Room 025

9:30 – 11:00 Parallel streams

International Internet Law – Room 025

chaired by **Dan Jerker B. Svantesson**

Dan Jerker B. Svantesson

Data localisation and sovereignty

"Our global Internet and world wide web are becoming less global and less worldwide. Calls for sovereignty are ubiquitous and come in many forms. Terms like 'data sovereignty' and 'digital sovereignty' are used without much apparent thought going into what such terms actually mean.

Data localisation is increasing in use and commentators typically seem to view it as all good or all bad with little room for nuances.

This paper considers the impact of data localization and the calls for sovereignty in the online landscape and seeks to place them within the framework of international law."

Anabela Susana de Sousa Gonçalves

Jurisdiction in cross-border infringement of personality rights

"The legal provision applicable to determine the court that has jurisdiction to decide claims regarding the cross-border infringement of personality rights is Article 7, Section 2, of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Article 7, Section 2, gives jurisdiction in non-contractual matters to the court of the place where the harmful event occurred or may occur. Called to interpret the concept of place of occurrence of the harmful event, the CJUE decided that the place where the harmful fact occurred or could occur simultaneously encompasses the place of the causal event, that is, the occurrence of the tort and the place of materialization of the damage, that is, the place of production of the damage.

However, the online infringement personality rights forced the CJUE to make a new interpretative effort, because the information that is placed online can be accessed in any country and the offenses that occur on the Internet can have a global reach and cause damage with greater geographical extension and repercussions in the legal sphere of the victim, especially due to the geographical relocation of users. The purpose of this presentation is to analyse the most recent cases of the CJUE regarding the cross-border infringement of personality rights."

Marek Swierczynski

Jurisdiction in Internet defamation lawsuits

In this presentation, I propose the introduction of a separate basis of jurisdiction for infringement of personal rights (including online defamation). The above proposal is directly inspired by the judgment C-800/19 of 21 June 2021 (hereinafter as the Mittelbayerischer judgment), in which the court, once again, referred to the concept of centre of vital interests formulated by in the eDate judgment for internet infringements. In the new judgment, the CJEU gravely misinterpreted both the scope of the Article 7(2) of Brussel I bis Regulation and the locus delicti being the connecting factor. The Court, once again, introduces new requirements and creates conceptual chaos. The solution to this problem will be to adopt an unambiguous and stable personal connecting factor that will not be subject to divergent interpretations by the Court, depending on the category of case. Indeed, the grounds for jurisdiction in the Brussels I bis Regulation should be expanded to include different types of torts. These provisions should be harmonized with the conflict of law provisions of the Rome II Regulation. Failure to amend the EU's jurisdictional rules will leave us with a growing state of uncertainty on the proper jurisdiction of the courts. Subsequent judgments of the CJEU will continue to surprise us as decisions of this Court seems to misplaced with regard to Internet infringements.

11:15 – 12:45 Parallel streams

Medical Data – Room 025

chaired by **Walter Hötzendorfer**

Kamil Szpyt

Civil liability for medical errors committed during cross-border telemedicine treatments

"Cross-border telemedicine is an area that has been developing intensively for several years. However, the outbreak of the COVID-19 pandemic and the subsequent closure of borders has undoubtedly accelerated this process and increased the importance of the procedures themselves. It has turned out that, in many cases, travelling to a neighbouring country for a long-planned specialist operation, which used to be easy, has now become impossible.

At the same time, it has turned out that, despite the importance of this issue, regulations in this area in many countries are really rudimentary. This causes many legal problems, particularly when a medical operation does not go as planned. This raises issues such as

(a) determining the law applicable to civil claims relating to medical errors committed during cross-border telemedicine procedures

(b) identifying the person responsible for the error.

The issue of who is responsible is further complicated when the operation was carried out by a device equipped with artificial intelligence. In this context, the recent proposals of the EU legislator to regulate the issues of liability for high-risk artificial intelligence seem to be totally unsuited to the specificities of telemedicine. It is precisely the above issues that are looked at in more detail in topic."

Federica Casarosa

Internet of Medical Things: is the EU legal framework effective to guarantee cybersecurity and data protection?

"Covid19 as a trigger for an enhanced used of technologies. Where direct contact was limited, if not prohibited, the availability of alternative means of contact through technology was exploited in all sectors. Health care is obviosly the sector experiencing most challenging times.

One of the most interesting applications was the use of IoT in medical sector or Internet of medical things (IoMT). IoMT was not unknown before, but the pandemics brought it in the spotlight offering several advantages as ragards contact tracing, coordination of treatment, and monitoring of the patients.

However, challenges and risks for security and privacy are still present both from external and internal factors. For instance, ransomware attacks, lack of standardization, malware altering medical data, battery draining attacks, loss of private medical information, lack of training and personnel competence are the most common security risks.

The paper will identify the legal framework applicable at EU level including not only the horizontal legislation, such as the General Data Protection Regulation – and the rules applicable to health data - and NIS Directive, but also sector specific legislation, such as the Medical device regulation. The analysis will allow to identify if and how the current legislative framework is able to provide effective solutions for the potential vulnerabilities of IoMT."

13:45 – 15:15 Parallel streams

" State of exception" , COVID style. Legal theory & IT implementation – Room 025

chaired by **Herbert Hrachovec, Andreas Kirchner**

Saisha Singh

Policing Using Technology During Covid–19: The Case of India

"The law enforcement agencies across the world, specifically the police forces, have found themselves acting as a vanguard, who stand at par with other groups and organizations, in the fight against a pandemic that has struck the world. Thus, COVID–19, standing as a foremost example of Public Health Emergency, has forced the law enforcement agencies to look out for new kinds of crimes, making use of technology, ushering in transformations to public perceptions regarding the police, among various other things.

This paper attempts to explore the status quo of the functioning of the police during the pandemic. It starts with introducing the role of police and transformations which have been witnessed during the times of this pandemic and takes into consideration specific practices across different countries and their ramifications on their respective demography. In the second part, the paper takes turn towards a specific case study, that is, of India. Towards the third part, the use of technology in policing is understood in a general manner, given that the same is still underdeveloped for different jurisdictions. In the final part of the paper, policing during pandemic and associated challenges are explored, which include behavioural aspects, as well as technological aspects in a brief manner. Proceeding in the direction of conclusion, the role of the police during a Public Health Emergency is summed up, and is contrasted with the role played by the public in this regard."

Herbert Hrachovec

The Fake Pandemic Emergency

The Covid 19 pandemic has led to administrative emergency measures worldwide. Those sanctions, limiting several well-established human rights, have in turn triggered significant non-violent as well as violent resistance. The Italian philosopher Giorgio Agamben was, from early on, one of its most vocal promotors. In "Homo Sacer" he conceptualized a permanent "state of exception" as the basic condition of the modern state. The aftermath of Covid 19 is, according to him, its consistent extension. Agamben's considerations hark back to Carl Schmitt, the controversial German constitutional scholar instrumental in legitimizing Hitler's regime change. The proposed talk will discuss the conceptual challenge to juridical thinking posed by legislation in cases of emergency and consider the arguments against restrictive state action put forward by deniers of the Covid 19 threat.

Andreas Kirchner

Privacy and Security in Covid Tracing Apps

The reaction to a global pandemic like the Covid-19 pandemic is an expression of it's time and place. Nearly every country in the world has come up with contract tracing software that runs on mobile devices and utilizes it's sensors (GPS / Bluetooth).

The degree in which privacy and security is built into the software depends on design, implementation, and testing of the contact tracing software (the professional engineering aspects),

but as well on the political, cultural, economical, and legal environment which shapes the development of the software. This talk consists of the following parts: (1) A description of an ""ideal"" contact tracing application with reference to earlier works from other researchers in 2020 and 2021. (2) A comparison between two existing and contrasting contact tracing software in India and Switzerland, that both inhert some properties from the ""ideal"" solution and have shortcomings as well. (3) Concluding thoughts of how these two solutions are embedded in specific cultural settings and contradictions and legal code with historic background.

15:30 – 17:00 Parallel streams

Law: Intellectual Property On-Line – Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Roman Bieda

AI system - the scope of the term and possibility of protection under intellectual property law

An ""AI system"" is defined as ""software"" in some of the earlier documents as well as in the draft of the regulation The Artificial Intelligence Act recently presented by the European Commission. Such understanding of an ""AI system"" prompts us to seek protection of an AI system as a work under copyright law. It also influences the contractual practice in respect of drafting contracts for the creation or implementation of an AI system.

Perceiving AI only as software is imprecise and may result in detrimental contractual practice.

In the process of machine learning, we must distinguish between an algorithm, a model, a model's parameters, a trained model and an entire AI system with an implemented trained AI model. In a business context, the software itself appears to be of secondary importance.

I will present a machine learning process on a specific example identifying its individual elements.

The individual elements of the machine learning process may constitute various intellectual property interests, protected under various intellectual property rights. I will define possibility of protection each of these elements under intellectual property rights.

This issue requires consideration in the process of preparing contracts for the creation and implementation of an AI system. The presentation will contain legal and technical issues.

Radim Charvát

Are Non-Fungible Tokens useful for Copyright Protection?

The NFT (""non-fungible token"") is one of the most significant phenomena in the world of blockchain at the moment, which surprisingly penetrates into the field of copyright. As a unique code associated with a digital version of a work of art, music file, written text, and other types of authorial works or other subject-matters, the NFT adds to the uniqueness of these digital versions while potentially increasing their value, in some cases astronomically. In this contribution, I will discuss especially the role of NFTs in the field of copyright, their nature and the advantages and disadvantages of their existence.

The NFT market has seen tremendous growth in recent times and therefore, I will discuss the uses of NFTs in relation to their potential to enhance the protection of authorial works through encryption in the blockchain. However, I will also try to outline the legal issues related to the use of these tokens, in particular the so-called NFT ""minting"" of works without the consent of the actual author or copyright holder. Last but not least, I will also look for an answer to the question whether non-fungible tokens are really non-fungible as an identifier of digital content. Attention will also be paid to other legal issues related to NFTs.

17:15 – 18:45 Parallel streams

Law: Intellectual Property On-Line – Room 025

chaired by **Andreas Wiebe, Matěj Myška**

Laura Grisales Rendón

Algorithmic transparency and trade secrets

With the popularization of algorithms and their potential impact on fundamental rights, algorithmic transparency seeks to avoid risks such as discrimination and invasion of privacy. However, there is a clash between protecting transparency and trade secrets, exacerbated by the fact that algorithms that influence everyday life are protected as trade secrets.

The EU Trade Secrets Directive protects algorithms owned by companies from any disclosure and does not directly consider algorithmic transparency. Although it appears that transparency and trade secret protection are entirely opposed, the Directive itself recognizes two scenarios in which trade secrets yield to the protection of transparency: an overriding public interest and the exercising of the right to freedom of expression and information.

Likewise, a consideration of both transparency and trade secrets is contained in the Platform-to-Business Regulation (P2B) and the General Data Protection Regulation (GDPR). The P2B Regulation obliges platforms to disclose the main programing parameters they employ while recognizing Union

competition law. The GDPR considers the freedom to conduct a business and poses the duty to avoid data subject's right of direct access to personal data affecting trade secrets.

Using a qualitative content analysis and empirical legal research methods, this paper analyze if clear explanations of algorithm's working parameters can provide algorithmic transparency while preserving trade secrecy.

Zoltán Gyurász

(Artificially) Intelligent Authors – Legal and Ethical challenges

Artificial intelligence is a new electricity, and it is difficult to imagine a sector that will not be transformed by it. Where a few decades ago only people could write poems, play chess or create innovations, today these tasks are commonly performed by artificial intelligence systems. These systems have revolutionized the way we work.

Recent patent applications, which identified AI systems as inventors, just as copyright cases for AI authors have accelerated the discussions about the extent to which and under what circumstances AI can create something new and original. However, this is not the first time that questions about AI have stirred up the debate in this way. More than 1.5 million scientific publications have been published on the topic of AI in the last 60 years. As it is well established already that AI disrupts our notions of traditional concepts of law and raises serious questions as to whether traditional forms of protection are still sufficient. Nevertheless, the automatization of the creative process falls into the field of legal science, which is very new. Therefore, it is appropriate to question whether the current legislation adequately addresses the scenarios in which AI systems create innovations and whether it can claim ownership of the created innovation.

In this paper, we shall look at the legal and ethical challenges of AI to the creative process, through analyzing the discissions of EPO , USPTO and UKIPO in the Dabus case. Then comparing them to the ruling in the ""Shenzhen Tencent Computer System Co., Ltd. v. Shanghai Yingxun Technology case. Posing the question of whether a normative system that is based on the idea that only natural persons can produce something new is appropriate in the age of AI.

Phillip Homar

Liability of Online-Platforms and Filehosting Services – Implications of the CJEU decision YouTube / Cyando

In June 2021, the CJEU has handed down its long-awaited decision in the case YouTube/Cyando (C-682/18 and C-683/18). The decision further develops the case-law on the right of communication to the public according to Art. 3 InfoSoc-Dir and clarifies the principles of liability of operators of user-upload-platforms (such as YouTube) and filehosting services (such as Google Drive, iCloud, Dropbox). Against this background, the presentation will analyze the implications of the decision: Specifically, it will be provide and overview if and under which conditions platform operators and filehosting services carry out an act of communication to the public, how this relates with the safe harbor provision of the ECommerce-Dir and to what extent the YouTube/Cyando decision will be relevant after the implementation of Art 17 of the DSM-Dir.

Room 030

9:30 – 11:00 Parallel streams

Law: Privacy and Personal Data – Room 030

chaired by **Jakub Míšek, Bettina Bacher**

Nina Gumzej

Challenges in the assessment of delisting requests in the aftermath of the GC and Others judgment (C-136/17)

In focus is analysis of the GC and Others judgment (C-136/17), which has despite its significance for the future evolution of RTBF in Europe so far not prompted such wide academic interest in comparison to the Google v. CNIL judgment rendered on the same day. An explanation will be made of the significant tailoring of data protection rules having been made in relation to sensitive data processing activities of search engine operators and of lacking repercussions for operators even where the very basic tenets of data protection law in that context were not observed. On the basis of the current GDPR, the presentation explores whether following the judgment the level of protection of data subjects has been changed. As I will argue, the judgment opens the door toward reconsideration of the role of original data publishers and of public interest in the required balancing between privacy and data protection rights of data subjects and the freedom of information of internet users. In that context one of the more important questions arising is on the level of involvement of original data publishers in examination of data delisting requests, without it jeopardizing one of the basic tenets of the right to delisting according to which it may be excercised regardless of actions taken for the purposes of removing published information directly at the source. Where the data were initially published for journalistic purposes, exploration is made of the common core laying behind the legal concepts of legitimate interest, compelling legitimate grounds, overriding legitimate grounds and substantial public interest in assessment of delisting requests, and brought into the context of operator's (Google's) declared compelling legitimate ground of public interest in accessing and imparting information. Namely, the latter might additionally to the

freedom of information of internet users also be interpreted to include the freedom of expression for publishers imparting information. In that context also discussed are Google's (currently challenged) practices of notifying publishers of delisted URLs and internal procedures according to which publishers may provide further relevant information and seek link restoring, which issue awaits resolution under the upcoming second part of EDPB RTBF Guidelines, and which might well receive its day before the CJEU in the future. The presentation ends with a discussion if examined developments affect the core of the RTBF with data protection legislation as the most proper venue for addressing delisting requests.

Céilan Hirsch

Be aware of the data breach notification

Article 33 par. 1 GDPR provides that "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." This legal duty to notify almost every personal data breach raises several issues and questions. I will focus on the main one: when does the 72-hour notice requirement start? The text says that the time period starts when the controller becomes "aware" of the data breach. According to the WP29, the controller is "aware" when he "has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." In its decision against Marriott, the Information Commissioner's Office had a different view and held that the controller becomes "aware" when he is "able reasonably to conclude that it is likely a personal data breach has occurred." Furthermore, in its decision against Twitter, the Irish Data Protection Commission that the time period starts when Twitter should have known that a data breach occurred, and not when it effectively became aware of it. The starting point of the 72-hour notice requirement has a very practical importance. For example, the Dutch Data Protection Authority recently imposed a fine of €475,000 on Booking.com for reporting a data breach 22 days too late. The main issue, in this case, was when Booking did become aware of the breach. My presentation will focus on what it means to become "aware" of a personal data breach, by analysing several examples and discussing the main issues therein. I will also discuss from a practical perspective how a controller may meet the burden of proof that it has timely satisfied the 72-hour notice requirement.

Jan Klouda

Privacy compliance in latest judicial practice

Laws and regulations define a strict privacy compliance regime. This regime stresses organizations and stimulates high value spend under the threat of excessive regulatory penalties. Privacy regulation nevertheless appeared to lag behind technology development and lacked realistic view of capabilities of both data processors and cyber attackers. Latest Supreme Court view underpins compliance best effort based principles and recognizes their relevance for privacy. Judicial practice thereby promises to contribute to closing gaps between intentions of legislators and business reality

Dániel Eszteri

Blockchain and AI: Connection two distinct technologies to comply GDPR's data protection by design principle

The aim of the analysis is to present some of the general principles of data protection law that can be applied to automated decision-making built on blockchain-based data processing in order to comply with the provision of the European Union's General Data Protection Regulation (GDPR). The analysis focuses on the applicability of the 'data protection by design' principle during the development of such systems. The hypothesis is that because blockchain-based networks are built on distributed data processing operations, therefore data controlling or processing of participating nodes should comply some abstract data protection patterns predetermined and collectively built-in during the system's development phase. For the sake of better understanding, I presented the human mind and its 'uploading' with conscious and unconscious contents as an analogy to blockchain-based AI systems. My goal is to highlight that the fusion of blockchain and machine learning-based AI can be a suitable technology to develop serious automated decision-making systems (so called 'distributed AI'). The compliance of these distributed AI systems with data protection law's principles is a key issue regarding the very serious risks posed by them.

11:15 – 12:45 Parallel streams

Law: Privacy and Personal Data – Room 030

chaired by **Jakub Míšek, Bettina Bacher**

Matúš Mesarčík

Transparency of remote biometric identification systems in the EU law: Solving the unresolved problem?

Remote biometrics and its use in public spaces are currently one of the most discussed topics due to the proposed legal framework on artificial intelligence in the European Union. Several non-governmental organizations openly critique insufficient regulation of remote biometrics AI systems (including facial recognition systems) especially concerning prohibiting such practices. Furthermore, the use of biometry and facial recognition systems is also the dominion of the EU data protection law represented by the General Data Protection Regulation.

The presentation aims to provide an overview of the positive side of remote biometric systems and their implications for risks. One of the greatest risks is the lack of transparency as public awareness may be hampered during the use of such systems. Several aspects of transparency are a significant

part of the principle of transparency in the General Data Protection Regulation with the proposal on the artificial intelligence act adding legal obligations in the area as well.

Firstly, remote biometric systems in public spaces (especially facial recognition systems) are analyzed from the perspective of risks and benefits. Secondly, a legal framework related to such AI systems is presented. Thirdly, a comparison with the use of CCTV systems and non-remote biometry is made and differences concerning transparency are conceptualized. Conclusions and recommendations are summarized at the end of the presentation.

Nimród Mike

Privacy Preserving Biometric Authentication (PPBA)

Fully homomorphic encryption (FHE) is considered an appropriate technical measure to ensure data security, as both the legal framework and the industry best practices are highlighting the need of encryption during the processing of personal data (while at rest or in motion). FHE enables protected queries to different services, where a server computes a succinct encrypted answer without looking at the query in the clear.

The proposed Privacy Preserving Biometrics Authentication (PPBA) mechanism combines encrypted face identification and personal ID recognition to identify a user without storing any sensitive information on the server side. The main value of this approach is in preserving privacy of user while processing the authentication data. With the proposed solution, the data stored at the cloud does not violate the privacy of a user and remain GDPR compliant.

PPBA is developed in a form of a smartphone plugin that uses biometric data in a privacy concerning manner, and a special cloud service dedicated for the operations over encrypted data for protecting the data from violating the privacy. The data flow describes the entire authentication process from user registration to login. The applied HE provides a layer of data security that enables full functionality of the solution, while still preserving user privacy. This is arguably what the full functionality principle of Privacy by Design aims to achieve – a design of positive-sum, not zero-sum.

Gergely László Szőke

Health Data & scientific research – how some 24-year-old national provisions may fit the GDPR

In the world of Big Data, the secondary use of personal data has become a key issue. This is also a vital question in the field of scientific research concerning health data – how the vast amount of data originally collected for providing health services can be used for scientific research?

In the last years, we've conducted a data protection impact assessment in Hungary to answer how a public university may use the health data collected by its clinical centre for scientific research. One of the biggest challenges was that actual anonymization is not possible in many cases. Another big challenge seemed to be the old Hungarian regulatory regime in this field. Is it possible that some 24-year-old provisions may fit into the regulatory system of the GDPR? Is it possible to turn to court in order to enforce access to patients' personal health data? And finally and more theoretically: may it happen that despite the intentions to unify data protection regulation at the European level, there may be some crucial fields where the role of the national rules plays a key role in answering some fundamental question, risking that national regimes may significantly vary?

My presentation intends to answer these questions.

Laura Słocka

Should we process neurodata based on data subject's consent? – validity of consent in neurotechnology on the ground of the GDPR.

Due to the dynamic development of neurotechnology a question about the currency of the European personal data protection system arises. In the light of neurorevolution neurodata as very sensitive brain data is not sufficiently protected by the GDPR. As a result of not qualifying all neurodata as special categories of personal data controllers have many possibilities to process them. In particular, the legal basis for the processing of neurodata, that do not directly fit into art. 9 sec. 1 of the GDPR, can simply be unlimited consent according to art. 6 sec. 1 let. a of the GDPR. Paradoxically although consent implements the individuals' will ideally, it creates the most threats to the individual and the entire society (e.g. behavioural profiles based on neurodata used during the election). For consent to be valid it must be freely given, specific, informed and unambiguous. The neurotechnology user can provide some information unconsciously or even against their will. It is practically impossible to indicate the full scope of all collected neurodata in advance, because a person is not able to fully control own brain activity, so data subject does not know what scope of data will be revealed. These currently irremovable problems raise doubts about the validity of consent as the legal basis for neurotechnology. Adopting an evolutionary interpretation of GDPR and implementing some legal restrictions on neurodata processing will be presented as a solution to neurosecurity problem.

13:45 – 15:15 Parallel streams

Law: Privacy and Personal Data – Room 030

chaired by **Jakub Míšek, Bettina Bacher**

Melchiorre Monaca, Angela Busacca

Social network Services are really free of charge? Brief reflection on Italian Council of State sentence n. 2631/2021

In March 2021, the Council of State (the highest body of Italian administrative justice) confirmed the judgment against Facebook, recognizing an unfair commercial practice to the detriment of

consumers for the indication "Facebook is free and always will be", because in reality consumers "pay" for FB services with their data which are used for profiling purposes.

The story originates from a sanctioning provision of the Italian Authority for Competition and the Market (AGCM) which in 2018 had imposed a fine of 5 million euros, sanctioning the social network membership form as an unfair practice; in the clauses of the form, users were informed of the free service, but not of the profiling (consequent to the authorization to personal data process activities) and of the use of the collected data for commercial purposes. According to the AGGM, this commercial use represents the consideration "paid" by consumers, since online advertising and marketing activities carried out due to profiling constitute 98% of Facebook's turnover.

Against the decision of the AGGM, FB had appealed to the Regional Administrative Court (TAR) in first instance and the Council of State (CdS) in second instance; both bodies of administrative justice have, however, confirmed the sanction and the qualification of unfair commercial practice for the accession clause.

Tihomir Katulić

Institutional and Systemic Challenges to Data Protection - Updating the National GDPR Implementation Act

Three and a half years of GDPR application are behind us and EU Member States have had varying degrees of success. Croatia, the newest EU Member State has had its own share of issues and problems apparent in the number of processed cases, issued fines and other corrective measures. At least some of those problems stem from unambitious provisions of the national application act, the Act on Implentation of the General Data Protection Regulation or from complete lack of there of, as the Act has notably missed the chance to regulate certain functions and offer additional mechanisms to ensure controller compliance, fine tune exceptions and limitations and fill out gaps left out by the EU legislators to ensure compatibility. The paper will explore the effect of its current provisions on various aspects of the national data protection system, the function of the supervisory body and the jucidial control of its decisions, present key statistics and offer various suggestions de lege ferenda.

Isadora Neroni Rezende

Purpose Limitation and Smart Cities: Investigating (In)Compatibility Scenarios in Public-Private Sector Interplays

With the AI and the IoT, cities are undergoing a process of digitization. Distributed networks of public and private actors are participating in this transformation, also collaborating through public-private partnerships (PPPs). The smart city paradigm relies on seamless data flows within urban infrastructure, ensuring the responsiveness of public services to citizens' needs and available resources. Data may also travel between different actors, whose interests and goals may vary greatly. In this perspective, the purposes of the data processing may suffer unforeseen changes, unbeknownst to data subjects.

Hence, this paper explores how the purpose limitation principle is affected by data practices in smart cities. Pervasive technologies are already putting this basic tenet of data protection law to the test. Also, the increasing diversity of public authorities and companies processing data in the city is only aggravating these issues. To better understand these hurdles, I firstly investigate the requirements of purpose limitation and compatibility as enshrined in EU data protection law. Secondly, I focus on the compatibility criterion to see how this applies in different interplays, possibly taking a PPP form: (i) public administration-private sector; (ii) private sector-law enforcement; (iii) law enforcement-public administration. Finally, from a governance perspective, I examine how the proposed Data Governance Act may further impact on the principle at hand in smart cities.

Attila Kiss

Position and tasks of a DPO – in theory and according to their self-assessments

GDPR seems to define the position and core tasks of a data protection officer (DPO), however the Article 29 Working party (WP243), the Dutch supervisory authority ("Positionering van de FG") and also a wide range of scholars (e.g. "The DPO Handbook" by Douwe Korff and Marie Georges) felt it important to clarify on the responsibilities of and suggested practices for a data protection officer. In 2019 and 2020 the author of the abstract was responsible for organizing the Annual Conference of DPOs notified to the Hungarian Data Protection Authority and was curious how well DPOs can fulfil their mandates in reality. Therefore all DPOs notified to the authority were invited to submit an online anonym self-assessment on their skills and on performing their duties previous to the conferences. GDPR Art. 38-39 as understood by experts and data protection authorities will be compared to two years' results of the online surveys, and potential reasons behind the results will be analysed during the presentation.

Room 034

9:30 – 11:00 Parallel streams

Psychology of Cyberspace – Room 034

chaired by **David Šmahel, Hana Macháčková**

Nino Gugshvili, Karin Täht, Dmitri Rozgonjuk, Maris Raudlam, Robert AC Ruiter, Philippe Verduyn

Two Dimensions of Problematic Smartphone Use Mediate the Relationship Between Fear of Missing Out and Emotional Well-Being

t has been shown that both fear of missing out (FoMO) and problematic (i.e., excessive) smartphone use (PSU) are negatively associated with indicators of emotional well-being. Moreover, FoMO has been found to be a key predictor of PSU. This suggests that PSU may mediate the relation between FoMO and decreased emotional well-being but this pathway has never been tested. Moreover, in most studies on PSU, the multidimensional nature of this construct has been ignored. The aim of the present study was to address these gaps by directly testing the mediating role of (subdimensions of) PSU in the association between FoMO and emotional well-being. We conducted a cross-sectional study with Estonian participants (n = 426). Using a simple mediation analysis, we found that PSU partially mediated the relationship between FoMO and decreased emotional well-being. Using a parallel mediation analysis, we found that two specific dimensions of PSU were significant mediators of the relationship between FoMO and decreased emotional well-being: Cyberspace-oriented Relations and Physical Symptoms. This suggests that the negative relationship between FoMO and decreased emotional well-being is due to FoMO stimulating (a) online relationships at the cost of offline interactions and (b) Physical symptoms associated with excessive smartphone use. Overall, this study provides a fine-grained analysis of the relationship between FoMO, PSU and emotional well-being.

Tsameret Ricon, Michal Dolev Cohen

Young Adults sexts (YA's)- A correlation between Sexting use, Moral judgment and Emotional regulation.

Sexting is a prevalent behavior among Young Adults (18-25). Findings suggested that sexting is most often a reciprocal behavior and that most young men and women report sharing sexts within a dating relationship.

The purpose of the current study was to profile this age group in terms of sexting use and its relation to moral judgement, emotional regulation and empathy. Literature suggests that YA's tend to engage in a risky behavior due to their under developed impulse control and are being judged unfairly for lack of moral values and empathy.

682 Israeli's young (18-25) have participated in this research (M=22.44, SD= 2.04). Most of them were single (88%) and living with their parents. Half of them (55.5%) were in intimate relationships. All participates were ask to complete a scale of sexting use, empathy, moral judgement and emotion regulation questioners.

Results showed that 43.4% of the total group of YAs' were sexting. 45.9% of the group had sent sexts. 47.9% of them received sexts. Significant positive correlations were found between sexting and difficulties in emotional regulation and Self-interest judgement. Negative correlations were found between sexting behavior and Humane/ethical judgement. The later was also positively correlated with empathy and negatively correlated with emotional clarity. Findings provide further understanding and knowledge of this interesting group emphasizing the importance of ability of emotional competence.

Michal Dolev Cohen, Tsameret Ricon

Modern talking: Parent-child dysfunctional communication about sexting

Sexting (sending and receiving sexual messages) could entail risk for adolescent users; hence, it is important that parents are able to address their children's sexuality and mediate to them the implications of sexting. The goal of the current study was to identify parental factors that lead to dysfunctional communication about sexting among 427 parents of Israeli adolescents (ages 10–18) and to determine whether parents' perceived severity of sexting and perceived susceptibility of sexting function as mediating factors. Parents completed a set of questionnaires online. Findings indicated that of the parenting styles examined, authoritarian and permissive styles were positively associated with dysfunctional parent-child communication. Authoritative style was inversely related to dysfunctional communication and was mediated by positive attitudes regarding sex education. Additionally, authoritative parents were capable of assessing the severity and susceptibility of their children's sexting activities. It appears that the quality of the discussion initiated by authoritative parents enabled them to be aware of adolescent behaviors and phenomena and to modulate their communication about the implied risks. Findings suggest that perceiving the implications of sexting as too risky diminishes parents' ability to conduct a high-quality discussion. In conclusion, parents need to mediate and conduct constructive discussions with their children.

Ugnė Paluckaitė, Kristina Žardeckaitė-Matulaitienė

Adolescents' intention and willingness to engage in photo disclosure on social networking sites: the comparison of neutral and problematic photo disclosure

Nowadays sharing photos online is one of the most popular activities among adolescents on social networking sites (SNS). However, not every kind of photo disclosure on SNS can be called as risky or problematic. Thus, the aim of this study is to compare how Prototype Willingness Model (PWM) explains adolescents' intention and willingness to engage in neutral and problematic photo disclosure on SNS. To reach this aim, the quantitative study using random sampling was organized (N=444; Mage=14.65, SDage=1.36; 56.9% female). Students were asked to fill in the questionnaires, assessing the factors of reasoned (intention) and reactive (willingness) pathways of the PWM. Structural equitation modeling (SEM) has been used separately for neutral and problematic photo disclosure. The results of the hypothesized models showed an acceptable fit for neutral (χ^2= 588.85 (404), p<.001; RMSEA=.029 [.024; .034], CFI=.976, TLI=.971) and problematic (χ^2= 1127.63 (691),

p<.001; RMSEA=.034 [.031; .038], CFI=.961, TLI=.956) photo disclosure. According to the results, adolescents' neutral photo disclosure on SNS is better explained by the factors of reasoned pathway (intention R^2=.45) than the reactive pathway (willingness R^2=.24); problematic photo disclosure on SNS is well explained by both, the factors of reasoned pathway (intention R^2=.61) and the reactive pathway (willingness R^2=.54). Thus, it is possible to state that adolescents' photo disclosure on SNS differs by its content.

11:15 – 12:45 Parallel streams

Psychology of Cyberspace – Room 034

chaired by **David Šmahel, Hana Macháčková**

Lucija Vejmelka, Miroslav Rajter, Roberta Matković

Impact Of Covid 19 At Online Behaviours Of Croatian Adolescents: Research Of Internet Habits And Cyberbullying

The Internet activities of adolescents came into focus given the increased use of intent during the COVID 19 epidemic. Adolescents realize their informational, social, emotional and other needs through digital tools and online communication become normative standard of their generation. Although some research confirms the positive impact of online communication and social networks on various aspects of their lives, the online environment is a setting for problematic Internet use, including cyberbullying. Institute of Public Health of Split-Dalmatia County conducted a quantitative online survey of internet habits and problematic internet use in 2 waves 2017 (N=822) and 2020 (N=424) with adolescents from 12-18. Research followed ethical standards of research with children. A questionnaire of sociodemographic characteristics of the child and parental supervision during internet use were constructed. A questionnaire on children's online activities based on LaRose and Tsai and standardized instrument- ECIPQ to measure the cyberbullying were used. Categories of cyberbullying perpetration and vicitimization and their comparation on the first and second research wave during the actual pandemic. The results of the research are important for understanding the impact of the covid 19 pandemic on the problematic use of the Internet, especially cyberbullying. Research Will provide insight of the protection potential of parental control in children's participation in cyberbullying.

Jana Blahošová, Michal Tkaczyk, David Šmahel

Gender differences in online conversation topics and self-disclosure: Content analysis of Czech adolescents´ instant messaging conversations

Although lot of studies examined gender differences in online self-disclosure of adolescents and topics of their online posts, most of them focused on publicly available content (i.e. discussion forums) and provided inconsistent results. This paper examined gender differences in 2,022 authentic online conversations from Messenger provided by 22 adolescents aged from 13 to 17 years. Using quantitative content analysis, the text was coded for topics and frequency of self-disclosive utterances along with depth and breadth dimensions of self-disclosure by two coders. The results showed that discussion topics differed by gender of participants in the conversation. Boys conversed more about friends, classmates, public issues and playing online and offline games. On the other hand, girls talked more frequently about romantic or sexual partners, family members, and school. In the case of self-disclosure, there was not a difference in frequency of self-disclosive utterances, but these utterances differed by gender within the depth and breadth dimensions; boys shared more information without emotional or evaluative aspects, whereas girls disclosed facts together with their emotions, opinions or wishes more than boys. The results also suggest the importance of the gender of the conversational partner in self-disclosure, because girls were more self-disclosive in the company of other girls whereas boys´ self-disclosure did not change according to gender of the conversation partner.

David Lacko, Hana Machačková

The Influence of Online Advertising on Adolescents' Perceived Credibility of Information Related to the Fitness/Dietary Supplements

Most adolescents seek health-related information online. However, such information is often written in the form of an advertisement presenting products that could jeopardize their health. Furthermore, modern ads may tend to conceal their real purpose which makes their recognition much harder (i.e., native ads). The perceived credibility of such advertised information by adolescents might have an impact on their buy intentions and usage of potentially noxious products. The aim of the research is, therefore, to examine the influence of advertising on the perceived credibility of online information, especially fitness-related products and dietary supplements. We present a pre-registered experiment on 681 Czech adolescents. Participants were randomly split into three groups. Each group was exposed to a fictional website that contained a banner ad, a native ad, or did not contain any ad. Results suggest that the presence of an ad on a website decreases the perceived credibility of the information. Specifically, native ads decreased it for girls, whereas banner ads decreased it for boys. There was no difference between younger and older adolescents, nor a difference between banner and native ads. Adolescents were generally successful in identifying both kinds of ads and they showed rather low purchase intentions for the advertised products. The potential implications of our findings for adolescents and their parents will be discussed.

Hana Drtilová, David Šmahel, Martina Šmahelová

Advantages and Disadvantages of Internet Use: The Perspective of Women with Eating Disorders Experience

Even though the internet is a common source of information and treatment for people with eating disorder (ED) experience (Peebles et al., 2012), the motives for illness-related searches have rarely been investigated beyond the perceived negatives. This study explores how women with ED experience reflect upon the advantages and disadvantages of their ED-related internet use. We expand the framework of the Uses and Gratifications Theory (U&G) into the context of users with ED experience through 30 semi-structured interviews with women with ED experience, aged 16 to 28, who live in the Czech Republic. Thematic analysis revealed four themes related to the pros and cons of their internet usage: ED-related Information Content; Internet Features Important to Users; Body Image; and Social Interaction. The results challenge the binary view of ED-related internet use and question some presumptions of U&G Theory within the specific context of users with ED experience.

13:45 – 15:15 Parallel streams

Psychology of Cyberspace – Room 034

chaired by **David Šmahel, Hana Macháčková**

Hayriye Gulec, Nikol Kvardová, David Šmahel

The Roles of Trust, E-health Literacy and Parental Influence in Online Health Information-Seeking Behaviors of Adolescents

Seeking health information online is prevalent among adolescents. Yet, there is limited evidence on the characteristics of youth that are associated with online health information-seeking behaviors. Furthermore, the role of parental factors has been mostly a neglected topic in the field. The current study aimed at evaluating adolescent and parental characteristics together in explaining the online health information-seeking behaviors of adolescents. The adolescent characteristics included the level of e-health literacy and trust in online health information. The frequency of online health information-seeking and e-health literacy mediation reported by parents were the parental variables. Health information websites were separated based on their content and the analyses were conducted separately for the websites that contained information about diseases (Covid-19, other diseases, and medications) and the websites that contained information about promoting health (diets, weight loss, and exercise). Czech adolescents (N= 1530; 50% girls) aged 13-18 and their parents (64% women) participated in the study and completed the respective online questionnaires relating to the study variables. The data were collected in 2020 as a part of the FUTURE project: Modelling the future: Understanding the impact of technology on adolescents' well-being (GX19-27828X). The proposed models were estimated using Structural Equation Modeling with Robust Maximum Likelihood estimator. The fit indices were within the acceptable range for disease-related (CFI= 0.95; TLI= 0.94; RMSEA= 0.04 [0.040-0.048]) and health-promoting websites (CFI= 0.95; TLI= 0.94; RMSEA= 0.04 [0.039-0.048]). Consistent with the hypotheses, adolescents' level of e-health literacy and trust in online health information and the frequency of parental online health information-seeking and e-health literacy mediation were positively associated with online health information seeking behaviors of adolescents. The presentation will introduce the suggested models and summarize the preliminary findings related to the direction and magnitude of the associations between adolescent and parental characteristics.

Visu-Petra, Silvia Bocăneț, Vlad I. Bocăneț, Mateja Radojković

Individual Predictors Of Identity Theft In Social Media: Attitudes Towards Lies, Impression Management Strategies And High Callous Unemotional Traits

Our study explored the individual differences (attitudes toward lies, impression management strategies, and callous unemotional traits) which could underpin the likelihood of being a victim or a perpetrator in the online world. The types of minor offenses we investigated are various forms of identity theft in the online environment. The target group were students – Computer Science (37.5%), Economics (29%), or Social sciences (mainly Psychology, 19.5%) or university graduates who filled in online questionnaires through Google Forms (N = 389): the Impression Management (IM) (Paulhus, 1991) scale, Lie Acceptability Scale (Oliveira & Levine, 2008), Inventory of Callous-Unemotional Traits (ICU) (Frick, 2004), and Online Identity Theft Questionnaire, a novel questionnaire we developed to measure the likelihood of becoming a victim, a perpetrator and the perception of identity theft online crimes. Results confirmed that people who considered lies more acceptable committed more social media identity theft crimes. Also they perceived such offenses as less severe and had moderately higher calousness levels. However, they reported lower levels of Impression Management strategies, designed to tap purposeful tailoring of responses to impress an audience. Implications for identifying and preventing online identity theft are discussed.

Michal Božík, Kateřina Lukavská, Jaroslav Vacek, Ondřej Hrabec, Michaela Slussareff, Martina Píšová, David Kocourek, Lucie Svobodová, Roman Gabrhelík

Measuring parental behavior towards child's use of media and screen-devices: the development and psychometrical properties of Media Parenting Scale for Parents of School-aged Children

Children's excessive screen use is associated with health risks such as obesity, sleep problems, attention problems and others. The effect of parental regulative efforts focused on screen/media use (media parenting) is currently unclear and difficult to examine given the het-erogeneity of measuring tools used for its assessment. We aimed to develop an inventory that would enable reliable and valid measurement of media parenting practices (especially active and restrictive

mediation) in parents of primary school children. The inventory builds on the existing tools, it is comprehensive, yet easy to use in research setting. The original MEPA-36 (36 items) and revised MEPA-20 (20 items) inventories were examined using data from 341 Czech and Slovak parents of children aged between 6 and 10 years. Psychometrical properties were es-timated using confirmatory factor analysis and reliability analysis. Model fit was better for MEPA-20 and similar to other currently available tools. Both active and restrictive mediation subscales showed high internal consistency. The internal consistency of newly constructed risky mediation subscales (risky active, risky restrictive and over-protective mediation) was low. MEPA-20, especially active and restrictive mediation subscales, can be recommended for re-search on media parenting in context of screen / media use of school-aged children.

Martina Píšová, Kateřina Lukavská, Jaroslav Vacek, Ondřej Hrabec, Michal Božík, Michaela Slussareff, David Kocourek, Lucie Svobodová, Roman Gabrhelík

The impact of parental Technoference on child use of screens

Abstract: The term ""Technoference"" means inattentional behavior from a person, who is looking to the screen instead of to the other participants of communication. The answers of ""technoferent"" person are often short and without any interest about the others. This behavior is source of negative feelings (frustration and resignation on the next questions) in the opposit site of comunication. Relationship between these two persons is impaired and the positive aspects of deep comunication face to face are lost.

This theme is focused on Technoference in parent-child relationship, and we would like to examine these questions: 1) Is there an association between parental Technoference and parent use of screens? 2) Is there a positive association between parental Technoference and child use of screens increase too? For answering these questions, we analysed data from 341 Czech and Slovak parents of children aged between 6 and 10 years.

Our results suggest, that there is a relationship between parent Technoference and their amount use of screens and children use of screens is associated with parent Technoference too. In our next research we would like to focused on the impact of parental Technoference in different child age categories.

15:30 – 17:00 Parallel streams

Legal Informatics – Room 034

chaired by **Erich Schweighofer, Jakub Harašta**

Adrienn Lukacs

Artificial intelligence and anti-discrimination: towards equality during recruitment?

Technological development is fundamentally defining our everyday lives in the 21st century - and the world of work is no exception. These innovations also gain ground in the recruitment process. Algorithms and artificial intelligence are more and more commonly used in the employment context. For example, a robot called Tengai, began testing in 2019 with the purpose to conduct interviews without bias. Another robot, Vera was created in 2016. Vera uses AI-based software technology to recruit and select candidates: it can even conduct a video interview with the candidate.

One of the challenges that arises with HR professionals is that prejudices or bias can also – either consciously or subconsciously – influence the decision making. In such cases, protected characteristics also play a role in judging the candidate – violating his/her right to equal treatment. The application of algorithms might provide a solution and can contribute to guarantee anti-discrimination. However, the application of an algorithm alone is not a guarantee of equal treatment, such a system must meet strict conditions.

The presentation examines whether the use of algorithms raises new types of questions in the field of anti-discrimination? Can discrimination occur when an algorithm is used? What rights do individuals have if an algorithm makes the decision in the recruitment process? The presentation covers these issues, with special regard to the right to equal treatment and Article 22 of the GDPR.

Tereza Novotná

Multilayered application of different court decisions retrieval methods and their evaluation

The Czech Supreme Court produces approximately between 6 and 7 thousand decisions every year. These decisions are available through the search interface of the Supreme Court website, which doesn't offer many search options and methods. Therefore, these decisions are nowadays still mostly processed manually by lawyers, judges, assistants or academics. The author of this presentation applies different NLP methods to Czech Supreme Court decisions in ongoing research to discover whether these methods are suitable for practical use during a court decisions retrieval. To answer this research question, all the methods experimentally applied are evaluated by a group of Czech lawyers and judges to assess their precision and efficiency.

In a previous phase of research, topic modelling, citation analysis and doc2vec method were used for the processing of Czech Supreme Court decisions. These three methods were evaluated by a group of lawyers and the doc2vec model retrieving semantically similar decisions was the most precise according to this group. Subsequently, the doc2vec model was applied in a combination with two other methods to discover whether this multi-layered application of methods may lead to more precise results in court decisions retrieval. Results of multilayered application of methods are again evaluated by a group of lawyers and they are compared to the results in previous research.

Angela Bussaca, Melchiorre Monaca

Using AI for justice: principles and criteria of EU "Ethics Charter on the use of AI in judicial systems

Combined use of AI and Big Data makes it possible to apply automatic decision-making in the public administration. The debate is focused on the possibility of using algorithmic decisions also in administration of justice: the use of algorithms capable of choices would overcame the (propensity for) typical human-decision errors, in favor of the more certain (on paper) efficiency of algorithmic decisions. The creation of a predictive justice system raises doubts especially in consideration of factors that could alter the algorithmic logic, e.g. the quality of data and the possibility of system error. With reference to risks of the use of AI for justice purposes, in December 2018, the EU Commission for the Efficiency of Justice adopted the "Ethics Charter on the use of AI in judicial systems and in related areas" that identifies 5 fundamental principles that can guarantee its efficient use (respect for fundamental rights / non-discrimination / quality and safety / transparency - impartiality in data processing/ possibility of control by the user).

The proposed paper, after a brief survey of the critical aspects of the use of AI systems and an analysis of the contents of the EU Ethics Charter, will focus on the possibility of using AI for forecasting and non-decisional purposes, highlighting how the forecasting method it can optimize use, especially in civil law systems.

Room 038

9:30 – 11:00 Parallel streams

Internet and Society – Room 038

chaired by **Jakub Macek, Iveta Jansová**

Kinga Sorbán

The regulation of pornographic content in Europe – is the current law fit to tackle contemporary issues?

The popularity of social media resulted in an enormous amount of user-generated content being shared online every day. Several genres of user-generated content exist, ranging from travel vlogs to explicitly sexual material. Some these content are fun and completely harmless, while others are detrimental to certain individuals and to society (such as the non-consensual distribution of sexual content). This paper focuses on the regulation of harmful sexual content, which is a complex issue. This can be illustrated by the fact that it can be examined from three distinct legal perspectives: the online publication of sexual content can be viewed from a constitutional, a content regulation and a criminal point of view.

The aim of this paper is to explore how the contemporary issues related to pornographic content can be tackled by regulatory initiatives, taking into account the existing measures to restrict the publication of sexual content. In this context the main aim of the article is to discuss the obligations of online platforms as they relate to the restriction of sexual content. As such the paper's goal is to identify the issues that platform providers face when it comes to the moderation of these works. By exploring the current regulatory background of the dissemination of pornographic material the paper will highlight why it is unfit to for facing new threats of this nature on the internet.

Thomas Roessing, Jakob Henke, Lisa Barbara König, Nils Makritzki, Hannah Schmidt, Michael Steinbrecher

Journalists and digital media – the case of Germany

The Internet, and social media in particular, has become an important platform for communication and information for people everywhere. Digital technologies also influence and transform the work of journalists, in traditional mass media as well as in online journalism. As part of a multi perspective study on journalism, politics and the public in Germany, we researched the relationship between journalists and digital communication. Research questions include: (1) How important find journalists digital technologies for their profession? (2) Do journalists use social media for journalistic research? (3) Do journalists trust social media as a source?

752 journalists from a wide variety of media outlets responded to our online questionnaire. Results indicate that four out of five journalists expect social media to be important for the future of journalism. 86 percent expect this for knowledge of technology among journalists. Most journalists use social media for journalistic purposes on a regular basis. In general, journalists do not trust social media often, but those who use social media frequently tend to trust it more than those who use it infrequently. Additional findings indicate that most journalists are not very fond of robotic journalism (automatic generation of content). Bosses are much fonder of robotic journalism, than simple reporters and freelancers. Eventually, the paper discusses the relevance of the findings for the future of journalism in Germany, and beyond.

Jisang Lee, Dongjoo Choi, Wongi Choi, Gyungsang Lee, Hyungyung Kim, Jaehee Kim, Bongeon Seo, Sujin Han, Jongik Lee, Juhan Park,

A Study on Policy and Practical Implications for Prevention of Youth Cyber Violence

The purpose of this study is to render policy suggestions at multiple dimensions to contain and prevent the recently evolving problem of youth cyber violence.

Hyunkyu Lee, Sunyoung Lee, Yeojin Kim, Jiwon Choi

With this research objective in mind, and through a meta-analysis on resources from both inside and outside of South Korea, the followings are the conclusive policy recommendations:

First, the reestablishment of the concept of cyber violence in the related laws and legal and institutional strategies to effectively address the punishment on offenders and the support for the victims are necessary.

Second, the use of online non-face-to-face methods such as big data technology and AI in encumbering cyber violence must be considered.

Third, the current preventive education of cyber violence must be adjusted at a policy level to fully capture its evolved form today.

Fourth, through the action plans which entail connecting to the adolescents out in schools and working with them, the prevention of youth cyber violence and the promotion of violence-free culture ought to be precipitated.

Lastly, the establishment of an international community for eradicating the global youth cyber violence problem is necessitated.

11:15 – 12:45 Parallel streams

Internet and Society – Room 038

chaired by **Jakub Macek, Iveta Jansová**

Christine Trültzsch-Wijnen, Ana Jorge, Ranjana Das

The Role of Digital Media in Parent Networks

Lots of research has been conducted on how young people grow up with ICTs. Less is known about how ICTs shape networking among parents. Whilst there has been a proliferation of both formal and often conflicting parenting advice online, an increasing reliance on technology for schools and parents to communicate, and numerous apps and platforms for parents to connect informally, we do not know enough about the diversity, difference, exclusivities and marginalities that these mediated connections produce and maintain.

We conducted a qual. pilot study in 3 European countries (UK/PT/AT). In each we conducted 4 interviews with families that were selected on the principle of constructing the most heterogeneity (number/age of children, SES, type of family, migration status etc.) resulting in a sample of 12 families. The focus of our research was on how structural/cultural factors shape the role ICTs play in the production and maintenance of parent networks but also on how digital networking among parents influences the handling of crucible moments in family live and in the context of developmental and educational challenges. The interviews were conducted in June/July 2021. Our preliminary analysis shows the juxtaposition of offline and online networks which often accentuates the processes of family's social (dis)integration. We will present this and results of further analysis and discuss the implication of our results for further research.

Sascha Trültzsch-Wijnen

Children's use of digital media during covid-19 in Austria and across Europe: Results of the European research project KiDiCoTi

The Covid-19 crisis had serious impacts on all parts of everyday life, also for families with minors: With closing schools and switching to remote schooling without proper preparation for teachers, pupils and parents. The project "Digital Lives of Kids during Covid 19 times" included teams from 11 European countries and conducted a representative quantitative survey (CAWI) with regard to the impact on digital media usage of children and parents' challenges during this time. The study included families with children aged 10-18 (both 6495 parents and children). This presentation will – starting from the Austrian case – outline selected findings in a comparative European perspective. We will discuss the use of digital media for leisure activities as well as home office and remote schooling including potential risks and opportunities and also parental mediation strategies. Starting from a perspective on Austria we will show differences between European countries and discuss possible reasons for different strategies of remote schooling as well as parental mediation in order to outline best practise examples and to present recommendations for stakeholders in the context of the European Union Strategy for a Better Internet for Children (COM 2012).

Marie Oldfield, Ella Haig

Belief Systems and Cyber Security

Artificial Intelligence is becoming widespread and as we continue ask 'can we implement this' we neglect to ask 'should we implement this'. There are various frameworks and conceptual journeys one should take to ensure a robust AI product; context is one of the vital parts of this. AI is now expected to make decisions, from deciding who gets a credit card to cancer diagnosis. These decisions affect most, if not all, of society. As developers if we do not understand or use fundamental modelling principles then we can cause real harm to society. Recently more serious effects of AI have been observed. Dehumanisation is the human reaction to overused anthropomorphism and lack of social contact caused by excessive interaction with, or addiction to, technology. This can cause humans to devalue technology and to devalue other humans. This is a contradiction of the use of 'social robots' and 'chatbots', indicating that the negative effects of this technology would outweigh any perceived positive effects. Also, within cyberspace, anthropomorphism and similar techniques based on deep philosophical principles can, and are, being used to alter the behaviour of humans. These techniques are used to manipulate human behaviours at a basic level in the human mind. As

these types of techniques are becoming more widespread, it is clear that we are entering unchartered territory that holds a vast array of consequences for society.

13:45 – 15:15 Parallel streams

Law: Cybersecurity, Cyber-Warfare – Room 038

chaired by **Václav Stupka**

Jarosław Greser

Cybersecurity of medical AI systems

The development of the internet has led to the emergence of new modes of providing medical services. One of the most dynamically developing technologies is artificial intelligence (AI), which supports medical professionals as they interpret results, select diagnostic methods or develop disease progression models.

The foreseeability and correctness of diagnosis provided by artificial intelligence algorithms depends on its cybersecurity. The main cybersecurity weakness related to this technology are attacks on the reliability and integrity of the data used to train algorithms and then make decisions. Data poisoning and adversarial attacks are particular threats. In the case of medical systems, an attack can result in the deterioration of a patient's health or lead to death, and it can also cause huge social costs such as undermining confidence in health systems. For this reason, they can be used as a tool both for terrorist attacks and for operations by hostile states aimed at destabilising the situation in other countries.

This presentation aims to illustrate regulations that govern the cybersecurity of medical AI. In particular, I will focus on the provisions set out in:

1.Proposal for the EU Artificial Intelligence Act, 2.Regulation 2017/745 on medical devices, 3.NIS Directive and proposal for NIS 2 Directive

Tamas Szadeczky, Zsolt Bederna, Zoltan Rajnai

Strategic analysis of cybersecurity incidents

In the current social and economic processes, information and communication services play a decisive role, changing several entities' operations. The growing dependence that has developed over the last two decades made the security needs introduced political will, which has resulted in an iterative evolution of the regulatory environment. Hence, the legal framework requires that several entities develop protection that includes controls enhancing both preventive and reactive in a risk-proportionate manner under the business value to be protected. Nevertheless, due to the nature of cybersecurity, the development of such capabilities is not the task of a single organisation but all entities involved in cyberspace, including, e.g., individuals, non-profit and for-profit organisations, public sector actors. Therefore, each involved entity should design protection capabilities in a risk-proportionate manner, which requires strategic approaches and tools and requires organisations to learn from security incidents. This paper reviews the essential formal security strategy formulation tools, applying Facebook's case based on publicly available information. The analysis aims to confirm the importance of management's attitude and support for tackling cybersecurity's challenges.

Nynke Vellinga

The EU Legal Framework on Cybersecurity in Vehicles: Beyond Technical Vehicle Regulations

As a 2015 Jeep Cherokee hack illustrated, cybersecurity has become of great importance to road safety. A hacked vehicle can pose a great danger to those inside and outside the vehicle, as a hacked vehicle could potentially turn into a murder weapon or could be used in a terrorist attack. Especially when multiple vehicles are hacked at once, there is the potential to disrupt society by, for instance, blocking important roads into a city.

These cybersecurity risks have been acknowledged by the United Nations' World Forum for Harmonization of Vehicle Regulations, which recently adopted two new UN Regulations aimed at increasing the cybersecurity of vehicles. These UN Regulations No. 155 and No. 156 focus on keeping the vehicle's system safe by keeping hackers out and on increasing the security of the process of updating the vehicle's software.

In addition, the existing EU legal framework can contribute to increasing vehicles' cybersecurity. This goes beyond the traditional vehicle legislation of the Type-approval Regulation (2018/286) and the General Safety Regulation (2019/2144). Other EU legislation, such as the Product Liability Directive (85/374/EEC) and Directive 2019/771 on contracts for the sale of goods, are all relevant to the cybersecurity of vehicles. The importance of these and other EU legislation will be outlined in this contribution, which will lead to the identification of legal lacunas as well as a proposed way forward to ensure vehicle cybersecurity.

Jozef Andraško

Proposal for a NIS 2 Directive. A step forward?

NIS Directive as the EU's first cross-cutting regulatory tool in the area of cybersecurity has proven its limitations and has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. The low level of cyber resilience of businesses operating in the EU, the inconsistent resilience across Member States and sectors and the low level of joint situational awareness and lack of joint crisis response are the main issues

identified by the evaluation on the functioning of the NIS Directive, conducted for the purposes of the Impact Assessment. Proposal for a NIS 2 Directive aims at elimination aforementioned issues.

First of all, the author focuses on new categories of entities falling within the scope of the NIS 2 Directive, in particular essential and important entities. The author will compare the identification process used in NIS Directive with a uniform criterion that determines the entities falling within the scope of application of NIS 2 Directive (size-cap rule).

Secondly, the author will compare the scope of risk management requirements and reporting obligations applied in NIS 2 Directive with risk management requirements and reporting obligations applied in NIS Directive.

Last but not least, the author deals with competent authorities' new supervision powers as well as new administrative sanctions for breach of the cybersecurity risk management and reporting obligations that can be applied.

15:30 – 17:00 Parallel streams

Law: Cybersecurity, Cyber-Warfare – Room 038

chaired by **Václav Stupka**

Jakub Vostoupal

The legal aspect of cyber-attribution: Dead or alive?

Who's to blame? A simple question, yet as old as humanity itself. It is an essential part of interpersonal relations, yet it is often referred to in the literature as an insurmountable problem connected with cyberspace and the international law. The purpose of this paper is to present the process of attributing cyber-attacks not only from a legal perspective, in which it builds on the paper from the last year's conference, but also to link it with a political and technical perspective. Why? Because for all the scholarly debate over whether norms of the international law can be applied in cyberspace, academics have failed to note that the international security community no longer places any trust in the legal attribution.

The paper maps the attribution process through the technical, operational, and strategic levels, clarifying in each what questions and goals are being addressed, and analyses the current attribution regimes used by the EU through the Cyber Diplomacy Toolbox and the Blueprint for a coordinated response to large-scale cybersecurity incidents and crises at the Union level. The last part of the paper focuses on the communication layer of attribution, presenting a framework for public attribution of cyberattacks introduced by Egloff and Smeets and assesses whether the legal concept of attribution still has merit in light of current attribution tools.

Rafael Prabucki

How much about cybersecurity and cyberwarfare should a post-graduate lawyer know?

The contemporary reality faced by lawyers, including judges and other professionals, is the reality of IT activities made possible by the Internet. On the one hand, mankind lives in a global village; on the other, such a society is easier to manipulate. Unfortunately, law graduates, i.e. people who learn how to operate and work with information, very often fail to relate their skills they had acquired during the period of study to the world in which information is composed of electronic data.

Threats posed by cyberspace affect them not only on an individual, personal level, but on a professional level as well. This raises a very important question - what knowledge should a modern lawyer be equipped with and how much should he know about cyber security? Answering this question requires examining a range of issues - starting from knowledge of how modern information sources found in cyberspace work and finishing on knowledge of threats to the cybersecurity.

It also raises the important question of whether there should not be at least some courses in legal studies on cyber security, ranging from courses on the basics to courses in the broader context of cyber security discussing new technologies that can help ensure information security.

Anna-Maria Osula

EU's Common Position on International Law and State Behaviour in Cyberspace

Arguably, the UN Group of Governmental Experts (GGE) has been the most reputable platform for agreeing on international norms for States in cyberspace since the end of the 1990s. In addition, the Open-Ended Working Group (OEWG) was established to offer a parallel venue for discussing pertinent issues related to State behaviour in cyberspace. The applicability and interpretation of international law has been one of the biggest challenges within these debates. The 2021 UN GGE report was a breakthrough in clearly stating the applicability of International Humanitarian Law and underscoring several other important legal principles.

European Union (EU) Member States have been active members of the UN GGE and OEWG since the beginning of the processes. The new EU Cybersecurity Strategy posits an ambitious plan to "advance, coordinate and consolidate Member States' positions in international fora, and /.../ develop an EU position on the application of international law in cyberspace." Is it possible to find a common view between 27 EU Member States (MSs)? This paper analyses different EU MSs' official international law positions and proposes areas where there could be a common standing. The paper

also identifies major differences in current interpretations. The paper will contribute to both legal and policy discussions and be valuable input to domestic and regional stakeholders.

Anna Golikova

Multidimensional approaches to regulation of cyber conflicts

Cyberspace is still a dimension that is poorly regulated by international law. Although there have already been attempts to develop a unified approach to regulation and to establish a so-called "set of rules", so far, any initiative in this direction has encountered obstacles that make it difficult to achieve any progress. Two Tallinn Manuals and the Resolutions adopted as a result of the activities of the UN Group of Governmental Experts were among the first "legal" documents in the cyberlaw field. However, the success of these initiatives is rather limited – two Tallinn Manuals avoided statements reflecting lex ferenda, and in June 2017, 25 members of UN GGE could not come to an agreement on the applicability of international humanitarian law to conflicts in cyber sphere. In December 2018, members of the General Assembly agreed to work in two separate projects. Russia became an author of Resolution 73/27 and the Open-ended Working Group was established. In parallel, the sixth UN GGE for the period 2019-2021 continued its work. This situation clearly demonstrated that the world community is divided over cybersecurity issues. The key questions for the world community remain: Is international law with its historically shaped norms, and especially international humanitarian law, applicable to regulate relations in cyberspace? How to carry out attribution in cyberspace and, as a consequence, how to determine jurisdiction and sovereignty in cyberspace? The most difficult question remains how a compromise can be found between the two positions – on the one hand, supporters of the Tallinn Manual, and on the other, its opponents, and UN GGE members on the one hand and countries that have joined the Open-ended Working Group?

Monika Palotai

Law and order on the Cyber Battlefield

War is a profitable business and where there is a conflict, there is Private Military and Security Company that seeks to leverage and reap the profits. PMSCs are not cowboys protecting a town from crime and are not desperados terrorizing and extorting it either. But they are corporate entities acting on behalf of a state or another non-state actor. Just like the participants and their role has evolved over the years and has adapted to the current market trends and needs, the battleground has changed as well. Cyberspace has become the new battleground for geopolitics. The world's conception of cyberwar changed forever in 2010. The security community had come to the shocking conclusion that the malware, Stuxnet, was in fact the most sophisticatedly engineered code ever for a cyberattack. It was the first cyberattack designed to directly damage physical object, the centrifuges used in Iran's nuclear enrichment facilities. It has also become the casus belli for the global cyber arms race that followed. States are now being entrepreneurial in contracting and deploy PMSCs to exploit their hackers as proxies to project power and to pursue state interest. But these modern-day mercenaries always have had the potential to unleash major damage that undermins global security, stability, and infringe human rights. This study explores the new global roles of the PMSC's in connection with applicability of the existing legal framework for the virtual battleground.

Room 133

9:30 – 11:00 Parallel streams

Law: Government 2.0, eJustice – Room 133

chaired by **Ludwig Gramlich, Pavel Loutocký**

Robert Müller-Török, Miroslav Fecko, Alexander Prosser, Silvia Rucinska

COVID-19 Vaccination Strategies – A critical comparison of the IT systems and digital tools used in Austria, Germany and Slovakia within the overall government policy framework

Since December 2020, when vaccines became available, all nations face the task of vaccinating their residents – or at least the proportion, which accepts vaccination. The vaccination campaigns should meet the following requirements: Use the scarce resource (vaccines) efficiently, i.e. not have to dispose vaccine that is unused or that degrades due to issues with cold chain logistics (1), vaccinate as many people as possible within a given time frame according to priorities set by the medical authorities (2) and provide a reliable proof of vaccination. (3). A side condition is that the priority order should be maintained, i.e. no one should be enabled nor encouraged to skip the line and overtake people who are more in need of a vaccination. A proper documentation, which enable boosters probably necessary in the future is included in (2).

This encompasses several functions, from procurement, logistics, materials management at vaccination centers, vaccination registration to issuing a vaccination certificate. These functions should be accompanied by an – ideally integrated – information system landscape plus the digital tools enabling a potentially very large number of inhabitants to use these systems.

The conference contribution analyses the systems and digital tools used in Austria, Germany and Slovakia for registration with a focus on the following questions:

(1) Vaccination registration tools in Austria, Germany and Slovakia – their basic architecture and integration

(2) Were the systems used part of bigger systems, the functionality including also vaccination certification, contact tracing & warning, epidemiological management, testing or even overall medical file systems?

(3) Were government registers and databases (re)used in application of the "once only" principle? How were the potential recipients identified? Registers of residents (probably derived from social security registers) or a "sign in if you like" policy?

(4) Were these systems also used or at least useful for logistics planning and administration?

(5) How did integration with the (electronic) proof of vaccination work?

Vaccination is only a part of the overall COVID-19 pandemic management of the government. The question arises, whether the respective system(s) used is or are well integrated in an overall orchestrated policy framework or whether is the issue was handled as a one-shot transaction.

The goal of the paper is to derive the lessons learnt for future similar pandemic situations. The authors assume that annual or bi-annual boosters will likely be necessary in order to keep the population safe. Hence the systems used must also be fit for serial production, not only for the current campaigns.

Jan Mazur, Maria Patakyova ml., Barbora Gramblickova, Matej Kacaljak

Regulation of Social Media Platforms: Towards a Holistic Regulatory Approach

In recent years a consensus has been reached around necessity to regulate social media platforms (SMP), primarily virtual monopolies such as Facebook. SMPs contribute to political destabilization, spreading of misinformation and hate speech within highly networked cyberspaces, while building on unique network economies, vast loads of users' personal data and unaccountable platform algorithms and architecture. However, there is no prevailing consensus among leading economies, politicians, and regulators as to the regulatory objectives or methods of regulation. Self-regulation seems to be insufficient, although preferred by the platforms themselves, as they experiment with various self-regulatory interventions. Private law and public law regulatory interventions are ranging from market-based approaches, oriented on changes to corporate purpose or governance structures, more traditional, yet refreshed competition law approaches, proposals for establishing multi-jurisdictional platform supervision, or even tax-based solutions, which are difficult to implement in the cyberspace. This contribution provides current overview of respective regulatory objectives and methods with the ambition to further the debate on platform regulation. Various regulatory approaches are reviewed based on their feasibility, potential impact, governance level.

Krystyna Rogala

Electronic enforcement of real estate in Poland - comparative legal analysis

The second year of the world's battle with the coronavirus COVID-19 allows us to claim that the pandemic was a massive impulse for the government's improvements and the introduction of ICT solutions in administration and the judiciary. This statement is also true from the perspective of the Polish experience. Examples of this movement are the changes introduced by the Act of May 28, 2021, amending the Act - Code of Civil Procedure, and certain other acts. Apart from introducing electronic service for professional attorneys, extending the use of remote hearings in Polish civil proceedings, this act introduces to the Polish Code of Civil Procedure the institution of electronic real property enforcement via ICT system, which has been postulated for years by the doctrine. This presentation discusses the introduced institution in comparison to solutions existing in other legal orders and also in terms of its practical implementation. The author aims to examine whether the introduced institution meets the earlier demands of the representatives of the doctrine and what practical effects Poland can expect from the introduction of electronic enforcement of real estate will have in the current Polish economic reality.

Saisha Singh

Policing using technology during COVID-19: The case of India

COVID–19, standing as a foremost example of Public Health Emergency, has forced the law enforcement agencies to look out for new kinds of crimes (the same being conducted with or without the aid of technology), ushering in transformations to public perceptions regarding the police, among various other things.

This paper attempts to explore the status quo of the functioning of the police during the pandemic. It starts with introducing the role of police and transformations which have been witnessed during the times of this pandemic, and takes into consideration specific practices across different countries and their ramifications on their respective demography. In the second part, the paper takes turn towards a specific case study, that is, of India. Towards the third part, the use of technology in policing is understood in a general manner, and specifically about indian practices. In the final part of the paper, policing during pandemic and associated challenges are explored, which include behavioural aspects, as well as technological aspects in a brief manner. Proceeding in the direction of conclusion, the role of the police during a Public Health Emergency is summed up, and suggestions for improvement specific to the Indian jurisdiction are made.

Pavel Loutocký

European Digital Identity and its Promises

The European Digital Identity is to be prepared for availability to all EU natural and legal persons and should be used for both online and offline public and private services across the EU. It will offer set of instruments through digital wallet serving to identify or use other trust services introduced by eIDAS regulation such as time stamp, electronic seal etc. The purpose of a European electronic identity is to provide a comprehensive tool that is both sufficiently trustworthy (in the case of private providers, there is uncertainty about the handling of relevant data) and backed by public authority. The intent of this contribution is to offer information and analysis of introduced tool and also to asses potential and problems of such solution.

11:15 – 12:45 Parallel streams

Law: eCommerce, Digital Single Market – Room 133

chaired by **Pavel Loutocký**

Attila Menyhárd

Platforms' liability for defects of goods and services

Less attention has been paid so far to the liability of online service providers acting as commercial agents. The importance of the question, whether the online service provider as a commercial agent can be held liable for the defects of the goods and services sold to consumers via the platform is increasing rapidly. The regulatory framework of the European Union is certainly not ready to react properly to this challenge. The product liability rules, construed by the ECJ as an exclusionary regime, do not cover the liability of learned intermediaries (ECJ C-327/05, Commission v. Denmark) while the position of the online service providers as commercial agents does not fall under the scope of the Directive on self-employed commercial agents. The absence of regulation complies with the traditional view that the agent shall not be liable for the defects of the product. This immunity of the agent against damages claims arisen from the defects of the product sold via the platform does not seem to be compatible with the role of platforms often providing – practically – the only way of access to the goods and services offered to consumers. They also build very much upon the trust of customers. The litigation against Amazon in the U.S. presents a new development which also is a sign of a growing gap between the American and the European legal approach. This should result in increasing tension in the globalized environment of business.

Iga Małobęcka-Szwast

Competition in the digital advertising sector – time to change the rules of the game?

Digital advertising is now the leading form of advertising and thus one of the most effective way of reaching consumers in the digital economy. A large majority of consumer-oriented service providers in the digital sector either offer their services free of charge and compensate them by selling targeted advertising services, or offer paid services but need to rely on advertising services provided by third parties. Since digital advertising has become a driving force and essential input for most businesses in the digital economy, ensuring healthy competition in the digital advertising sector is highly relevant. Thus, it comes as no surprise that practices of digital advertising service providers have been put under the spotlight of competition watchdogs. On 4 June 2021 the Commission initiated formal antitrust proceedings against Facebook for a potential breach of EU competition rules in the digital advertising sector. The Commission intends to assess, in particular, whether Facebook violated EU competition rules by (1) using advertising data gathered from advertisers to compete with them in markets where Facebook is active; and (2) tying its online classified ads service Facebook Marketplace to its social network. In my paper I would like to focus on the developments in the digital advertising sector from the competition law perspective and consider which tools (competition law or regulation) are better placed to ensure a level playing field for digital market players.

Kamila Brylak-Hudyma

Trusted flaggers

The presentation discusses the topic of so-called trusted flaggers who according to the EU Communication from the Commission to the Parliament dated September 28th 2017 are specialised entities with specific expertise in identifying illegal content, and dedicated structures for detecting and identifying such content online. Their main aim is to find illegal content on online platforms and then report it to each platform. Such notices from trusted flaggers should be able to be fast-tracked by the platform. In comparison to ordinary users, trusted flaggers can be expected to bring their expertise and work with high-quality standards, which should result in higher quality notices and faster takedowns. Therefore, the EU encourages close cooperation between online platforms and trusted flaggers. Some platforms like for example YouTube have already created their own Trusted-Flaggers Programs. The author presents already established definitions and regulations regarding trusted flaggers in particular in the Digital Service Act but also describes their responsibility and role in the fight against illegal content which is published via online platforms. During the presentations, the author indicates the advantages and disadvantages of the institution of trusted flaggers and tries to assess whether this institution can contribute to the improvement of Internet safety. The topic of the trusted flaggers seems to develop, therefore the discussion on the shape of this institution is an urgent issue.

13:45 – 15:15 Parallel streams

Law: eCommerce, Digital Single Market – Room 133

chaired by **Pavel Loutocký**

Francesca Gennari

Liability for home IoT standards. Are things finally moving on?

This abstract is the follow-up of a paper I presented at the Cyberspace conference last year. In 2020, I drafted an early stage research paper whose objective was to identify which kind of liability Standard Setting Organisations (SDOs) might incur whenever a standard created for an IoT home object turns out to be defective. As far as the EU is concerned, in the recent past, national courts and Member States (MS) did not hold these international SDOs liable for the production of defective technological standards because of their non-profit nature. However, each Member State could apply remedies such as tort liability rules, new conceptions of duty of care and defectiveness of the product. The research question of this new part of my work is to understand how new and forthcoming EU legal and policy instruments, such as the proposal for AI regulation and the Commission preliminary report about domestic IoT, will contribute to the debate about SDOs liability and liability for domestic IoT technology in general. With the same legal oriented methodology of last year, there will be an analysis and a forecast of the remedies the EU might suggest to the MS, such as new insurance schemes for some kinds of IoT objects, the update of the Product Liability Directive and the General Product Safety directive. The expected result is further harmonisation and guidance in a topic such as liability, for which the EU has not an exclusive competence.

Seyedeh Sajedeh Salehi, Marco Giacalone

Consumers, Small Claims, and the Pursuit of Justice: A post-COVID Mediation Perspective

This study departs from the observed need – at the current era of COVID-19 pandemic – to overcome the insufficiency in access to justice in resolving cross-border low-value claims arising from online transactions in the EU. Currently, there is a wide gap in access to justice for consumers choosing litigation for their cross-border small claims across the EU. This is particularly significant as there is a considerable rise in consumer complaints due to the Online shopping malpractices. The internal justice systems of the Member States do not fulfill consumers' needs to have an efficient access to justice for their low-value transnational disputes, since the ordinary civil proceedings are too lengthy, costly, and sophisticated for lay citizens. On that account, this study firstly aims at exploring the impact of COVID-19 on consumers' access to justice (in conforming to the right to a fair trial as enshrined by Art. 47 CFR and Art. 6 ECHR) for their cross-border small claims arising out of e-transactions across the Union. Next, it discusses about the possibility of using Online mediation as a viable solution with evidence from other jurisdictions i.e., UK, US, and Canada. Finally, this research proposes a hybrid-model of dispute resolution for small claims that may assist improving consumers access to justice in cross-border small claims.

Pedro Dias Venâncio

Artificial Intelligence & Fair Competition

Competition presupposes an open market, with freedom of private economic initiative, plurality of economic agents, and freedom of choice for the consumer.

Traditionally, legal systems protect the proper functioning of competition by protecting/promoting private economic initiative; by limiting dominant or monopolistic market positions; by protecting consumer rights; and also by repressing acts contrary to ""fair competition"".

The issue we intend to address in this presentation is related to the proliferation (or even generalisation) of the use of search engines and intelligent distribution of contents available online.

Some studies point out that the influence of these automated mechanisms for determining the information we access has an extreme impact on competition.

Furthermore, the exponential growth of Information Society Service platforms has maximised the direct and/or indirect network effect, with potentially perverse effects on competition.

In our presentation we will try to highlight in particular the risks of the generalisation of ""intelligent"" search algorithms as a factor of potential distortion of competition in e-commerce (direct or indirect).

We will also analyse the adequacy (or not) of the current legal regime on unfair competition in the prevention and repression of the potential negative effects of these practices in the market.

15:30 – 17:00 Parallel streams

Usable Security and Privacy – Room 133

chaired by **Vashek Matyas, Lydia Kraus**

Martin Ukrop, Pavol Žáčik, Vashek Matyas

Assessing Real-World Applicability of Redesigned Developer Documentation for Certificate Validation Errors

We face certificate validation errors commonly, yet the related tools and documentation had been shown to have very poor usability. Previous research suggests that just improving the error messages and corresponding documentation can have significantly positive effects. Our work aims at increasing the usability of certificate validation by 1) redesigning the API error messages and the corresponding documentation, and 2) validating the real-world applicability of the redesign by

investigating the opinions of 180 IT professionals. We focus on the perceived obstacles, desired ideal form and overall satisfaction. The redesigned documentation exhibits a reliable significant decrease in perceived incompleteness, with a small amount of perceived bloat and tangle. The redesigned documentation, now published at a dedicated website, is preferred by 89% of our study participants.

Katarína Galanská, Kamil Malinka

Usable Security from IT Professional's Perspective

This work aims to study the current state of the usable security guidelines, standards and other materials and investigate the IT professionals awareness of these materials. At first the survey has been carried out. The participants were professionals working in software development. Overall results showed that half of the participants are not even aware of the term usable security and less than a half of the participants claims to use any standards or guidelines in terms of usable security. The evaluation of these materials shows the insufficiency in applicability. According the the analysis of the study it was possible to define the requirements for the educational aid. The proposed software is an application aiming to increase users' awareness by reading about selected areas within usable security and completing quizzes. The purpose of the proposed application is to help the newcomers and make the area of usable security more accessible. The focus is given to specific areas, where the lack of usability can result in a huge increase of security risk. The impact of the implemented software was evaluated by conducting a second user study, where the participants were people working in software development. The participant was guided to read about four selected challenges and take quizzes associated with them. The results showed that the education aid helped the participants to understand selected challenges within the field of usable security.

Vojtěch Jelínek

The usage of multi-factor authentication amongst university students

In last decade the multi-factor authentication (MFA) became a possibility on a big number of websites, mainly the EU directive for electronic payments lead to MFA being required on banking and financial websites. Aim of the work was to analyze the usage of MFA amongst university students and how they rate the usability of different MFA methods. The data were gathered through an online survey. The main findings are that most students use MFA at least in some contexts (mainly financial), and their usage of MFA is mainly influenced by technical knowledge and the number of devices where the students had to use MFA. The perceived usability was influenced only by the students voluntariness to use MFA. The perceived usability was higher for MFA methods that did not require rewriting of alphanumeric code from one device to other. From the results, we can say that university students in Czech Republic are familiar with the MFA process, this is probably because they know it from the banking websites. Also, MFA methods that need less cognitive work from the user are preferred and should be offered to the users.

Room 136

9:30 – 11:00 Parallel streams

Artificial Intelligence in Financial Seruices (special track) Presentations of abstracts – Room 136

chaired by **Alex Ivančo**, **Joseph Lee**

Anna Wyszecka

Robo-advisory applications – possible to be fully automated?

I would like to analyze the possibility of using only Artificial Intelligence (AI) in investment advisory services provided by banks or other financial institutions in connection with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and the repeal of the grounds of Directive 95/46 / EC (GDPR). In my speech, I would like to focus on the selection of financial instruments made by AI, taking in to consideration profiling and the principles of personal data processing, e.g. transparency. Moreover, I will focus on the scope of the obligatory information given to the client under Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment companies and defined terms for the purposes of that Directive, related to the way the automated consulting service is provided. In the sum up of my speech, I will try to answer the question "Is it possible to automate investment advisory services?" and prepare a list of the requirements that the IT system must fulfil in order to comply with the law.

Alexander Roland Szívós

AI and financial literacy

One of the most important component of the global policy-making agenda is the need to strenghten financial literacy since the global financial crisis. The digitalisation of financial products and services highlight the importance of digital financial literacy. Artificial intelligence technologies are permeating financial services sectors. The application of the technology to personal finance management is providing new tools to support consumers and entrepreneurs in improving their financial lives and well-being. However carry new risks both mature and emerging markets. These

risks, if not properly addressed, may pose serious threats to the financial well-being of individuals and entrepreneurs. The paper will discuss the possible effects of integrating AI for financial services in the scope of financial literacy. Will the financial consumers be prepared to trust machines and the companies behind them? Will they understand the underlying technology? How can the regulatory framework help the healthy integration of AI? The paper mostly concentrates to the European point of view.

Alessio Azzutti

The Limits of the EU MAR/MAD Enforcement Regime in Deterring Market Manipulation by AI Trading

The financial trading industry was a pioneer in adopting AI solutions. But when considering the technical specificities of specific ML methods that allow for approximating truly autonomous trading agents (i.e. the "black box" problem), some technological-related risks are emerging, including hard to deter AI forms of market manipulation.

Specifically, this study questions the efficacy of the EU MAR enforcement regime to ensure credible deterrence. Generally, AI trading poses severe challenges for effective detection. Moreover, the autonomous and black-box nature of specific AI applications add an additional layer of complexity for liability attribution for AI misconduct. Thus, this study discusses the merits of a number of possible changes to the EU legal systems to achieve legal certainty and credible deterrence: (1) Abandon the scienter-based assessment of market manipulation in favour of a new legal test that emphasises market harm; (2) Adopt new liability rules and further harmonisation of enforcement regimes within the EU; (3) Revise existing supervisory arrangements towards enhanced centralisation of powers on ESMA and introduce innovative market-based solutions to MAR enforcement (i.e. "bounty-hunters"").

Overall, these proposals aim to reform the current EU enforcement regime to achieve credible deterrence vis-à-vis AI market manipulation to safeguard EU capital markets' integrity and stability, in view of effectively attaining the Capital Market Union project.

Tamás Bicskei, Gergely Rideg

Liability for the use of artificial intelligence in financial markets and regulations in Europe

The purpose of this paper is to evaluate the use of artificial intelligence in the financial sector from a civil liability perspective. The authors have examined cases where plaintiffs claimed that the malfunctioning of an agent caused substantial damages to financial companies trading in stock markets. Within this paper, the authors would like to consider the possibility of a malfunction within the agent not causing unexpected damages, but creating extraordinary earnings for the company that employs them. The paper finds that the software company providing the agent to the trader may be eligible for unjust enrichment under certain conditions. The opacity of artificial intelligence systems however creates difficult situations for parties to establish fact concerning trading agents. Thus the authors argue that both legislation, and legal professionals in the field should strive to design situations where risks arising from the black box effect of AI systems can be minimalised.

In view of the above the authors seek to answer the question of how the extra profit achieved by artificial intelligence affects the rules of the stock markets. The paper seeks to answer the question of how stock market actors relate to the fact that it is organized not only by human operators but also by artificial agents. The study might help us to get closer to understand the legal nature of artificial intelligence and thereby to outline a more diversified regulatory environment.

11:15 – 12:45 Parallel streams

Artificial Intelligence in Financial Seruices (special track)
Academic position – Room 136

chaired by **Alex Ivančo**, **Joseph Lee**

Clara Martins Pereira	**Does the new EU strategy for AI adequately addresses the systemic risk created by AI FinTech?**
Vincenzo Bavoso	**Reconceptualising financial intermediation in the age of fintech**
Aline Darbellay	**The Role of Algorithm-Driven Information Gatekeepers in the Financial Markets**
Antonios Karaiskos	**Artificial Intelligence and Financial Services in Japan: Focusing on Consumer Protection Issues**
Manuela Geranio	**Data Production by Market infrastructures and AI developments**
Joseph Lee	**Regulating AI in financial services industry: An access to finance perspective**

13:45 – 15:15 Parallel streams

Artificial Intelligence in Financial Seruices (special track)
International approaches to regulation of AI in financial seruices – Room 136

chaired by **Alex Ivančo**, **Joseph Lee**

Mattias Levin	**Within broader context Digital Finance Strategy, outline EU approach to regulation AI and supervision in financial services**
Marco Enriquez	**Natural Language Processing (NLP) for Financial Regulation**

Iota Nassr — **Highlights of the OECD report "Artificial Intelligence, Machine Learning and Big Data in Finance" (2021)**

Marcus Tsai — **AI related regulations and Sandbox in Taiwan**

15:30 – 17:00 Parallel streams

Artificial Intelligence in Financial Services (special track)
National approaches to regulation of AI in financial services and development of innovation – Room 136

chaired by **Alex Ivančo**, **Joseph Lee**

Valérie Hoess — **AI and Innovation in Financial Services – Implications for market structure and regulation**

Dominik Freudenthaler — **The Regulatory Sandbox in Austria**

Anikó Szombati — **AI in Finance - opportunities and risks**

Tomáš Olexa — **Regulation of AI from a supervisor's perspective**

17:15 – 18:45 Parallel streams

Artificial Intelligence in Financial Services (special track)
Presentations of abstracts – Room 136

chaired by **Alex Ivančo**, **Joseph Lee**

Paweł Szczęśniak

The problem of qualifying sales revenues on online auction portals according to Polish regulations and jurisprudence

According to Polish Personal Income Tax Act, there is a problem with the qualification of revenues from sales on online auction portals (e-commerce). The sale of movables, if made before the expiry of six months from the end of the month in which the acquisition took place, is not subject to personal income tax. Such classification of revenues is possible when the sale of movables does not take place as part of business activity. However, if the sale is made on a continuous basis and for profit, the income obtained should be classified as income from business activity, and not from the sale of assets belonging to personal property. It is noted in the jurisprudence that the taxation of revenues from sales on online auction portals is not determined by the subjective opinion of the taxpayer, but by the objectively established features of its activity. Therefore, only a precise determination of the facts allows to determine whether the taxpayer's activity had features corresponding to business activity or was the management of private property. This paper aims to present the detailed criteria for taxing revenues from sales on online auction portals. The basic research method will be the analysis of judicial decisions. The conclusions resulting from the paper will have a significant application value also in terms of comparative law.

Nadia Pocher

Self-hosted Cryptocurrency Wallets and the 2021 EU AML Package

Jan Hospes, Christof Tschohl, Walter Hötzendorfer, Sebastian Schneider

Exchange of Information on Cryptoassets under DAC 8 – Scope & Data Protection

The EU Commission is striving to subject cryptocurrencies to sets of rules for the exchange of information in tax matters. The lack of a uniform definition, the vast spectrum of heterogeneous forms and purposes and the number of inherent and unique characteristics makes it difficult to find a common definition of cryptoassets. In order to understand how cryptoassets fit within existing tax systems, the key components of already existing definitions introduced by the FATF-Recommendations together with the 5th AML Directive and the recent proposal of MiCA are analysed. Based on this analysis a new definition is proposed.

The cryptoasset market involves various market actors. The contribution shall discuss which actors should be included in the scope of the reporting duties and which definitions may apply.

Reporting duties may lead to intensive data processing. Particularly the collection of wallet-IDs in cohesion with KYC-data appears to be intrusive, as it can be used to trace a data subjects complete transaction history in the blockchain without any need for further information.

The contribution considers and systematises the legal bases on which the tax administration collects data on taxpayers and how its handling of the collected data can be reconciled with the fundamental rights of taxpayers, with tax secrecy and with data protection. On this basis, recommendations towards enhanced data protection and data security are given.

Seyedeh Sajedeh Salehi, Marco Giacalone

Walking on the Edge of Reality and Virtuality: Dispute Resolution in Cryptocurrency Transactions and Users' Rights

In the last decade, investments in cryptocurrencies have gained a lot of momentum. According to data provided by Statistica (a world-leading business statistics source) the number of cryptocurrencies worldwide has dramatically increased from 66 in 2013 to 6044 in July 2021 with the total market capitalization of 1.381 trillion dollar. Cryptocurrencies are traded on (centralized) cryptocurrency exchanges that function as an intermediary between buyers and sellers. The frequent use of these digital platforms by investors has given rise to issues like technical and/or security problems causing loss of funds, thus infringing the users' rights. Despite, there is still a lot of grey regulatory area about effective remedies for investors in cryptocurrency-driven disputes. Therefore, the main objective of this research is to analyze the effectiveness and compatibility of different methods of dispute resolution for cryptocurrency related disputes.On this account, this study first gives a brief overview of the role of cryptocurrency exchanges in transactions and the most frequent issues that users face by using these platforms. The second section deals with the available dispute

resolution methods and evaluates their efficiency in facilitating access to justice for the users. Finally, this study discusses whether Online mediation and Online negotiation (as part of the Online Dispute Resolution regime) can be deployed as the most effective methods for resolving cryptocurrency disputes.