. People indicated to be more likely to buy the product when there was good as compared to poor fit, mediated by trust, expertise, and identification, but again only for influencers with a high number of followers. Our findings show that product-endorser fit and popularity are also important factors for influencer success. Moreover, traditional processes such as parasocial interaction and credibility seem to explain these effects.

Ugnė Paluckaitė, Kristina Žardeckaitė-Matulaitienė

Adolescents' intention and willingness to engage in risky photo disclosure on social networking sites: testing the Prototype Willingness Model

Researchers state that around 80-90% of adolescents share photos on social networking sites (SNS), which may have positive and negative consequences on adolescents' health. However, it is still unclear why adolescents engage in such kind of behaviour. Thus, the aim of this study is to find out if Prototype Willingness Model (PWM) can explain adolescents' risky photo disclosure on SNS. To reach this aim, the qualitative study using random sampling was organized (N=444; Mage=14.65; 56.9% female). Students were asked to fill in the hard copies of questionnaires, assessing the factors of reasoned (intention) and reactive (willingness) pathways of the PWM and risky photo disclosure on SNS. The results of the multilevel regression analysis ($F=239.19$, $p<\alpha$) showed that intention to engage in risky photo disclosure is explained by 71.8% of model's reasoned pathway factors, with the strongest predictor of past risky photo disclosure on SNS ($\beta=.71$, $p<\alpha$). The results of the hierarchical regression analysis showed that compared to reasoned pathway variables alone ($F=50.35$, $p<\alpha$; $R^2=35.3\%$), the additional reactive pathway variables ($F=35.89$, $p<\alpha$) improved adolescents willingness to engage in risky photo disclosure by 1.7%, with a strongest predictor of past risky photo disclosure on SNS ($\beta=.25$, $p<\alpha$). Thus, it is possible to state that adolescents' risky photo disclosure on SNS is better explained by the factors of reasoned pathway (intention) than the reactive pathway (willingness).

Natalia Waechter

Self-socialization in social media. Young people's challenges between individuality and collectivity

In research it has become widely accepted that online environments have to be considered relevant for young people's social and psychological development. Taking further into account the theoretical concepts of transition theory and self-socialization, this presentation discusses how young people master their transition into adolescence in particular gender-specific online environments autonomously from adult assistance. Thereby it focuses on the challenges the teenagers experience on Instagram and in online multiplayer computer games. In the research project "The Profiler", funded by the Austrian Ministry of Science, we applied an explorative, qualitative approach and sampled 36 female and male school students, aged 13 and 15, for conducting problem-centered interviews and group discussions. The results describe that one of the main girl's challenges is the production of the "perfect selfie" whereas one of the main boys' challenges is to develop strategies that prevent getting insulted through hate speech. The teenagers face gender-specific challenges but share the common goal of becoming accepted in their peer context. The results support the theoretical concept of self-socialization by showing how

adolescents use social media to negotiate central aspects of their identity development (i.e. self-presentation and peer belonging) in their transition into adolescence.

Internet and Society - Room 148

chaired by **Kristian Daneback, Jakub Macek**

Tomáš Karger

The economy of platforms: property and market boundaries in the age of sharing

This contribution aims to reconceptualize the variability found in sharing economy, user generated content and online media distribution as being part of a single underlying phenomenon, the platform economy. Drawing upon findings about free and open source software (FOSS) communities as one of the key influences on the internet culture and adopting the perspective of Viviana Zelizer, the co-existence of informal personal relationships and formalized market exchange is examined as a connection between circuits utilizing different media of exchange. Although originally community driven and informally governed, platforms are today designed to accumulate social capital, regulate social interaction and translate it into monetizable services. Ownership is exercised not on the level of circulating content, but on the level of control over platforms (and the social capital accumulated). In this way, platforms represent the dominant organizational principle of the new economy.

Magda Petrjanosova, Romana Medvedova

New media use in Slovak youth

In our research project we look into the question whether new media are really lowering the trashhold for civic participation. However, using them assumes not only willingness but also access to information and communication technologies (ICT), and a certain level of skills. In Slovakia, the digital divide still exists and one of the most endangered groups is youth from socially excluded and poor communities, most often from the Roma minority. Therefore, in this paper we focus on ethnic majority youth and disadvantaged ethnic minority youth.

In a pilot probe we used focus groups (N=16, age 14-16) and semi-structured individual interviews (N=8, age 20-25) with young Roma from excluded communities, and focus groups (N=27, age 14-17) with ethnic majority youth in order to compare their experience. We analysed the transcripts using thematic analysis focusing on opportunities, forms and motivations for new media use in general and for civic participation (online and offline) specifically.

Compared to the ethnic majority youth, the young Roma have very limited access to internet and ICT in general, they use new media rather passively and just for fun. They have mostly no experience, no skills and no model needed for a more active use.

Law: Cybercrime, Digital Evidence - Room 208

chaired by **Aleš Završnik, Václav Stupka**

Kitti Mezei

The criminal use of cryptocurrencies: legal challenges and considerations

The legal status of cryptocurrencies is a gray area in most legal systems. Although criminals increasingly abuse cryptocurrencies to fund criminal activities. The presentation analyses solely the criminal use of cryptocurrencies and related legal questions. For example money launderers have evolved to use cryptocurrencies in their operations, therefore legislative changes at EU level, or the uniform application of existing anti-money laundering regulations have been required. In a trend mirroring attacks on banks and their customers, cryptocurrency users and exchangers have become victims of cybercrimes themselves. Conventional crimes may be committed via cryptocurrencies such as fraud and extortion. Darknet criminal markets use cryptocurrencies as payment instruments since they offer better anonimity and some of them greater privacy. They are less treacable and their decentralised system challenges the legislators of substantive criminal law, procedure (e.g. seizure related questions) and law enforcement as well as.

Judyta Kasperkiewicz

Cyberfraud on the cryptocurrency market - falls of crypto-currency exchanges from the legal perspective

A cryptocurrency market is a place where it is relatively easy to conduct criminal activity. Since the mechanism of functioning of cryptocurrencies is not entirely dependent on objective factors, so it is susceptible to speculations and high risk of losses.

In cases of cryptocurrency exchanges, fraud is most often committed, and in some cases, the form of a Ponzi scheme may occur. It is a reason why it is important to explain:

- How do cyber criminals conduct business in the criminal cryptocurrency market?

- When can a person suspect that the Initial Coin Offering may be an initiative to create a financial pyramid?

Apart from the above, the following legal questions arise:

1) How to regulate the cryptocurrency market? Which legal solutions are the most effective in the world?

2) How to deal with the cross-border problem regarding this type of cybercrimes?

The best illustration of the aforementioned problem is the example of the Polish BitMarket.pl cryptocurrency exchange, which fell on July 8th, 2019.

It seems that the problem of frauds on the cryptocurrency market is nowadays a crucial issue which attracts potential criminals on one hand but also deters other investors. Therefore, concerning the development of this market, it is worth raising the issue and dispelling existing questions and doubts of the legal nature.

Cyriacus Chimaogwu Orlu, Felix Eboibi

The gloomy prognosis of institutionalization of plea bargain in cybercrime prosecution

The enactment of the Nigerian Cybercrimes Act 2015 was thought to be the missing link in the eradication of cybercrime in Nigeria considering Nigeria's popularity in the perpetration of cybercrime globally. Recently, the quest by cybercrime prosecutors to enforce the Nigerian cybercrime legal framework to curb the menace of cybercrime has resulted to the use of plea bargaining in most cybercrime matters before the Nigerian courts. This has great impact on cybercrime defendants. One of the greatest anomalies is the consistent employment of hard bargaining tactics by cybercrime prosecutors relating but not limited to take-it-or-leave-it offers, threats to seek convictions at all cost, exploding offers etc. The institutionalization of these tactics can arguably create a forced and tensed environment for an otherwise innocent defendant to plead guilty and failure to litigate matters. Most importantly, it can result to defendants engaging in bad agreements in order to avoid proposed bogus sentences after trial. This paper argues from a comparative perspective that the Nigerian courts should curtail the institutionalization of the tactics of prosecutorial hard bargaining in course of plea bargain arrangements to enhance the protection of defendants' constitutional right to counsel and a better plea bargaining process. Otherwise, defendants would continue to be denied the right to counsel representation and effectual assistance of counsel in plea bargaining process.

István Ambrus

Artificial Intelligence and Criminal Liability

The traditional flow-sheet for criminal responsibility presupposes that a natural person commits a human action or omission and that the court declares the personal liability of the human perpetrator and applied criminal sanctions.

It looks weird in continental legal systems to put the question whether the artificial intelligence itself shall be a subject of criminal responsibility. Apparently, within nowadays' criminal law there is only negative answer for that question, since the criminal responsibility is underpinned by human actions and personal culpability. Therefore we need to pose the question who to be blamed for those possible damages. One of the possible solutions for the problems of criminal liability, the concept of „man behind the machine". Although it would be quite hard to implement this construction for criminal responsibility into the German-rooted continental criminal law systems: certain concerns of causality and those concepts of wilfulness, recklessness and negligence would be remarkably hard to prove.

The prospective changes in the consideration of criminal responsibility in terms of the artificial intelligence reveal the so-called corporate liability. A prospective private-law-like strict liability may reveal as a form of criminal responsibility, whereto no wilfulness or recklessness is needed to be proven but only the fact, who was the actual owner or licensed holder of the artificial intelligence driven device itself.

Democracy meets Digitization - Elections and Participation in the Digital Age - Room 211

Workshop

Christine Leitner

Empowerment of European Mobile Youth (EMY) – Two case studies from Austria and Estonia

EMY (www.europeanmobileyouth.eu) is a two-year project co-funded by the European Commission. It is based on case studies in two EU member states, Austria and Estonia. Austria has been the first EU member state to grant its citizens the right to vote in all elections (including EU elections) at the age of 16; Estonia is a pioneer in promoting the use of online voting ('e voting').

EMY is about bringing EU citizenship to life, in particular for young voters. EU citizenship is much more than a fictional concept or an imprint on a passport. It is a fundamental right of every citizen of an EU member state. There is a sense that mobile EU citizens, as a group, have been widely neglected by EU member state governments. Governments need to step up their efforts to better support mobile EU citizens. The judicious use of IT could be a key enabling factor, e.g. online registration for elections and e-voting services. More, and better information on the political discourse and candidates in all EU member states could also be delivered online.

This is where EMY comes into play:

• Young people are the most mobile group within the EU living in large numbers outside their home countries, especially for studying.

• They do not fully exercise their rights to engage in political life in their host country.

• They are - in general - least engaged in traditional political participation.

• There is a general feeling of lack of relevant information, transparency, and the feeling of 'my voice does not matter!'

EMY is looking to identify the reasons why mobile EU citizens are not exercising

g their voting rights and to find ways to encourage more active engagement and participation. Earlier studies have singled out a number of potential barriers:

• electoral systems are not fully harmonised across the EU;

• there is a lack of timely and accessible information; and

• there are technical and administrative issues that make it more difficult for this group to participate.

This session will present the first results of mapping exercises and stakeholder consultations conducted before the European Parliament elections 2019 in Austria and Estonia.

Robert Müller-Török

Current Authentication in e-Participation in Baden-Württemberg - Issues and Consequences

E-Participation is highly valued in politics in the Federal State of Baden-Württemberg, Germany. Unfortunately Authentication of the persons participating is mostly reduced to providing a valid e-mail-address. Empiric work of the author showed that no strong authentication nor identification is required. Together with other researchers he proofed that "Donald Trump" and "Olga Orlowska" were enabled to participate in participatory budgets of municipalities (including the State Capital Stuttgart), questionaires and even the official citizens participation portal of the Federal State. This would not be a major issues if the results of the "citizens' participations" were not taken for serious by both politics and media. This paper describes some prominent application where no reliable authentication takes place, analyzes the interpretation of the results by politic and media and outlines the consequences. Possible remedies are described and analyzed for feasibility. Unfortunately no commonly available and used strong authentication/identification exists in Germany, the eID of the national ID card is unfortunately used by a tiny fraction of the citizens only - and available for German nationals only.

Domenica Bagnato, Alexander Prosser

The Impact of Council of Europe Recommendation CM/Rec(2017)5 on the Viability of eVoting Protocols

In 2004, the Council of Europe introduced the first Recommendation on eVoting introducing legal, operational and technical standards. In 2017, this Recommendation was updated using the experience made with eVoting thus far. This new Recommendation introduced two main improvements,

• A requirement for strict implementation of voter secrecy that can only be realised by providing technical, and not only organisational safeguards;

• Verifiability both generally as well as individually by each voter, whereby general verifiability is required for the end result of the election, individual verifiability is only required until entry into the electronic ballot box; verifiability in both cases includes the accurate count/representation of the vote, not the mere fact that the vote was included in the result/entered the ballot box.

Both requirements – and particularly the combination of both – raised the bar for eVoting systems considerably.

On the most general level, eVoting protocols can be divided into two groups according to whether the anonymisation happens before or after the electronic ballot is entered in the electronic ballot box. This paper takes two popular protocol classes – "envelope" protocols for anonymisation after entry into the ballot box and token protocols for anonymisation before that – and analyses how far these protocols can fulfil the requirements set by Rec(2017)5. The contribution will show that the degree to which the Recommendation can be fulfilled varies considerably depending on which protocol class is used to implement a system. On the same token, the contribution also analyses how current Blockchain/distributed ledger technology may contribute to achieve the quality standards set in the Recommendation.

Law: Government 2.0, eJustice, ODR - Room 214

chaired by **Ludwig Gramlich, Pavel Loutocký**

Zbyněk Loebl

Designing Online Civil Courts

First courts are now moving processes online and using ODR processes as well as predictive analytics and artificial intelligence (AI) for the first judicial tasks. Furthermore, such e-courts and other judicial uses of technology are flourishing due to their proclivity for furthering efficiency and expanding access to remedies. Nonetheless, there is danger that the rush to digitization will ignore due process and transparency in the name of efficiency. Accordingly, my presentation will provide brief background on the growth of online courts and raise concerns for policymakers to consider for the preservation of fairness in public dispute resolution. Online courts should focus on user perspective – not efficiency (cost cutting) nor judges or lawyers, although the state, judges and lawyers are also important stakeholders. This focus on user access and user empowerment is similar to the private ODR systems which started more than 10 years ago and reflects the current desires of people regarding the online environment. My presentation will provide a high-level glimpse at how online courts for civil, commercial and administrative cases should be designed with a focus on end-users of the justice system. New online courts are radically different from our traditional courts and this will continue. From the user perspective, mobile access to justice will be pivotal along with improving fairness and transparency-- and possibly saving costs in the long run.

Seyedeh Sajedeh Salehi, Marco Giacalone

Algorithmic Dispute Resolution in Cross-border Civil Conflicts in the EU

The 2019 EU Justice Scoreboard proves that several EU Member States such as Italy and Greece have very long proceeding time needed for resolving civil disputes. Besides long-term litigation, too costly proceedings, the existing language barriers and diverse interpretations of EU applicable rules are also considered as other obstacles that hinder the efficient access to justice in cross-border civil dispute resolution. These major hurdles increase the risk of injustice for resolving transnational civil disputes at the EU level. In contending with these issues, CREA (Conflict Resolution with Equitative Algorithms) Project was established with the aim to conduct a deep solution-oriented analysis in finding suitable dispute resolution methods based on applying algorithms to solve cross-border conflicts, benefiting judges, lawyers and disputants as an assistive tool to reach an agreement for cross-border civil disputes. The purpose of this paper is to examine the connection between

application of the game-theoretical algorithms in cross-border civil dispute resolution and the rise of access to efficient justice and parties' satisfaction for achieved settlement. The results of this study will emphasize on the value of reaching an amicable agreement between disputants based on applying algorithmic dispute resolution mechanism, as an alternative to traditional litigation, that leads disputants into a more efficient and just solution prior or during the litigation.

Damian Klimas

Legal barriers of IoT development in Poland with regard to smart cities

IoT development is gaining considerable recognition in the international policies throughout the world. Speaker shall define smart city, present the overall characteristic of polish smart city ecosystem, indicate perspectives of smart city development and the scope of using IoT as part of smart cities concept. Speaker will identify the key legal and organizational barriers of IoT in Poland, with particular emphasis on smart cities from a review of existing legislation and attempts of polish Ministry of Digital Affairs to overcome said barriers. The speech will make an attempt to recognize the most important legal barrier categories to the development of smart cities in Poland, such as:

- Lack of legal provisions allowing the use of IoT / M2M devices in transportation services;

- Insufficient possibilities of creating clean transport zones in spite of the problem of air pollution in Polish cities;

- Lack of legal possibilities for road management in cities to use automatic detection systems for certain infringements regarding clean transport zones;

- Lack of legal regulations allowing the structural use of IoT systems and devices for conducting screening programs, epidemiological studies or the use of Big Data in medical activities;

- Restrictive regulation regarding location data, which may be processed based on the consent of the subscriber or end user only for the purposes necessary to provide services;

- Regulatory restrictions regarding data-mining.

Every barrier shall be presented shortly, nevertheless topped with legal basis of barrier and suggestion of improvement.

The speaker is a co-author of report about „IoT in Polish economy" written in 2019 by experts of IoT working group in Polish Ministry of Digital Affairs. The speech shall be a short summary of ongoing works in legal stream of IoT working group in Polish Ministry of Digital Affairs.

12:45 - 13:45 Lunch

13:45 - 15:15 Parallel streams

Law: Intellectual Property On-Line (Data) - Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Michaela MacDonald

Data ownership: a way forward or dead end?

Artificial intelligence and specific disciplines in this field rely heavily on the availability and use of vast amounts of data. However, the power that stems from such aggregated data cannot be left unchecked.

Top-down regulation such as the GDPR or consumer protection legislation confers specific rights on the data subjects, including the right to access, correct or erase personal data. Will this approach have a significant impact on individuals' ability to control their data or would a bottom-up approach result in actual empowerment of data subjects?

This could be achieved by recognising rights enjoyed by data subjects as akin to property rights and thus granting them ownership in them. Another option could be establishing data trusts that would impose a fiduciary duty on the trustees to exercise the rights conferred on behalf of the data subjects.

Can data give rise to property rights and is this relevant for the concept of data trusts at all?

Kamil Szpyt

Legal issues of acquiring and using non-personal data for the purposes of artificial intelligence functioning

It can be said with complete confidence that without data there would be no artificial intelligence. Entire functioning of AI is based on in. And, even though 2018, due to the entry into force of the Regulation of the GDPR, was dedicated to personal data, 2019 should be considered the year of machine generated data (non-personal data). Almost exactly one year after the Regulation of the GDPR, Regulation (EU) 2018/1807 of the European Parliament and of The Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union enters into force.

The following presentation is aimed at, among others things, presenting the meaning of the legal act for the development and functioning of artificial intelligence. It will also indicate areas which ought to be improved in the future. It will also include an attempt to find provisions of the law that constitute the basis for the protection of machine generated data (trade secrets, know-how) and the answer to the question whether in the near future there will be a need to separate a new subjective right for machine generated data.

Law: Privacy and Personal Data (AI) - Room 038

chaired by **František Kasl, Jakub Míšek**

Gabriela Bar

Ethical AI designed transparently for data protection

Machine learning (including inverse reinforcement learning) leads to the creation of artificial superintelligence (AI at the level of human or superior). It is important, however, how the machine learning data is acquired and protected. The existing model of protection of personal data is insufficient at a time when data is processed in huge data sets, using algorithms, without human intervention. Data subjects do not know how their data is used and how different types of predictive models are created. This leads to a loss of control over data and creates threats to manipulate data (and consequently manipulate the entire society). The creators of AI should therefore pay special attention to providing data subjects with the possibility of secure processing of their personal data used in machine learning, enabling people to maintain control over their identity. Risks related to AI do not rely on AI maliciousness (we should not attribute human qualities to it and fear hostile attitudes towards humanity), but on the competences of AI. Regulations such as GDPR are not enough. The basic human right - the right to privacy, will not be respected if people are unable to control what is happening with their personal data. This is why the work on the development of guidelines for a friendly and ethical AI is so important (European Comission, IEEE). We should strive to make our goals consistent with the goals of AI and that the latter are transparent for us.

Daria Onitiu

Discerning the user's 'fashion initials': how neural networks in intelligent fashion recommender systems are privacy intrusive

Data personalisation including machine learning algorithms in intelligent fashion recommender systems are intended to give the user's shopping journey an interactive and non-intrusive tone. This paper aims to investigate issues of privacy regarding the use of neural networks for image processing in intelligent fashion recommender systems, including the connection between apparel and user profiles. Neural networks for image processing in intelligent fashion recommender systems are used to extract product representations from unstructured data and to address fashion descriptors of style or fit characteristics as well as target groups. This model creates a space whereby representations of all products are assigned to the embedding layer for customer- product interactions. The ways these two embedding layers interact are not observable to the user, altering the user's conceptual sphere to express and exclude oneself from participating in the interactive shopping experience. These aspects, raising issues of information control and intimacy, underpin the main argument of this paper, arguing that the use of neural networks in intelligent fashion recommender systems inducing insights on user profiles, necessitate a closer scrutiny under the General Data Protection Regulation (GDPR) in light of the user's nuanced including contextual understanding of privacy.

Denitsa Kozhuharova

Automated decision-making in the field of integration: data protection & ethical aspects

The recent migrant wave experienced in the EU posed many challenges, and data protection is not amongst the most obvious ones. However, as both host countries and third countries' nationals accustom themselves to this new environment, the need for new, innovative and ict-enabled services to enhance the process of integration emerge. And since the General Data Protection Regulation was adopted in 2016, data protection has entered the societal focus as a primordial consideration, especially in the context of electronic service. This paper explores the data protection challenges met in the course of the IMMERSE system design under the framework of the EU-supported project MIICT. In particular, the paper examines how the principles of purpose limitation, data minimisation, data protection by design and by default are taken into account in the service. As the system is conceived to service a vulnerable target group – migrants, asylum seekers and refugees, the ethical aspects relating the personal data protection are likewise given appropriate attention. The paper concludes with specific decisions and recommendations that are to be observed not only during the development process, but also in exploitation stage.

Lucas Cardiell

Privacy the Age Artificial Intelligence and Robotics a Case Study: Social Companion Robots and the Right to Privacy

Robotic and artificial intelligence (AI) technologies are now essentials part of everyday life: from self-driving cars, personal assistants like Apple Siri or Microsoft Cortana to public and domestic robots like Pepper, vacuuming, pet, and sex companion robots. These technologies can enhance the efficiency and productivity as well as wellbeing of people, on the other hand they have rightly sparked various human rights challenges to non-discrimination, dignity, autonomy and self-determination or privacy and others.

The purpose of this research is to examine the privacy implications generated by AI-based technology: Social Companion Robots (SCRs). SCRs collect, store, process and transfer a huge amount of personal information with the advent of the Internet, issues related to information privacy have gained importance in the theoretical and legal discourse which is framed as an issue of data protection. However, this is a rather simplistic view of the relationship between privacy and new technologies, including SCRs. My account here is that this view fails to take into account the dynamic function of privacy as a broad concept. The right to privacy, as provided in various international legal documents, e.g., art. 17 of the ICCPR or art. 12 of the UDHR, requires that the conceptualization and the scope of privacy protection must extend beyond the information dimension of privacy and data protection to capture the complexity of privacy issues presented such technologies.

Psychology of Cyberspace - Room 133

chaired by **David Šmahel, Hana Macháčková**

Tena Velki, Marija Milić

Stress as trigger for risky online behavior in adolescents

Adolescents belong to the riskiest group of information communication users and stress is well-known trigger for different real-life risky behaviors, i.e. drugs, violence, etc. But the role of stress in online risky behavior is still not sufficiently studied.

The aim of study was check the mediating role of stress in associations between real-life risky behaviors, information security knowledge and life satisfaction with risky online behavior.

Participants were students (N=883, 40.5% male and 59.5% female) with average age of M=21.93 years (SD=4.29). They fill out Users' Information Security Awareness Questionnaire, Youth self-reported delinquency and risk behaviors questionnaire, Life satisfaction scale and Perceived Stress Scale.

Regression analysis had shown mediating role of stress ($F(4,799)=17.24$, $p<0.01$, $\Delta R2=0.01$). Stress had partially mediating role in in association of real-life risky behavior ($\beta1=0.089$, $p<0.02$, $\beta2=0.097$, $p<0.01$) and information security knowledge ($\beta1=0.239$, $p<0.01$, $\beta2=0.247$, $p<0.01$) with online risky behavior whereas stress strengthened these associations. For association between life satisfaction and risky online behavior stress had full mediating role ($\beta1=-0.084$, $p<0.05$, $\beta2=-0.022$, $p>0.05$) whereas in presence of stress this association became statistically non-significant. It can be concluded that in some real-life situations stress can be trigger for risky online behavior in adolescents.

Gabriella Kulcsár

Prevalence and prevention of bullying and cyberbullying in Hungarian schools according to school principals

In order to introduce successful prevention programs for traditional bullying and cyberbullying among youth, support from school principals is essential. In order to appeal to them, it is important to understand their perceptions. The purpose of my research was to examine the perception of Hungarian school principals regarding the prevalence of bullying and cyberbullying in their institutions, and also on the subject of the relationship between bullying, cyberbullying and other youth disturbances. School-based prevention efforts were also surveyed. An online self-report questionnaire about the aforementioned issues was sent to the entire population of Hungarian education institutes, specifically addressed to the principals. The response rate was 20%. The vast majority (82,8%) of the respondents admitted to having bullying and cyberbullying problems among their students. While a perceived relation between bullying, cyberbullying and other disturbances is observed in some cases, the link is complex. As for currently employed prevention measures, there is a general lack of long-term whole-school approaches. The responses show that many schools either avoid facing the problems or feel limited in their ability to address them. Financial problems and not enough school psychologists worsen the situation. Schools needs to be introduced to long-term, community based, low cost whole-school approaches in order to strengthen their prevention efforts against bullying and cyberbullying.

Natalia Valkovicova, Nikol Kvardova, David Smahel, Hana Machackova

Do Mobile Phone Bans Work? An Analysis of Phone-use Rules in Czech Schools

The use of mobile phones during breaks at school has been a controversial topic among parents, teachers, and even the media for the past few years. Some state that phones prevent children from face-to-face communication (Russell, 2018; Kopecký & Szotkowski, 2019) and that children are subsequently restless and inattentive during lessons (Kopecký, 2018; Wright, 2018). However, there is little research on this topic, and we lack empirical evidence for the impact of phone-use rules during school breaks. To fill this gap, we investigated the common activities of children and adolescents during school breaks and made comparisons between schools that allow mobile phones and those that do not. Similarly, we explored some of the difficulties, such as reduced in-class concentration. Our results are based on data from 1,031 children and adolescents aged 11-17 in the Czech Republic, where 46% of schools have banned mobile phones during school breaks and 54% have not. The most frequent activity during breaks was communicating with classmates, whether phones were allowed or not. Similarly, there were no differences for other school-break activities, like communicating with classmates, doing schoolwork, and reading books and magazines. We found that adolescents who are allowed to use phones are a little less physically active and more often spend their time passively. Mobile phone rules in schools were also not associated with the school break-related difficulties, such as the reduced in-class concentration and post-break weariness.

Michaela Slussareff, Hana Friedlanderová, Zdeněk Šulc

How the Czech Parents Form Their Strategies For the Media Use In Their Children

Within this study we search for patterns in parental attitudes and strategies arising around the use of screens with their children. We observe the main characteristics, such as quantity and quality of media use but as well the parental motives, concerns or their own media use. We search for the main determinants beyond the classic demographic characteristics to explain how the parental media strategies are formed. We outline our conclusions from data collected on the sample of 230 Czech parents of three to five years old children. The respondents come from quota sampling that respects the basic demography in the Czech Republic (education, region and size of habitation).

New Media and Politics - Room 148

chaired by **Monika Metyková, Alena Macková**

Sakari Merik Ishetiar

The Destabilization Imperative: Why Authoritarian Regimes risk international condemnation to interfere in other countries

The arrival of mass communications has forced authoritarian regimes to move beyond policing only internal information, which has become all but impossible, toward attempts at control outside of their own borders. Foreign information exposes the public to alternative models of governance other than that employed by the authoritarian, weakening the authoritarian's "illusion of no choice."

When these alternative models catch on, they give the public a standard to rally behind, and create an existential crisis for the regime by reducing control over life chances. Given that preventing inbound information is impossible in the 21st century, authoritarians have turned to weakening the appeal of foreign governing systems. Disinformation poisons information abroad without exposing the source to excessive risk, using four mechanisms:

Narrative Shaping, where the outlet seeks to control which parts of a story are disseminated and emphasized before the story ever reaches the public;

Narrative Laundering, where the outlet seeks to disguise the origin of a story, often leading to greater credibility than reports from the outlet alone;

Misdirection/Rule by Law, a rebalancing of power by which existing laws or norms are retooled to reduce the credibility of challenging voices; and,

Gaslighting, where the outlet causes the target population to doubt their own ability to arrive at a logical conclusion, or to doubt the possibility of truth itself.

Felix Emeakpore Eboibi, Cynthia Nwabundo

Legal Implications of Shutting Down the Internet and Media during Electoral Process in Africa

Globally, the shutting down of internet and media during elections is becoming an issue of great concern due to its necessity. The act is predominantly on the rise in African countries. Uganda, Burundi, Egypt, Gabon, Sierra Leone, The Central African Republic, Niger, The Democratic Republic of Congo and recently Gambia have all shut down internet during elections. Although, election is not a criteria for development, it is an avenue for Africans to elect leaders of their choice and when these leaders gain political authority, they are empowered to fashion out policies that would be beneficial to the electorates living standards. Consequently, this paper investigates the legality or otherwise of shutting down the internet during elections in Africa. It argues that in this 21st century where countries are guarding their democracy jealously, shutting down of the internet during elections is anti-democratic; out of proportion and without careful judgment in their very nature. It is an outright disregard of human right to access the internet, associated directly with the violation of the rights to freedom of expression, association, peaceful assembly; access to information; rights to free and fair elections and to enjoy the right to technology. In order to avoid shutting down of internet during elections to be the rule rather than the exception in Africa, this paper suggests the deployment of electronic or internet voting in the conduct of elections in Africa.

Augusté Dementavičienė

How New Technologies Shape the Understanding of the Political Act: the Case of Digital Vigilantism

The main aim of this paper is, by using the case of Digital Vigilantism, to show how the concepts: the self, the body, the community, the space, the act (which are the basis for the law and politics) is changing. The additional question is whether the understanding of stable "self, space, body" was the illusion (D. Haraway) and how this illusion was shaken by the technological challenges? The swarm is a metaphor which Zygmunt Bauman uses to show how understanding of communities is changed in liquid modernity. Bauman understanding of the swarms is very basic and could be easily criticized by the biologists, but the main idea is that the swarms are based on untied, uncontrolled, short-term relationships between consumers/users to achieve some goals. Swarms could be massive in numbers and have a lot of power for a very short period of time. One of the examples could be Digital Vigilantism. DV is an act of punishing certain citizens (they are believed to deserve being punished) by other Internet users. F.e.g. to put someone's personal information (address, health records, phone number, etc.) on display for everybody in order to spread shaming acts. The problem is that people are interested in some actions for a very short period of time, but political act/change requires an active and stable effort. The main intrigue is whether the political act itself will change influenced by the "swarm effect" and how this possibility of change is interconnected with the cyborg way of living.

International Internet Law - Room 208

chaired by **Dan Svantesson**

Dan Svantesson

"I don't want to say I told you so, BUT..." - EU law and geo-location technologies

Lawmakers in the European Union – including the Court of Justice of the European Union – have a history of turning a blind eye to geo-location technologies. This is both surprising and problematic given the importance of geo-location technologies. However, now – under the label of 'geo-blocking' – these technologies are very much the 'flavour of the month' with two Regulations, and a series of court cases focused on geo-location technologies and their impact on matters of jurisdiction.

This paper examines the current, somewhat schizophrenic, EU attitude towards this technology that stands to transform the Internet as we know it.

Erich Schweighofer, Jakob Zanol, Isabella Brunner

Cyberattacks and „Hackback" - International Law from an Austrian Perspective

Within the KIRAS-Project ACCSA (Austrian Cyber Crises Support Activities) the authors evaluated the options of various stakeholders within Cyber Crisis Management. This was part of the development of a Cyber Crisis Management toolbox, a system for software-supported training and exercise that spans over several communication levels (e.g., engineering, management, first responder, policy makers). This toolbox supports the analysis and validation of a wide range of options through non-linear and dynamic exercise paths based on the exploratory scenario analysis.

One important part of the legal analysis was the evaluation of possible measures taken by state actors with regard to harmful cyber-operations from outside the states jurisdiction. This includes the possibility of counter-operations against other private or state actors and the lawfulness of these

actions under International Law. Because of the international character of the Cyberspace Conference, this contribution will focus on International Law and the main issues of acts of aggression and self-defence, responsibility and attribution of attacks in a cyber-context and with regard to critical infrastructure, giving an overview on current literature and the Tallinn Manual 2.0 and presenting the guidelines developed within ACCSA.

Michał Czerniawski

Scope of application of the right to be forgotten online

The EU's right to be forgotten was first articulated in 2014 by the European Court of Justice. In case C-131/12 Google Spain, a Spanish citizen was successful in demanding information regarding himself to be deleted from the Google's search engine so it couldn't be find when searching for his name. However, in this case the CJEU didn't decide on the scope of application of this right.

The lack of Court's analysis regarding the application of the right to be forgotten online resulted in public dispute between Google Inc. and Article 29 Working Party. Ultimately, it led to another case, C-507/17 Google Inc. v CNIL, which should be decided in 2019. The ruling in this case may change the Internet as we know it , as the Court will decide whether the EU data protection law should be applicable globally and may force data controllers to apply specific technical measures to ensure that data subjects' rights are respected. In particular, the Court's reasoning may go in two directions: allowing the application of this right to Google search engine worldwide or forcing Google to apply geo-blocking, i.e. limiting access to certain information on particular territory.

In my paper I will try to answer the question whether the right to be forgotten can be applied globally.

Law: Cybersecurity, Cyber-Warfare - Room 211

chaired by **Václav Stupka**

Jan Klouda

Organizations and states need consolidate to contest cyber attackers' readiness

Protecting critical infrastructure as a key national security asset has become a necessity. Technology life-cycle, deployment cost and its role in national security do not allow for hurried solutions regarding such infrastructure but require mid- to long-term planning, coordination and information sharing between the state and involved industries.

Most dangerous cyber attacks are well organized and funded but coordination of defensive efforts is lagging behind. Information asymmetry and insufficient trust between involved authorities and organizations undermine cybersecurity readiness. Moreover, geopolitical pressures impair the ability of organizations distinguish real threats from activism.

Czech law defines framework for defendable cybersecurity perimeter. It is legitimate that agencies and organizations inquire into each other's measures to improve their cybersecurity readiness. However, they also hold back coordination and information sharing. Consequently, authoritative measures may appear ineffective or harmful.

National agencies possess data that organizations do not, and vice versa. Organizations also control execution and support or jeopardize cybersecurity.

Alignment and information sharing are necessary for effective cybersecurity defence. Agencies and organizations should actively and regularly collaborate to promote cybersecurity as visible nationality. It will grow reputation of institutions involved and improve effectiveness of adopted measures.

Tihomir Katulić

NIS Directive in Croatian Law: Institutional Overlap and Other Open Questions

Information security and related concepts were first introduced into Croatian legal system following the adoption of the Information Security Act in 2007. While this act offered and codified the national implementation of measures as suggested by the EU Cyber Security Strategy in 2001, the Act did very little concerning the wider regulation of information security and focused on mandatory measures applicable solely to public institutions and government bodies.

The framework of information security in Croatian law dramatically expanded in the following decade and now includes the regulation of critical information infrastructure, state information infrastructure and the new Act on cyber-security of the operators of essential services and providers of digital services that transposed the Network and Information Security Directive into Croatian Law followed by a national Regulation accompanying the application of the Act.

The paper examines the existing institutional framework, explains specific national provisions and offers suggestions de lege ferenda following the first year of application.

Ivana Kudláčková, Jakub Harašta, David Wallace

Cyber Weapons Review Requirement in Situations below the Threshold of an Armed Conflict

Cyber weapons are getting at the forefront of attention over a period of last years. As the discussions intensify, many pressing issues still remain unsettled. One of those issues is undoubtedly the scope of legal requirements associated with deployment of cyber weapons. The line between war and peace is blurring and besides well-known notion of an armed conflict (international or non-international one), so far new and not-so-new concepts of hybrid threats and gray zone conflicts come into consideration. This situation represents a weak spot because there is not a precise international law regulation of cyber weapons that might by deployed in these scenarios.

Motivated by the paper Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis written by Colonel David Wallace, the paper will bring forward the research question where such a requirement of a weapons review in situations below the threshold of an armed conflict fit in the fabric of international law. To do so, the structure will be as follow. First, to introduce a working definition of a cyber weapon. Second, to clarify the concepts of hybrid threats

and gray zone conflicts that fall between the war and peace duality. Third, to examine if there are any limits imposed by international public law on deployment of cyber weapons in the above-mentioned situations.

Donald Ferguson

A cyber kill chain framework cybersecurity legal analysis

The nature of cyber attacks complicate the drafting and assessment of cybersecurity law. Cyber attacks involve a variety of threat actors using a variety of tactics, techniques and procedures in a complicated technological landscape targeting diverse resources. The features of cyber attacks change over time, including in response to measures that may result from cybersecurity law itself.

We propose a framework for analysis of cybersecurity law using cyber kill chains. Cyber kill chains model the tactical phases of cyber attacks by advanced, persistent threat actors. The tactical focus of cyber kill chains provides the framework with breadth of scope and duration of scope. Breadth of scope refers to the ability of the framework to apply across industries, threat actors, techniques, procedures, technologies and targets. Duration of scope refers to the ability of the framework to apply over time, where threat actors, techniques, procedures, technologies and targets change. The use of cyber kill chains to analyze cybersecurity law also benefits from the ability to test the law empirically, by applying real world attack scenarios and observing how cybersecurity law addresses each tactical phase of the attack.

A cyber kill chain will be developed from 12 kill chain variants proposed to date in the literature, modified for legal analysis by adding steps up to and including litigation, and used the to assess the NIS Directive (2016/1148).

Law: eCommerce, Digital Single Market - Room 214

chaired by **Pavel Loutocký**

Katarzyna Południak-Gierz

Problematic liability for performance of a personalized contract – the end of objectified legitimate expectations standard?

The research addresses decoding the content of a contract concluded with the use of personalizing mechanisms and the adequacy of current rules on contract liability in case of these agreements.

Applied technology affects not only the wording of the contract but also its interpretation. Until now in EU consumer law the standard of legitimate expectations constituted the predominant benchmark. It allowed for rationalizing individual consumer's assumptions as well as balancing entrepreneur's interest in limiting contractual liability to the objectively foreseeable scope and consumer's interest to obtain protection of reasonable and justified expectations upon which he made contractual decision. However, personalizing tools allow for individualizing mass contracting so that the content presented to individual consumers leads to maximization of entrepreneurs' profit. The objectified legitimate expectation no longer effectively balance the aforementioned interests as the technology allows for abuse of irrationality and individual circumstances. Hence, should the performance of the contract be determined in accordance with data gathered by the entrepreneurs tools, with data used for personalization in this instance or expectations of typical profiled consumer regarding data the entrepreneur should know of?

Also, if the application of personalization affects the content of the contract, it translates into changes in scope of liability for lack of or improper performance of contract.

Zsolt Ződi

Regulatory Problems of Financial Robo-Advisors

At the beginning of the recent decade a new phenomenon emerged in the financial advisory market: the robo-advisors. These systems can provide financial advice, or even handle portfolios without, or with very little human intervention. They started to spread across Europe and especially in America very rapidly. The European financial regulatory agencies, (European Supervisory Authorities), as well as the American organizations paid growing attention to the regulatory aspects of these applications. On the one hand it is obvious that all the regulations and restrictions, that apply to the normal advisory activity, (like Markets in Financial Instruments Directive, MIFID II, which, inter alia specifies the information that should be provided to clients, that this information should be fair and correct, and suitable for the client), apply to these software, (or rather the owners of these software) as well. On the other hand the general rules of GDPR's on automatic decision making and profiling seem also to be relevant to this activity. Both regulations raise some questions, which are valid in the context of other AI based decision making too. Namely: how can we guarantee in the future, that these decisions will be transparent, non biased, explainable, and will remain under human control? In my presentation I will make an overview on the robo-advisors, I will shortly present the recent regulatory landscape, and raise some regulatory issues, that emerged recently.

Tomáš Kozárek

The main challenges of multilateral regulation of identity management

The area of e-commerce is constantly growing part of trade. Even in time of word economic crises the e-commerce was boosting. This rapid e-commerce development brings a great number of challenges which are more or less obvious. One from these challenges is a question of identity management.

Everyone needs to prove her/his identity or at least declares her/his identity in electronic transactions. The request of identification is imperative of contractual relations, especially in electronic world. If you do not know who is your contractual partner, you will not be able to claim your rights in case of any breach of contract. Identification in electronic world could be tricky and non-reliable. For example every website provider can operate with totally different identification scheme. Nevertheless, we must deal with it. Several regulations of identification in electronic world

exist on national level, but none of them on the international level. There is an attempt to create multilateral instrument in United Nations Commission for International Trade Law (UNCITRAL), but there are several challenges which complicate any attempt to create multilateral framework for electronic identification.

The aim of this paper is to describe the main challenges of any multilateral regulation of identity management with special look on UNCITRAL work.

Newman Richards, Felix Eboibi

The Legal Implications of Electronic Taxation in Africa: Lessons from Europe and the United States

Advancement in Information Communication Technology over the years has changed the way people now live their lives and conduct their businesses. In the last two decades there has been an increasing dependence on the use of computer systems and networks in running of both Government and Private Businesses in Africa. Consequently, tax administrators in Africa in line with global trends are shifting from manual processes to electronic tax systems. Although, the adoption of information communication technology has obvious advantages, it does not come without some potential challenges. One prominent challenge to the introduction of electronic taxation is the activities of cybercriminals. A consequence of this is that taxation is now exposed to the challenges of electronic tax frauds (cyber tax crimes). The objective of this paper is to identify the ways electronic tax systems can be protected and sustained in Africa and how incidences of cyber tax crimes can be prevented and curtailed in Africa drawing from the lessons the experiences of the United States of America and some countries in Europe present.

15:15 - 15:30 Coffee break

15:30 - 17:00 Parallel streams

Law: Intellectual Property On-Line (Art. 17 DSM)- Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Matěj Myška

Exceptions and Limitations to Copyright Law and Art. 17 DSM Directive: How to Make it Work?

The (in)famous Art. 17(7) DSM Directive simply states, that the users shall be able to rely on specific set of exceptions or limitations to copyright law when sharing user generated content on the platforms. This shall also contribute to the "striking of balance" of fundamental rights and interests of the parties involved. The Art. 17(9) DSM also stipulates, that the users should be able to make of effective complaint and redress mechanism if the user generated content relying on these exceptions and limitations is overblocked.

The implementation and operationalization of this idealistic rules however generates a plethora of problems, incl. the paradigmatic shift of the availability of the content from "available-until-proved-infringing" to "blocked-before-anything-else" (as stated e.g. by Elkin-Koren, Niva. „Fair Use by Design""). University of California Law Review 64 (2017).. Within the context of the previous case law of the CJEU and the existing doctrine (especially Senftlebens seminal article Senftleben, Martin. „Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market"") the contribution explores the possibility of strengthening and more flexible re-interpretation of the current exceptions and limitations (including payment of "fair compensation" (as is the case in privileged private copying)) providing for more legal certainty as one of the solution to the identified problems.

Andrea Katalin Tóth

Algorithmic Copyright Enforcement, Artificial Intelligence, and the Problem of Free Speech

By burdening them with primary liability, Article 17 of the Directive on Copyright in the Digital Single Market set a high incentive for content-sharing platforms to filter out any potentially unlawful content with the help of algorithmic enforcement employing cutting edge technology, including artificial intelligence. Although the idea behind compelling these platforms to ensure the unavailability of unauthorized content was intended to create an obligation, it also bestowed a significant power to these private companies to decide what could qualify as a copyright exception. This authorization to effectively regulate speech is even more questionable as copyright is often asserted for reasons external to IP, providing an efficient tool for corporate censorship based on misuse.

Although copyright's history is about balancing between rightholders' proprietary interests and users' fundamental rights, the question arises whether technological advancement warrants a new approach to regulation of speech and platforms. The legislative intent and political discourse behind Art. 17 were seemingly obvious, however, the potential impacts of the rule and the likely direction of AI's development have not been thoroughly considered. This paper suggests that (with tools found in the directive itself) careful balancing should be exercised while transposing these provisions into national law in order to protect fundamental rights without compromising the effectiveness of new technologies.

Daniela Caterino

User Generated Contents in EU Digital Copyright Directive

Aim of the paper is to analyse the approach of the EU legislator to the subject of UGCs, as reflected in the evolution of the text of the proposed EU Directive on Digital Copyright, by framing it in the general perspective of copyright in the digital context.

The paper will:

a) examine the definition and the most important categories of UGCs, such as fan films, doujinshi et similia;

b) analyse the regulatory context in EU countries before the Directive, with particular attention to exceptions and limitations to copyright referred to in art. 5, lett. d) and k), dir. 2001/29/EC (such as criticism, parody, pastiche);

c) focus on final text adopted by Parliament and Council last June.

The final text proposes a more advanced approach by:

a) framing the right "to upload and make available content generated by users for the specific purposes of quotation, criticism, review, caricature, parody or pastiche" into the framework of "a balance between the freedom of expression and the freedom of the arts, and the right to property, including intellectual property" (Whereas n.70).

B) obliging Member States to provide specific exceptions to copyright in their law in order to affirm the legitimacy of the UGC.

The conclusions will comment on the concepts of author, autorship and creativity in the digital context and on the desirability of an ad hoc general exception for UGCs, along the lines of Canadian Copyright Modernization Act 2012.

Usable Security and Privacy (Developer-centred security) - Room 038

chaired by **Lydia Kraus, Vashek Matyáš**

Peter Leo Gorski, Luigi Lo Iacono

On the Influence of Information Flows in Secure Software Development

Over 23 million software developers around the world develop a variety of software that is becoming increasingly important in our lives. Security and privacy-preserving functionalities are, henceforth, a necessity in digital applications, services and products. Because not every software developer is a security expert and the implementation of security safeguards is a complex and error-prone task, all components of a development environment should provide the best possible support in the development of secure software.

Since Application Programming Interfaces (APIs) are elementary building blocks in the implementation stage of software development, the talk deals with the question of how Security API providers can effectively and efficiently tell their users how to use an API correctly. This can be achieved by implementing important and security-relevant information at the right place, at the right time and in a usable way. Therefore, a model will be presented which can serve as a research tool to analyse security information flows in the implementation stage of software development. The model will be derived, further explained in detail and vividly illustrated with results of current research in the field of developer-centered usable security. This will lead to a discussion to what extent information flows can help software developers applying security APIs and implementing secure software. The model will also show the current state of research and further research needs.

Matěj Grabovský, Martin Ukrop, Lydia Kraus

What Is (Un)Satisfying About Using TLS Libraries?

TLS is crucial to network security but TLS-related APIs are repeatedly shown to be unusable and misused. While effectiveness and efficiency are sufficiently covered by the existing research, user satisfaction with the API seems to be under-researched. We aim to investigate usability of TLS-related APIs in multiple libraries, focusing on user satisfaction. We conducted a small exploratory study with nine students comparing the APIs of three popular security libraries: OpenSSL, GnuTLS and mbed TLS. We qualitatively analyzed the submitted reports commenting on API usability and tested the created source code. Participants' overall satisfaction was very varied. However, multiple comments concerned documentation, example code snippets, the API level of abstraction and error handling. As Checking for revoked certificates turned out to be especially complicated, while other certificate checks and TLS version enforcement seemed reasonably easy. None of the tested libraries was perceived as universally better – there were conflicting opinions on both the interface and documentation. Several usability issues were shared among participants, forming a target for closer inspection and subsequent improvement.

Martin Ukrop, Lydia Kraus, Vashek Matyas, Heider Ahmad Mutleq Wahsheh

Will You Trust This TLS Certificate? Perceptions of People Working in IT

Flawed TLS certificates are not uncommon on the Internet. While they signal a potential issue, in most cases they have benign causes (e.g., misconfiguration or even deliberate deployment). This adds fuzziness to the decision on whether to trust a connection or not. Little is known about perceptions of flawed certificates by IT professionals, even though their decisions impact high numbers of end users. Moreover, it is unclear how much does the content of error messages and documentation influence these perceptions. To shed light on these issues, we observed 75 attendees of an industrial IT conference investigating, different certificate validation errors. Furthermore, we focused on the influence of re-worded error messages and redesigned documentation. We find that people working in IT have very nuanced opinions regarding the tested certificate flaws with trust decisions being far from binary. The self-signed and the name constrained certificates seem to be over-trusted (the latter also being poorly understood). We show that even small changes in existing error messages and documentation can positively influence resource use, comprehension, and trust assessment. Our conclusions can be directly used in practice by adopting the re-worded error messages and documentation.

Psychology of Cyberspace - Room 133

chaired by **David Šmahel, Hana Macháčková**

Christiane Atzmüller, Ulrike Zartler

Designing vignette experiments for measuring online civil courage among adolescents

Vignette experiments that are implemented in quantitative surveys, i.e. Factorial Surveys, have a high potential for studying emotional topics, such as violence perception and criminal behavior, as vignettes can serve as valid and context sensitive proxies for real world settings. However, a considerable risk of biases in the vignette ratings comes into effect if the presented vignettes are not sufficiently able to evoke emotions that correspond to real settings. These shortcomings have been largely neglected in the scientific discussion.

We aim at demonstrating challenges and suggesting related solutions by presenting design features of a study on online civil courage among adolescents dealing with perceived violence on the internet. Findings are based on a representative survey among 1,868 students aged 14 to 19 years in Vienna, Austria. We present (1) the selection procedure of youth-appropriate vignette scenarios, (2) the construction of the experimental vignette design, (3) the creation of the vignette stimulus content in collaboration with adolescents, (4) design decisions for the presentation mode and (5) the implementation of the constructed scenarios within an online survey with simulated social media profiles. Results show significant main- and interactions effects for both vignette and respondent level, giving insight into juvenile judgement principles concerning their cognitive and emotional evaluation of online attacks and their intervention behavior.

Birgit Ursula Stetina, Zuzana Kovacovsky, Jan Aden, Anastasya Bunina, Armin Klaps

Women and Online-Pornography: Exploring gender differences in pornography users

Recent studies show more similarities between males and females regarding pornography consumption on a neuronal level than expected (Mitricheva et al., 2019). What does that mean for clinical aspects of online pornography consumption?

A sample of 93 online pornography users (51.6% male and 48.4% female) was surveyed in a cross-sectional design using an online questionnaire including questions about sexual preferences in real life and online as well as several clinical scales such as the Internet Sex Screening Test (ISST, Delmonico, 1997) the abbreviated version of the Sex Addiction Screening Test (SAST-A, Carnes, 1989 abbr. by Delmonico & Miller, 2003) and the Internet Addiction Scale (ISS-20R, Hahn, Jerusalem & Meixner-Dahle, 2014).

Women report that they have changed their preferences since consuming online sexual content significantly more than men (T(89.993)=-2.153,p=.034). Female participants state significantly more interest in online sexual behaviours (T(71.149)=-3.456,p=.001), more online sexual compulsivity (T(56.761)=-3.631,p=.001) and more isolated online sexual behaviour (T(85)=-2.965,p=.004). Males report significantly more problematic online behaviour (ISST:T(69.756)=3.823,p<.001) and usage of more hours per week (T(41.685)=3.729,p=.001).

Female pornography users seem to be more similar than expected but still different including a change in preferences. Further studies focusing on women's consumption in a more specific way need to reveal if there is a trend.

Michal Ptaszynski

Automatic Cyberbullying Detection: A ten year struggle in trying to make Internet a safer place

Recent decade has brought to light a problem of unethical behaviors in Internet environments. It is the problem of cyberbullying (CB), defined as exploitation of open online means of communication, such as Internet forum boards, or Social Networking Services (SNS) to convey harmful and disturbing information about private individuals, often children and students. To help with mitigation of this problem we started the research on Automatic Cyberbullying Detection in 2008, with a motivation to help school teachers and parents engaged in Internet Patrol activities. We started the research as a long term project, in which we aimed to contribute to detecting, preventing, and ultimately solving the problem of cyberbullying. In the presentation I will talk about what we accomplished during the first 10 years of our study. In particular, we firstly aimed at developing a systematic approach to the automatic detection and classification of cyberbullying entries, which could help and ease the burden of the Internet Patrol members. One of the main goals of the project has been to create an Internet Patrol support solution for automatic spotting of cyberbullying entries on the Web and reporting them to appropriate organs. In the lecture I will present some of our most important results followed by recent developments and near future plans.

Manipulative Techniques On-Line - Room 148

chaired by **Miroslav Mareš**

Petra Mlejnková

Vulnerability of the Czech society in context of disinformation

The contribution deals with the intensively discussed issue of vulnerability of individuals in the context of disinformation and propaganda. The results from research testing different manipulative techniques of propaganda will be presented. It will be discussed, which techniques are more powerful and how are we good in their recognition.

Arianna Rossi, Gabriele Lenzini

An explorative plunge into the dark (patterns) of social media

Lately, researchers, journalists and regulators are devoting attention to dark patterns, defined as "design choices that benefit an online service by coercing, steering or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they would not make" (Mathur et al., 2019). Dark patterns can be understood as implementations of persuasion strategies that have been studied to understand how and why marketing and social engineering are successful. Yet, the

strategies and design choices that nudge users to provide more personal data than necessary have only partially been investigated.

In this paper, we firstly critically discuss the existing definitions with respect to "coercion" and "deception". We determine what makes the darkness of design patterns and to what extent it can be argued, and proved, that users would take different decisions without such influence. Secondly, we compare and systematize taxonomies of dark patterns and their implementation of persuasion principles impacting buying behaviors and decisions concerning security and privacy. Thirdly, we propose a comprehensive definition and develop a taxonomy of dark patterns for personal data gathering, that we validate by analysing a specific set of social media. Unlike most previous work, we also focus on interface design elements, like the use of colors and icons, the position of buttons, the number of clicks and taps necessary to perform a task, etc.

Legal Informatics - Room 208

chaired by **Erich Schweighofer, Jakub Harašta**

Ilaria Angela Amantea, Luigi Di Caro, Llio Humphreys

Modelling Norm Types and their Inter-relationships in EU Directives

Every single norm has to be interpreted in the context of other norms. There is a lot of research on detecting and linking legal citations, but our interest is in implicit links. Often there are goals, principles and values that have to be balanced, but are not found in the article you are examining and not cited explicitly. Other norms may also affect the limits, scope, jurisdiction or temporal validity of the article under consideration. The degree of interpretation required is dependent on the nature of the legal document itself. For example, EU directives are very abstract for political reasons and this implies multiple interpretations, whereas clinical guidelines, for example, are very technical and precise, so the interpretation is unequivocal. We began our work with an open mind, an approach inspired by grounded theory. Our team is made up of researchers with a background in Law, Computer Science and Legal Informatics. Our initial goal was to detect semantic links between articles and recitals in a specific directive. But during this work, we came to understand that there are more links then we had imagined and that these links exist for many different reasons. So we decided to take a step back and classify the links we found. We are arrived at the following categories: Conceptually Similar, Constitutive, Motivation, Impact, Indirect Internal, Via Other Law, Procedural, Contextual and Norm Group. We will present each category in detail and provide some examples.

Peter Kovacs, Adrienn Princz, Vivien Kardos

Examining the (legal) IT competences of law students

In parallel with the development of ICT services the scope of special digital information and communication services and databases supporting state and public administration legal activities broadens, as well as the opportunities to use these. Knowledge of these services and their use are as fundamental expectations from the lawyers of the future.

The question is, what computer science, legal informatics and otherwise digital competences do the law students of the present have and whether they know these possibilities at all together with their advantages and risks. Besides, it is also a question which of these systems they do, could or would use, and to the use of which they could adapt.

In our paper, we present the main findings of a study conduct with the participation of over 200 Hungarian law students. From the preliminary results of our survey conducted through the DigComp framework it can be clearly seen that the student do not, or if yes only to a minimal extent, as aware of trends in legal informatics and the challenges of the field.

Tereza Novotná

Semantic similarity of texts of judicial decisions of the Czech Supreme Court

Czech Supreme Court produces a few thousands of judicial decisions per year. Thus, lawyers, judges or legal scholars are provided new tools for automatic analysis of judicial decisions. The tools or legal information systems automatically classify decisions according to keywords, topics or related parts of regulatory texts. Mostly, these tools are commercial based on either algorithms that are mostly part of trade secret or either they are based on subjective opinion of employees of these commercial companies.

In this contribution I will provide a transparent methodology of automatic processing of texts of dataset of the Czech Supreme Court judicial decisions. I will count a semantic similarity of judicial decisions and show that decisions with similar legal topic have higher semantic similarity. Finally, I will visualize the data into network to show the clusters of similar decisions. I will show that these methods may be helpful for lawyers to analyse the decisions automatically on the transparent basis.

Law: Cybersecurity, Cyber-Warfare - Room 211

chaired by **Václav Stupka**

Václav Linkov

Human factors in cybersecurity of autonomous vehicles

Autonomous vehicles (AV) will be vulnerable to cyberattacks especially in stage when they will communicate with other vehicles and infrastructure. Human factors importance in failure in AV cybersecurity will increase. People's failure is connected to level of multitasking, frequency of cyberattacks, authentication appropriateness, ability to react in stress, or cultural specifics. It is important to identify human groups vulnerable to AV cybersecurity failure and develop methods how to educate them to minimize the risk and ways how AV should communicate with driver under stress to guide him to correct behavior. Human factor failure is crucial also in case of employees of companies in charge of AV developments and AV infrastructure maintenance. These companies

should select loyal employees with minimal risk to be corrupted by hackers looking how to get access to AV. Hackers' motivations and goals should be also studied to be able to prevent cyberattacks. Combined study of human factor vulnerabilities of drivers, AV professionals, and hackers will ensure good security of AV.

David Kosar

ECtHR and Cybersecurity

The aim of this article is to explore the recent case law of the European Court of Human Rights concerning cybersecurity. To set the stage, I will first focus more broadly on the jurisprudence of the European Court of Human Rights dealing with new technologies and data protection. Subsequently, I will zero in on mass surveillance and other cybersecurity issues in the Strasbourg case law.

Onur Dur

Definition of Cyber-Terrorism: Joint Reading of International Law and Insurance Law

Definition of terrorism is still controversial. Definition of cyber-terrorism is even more controversial due to its added technological complexity. Therefore, a new and comprehensive approach is necessary to adequately describe this new risk threatening public security and economic order.

An internationally agreed definition is the first step towards ensuring international cooperation against cyber-terrorism. Otherwise, it would foster unilateral positions as it is in the global fight against terrorism.

Insurance industry is also concerned with the definition of cyber-terrorism. As insurers firstly have to define the risk, they subsequently make the assessment whether the injury within the policy or not. Therefore, definition of terrorism and more recently definition of cyber-terrorism became a particular interest in Insurance Law field.

The premise of this paper is to provide an intra-disciplinary approach on the possible elements of the definition of cyber-terrorism. In this quest, Public International Law and Insurance Law are mutually reinforcing each other. While International Law offers deeper theoretical foundation, Insurance Law can propose more illustrative case-law and sectoral practice.

For the scope of this paper, Insurance Law is represented by UK and US Insurance Law as their market shares are representative in the global insurance market specialized in terrorism insurance. Comparative legal methodology will be employed for this essay.

Pavel Loutocký

Qualifications Framework as Crucial Step to Improve the Area of Cybersecurity

The area of cybersecurity is increasingly crucial in current day interconnected world. This translates into particularly dire demand for qualified experts. These encompass not only highly skilled IT specialists, but also other related professionals with legal, administrative, economic or security studies backgrounds. Despite major employment opportunities in this field, the standard education frameworks nowadays do not produce adequate numbers of qualified workforce required in this field. Furthermore, the dynamic nature of this area required intensive continuous learning mechanisms in place that allow for gradual and systematic improvement in individuals expertise and capabilities. However, establishment of such training programs and qualification validation requires first a thorough analysis of the current and future needs of the field, that would be translated into a comprehensive and complex qualifications framework. The main aim of the speech is focused on introducing main approaches and obstacles to create such a scheme, it will also introduce unique approaches at lease for European states.

Liability v. Compliance in Engineering - Room 214

chaired by **Herbert Hrachovec, Andreas Kirchner**

Agata Justyna Ferreira

How to regulate blockchain - unique regulation for unique technology

Over the last ten years a little known, underrated and niche blockchain technology has risen to prominence. Given the exponential development of this technology it is not surprising that the regulators struggle to keep up since the laws and regulations only change incrementally. There is a considerable gap between sophistication and application of blockchain technology and a legal and regulatory void in which it operates. Blockchain is a very empowering technology, allowing peer-to-peer transacting in trustless, borderless, secure and immutable environment. It is capable of creating a disintermediated, self-governing digital space warranting virtual exit for its participants from the established institutional structures. Currently emerging landscape of blockchain regulations presents a diverse picture, from a complete ban on initial coin offerings in China to one of the most progressive regulatory approaches in Malta, regulators´ approach varies. The objective of the regulation should not be to slow down, limit technology or stifle innovation, but instead the regulatory goal should be to create standards, ethical and good governance principles and facilitating interoperability. The regulators should be forward looking, pro-active and work in collaboration with the relevant stakeholders and international partners to avoid fragmentation, mitigate risks and encourage innovation. It is not necessarily the case in todays´ diverse, fractured and inconsistent regulatory environment.

Mikołaj Domagała

Autonomous vehicles as a remedy to combat communication exclusion

The author of this speech undertakes analysis of the so-called communication exclusion and the impact of autonomous vehicles on reducing such exclusion. The core of the speech is a research question from which one should proceed in order to further analyze the topic. The research question is: Will autonomous vehicles increase the level of mobility of people with reduced mobility, i.e. people with disabilities, the elderly or those who do not have a driving license? When analyzing the

above question, it is important to consider legal, economic, technical and social barriers that may arise in connection with the use of autonomous vehicles by people with reduced mobility.

The problems raised by the speaker during the speech are: (1) potential software failures, (2) limited cyber security, (3) limited price availability of autonomous vehicles, (4) failure of adaption autonomous vehicles to the needs of people with reduced mobility, (5) lack of legal regulations allowing autonomous vehicles to move on public roads and (6) lack of provisions enabling persons who do not have the driving license to drive the fully autonomous vehicles. Then the author presents the proposed solutions to the indicated problems. These are: (1) forcing manufacturers to constantly upgrade software, (2) mandatory installation of anti-virus programs, etc., (3) adoption of the upper price limit for autonomous vehicles, (4) the need of legal guarantee of the so-called universal design of autonomous vehicles, (5) amendment of the provisions authorizing the use of autonomous vehicles also for driving on public roads, (6) permission to carry passengers without a driving license.

Autonomous vehicles can become a great help in everyday life for people with reduced mobility. However, using the potential of this type of vehicles will not be possible without proper interference of the legislator and advised implementation of developed solutions.

Rafał Tomasz Prabucki

To block, or not to block – hypeledger blockchain solutions for digital registers of shares. Case study from Polish LegalTech market

The paper presents briefly what blockchain and hyperledger are and attempts to answer the question whether we can trust the hyperledger solution. Then the author goes on to explain the phenomenon of the concept of decentralizing registers. In this way the author points out that solutions are being developed to digitize the registers required by law. As an example, the author presents the case study of registers of shares based on blockchain.

Finally, the author points out that national institutions lose their monopoly on data collection. More and more information is being collected by technological companies that offer the digitization of legally required registers. This is accompanied by an interesting phenomenon. Subsidiary registers are beginning to collect more data than their equivalents held by national entities. Will those in power seek to accept the changes? Or maybe they'll try to block the changes?

17:00 - 17:15 Coffee break

17:15 - 18:45 Parallel streams

Law: Intellectual Property On-Line (Limits) - Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Philipp Homar

Photographs of Works of Visual Art in the Public Domain

After copyright has expired, works of visual art fall into the public domain and can be used by anyone without seeking authorization from rightholders. This freedom is undermined in practice when users use photographs of works of visual art. In this case, copyright and neighbouring rights restrict the freedom of users (cf. German Supreme Court 20.12.2018, I ZR 104/17 – Museumsfotos). Against this background, Art 14 of the Directive on Copyright and Related Rights in the Digital Single Market (DSM-Dir) restricts the protection of photographs of works of visual arts that have fallen into the public domain.

However, the provision leaves some room for interpretation and leaves several questions unanswered. Therefore, the paper sheds a critical light on Art 14 DSM-Dir, addresses open questions and analyses whether the provision will contribute to fostering access to cultural creations and cultural heritage.

Michal Koščík

Preservation of the cultural heritage and the use of out-of-commerce works in the era of DSM directive

The contribution will follow up on the presentation that the author made last year on a similar topic and on the article that was accepted for publication in December 2018 (1).

The paper will reflect on the developments in the area of digital cultural heritage in the year 2019 and analyse, whether the declared policy objectives were actually reflected in the wording of the Directive on Copyright in the Digital Single Market (DSM).

The paper will analyse the mandatory copyright exception for preservation of cultural heritage (the Art. 6) and rules for the use of out-of-commerce works and other subject matter by cultural heritage institutions. The article will analyse the relationship between the DSM directive and respective provisions of the InfoSoc directive, which remains in effect (most notably Art. 5 and Art. 5).

The paper will focus on the practical issues of digitalisation and emulation of digital works. Next, the paper will analyse the impact of DSM directive on collective licensing mechanisms in relation to digital works.

(1) KOŠČÍK, Michal; MYŠKA, Matěj. Copyright Law Challenges of Preservation of"" born-digital"" Digital Content as Cultural Heritage. European Journal of Law and Technology, 2019, 10.1.

Ondřej Hanák

Text and Data Mining in the DSM Directive: too restrictive approach?

The focus of this paper is the text and data mining (TDM), which is a practice especially employed in the area of artificial intelligence. The first part of the paper will briefly summarize the current legal status of TDM in Europe with a special focus on the Czech Republic. The second part will focus

on the TDM provisions in the DSM Directive and the problems they may pose. The third part will offer possible remedies to these problems.

The DSM Directive brings a completely new approach to utilizing copyrighted works in TDM. It specifically favors the TDM activities of public research organizations. On the other side, TDM activities of private entities are burdened by an opt-out possibility of the rightsholder. The DSM directive also omits an important question of using copyrighted works on the output of TDM.

My paper will examine two possible solutions to the aforementioned problems. The first is that the TDM could be completely removed from the scope of the Directive as the nature of TDM itself is not in conflict with copyright. The second possibility is that the TDM provisions should be at least stipulated differently to allow private entities to employ TDM methods more freely. The paper will also include a comparison with other countries (especially the USA and Japan) to argue that the European Union might be at a disadvantage in the area of AI in the future because of the restrictive approach to the TDM.

Usable Security and Privacy (User-centred security) - Room 038

chaired by **Lydia Kraus, Vashek Matyáš**

Lenka Knapová, Agáta Kružíková, Lenka Dědková, David Šmahel

User Perceptions of Usability and Security of Authentication Methods for Mobile Banking on Smartphones

With sharp increase in the use of smartphones and other mobile devices on daily basis, mobile banking is becoming more popular. It is important to provide end users with secure authentication methods that are easy to use at the same time. The purpose of this study was to evaluate user perceptions of various authentication methods in the context of mobile banking, specifically NFC hardware token, card reader, fingerprint, PIN code, and their combinations.

We conducted a large-scale user study of two authentication scenarios in a simulated mobile banking environment on a sample of 250 adults aged 26-54. Each participant went through two scenarios on a smartphone which included activation of the service, log-in, and payment order. In each scenario, participants underwent both a single-factor authentication procedure as well as a two-factor procedure. The tested methods were an NFC hardware token and a fingerprint or a PIN code in the first scenario and a card reader and a fingerprint or a PIN code in the second scenario. Participants also answered related questionnaires before and after the scenarios.

The primary focus of this study was on the end user perceptions of security and usability of these methods as well as preferences for various single- and two-factor authentication methods. The results have important implications for various parties such as banking institutions or governments enforcing online authentication of their citizens.

Psychology of Cyberspace - Room 133

chaired by **David Šmahel, Hana Macháčková**

Ondřej Javora, Kristina Volná, Tereza Hannemann, Cyril Brom

Do they learn better if you let them choose? Effects of customization in learning games for children: Work-in-progress paper

Little is known about what features of digital learning games stimulate intrinsic motivation of children and thereby improve learning. Cordova and Lepper in their study (J Educ Psy 1996, 88(4), 715-730) found out, that narrative and customization in learning games can improve intrinsic motivation and enhance learning outcomes. However, their study included a small sample (~15 children per group) and targeting only on procedural knowledge. Here, we aim at extending their study's part focusing on customization with a different instructional target (mental models acquisition) and a larger sample (planned N ~ 64 per group).

We have developed a learning game about photosynthesis and water circulation in plants and have started an experimental study with a between-subject design (2 groups, random assignment). In both conditions, children (9-11 years of age) were given the following goal: to build a plant in order to feed an animal (the learning part included building the plant). In the experimental (customizable) condition, children chose an animal, named it and picked a plant and environment where they wanted to build it. In the control conditions were all the variables assigned. We have measured prior knowledge, enjoyment, motivation, immediate learning outcomes and delayed learning outcomes.

So far, ~120 children have been examined. The study will be completed in October 2019. Preliminary results will be presented at the conference.

Daniel le Roux, Douglas Parry

Towards an Integrated Framework of Technology Use Dimensions

The past decade has seen growing interest in the effects of permanently connected living on human well-being. Prominent themes include anxiety and depression associated with the use of social network sites, cognitive control deficits associated with media multitasking, and addiction to technology. Due to the restrictions and inaccuracy associated with self-report measures of technology use, researchers have attempted to harness trace data to gain more accurate data about technology use behaviour. Such efforts include the development of applications which track smartphone use based on variables such as screen unlocks, active applications and session duration. While these instruments provide certain benefits over self-report, they are limited in their ability to elucidate the nature of use. To guide the improvement of data collection applications, a conceptual framework describing the dimensions of technology use behaviour is required. Despite a limited number of isolated efforts to develop such frameworks, no standardised or broadly accepted version currently exists. To address this challenge we are conducting a multi-phase project to identify, describe and integrate the dimensions of technology use. We believe that the resulting framework will advance research on technology use effects by contextualising discrepant findings

across existing studies, and informing measurement and instrument development/adoption in future studies.

Michael Henry

Instant Message Usage in Virtual Teams: A Systematic Review of Interruptions

As distributed work increases in frequency, the impact of Instant Messaging (IM) and other Computer Supported Collaborative Work (CSCW) tools increases. This increased use of collaboration tools can lead to increased communication within teams, but can also lead to high levels of media multitasking and information overload.

This presentation examines the different types of CSCW tools (instant messaging, social networking, and video chat, among others), and their frequency of use within organizations.

Secondly, this presentation examines existing research on the topic, looking specifically at the type and frequency of interruptions created by IM tools. Previous research has identified Work Interruption, Interactivity, and Communication Quality as separate factors of IM tools (Ou and Davison, 2011). This presentation focuses on the interruption factor. To explore relevant studies, a PRISMA approach was used.

This presentation intends to discover common results across a broad set of journals, looking specifically at interruptions caused by IM tool usage in virtual teams.

Keywords: Instant Message, Virtual Teams, Interruptions

References

Ou, C. X., & Davison, R. M. (2011). Interactive or interruptive? Instant messaging at work. Decision Support Systems, 52(1), 61-72.

Marthe Möller, Rinaldo Kühne, Susanne E. Baumgartner, Jochen Peter

A Social Identity Perspective on the Effect of Social Information on Video Enjoyment

Research suggests that social information presented alongside online videos can alter viewers' video enjoyment. Based on the social identity framework, we conducted an experiment to investigate the role of two factors in this process. First, we investigated the role that the source of social information (i.e., in-group or out-group) plays in the effect of social information. Second, we explored how interactivity in the form of writing a comment while watching the video may alter the effect of the source of social information. Results indicated that social information created by in-group members is more influential than social information created by out-group members. However, no effect of interactivity was found, indicating that writing a comment while watching a video does not increase viewers' susceptibility to the effects of social information. These results shed light on the mechanisms and the social processes that underlie the effect of social information on video enjoyment.

Manipulative Techniques On-Line - Room 148

chaired by **Miroslav Mareš**

Klaudia Rosińska

Fake news as an effect of the Crisis in Media Communication

The paper will present the results of the author's research devoted to exploring the topic presenting fake news as a consequence of several crises in media communication. Fake news was named the 2017 word of the year by the Oxford Dictionary. This may seem as a natural consequence of the post-truth era, but it is also attributable to problems in the media communication process. I will present crises in journalism in the Polish media market and the question of the citizens' media literacy in Poland, which could be the main reason for the problem of fake news on the internet. My talk will present a theoretical analysis which will be the basis for further empirical research on this topic.

Gabriele Lenzini, Yining Wu

An Operational Framework to Detect Distrustful Statements in Online Conversation

The aim of this work is to develop a procedure to flag for potential verbal post-truth statements, vulgarly called lies, in written communications.

But what is a lie? In philosophy and in logic the question has been answered, and several definitions of different flavours of it (e.g., offensive and defensive lies, or deductive and adductive lies, bullshit and deceptive statements) have been proposed and discussed. However, they all make use of unobservable modalities like one's beliefs and intentions and for this reason they cannot be implemented in a tool. There is no natural language lie detector for them.

This work instead proposes an operational definition that, since it considers only what can be observed in a dialogue (i.e., one's utterances) and since it assumes that when a speaker states something, in that moment s/he believes her/his words and s/he intends to say it, cannot be characterised as ""a lie""; rather our definition characterise what we call an untrustful statement. Formalised in linear time logic with dialogue predicates, the definition fits the interest of security analysts, and makes it possible to have tools that warn users about potential presence of it in a dialogue, thus flagging for potential situations that may carry attempts of frauds and of deception, and that can potentially hide a lie.

Legal Informatics - Room 208

chaired by **Erich Schweighofer, Jakub Harašta**

Ondřej Svoboda, Alex Ivančo

AI Principles and emerging fragmentation of global AI governance

Internationally, many states have launched ambitious strategies to promote AI and correspondingly, AI has become an object of considerations how to regulate this development at transnational level. Currently, there are at least 27 proposed AI principles with a cross-border scope, which show how states, research institutes or business around the world are approaching AI. This increasing number of those initiatives raises various questions. In this respect, AI principles help to frame the global AI debate. They represent different sets putting different emphasis on different topics. On the other hand, they may complement each other and provide building blocks for a broader consensus as well. All initial proposals are of soft law nature. Nevertheless, in the future, they can form the basis of binding international standards or help governments design national legislation as "hard legalization" followed in other new fields in the past. In any case, AI principles will likely define social and ethical considerations about the next development of AI. The proposed contribution will focus on the current state of play in a landscape of international AI governance, considering and comparing various initiatives. We will evaluate existing AI principles and make a case against possible fragmentation. In order to respond constructively to current trends, we will argue for more active role of relevant international organisations in developing transnational rules for AI.

Nimrod Mike

Who is the maze runner?

The ramifications of GDPR , an evolutionary, yet not revolutionary, piece of legislation, already reach beyond expectations. Since intrusions of privacy are omnipresent, regulatory actions are inherent for the ever changing typology of privacy intrusions.

The GDPR points out that the Data Protection Officer ('DPO') shall have a role of consultant on specific issues related to data privacy. This is a new profession that can pragmatically shape the enforcement of privacy preserving policies inside every organization.

As the consultant role is flexible, it is also subject to change. Replacement would be possible with an intelligent legal chat-bot, which improves access to legal information. Among other benefits, the chat-bot could be deployed for less costs, would have permanent availability, would be capable of multitasking, but most importantly would have a lexical knowledge on the basics of data protection law.

One side of the coin is still under question: it is debatable if the managerial skills can be matched. The aim for of presentation is to draw a comparison between the skillset of a human DPO and a conversation entity developed with the use of IBM Watson platform and WebProtégé. By the end one question should be answered: is this a profession for individuals or for virtual assistants?

Medical Data - Room 211

chaired by **Walter Hötzendorfer**

Melchiorre Alberto Monaca, Angela Busacca

AI and data mining in the processing of health data for diagnostic and treatment

The AI systems used in the medical-health field offer innovative and absolutely new scenarios: from the use of robotics in the surgical field, to software that, through data mining processes make it possible to compare health treatments by identifying the physical characteristics and anamnesis (detailed) for each individual patient in each phase of medical treatment, to the interaction between multiple databases and automated processing systems to improve medical diagnoses and prognoses. For each of the indicated hypotheses, however, the (common)starting point is the ""datafication"" of the patient; "datafication" means a process that will generate a flow of data able, on the one hand, to create an ecosystem of health protection based on data mining processes and exponentially more ef-ficient than the current one (based on the linear use of data), but on the other hand that exposes the interested patients to the risk of (unwanted) dissemination of data and (unauthorized) processing.

The proposed paper, starting from the technical consideration of the most used AI and data mining systems in the health sector, will analyze the risks and propose some of the possible solutions (technical and legal) for the protection of data in the processing activities.

István Borocz

The exposed psyche and the constitutional grounds of mind-reading

Novel technologies aim not only at passively 'reading' the human mind, but, building on the gathered information, actively affect and -presumably- enhance it. Hardware and software (such as computers, mobile phones, mobile applications, etc.) are currently the most prominent and straightforward tools for the 'enhancement' of the human mind, thanks to their unrestricted accessibility and effectiveness. Furthermore, various neuro-technologies are being used to study, map and interfere with the human brain, referred to as braincomputer interfaces (or BCIs)[1], which can "(1) detect brain activity directly, (2) provide feedback in real-time or near-time, (3) classify brain activity, and (4) provide feedback to the user that reflects whether she/he successfully attained a goal".[2] Combined with other techniques, these technologies are presented as able of deriving data from the human mind, but also actively or reactively interacting with it.

Such practices, in addition to potentially blurring the lines between Artificial Intelligence (AI) and the human brain, pose numerous ethical and legal challenges. From a legal perspective, concretely, they trigger the question of whether interference with the 'privacy of the mind' is permissible. So far the human brain and mind have remained mostly neglected, unexplored realities, and relatively obscure terms in the legal nomenclature and frameworks of both the Council of Europe and the European Union.

The goal of this contribution is to elaborate on the intrusiveness and, consequentially, the permissibility of brain-related data practices on the right to privacy (art. 8 of the European Convention on Human Rights, ECHR) in particular on the 'forum internum'[3]. Concerning the guarantees other relevant traditional values, such as human dignity or the right to personal fulfilment, art 8. can be understood as a subsidiary right,[4] invoking a two-tier approach. First, there

are the core values (i.e. human dignity or the forum internum) which enjoy absolute protection and second, the values which can be subject to interference. The contribution tackles such a legal question by examining how law interacts with science in defining mind reading, and proposes in this context a discussion of what is privacy of the mind and how it can be interpreted according to the ECHR and the jurisprudence of the European Court of Human Rights.

1Shih J J, Kursienski D J and Wolfpaw J R, 'Brain-Computer Interfaces in Medicine' (2012) Mayo Clinic Proceedings 87(3) 268–279, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3497935/

2 Burwell S, Sample M and Racine E, ' Ethical aspects of brain computer interfaces: a scoping review' (2017) BMC Medical Ethics 18(60) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5680604/

3 Taylor P M, UN and European Human Rights Law and Practice (Cambridge: Cambridge University Press, 2005)

4 Peters A, Altwicker T, Europäische Menschenrechtskonvention (Beck, 2012) p. 19

Liability v. Compliance in Engineering - Room 214

chaired by **Herbert Hrachovec, Andreas Kirchner**

Tomasz Pawłowski, Martyna Kusak

„Garbage in, garbage out" – role of quality of data in transparency of AI

Recent years have brought a universal call for development of baseline standards for ethical AI, chief among which is transparency in the context of AI explicability. This topic has been touched upon in various academic research and national strategies on AI. Its importance has also been underlined by EU High-Level Expert Group on AI, European Commission for the Efficiency of Justice and EU Agency for Fundamental Rights. Even though the topic concerned has already been spotlighted at the EU level, both the science and practitioners still struggle with the question on how to ensure AI transparency.

This research paper will contribute to the discussion on transparent AI in the EU linking it with the topic of data quality. The authors will verify how data quality requirements could impact on and enhance AI transparency. To that end it will be presented: 1) how far reaching are the current requirements of transparency of functioning of AI in the EU, 2) and what are the current and under-development requirements for quality of data used by decision-making involved AI in context of fault and bias elimination. By doing so the authors will refer to: 1) the EU legal framework dealing with the topic concerned: GDPR, "Police directive" and Regulation on free flow of non-personal data, investigating to which extent these legal acts could guarantee the quality of AI raw material, 2) as well as to various ethics guidelines concerning trustworthy AI with focus on data use and transparency

Andreas Kirchner

Is Compliance Professional? An Inadvertent Flaw in Collectively Developed Software

In the age of digitalization and automation, the number of cases where software caused harm to their users increases. Studying the role of moral responsibility in a field of software development in corporations is therefore a fruitful exercise to help individuals and corporations to avoid harm caused by software (developers) and its surroundings in future. The talk has a modest goal: to reveal some of the moral challenges in a fictionalized case study of a bank, who exposed sensitive customer information at large scale, because a team inadvertently introduced a software flaw while fixing another flaw.

The central claim of the talk is the following: software engineers in corporations carry the burden of frequently conflicting standards: the corporate code of conduct along with its corporate culture, and on the other hand the professional principles. Their assigned role in the company demands compliance, and their professional education demands adherence to best practices, code of ethics, and professional handling of problems. The corporate culture tends to shift to simple compliance. If the professional demands are accepted at all, they are subordinated to the interests of the company. Still, in many cases the professional demands are not completely prevented from being raised. An extra effort (not necessarily described in the job description) is required to give priority to those demands, as individuals and as a team.

Herbert Hrachovec

Collateral Damages in Internet Software Design

Liability for the use of man-made devices has been discussed since antiquity. Plutarch, in his „Life of Pericles" reports on a philosophical discussion of the following mishappening: "... a certain ath-lete had hit Epitimus the Pharsalian with a javelin, accidentally, and killed him, and Pericles, Xan-thippus said, squandered an entire day discussing with Protagoras whether it was the javelin, or rather the one who hurled it, or the judges of the contests, that ‚in the strictest sense' ought to be held responsible for the disaster." If an Athenian died by an instrumentality without direct human involvement a special court had to resolve the case.

The Internet abounds with examples of unforeseen and undesired consequences of software pro-gramming decisions. A recent case is Chris Wetherell's complaint about the retweet button he de-signed: "We might have just handed a 4-year-old a loaded weapon". (http://bit.ly/2zkZrIM) This presentation touches on a number of instances of this type of unpleasant surprises, starting with the omnipresent e- mail and hypertext protocols (SMTP and HTTP) and proceeding to Android librar-ies supplying Facebook with unauthorized background information. An attempt to classify the de-gree of personal and/or institutional responsibility for such developments is made. The talk con-cludes with a discussion of the philosophical grammar of the term „responsibility" in face of the challenges mentioned.

19:30	Conference dinner (upon a special registration - not included in the conference fee) - Restaurant Padowetz, Masarykova 34, Brno