9:30 – 11:00 – Cybersecurity, cybercrime – Room 214

chaired by **Václav Stupka, Jakub Harašta**

Cristobal Bocos, Katia Tsironi & Eugenio Mantovani

The security of electronic medical records - Lessons from the IRIS project

The transition from paper-based records to electronic medical records (EMRs) promises to revolutionize healthcare provision and delivery in the EU, but it also creates serious security concerns, as the increasing number of cyber attacks perpetrated against hospitals in the last year indicates. This article, which originates in the context of an ongoing e-health project, deals with the security of EMRs, from a computer science and legal perspective.

The article explains, in the first part, what an EMR – a term that refers to the collection of information about the health status of an individual in digital format – is (Kierkegaard, 2011). It will do so by offering examples of EMRs compiled in different EU jurisdictions, and a description of the legal protection afforded therein.

The second part draws on existing literature on cybersecurity. After defining security, it describes, with the aid of a table, the vulnerabilities and risks associated to EMRs, e.g. ransomware, malware, breaches, and in relation to their storage systems, e.g., in the local servers of the hospitals or in cloud storage systems (ENISA, 2015). This section is complemented by references to the legal frameworks (criminal law, data protection law, etc.) that are mobilised in response to these risks (Agrawala & Johnson, 2007).

The classification of security concerns and the legal analysis will offer researchers in the field of regulation of technology, technology and health care management an updated source to advance knowledge in the area of cybersecurity and health research.

Main references

ENISA (European Union Agency for Network and Information Security): Security and Resilience in eHealth Infrastructures and Services, 2015

Kierkegaard, P., Electronic Health Record: Wiring Europe's Health Care. Computer Law and Security Report, 27(5), p.503-515, 2011

Agrawala, R., and Johnson, C., Securing electronic health records without impeding the flow of information. Int. J. Med. Inform. 76:471–479, 2007

1 IRIS - Interoperable platform for Remote monitoring and Integrated e-Solution, funded by INNOVIRIS (the Brussels Institute for Research & Innovation)

Ilona Stadnik

International cybersecurity regime: what is it and how can be achieved?

This study is devoted to exploration of possible international regime on cybersecurity. All parties involved in the debates can roughly be divided in two camps – adherents to multi-stakeholder model (equal participation of states, business and society in cyber governance) and supporters of sovereignty-based model (central role of governments).

The lack of shared definition of cyberspace and cybersecurity across the world has led to a relatively slow negotiation process for the formation of international cybersecurity regime. Interpretations are different: on the one hand it is about security of physical infrastructure; on the other it encompasses security of information flows that circulate though infrastructure. The study applies securitization theory to explain the differences in threat perceptions of three main international players – Russia, China, and the US.

Moreover, before the establishment of an international regime, it should be defined what cyberspace is in terms of international law – whether it is a global commons or a part of sovereign territory. Each extreme option implies a particular type of legal regime. Also, even where concept of territorial sovereignty cannot be applied in full manner (so for cyberspace), global governance is still possible – international regime for high seas and outer space are examples. Another open question for cyberspace is the role of private parties in governance.

The research question focuses on the features of international cybersecurity regime. Is it enough to adjust existing international law to cyberspace, or we have to invent new governance mechanisms? Consequently, the study focuses on benefits and problems of models for international cybersecurity regime: sovereignty-based, with private actors forced to follow governments' will, or, multistakeholder, with more or less equal participation of state and non-state actors.

9:30 – 11:00 – eCommerce, eFinance – Room 215

chaired by **Zsolt Balogh, Libor Kyncl**

András Márton

Trade Secret in the European Union and the United States

The act of highest future importance and impact on European and North American economy on which we are currently working is the Transatlantic Trade and Investment Partnership (TTIP). It is worth paying heed to its legal implications, next to the relevance in economy, labour market, customs and other fields. There is a potential threat to the confidentiality of information, technology and know-how—mostly electronic in our times—at those companies which expect market expansion and new customers from the partnership, because of the differences in legal regulation of trade secret between the two systems. In this work, I present the law of trade secret in the European

Union—where I shortly mention the Hungarian way, too, as an example—then the relating acts in the USA; and lastly I analyse the similarities and differences in regulation. Thus the paper contributes to the success of the legal side of the partnership, as it shows the points where the parties should discuss questions of fair trade.

Asim Jusic

Will Compliance with the Risk-Based Approach to Regulation of Anti-Money Laundering Stifle Fintech?

Fintech, the use of technology for financial innovation and provision of financial services, is a booming industry, promising to transform – and largely replace – traditional financing methods. Fintech includes crowdfunding, marketplace lending, virtual- and crypto-currencies, prepaid cards, etc. The Financial Action Task Force (FATF), the main worldwide anti-money laundering (AML) standard setting body, recently warned that Fintech is a tool that is extremely susceptible to money laundering and terrorist financing (MLTF). Monetary fines for lack of compliance with AML requirements are already being imposed on Fintech, as the case of Ripple Labs shows.

This paper argues that application of contemporary AML regulation in Fintech industries is problematic for two reason. Firstly, the current FATF risk-based approach to AML is costly, based on largely ineffective customer due diligence (CDD) and reporting requirements, and guided by overly subjective risk guidelines. In addition, more often than not, national legislative frameworks for governance of the financial industry and the prevention of money laundering are based on 20th century legal concepts that are hardly applicable to Fintech, leaving Fintech in a situation of considerable legal uncertainty. Secondly, considering that Fintech is a nascent industry, full-fledged application of the risk-based AML approach is hindering its growth and further innovations. Hence, the question is whether a special AML framework, or possibly exemptions from AML requirements, is required for Fintech.

9:30 – 11:00 – Government 2.0 – Room 109

chaired by **Ludwig Gramlich**

Jacek Gołaczyński

Impact of informatization on access to justice in the European Union

Access to justice is a fundamental right and one of the most important concepts in the field of justice. However, it is a right that faces a number of challenges throughout the EU. Access to justice typically means having a case heard in a court, but in wider meaning it shall be achieved or supported through mechanisms such as proper information about the law in force. Information on EU law and the national law on judicial cooperation in civil and criminal matters, European Judicial Atlas, Eurlex.eu, Curia.eu, European Judicial Network in civil matters are the projects that already expand the knowledge about law and justice in European Union. But what about transboundary proceedings? The speech will discuss electronical tools that makes access to justice much more wider. For example lodging of procedural documents electronically, electronically obtained european order for payment, european small claims procedure, as well as usage of e-signature in civil procedure and e-delivery. The speaker shall also present the Polish perspective in this matter and latest legislative achievements.

Eva Fialová

Algorithmic decision making in judicial proceedings

Human work is nowadays being replaced by algorithms. Automated processes substitute sophisticated activities. One of these activities is decision making in judicial proceedings, despite the fact that the core principle of legal proceedings is that judges have to decide cases imperially, in accordance with the law as well as their interpretation of the fact and the law. In the United States and also in some European countries an algorithm is already being used by courts to assess whether or not it is likely that the accused (or condemned) will commit another crime in the future or whether he or she will lead a proper life, in order to determine the length of imprisonment, whether to impose a suspended sentence of imprisonment or grant a parole. When using the algorithm for decision making, the judge does not decide based on the circumstances of the case and individual characteristics of the accused. It decides instead on the bases of profiles compiled from data related to other offenders which were collected in the past. It means that the algorithm works with a set of features that characterize certain previous cases and offenders, and makes conclusions about the circumstances that are unique to the accused about whom the court decides. The algorithmic decision making based on profiling raises concerns about the rights of the accused in the judicial proceedings. This paper focuses on those rights, especially on the right not to be discriminate and the right to a fair trial.

Berenika Kaczmarek-Templin

The impact of European Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market on national judicial (civil) proceedings

On 1st July 2016 the European Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market came into force. It lays down the conditions under which Member States recognise electronic identification means falling under a notified identification scheme of another State, lays down rules for trust services for electronic transactions and establishes a legal framework for electronic: signatures, seals, time stamps, documents, registered delivery services and certificate services for website authentication.

In view of the above changes, the question arises whether the Regulation will have an impact on national judicial proceedings, in particular with crossborder elements. Although documents with

electronic signatures, which exist in transactions, will be accepted in civil proceedings because it follows directly from the provisions that it should be possible to use trust services as evidence in legal proceedings in all Member States.

It may be questionable issue of the application of the Regulation for electronic communication with the court. Although the regulation says it should apply to public and private online services, courts, which can offer online services, are not public authorities, to which its provisions refer. It's worth considering whether the principle of equality of electronic signature with the handwritten signature may constitute an independent basis for electronic filing office in the court.

Anna Kościółek

Informatization of civil proceedings in Poland with respect to principle of its publicity

The use of modern technology in court proceedings in civil matters is not without impact on the implementation of the still-current postulate according to which "it is not merely of some importance but is of fundamental importance that justice should not only be done, but should manifestly and undoubtedly be seen to be done". Therefore, the paper is devoted to the analysis of the impact of recent years amendments, introducing modern information and communication technologies to the civil proceedings in Poland, on one of its fundamental principles, i.e. the principle of its publicity.

The analysis includes amendments introduced in the following spheres: openness of court sessions, both internal (referring to parties and participants of the proceedings) and external (referring to the wider public); obligation to notify the parties (participants) of public court sessions; recording the course of public court sessions and providing access to protocols; as well as public pronouncement of judgments. All of the above manifestations of publicity have been recently affected by introduction of modern technology to the civil proceedings in Poland.

Pavel Loutocký

ICANN: What a Global Future of internet Governance?

The questions associated with the future of ICANN and its possible transfer to the global multi-stakeholder community are highly relevant to be discussed in the moment. Such step was originally scheduled for September 2015 however many problems with future role of ICANN after such transfer in connection with internet governance were raised. One of the greatest concerns is connected with free and uninfluenced governance of the system of the domain names and thus of the internet, because different interests by different states could be applied against free and heterogeneous function of the domain name system. Such concerns are also raised because of particular inconsistency of decision-making process and such problem is still not fully eliminated nowadays at least to some extent. The main intent of the presentation is thus to assess possible risks with such important change as it may widely influence the administration of domain name system as we know it in the moment.

9:30 – 11:00 – Data Protection & Privacy Impact Assessments – Room 208

(special track organized by **d.pia.lab - VUB-LSTS**) chaired by **István Böröcz**

Raphael Gellert & Niels van Dijk

Addressing issues with DPIA methodologies: What can we learn from law?

The introduction of data protection impact assessments (DPIAs) are one of the novelties of the General Data Protection Regulation. They present new elements and challenges to data protection practice. At their core, DPIAs seem to consist of risk management methodologies (imported from organisational and business spheres), aiming to assess and manage "risks to the rights and freedoms of data subjects" resulting from data processing operations.

The idea of assessing risks to rights is however not as straightforward as it might seem. Beyond the fact that risks and rights are very different practices (one probabilistic and anticipatory, the other drawing on legal knowledge and operating ex post), this contribution wants to focus on challenges concerning DPIA methodology. Risk management methodologies have faced serious criticism in other assessment fields like environmental and health law. Of particular importance, their pretence at objectivity has been at the centre of discussions, due to their tendency to reduce "the full range of uncertainties to the more comforting illusion of controllable, probabilistic but deterministic processes". This however already presupposes a number of epistemic and theoretical commitments, which often mask subjective choices. In other words, whereas these methodologies present themselves as objective, the notion of risk has an inherent subjective dimension.

These findings have serious implications for the type and quality of data protection to be expected from DPIAs. Depending on the methodological choices, DPIAs could amount to little more than a managerialisation of data protection, telling us very little about what "risks to the rights and freedoms of data subjects" are, and could ultimately even undermine the data protection legal framework. Alternatively, a robust management methodology might have the potential to improve the protection of personal data, not least because of its anticipatory nature.

In this paper we argue that one way to ensure that DPIAs amount to more than "the new risk-based box-ticking" is to integrate lessons from legal practices with experience in articulating relations between risks and fundamental rights. This requires an analysis of case law concerning privacy and data protection on the one hand, and impact assessments on the other hand. We will extract two kinds of lessons. The procedural lessons will relate to how to organize the process of assessment, the status of risk as contestable evidence, the participation of those affected by the technology, and the proportional balancing of risk and right based knowledge. The substantive legal lessons will

relate to the concepts of risk, harm and probability at the core of DPIAs. We will explore whether the incorporation of such foundational legal lessons can have the potential of transforming the DPIA into a tool that can anticipate data protection issues in a legal fashion, which we call a court of upstream adjudication.

Dariusz Kloza & István Böröcz

Impact assessment in the European Union's new data protection law

The reform process of the European Union's legal framework for personal data protection was culminated on 27 April 2016 with the enactment of General Data Protection Regulation and – less popular – Police and Criminal Justice Data Protection Directive. Both instruments bring to the fore multiple uncharted novelties and one of them is a 'data protection impact assessment' ('DPIA'). Upon the entry into force of the new legal framework (28 May 2018), an obligation will be imposed on data controllers to conduct such an assessment for personal data handlings that are "likely to result in a high risk to the rights and freedoms of natural persons" (cf. Art 35 of the Regulation and Art 27 of the Directive). All these novelties have sparked continuous debates on their effectiveness, efficiency and practical application, further urged by the imminently upcoming applicability of the new laws.

Therefore we could not help but to take part in this debate and reflect on the way the well-established concept of impact assessment was adapted to the needs and reality of European data protection law. Having briefly overviewed the history of impact assessments in the areas of environment, technology and privacy, we critically assess the two legal requirements for a 'DPIA' set forth by the new Regulation and the Directive. We point out their positive, acceptable and negative elements. We conclude that these 'DPIA' requirements – predominantly due to their limited scope – have rather failed to live up to the expectations vested therein. Yet this failure could be remedied by a complimentary policy on impact assessment that would genuinely safeguard both individual and collective interests related to privacy. We therefore conclude with a few modest suggestions as to the contents of such a policy.

Paul Quinn

The Potential for Impact Assessments in Projects Related to eHealth and mHealth

The use of Impact assessments has gradually become more common in areas of technological innovation or novel practices where questions of privacy arise. This trend will likely take further root given the requirement set forth by article 35 of the General Regulation on Data Protection (GDPR). This article requires that data controllers conduct an impact assessment in a number of instances, including where the rights and freedoms of data subjects are at risk. As this presentation will discuss, the nature of such an impact assessment and the situations in which it is required make it ideal for use in projects related to eHealth and mHealth. Such projects frequently make use of large amounts of sensitive data and raise risks in terms of a number of important rights, including but not limited to rights linked to data protection. The broad nature of the impact assessment invoked in article 35 GDPR is suitable for not only considering questions linked to data protection and privacy but also issues related to stigmatisation, discrimination and other ethical issues that are often linked to health care projects. This presentation will discuss the potential use of impact assessments in such instances and discuss the benefits they can bring.

9:30 – 11:00 – Psychology of Cyberspace – Room 209

chaired by **David Šmahel**

Dmitri Rozgonjuk, Anna-Kati Pahker & Karin Täht

The Relationships between Facebook Usage Dimensions and Personality Traits

It has previously been shown that Facebook usage could be described as multidimensional: distinctions could be made between active-passive and private-public usage (Frison & Eggermont, 2015). However, this concept has not been validated with real Facebook usage data; neither has it been studied which personality traits could be associated with Facebook usage dimensions. This work aims to fill these gaps.

One hundred and twenty one adults (age 18-34, M = 22.52 ± 3.1; 64.8% female) completed the Multidimensional Scale of Facebook Usage (MSFU), The Rosenberg Self-Esteem Scale, the Short Five Personality Inventory, and provided real life data for Facebook usage (using Activity Log).

Data analysis showed that Facebook usage could be described with three dimensions: (1) active-public, (2) active-private and (3) passive Facebook use. Correlations with real usage data validated the results for active usage. Additionally, we found that Extraversion predicted active-public, Agreeableness predicted active-private, and Neuroticism predicted passive Facebook usage. Openness, Conscienciousness, and Self-Esteem were not statistically significantly correlated with different dimensions of Facebook usage.

This work has two main contributions: (1) real Facebook usage data has been used to validate the dimensionality of Facebook usage, and (2) the paper shows that Facebook usage differs in personality traits.

Martijn Burger & Efstratia Arampatzi

The Heterogeneous Relationship between Social Network Sites and Subjective Well-Being: What Kind of Use Fits What Kind of People?

Over the past years, several studies have examined whether online social contacts and the use of social network sites (e.g. Facebook, Twitter) can replace the importance of real-life social connections in our pursuit of happiness. At present, the evidence found so far has been inconsistent. Where early studies find a positive relationship between social network sites use and subjective well-being, other studies report no relationship or even a negative relationship between social network sites use and subjective well-being. One reason for these ambiguous results is that the relationship between social network sites use and subjective well-being likely involves both positive and negative effects, the balance of which is likely to vary across people and way social network sites are used. Most notably, active participation such as posting, commenting, liking and chatting on social networks sites, might have a different effect on subjective well-being than passive following or browsing other people's profiles. At the same time, the subjective well-being effects of both active participation and passive following might differ across people. For example, extravert persons might become happier from active participation, where introvert persons have more to gain with passive following. Using a survey among young adults in the United States and the United Kingdom, we therefore examine what kind of usage fits what kind of people – in terms of personality and social-demographic characteristics.

Felix Reer & Nicole C. Krämer

Social compensation or rich-get-richer effect? Modeling the connection between introversion and social capital outcomes of playing World of Warcraft

Some studies indicated that playing online games yields a 'rich-get-richer effect' and is especially socially beneficial for extraverted players (e.g. Shen & Williams, 2011), while other authors argue that online gaming could have compensational effects for shy players (e.g. Kowert et al., 2014). The current survey study (N= 409) shows that both perspectives are not mutually exclusive. Path analysis revealed that extraverted World of Warcraft players act more socially towards fellow players and hence have better chances to build up social capital than introverts. However, at least some of the introverted players used the game for social compensation. These players chose a more social playing style, which increased their chances to acquire social capital. The results demonstrate that the group of introverted players is more heterogeneous than previously thought and that the links between personality aspects and social outcomes of playing are quite complex and rather indirect than direct.

Cory Robinson

No Exchange, Same Pain, No Gain: Risk-Reward of Wearable Healthcare Disclosure of Health PII for Enhanced Pain Treatment

Wearable technologies have created fascinating opportunities for patients to treat chronic pain in a discreet, mobile fashion. However, many of these health wearables require patients to disclose sensitive information, including health information (heart rate, glucose levels) and personal information (location, email, name, etc). A risk/reward relationship of disclosure has been previously studied in interpersonal communication, digital communications, and health environments. Individuals using wearables for treatment of chronic pain may sacrifice social health elements, including their privacy, in exchange for better physical and mental health. Utilizing communication privacy management, a popular disclosure theory, this article explores the policy and ethical ramifications of patients disclosing sensitive health information in exchange for better health treatment and relief of chronic pain. The manuscript identities scenarios where a user must disclose information, and what factors motivate or dissuade disclosure, and ultimately using a wearable. Practical implications of this conceptual paper include an improved understanding of how and why consumers may disclose personal data to health wearables, and potential impacts for public policy and ethics regarding how wearables and their manufacturers entice disclosure of private health information.

9:30 – 11:00 – Privacy and Surveillance – Room 025

chaired by **Aleš Završnik**

Rolf-Dieter Kargl & Alexander Czadilek

Law Enforcement by Design

The Internet of Law (IoL) describes the interconnection and enforcement of law using Internet of Things (IoT) applications. These applications enable law enforcement agencies to carry out their duties without direct use of personnel at the place of the offense. In its first part this paper describes the implementation of these new technologies and surveillance measures into the existing criminal procedure code and evaluates them based on the elaborated criteria in project "HEAT – Requirements for the evaluation of anti-terror acts in Austria", which is subsidized by the Internet Foundation Austria under NetIdee.

In the second part the upcoming questions / problems regarding processing personal data by the aforementioned applications will be analyzed. One of the key points will be the certification of, as well as the implementation of privacy by design and privacy by default, in mentioned applications, as required by the General Data Protection Regulation.

For better illustration the presented theses will be complemented by practical examples, like breath analyzers built into cars or the surveillance of GPS data or the use of IMSI-Catchers for emergency

services. Regarding breath analyzers, it will be discussed if it is a violation of the purpose limitation principle if collected data are used for other purposes, like as evidence in a custody battle.

Primož Križnar

Bitcoin: an obstacle to the effective criminal investigation?

Physical currency is passe, because most of our transactions today involves plastic cards, communications between electronic devices and bank servers or other currency exchange web services. The money's value is also losing connection to tangible assets, so this »fiat money« could not be redeemed for valuable metals. Therefore, from the ashes of history, virtual currencies are rising, and one of the most popular among them is Bitcoin. In its digital form, based on mathematics, produced by the people and held electronically, no one can control its peer-to-peer function network, and despite the absence of physical form, it can be exchanged to physical currency, like euros. Nevertheless, its popularity is rising because of its anonymity, low cost of transactions and simple use. These two circumstances are blessed amongst society and represent holy Grail especially for individuals, involved in money laundering, financing terrorism or drug dealing. This is the reason, that law-enforcement agencies must have effective methods of investigation, but are there any? This article will try to answer this question by reviewing how bitcoin network functions, which criminal actions are possible to commit with its help, which investigation methods can be applied for identifying delinquent bitcoin user or his transactions and are those methods capable of dealing with the most common issues, like advanced encryption methods, obtaining IP address and privilege against self-incrimination.

Liva Rudzite

Processing of biometrical data in comparison with rights to privacy of an individual

Development of technologies change the nature of data processing and increase application of biometric data which force to deliberate perceptions how far is acceptable to make that kind of data processing and when it becomes excessive. Recently processing of biometric data was used mostly to detect criminal offences, but the last decade, especially in the light of growing terrorism threats, has marked more widespread processing of these data, reducing biometric data even to commercial level.

11:15 – 12:45 – Cybersecurity, cybercrime – 214

chaired by **Václav Stupka, Jakub Harašta**

Tuomas K. Tiihonen

Interplay of European Union competences in cyber security

The objective of this paper is to examine the development of cyber security policy in the European Union through three separate competences – the internal market, the Area of Freedom, Security and Justice, and the Common Security and Defence Policy – and make visible the effects development in one area has to the other competences. The theory of spill-over, the inadvertent (but arguably calculated) expansion of Union competences in an adjacent area from the legislative development in another, is used in the paper with pertinent examples from other policy areas to show that cyber security development in the context of the internal market and the Area of Freedom, Security and Justice affects development in the mostly intergovernmental Common Security and Defence Policy. Transatlantic cooperation in both EU-US and EU-NATO contexts is also included in the paper to show that impetus for reinforced cooperation in cyber security may flow also from the Transatlantic Trade and Investment Partnership agreement that is currently being negotiated. The paper will touch upon the current framing of European cyber security policy and the discourse that has lately revolved around the concept of resilience as a cornerstone. Is the emphasis placed on resilience an attempt to desecuritize the discourse and establish a clear presence for cyber security as a policy area predominately in the internal market sphere?

Ethan S. Burger

Cyber-Psychology: Combating the Insider Threat

The so-called 'insider threat' represents a major challenge to organizations' cybersecurity. There are ways that organizations may counter this threat.

As an initial step, organizations must have effective procedures for vetting new employees, thus avoiding potentially malicious or 'vulnerable' individuals from becoming insiders.

In addition, employee wrongdoing can be 'preempted' or prevented by having good cybersecurity hygiene. This objective demands accurately monitoring employees' activities. It requires that organizations have a good security system in place.

Such systems start with having an effective Chief Information Security Officer (and/or others persons fulfilling the relevant functions), and having appropriate security procedures, hardware, and software to prevent and detect the occurrence of cyber-incidents/attacks.

Lastly, when incidents occur, organizations need to respond effectively. This activity will involve a thorough investigation of the surrounding circumstances, including the organization examining its employees' conduct. The proper application of psychological evaluations play a critical role in these efforts.

Many organizations require that their employees hold security clearances, or at least undergo a thorough background check before being hired. Some organizations use polygraph machines as part of their internal security programs.

New technologies are being developed for possible employee screening, monitoring, and incident investigation. While these new technologies may be better at collecting and categorizing data than traditional polygraph machines, if the underlying scientific theory for their use is not valid, having more exacting tools will not lead to greater organizational security.

The American Psychological Association, the [U.S.] National Academy of Sciences, the [defunct] U.S. Congressional Office of Technological Assessment and other organizations have found that polygraph machines generate false negatives and false positives.

False positives have undesirable consequences for organizations and employees. Employees identified as being deceptive may lose their positions merely because they are anxious, Other employees seeing that their colleagues are unfairly treated, may seek new employment since they fear job insecurity. This situation is disruptive to organizations, at a minimum requiring the employer to recruit new personnel.

False negatives may cause organizations to mistakenly think an individual is not a malicious employee, when in fact, the opposite is the case. Enhance 'sensitivity' when measuring the reaction of persons undergoing a polygraph examination in fact may be undesirable, causing greater harm to organizations than they are worth. Therefore, it might not be justified to use these new cyber-physiological tools to identify insiders that present risks.

11:15 – 12:45 – eCommerce, eFinance – 215

chaired by **Zsolt Balogh, Libor Kyncl**

Pieter Van Cleynenbreugel

Heading in the wrong direction? The Commission's Geoblocking proposal and the future of EU eCommerce regulation

On 25 May 2016, the European Commission proposed a Regulation envisaging to prohibit traders from engaging in geoblocking practices, i.e. the practice of blocking one's website to persons established or residing in a particular Member State. In directly seeking to prohibit traders' practices, the EU secondary legislation proposal appears to take a new and more piecemeal approach to eCommerce regulation compared to previous EU regulatory initiatives in this field. Whilst the proposed Regulation tackles a topical issue and thus appears to offer a necessary step forward in enhancing cross-border eCommerce in the European Union, the envisaged piecemeal

approach within the proposal raises important concerns from an EU law, a technical and a law enforcement point of view. This paper will outline and contextualise the Commission's proposed Regulation and elaborate on the three legal and technical concerns it raises. It will subsequently propose a way forward in order to overcome those concerns. As part of that way forward, it will call for a more coherent and technologically-friendly regulatory approach to eCommerce at the EU level, coupled with the adoption a more explicitly intertwined EU competition law – eCommerce regulation strategy to be adopted by Member States' authorities.

Koji Takahashi

Bitcoin Ownership Dispute in the Aftermath of MtGox's Bankruptcy

The legal ownership of cryptocurrency is an important question where the person with whom cryptocurrency is deposited (such as the provider of an exchange or an online wallet) has gone bankrupt. The depositor would certainly have a contractual claim for the return of the deposit. But the deposit would be converted into the fiat currency which is legal tender of the country where the bankruptcy proceedings are opened. Furthermore, the depositor would have to join other creditors and could obtain only a proportional recovery. If the depositor could alternatively claim the ownership of the units of cryptocurrency which have been deposited, he would be able to obtain a full recovery outside the bankruptcy proceedings.

MtGox was once the world's largest provider of a Bitcoin exchange. After bankruptcy proceedings were opened with respect to MtGox, one of its customers filed a suit (hereafter the "MtGox case") in Japan against the representative of the bankruptcy estate, seeking the return of the Bitcoin units of which he asserted the ownership. This paper will examine this case and comment on the rulings of the Tokyo District Court and Kyoto District Court.

The Tokyo District Court's ruling, given on 5 August 2015, has been reported in English media as having denied the ownership of Bitcoins. So reported, it has caused an alarm among the Bitcoin users. If, however, the judgment in the original Japanese language is consulted, it should be possible to realise that the word "ownership" as an English word for translation is misleading. This paper will explain the difference between the English word "ownership" and the technical meaning of the Japanese law concept discussed in the original judgment. The appreciation of this difference should allay the concerns of Bitcoin users.

This judgment, however, is not free from any problems: a careful reading reveals theoretically challenging issues which have not been addressed by the Court. Had the plaintiff constructed his argument on the basis of "ownership", a wider concept than the Japanese law concept relied on by him, the Court would have had to address them. One of such issues is the test for determining the owner of Bitcoin units, a difficult question which becomes even more difficult when the Bitcoin units sought to be recovered are commingled with other units. Another challenging issue the Court did not address is what should be the choice-of-law rules for determining the law applicable to the ownership of Bitcoin units. In the case of a longer-established electronic money, it would not be impossible to deem it to be situated in the place where the server processing the transaction of the money is situated or where its administrator has its relevant place of business. The Bitcoin, on the other hand, is not managed by any specific entity and its transactions are processed on a distributed ledger. Those features make it difficult to localise Bitcoin units in a particular country for choice-of-law purposes. This paper will consider possible solutions to those challenging issues.

The difficulty of localisation also presents itself in jurisdictional questions, another feature of the MtGox case. The suit was first brought before the Kyoto District Court prior to being transferred to the Tokyo District Court. In the motion to transfer, the defendant argued that the Bitcoin units which the plaintiff sought to recover could not be deemed to be situated in Kyoto. This paper will conclude by commenting on the Kyoto District Court's ruling.

Denisa Jindřichová

Developments of cybersecurity on financial market

In the last years we alive progress of new communication technologies which allow new forms of speedy payments. Many clients use innovative payment instruments and different ways how to execute a payment transaction. Are all e-payments secure? Which rights and obligations have the users?

11:15 – 12:45 – International Internet Law – 109

chaired by **Dan Jerker B. Svantesson**

Michael Bogdan

The New EU Rules on Electronic Insolvency Registers

The paper deals with those provisions of the new EU Regulation No 2015/848 on Insolvency Proceedings (Recast) that will create a system of national insolvency registers and establish a decentralized system for the interconnection of such registers by means of the European e-Justice Portal.

Dan Jerker B. Svantesson

The Microsoft warrant case – jurisdiction, data privacy and law enforcement access to cloud data

In December 2013, the U.S. Government served a search warrant on Microsoft under the Electronic Communications Privacy Act of 1986 ("ECPA"). The warrant authorises the search and seizure of information associated with a specified web-based e-mail account that is stored at premises owned, maintained, controlled, or operated by Microsoft. Microsoft has opposed the warrant since the relevant emails are located exclusively on servers in Dublin, Ireland.

The matter raises interesting questions of jurisdiction, data privacy and law enforcement access to

cloud data, and has made its way up the US court hierarchy with the most recent decision being a ruling in Microsoft's favour by the Court of Appeals for the Second Circuit delivered 14 July 2016.

This paper analyses the Microsoft warrant case and its potential implications for the future.

Ulf Maunsbach

Innovative Private International Law

It can be concluded that there presently exists obvious legal challenges. This is perhaps most pressing in the field of information technology. Traditional borders are being blurred, new patterns are created and new concepts are established. Obvious examples are the handling of the increasing amount of cross-border transactions and cross-border relations.

These are examples in relation to which there exist problems as to how the law shall be applied. It can, to put it simple, be hard to find appropriate and functional legal solutions. In this kind of situations you need courage, creativity and knowledge or, to put it differently, innovations in law.

Within existing research on innovation, law is usually not discussed as an object of innovation. Instead law is usually presented as a supporting element that may facilitate innovation, e.g. by protecting an invention by patent law. In my paper I claim that it is also relevant to describe law and legal constructs as such as innovative, innovations in law. One example would be the limited liability company that is one of the primary reasons that made the industrialization successful. Another example is the inclusion of human rights as an important legal perspective, e.g. with the establishment of UN after the 2nd world war.

My paper builds on a research project at the Faculty of Law in Lund that presupposes that there are innovations in law and within the project we claim that it is important to build knowledge about innovations in law, with the purpose of enhancing legal decision-making. The research project will clarify what innovation in law is and it will create a basis for a new approach to legal research. In this paper my ambition is to use the initial finding from the project and apply that knowledge to legal constructions within the field of private international law.

Michał Wojdała

Evidence of the electronic medical records in crossborder proceedings - selected issues

One of the advantages arising from membership in the European Union includes the freedom of crossing borders of the EU countries. It results in increasing number of foreign travels, followed by more accidents occurring abroad, that require emergency health services. If a medical damage is inflicted during emergency health services, there might be a need of pursuing claims in cross-border proceedings. Medical records would then be one of the most important proofs in the proceedings.

Medical records are increasingly electronically-stored and its electronic form gradually displaces paper records. This should not come as a surprise, especially due to its undisputable benefits such as possibility of effortless access to the medical record online from any place and in any time. Yet, there are several problems related to effectiveness of taking this evidence, starting from the poor use of electronic health records in Poland to some technical issues referring to providing this kind of evidence to court.

The aim of this paper is to present a complex analysis of the use of evidence of the electronic health records as well as to attempt to find an answer as to why this kind of evidence is so poorly used in the proceedings and a solution to this matter.

11:15 – 12:45 – Smart Cities – 208

(special track) chaired by **Jakub Míšek**

Lukáš Hoder

Smart Cities, Smart Grids and Big Data: Is there any room left for privacy?

Smart Cities and Smart Grids, i.e. efficient infrastructure utilizing large amounts of data, have been made possible over the past several years thanks to the digital revolution, and current technological advances promise to further digitalize the physical world (the Internet of Things). The fuel that will propel these new developments forward is Big Data, large amounts of data that can be analyzed quickly. However, the EU's current legal framework is not well suited for this brand new world. The Data Protection Directive is more than twenty years old and the legal concepts which it is based on are becoming obsolete. The new General Data Protection Regulation does not seem to properly address the problems associated with Big Data either. Or does it? The article will look at the core principles of personal data protection law and compare them with the reality of Big Data. First, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Second, the data subjects must be informed about the logic behind processing their personal data. Third, the collected personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected. However, all these principles seem to be out of touch with the basic logic behind Big Data analysis. The article will build upon existing literature on the topic and will address the issues above.

František Kasl

Security Risks Hidden behind Fragmented Progression towards "Smart Cities"

"Smart city" represents a merger of the Internet of Things, Big data and Cloud based technologies, which leads to a multiplication of the potential complexities involved in the operation and security of such a system. However, additional risks may be hidden behind imperfections and vulnerabilities created by the fragmented pace of adoption of "smart" features by the current metropolitan areas. The continuous transformation of urban areas will be prone to conflicts between old and new

infrastructure, incompatibility between networks and products by various providers, and consequentially to a multitude of security vulnerabilities. A pivotal role should be given to possibilities for repeatable updates and improvements of the installed devices and their security. Substantial attention should be further devoted to an implementation of some form of data protection impact assessment framework, as well as to a strict emphasis on privacy by design by all introduced devices. Nevertheless, the progressive transformation of current cities into "smart cities" may face significantly larger challenges than any greenfield "smart city" project.

Dariusz Kloza & Niels van Dijk

Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies

Smart grids offer novel means of energy governance and promise an adequate response to environmental, societal and technical developments of the 21st century. Yet, at the same time, they are capable of invading the sacrosanctity of the most privacy-sensitive place – the home.

In this lecture, we will sketch several societal challenges that smart grids pose and amongst these the threat of abusive surveillance practices. They will next overview and critically assess the "light" regulatory approach that the European Union (EU) has taken as a response thereto. By pointing out the seven major drawbacks of this "light" approach, we will argue that its core element, i.e. a data protection impact assessment (DPIA) framework, is rather a missed opportunity. In their opinion, impact assessments of emerging technologies must be inclusive, easy to use and flexible, satisfying certain quality criteria.

11:15 – 12:45 – Psychology of Cyberspace – 209

chaired by **David Šmahel**

Daniel le Roux & CJ Thomson

Failing to Detach: The emergence of the 'always on' culture and how individuals cope with blurred work-home boundaries

The growing prevalence of continuous digital media use among university students in lecture environments has the potential for detrimental effects. In this study the focus is placed upon the implications of digital media multitasking in a university lecture context for academic performance and learning. Previous studies reveal that students frequently engage with digital media whilst in lectures. Moreover, research has shown that multitasking imposes a cognitive cost, detrimental to learning and task execution. We propose, accordingly, that the constant distractions created by digital media interrupt the thought processes of students and, subsequently, obstruct their ability to learn. To test this proposition we conducted a survey-based empirical investigation of digital media use and academic performance among undergraduate university students. The results suggests that media use poses a significant distraction to students which, in turn, draws their attention away from the material presented by lecturers. While this study focused on establishing this negative correlation, future studies should endeavour to describe the media usage patterns that are prevalent among students in both structured as well as self-regulated academic contexts. The intentions of this study are not to condemn students' media use, rather, we argue for sensitivity to the implications of unrestricted, unstructured use of digital media within lecture environments for attention and cognition. In this regard, we discourage blind techno-optimism and encourage mindfulness and critical thinking about technology's role in education.

Birgit Ursula Stetina, Armin Klaps, Zuzana Kovacovsky & Jan Aden

Is this the end of the (fantasy) world as we know it? Multiplayer Online Battle Arenas (MOBAs) versus Massively Multiplayer Online Role Playing Games (MMORPGs)

DotA, a representative of the Multiplayer Online Battle Arena (MOBA) online gaming genre, is played today by an estimated number of players above 20 million, world-wide (Guo et al., 2012). The "phenomenon" MOBA seems to replace the trend of Massively Multiplayer Online Role Playing Games (MMORPGs). MMORPGs once labeled as most "problematic" from a clinical viewpoint now show declining numbers of players. Are MOBAs the new "most problematic" gaming genre?

Using a cross-sectional design with a web-based questionnaire 3898 gamers (mean age 24.24 years; 91.5% male) from German speaking areas were surveyed using several clinical scales (IGD-20, ADS, …) were used. Participants were categorized according to their preferred game into nine genres. Statistical analyses included explorative methods, ANOVAs and t-test.

MOBA gamers show the highest scores in all clinical areas. Furthermore t-tests show especially significant differences between MOBAs and MMORPGs in addiction related questionnaires (IGD: $t(991)=-2.461$, $p=.014$; Engagement: . $t(960)=3.522$, $p<.001$; Addiction: $t(976)=-3.123$, $p=.002$)

Earlier explanations of problematic gaming behavior using game elements of potentially "addictive genres", such as a never ending storyline or an open never ending fantasy world, need reconsidering. The current results cannot be explained that way. There seem to be several unexplored factors which play a relevant role in explaining the phenomenon, potential moderating factors that need more studies.

Masoomeh Taghaddosi & Mohammad Ali Mazaheri

A Comparative study on the ways people face moral situations in real and virtual worlds

Introduction: the concept of "cyberspace" as one of the main structural components of the modern world is perhaps one of the most prominent changes which can depict the difference of

psychological sphere of the modern societies from that of traditional societies. The purpose of this study was to investigate the possible differences in the ways people react to moral dilemmas in cyberspace compared to the ones in the real world.

Method: The research design was causal-comparative. The population was all adults living in Tehran and the sample consisted of 365 persons. To make this comparison, 16 short scenarios (2 female-specific, 2 male-specific and 4 gender-neutral) were designed by the researcher in a way that each pair of scenarios measured a particular subject in the morality of relations once in cyberspace and once in real life.

Results: Findings of the study indicated that in most of the ethical issues raised ,for example, cheating, theft, entering the private space, and etc., there was a meaningful difference between the behavior and the moral judgment of persons in cyberspace and real life. Moreover, the results also suggested that the magnitude of these differences, With regard to the type of moral topic, have changed, but, except for few cases, are not influenced by individual characteristics.

Conclusions: The pattern of the results suggested that due to specific features of cyberspace such as anonymity, lack of outer control, etc., persons facing relatively similar situations in both spaces, tend to deal with moral issues in a more lenient way in cyberspace.

Jakub Remiar

How to use Virtual Reality in Psychology

This talk is the continuation of the last year's talk about the possibilities of virtual reality in psychology. This emerging medium is still continuing to grow in scale and also usage in many fields including psychology. Despite many opportunities this new technology offers, many obstacles prevent it to be commonly used in psychological laboratories. Omitting the technical skills that are needed, design flaws are very prevalent in many of the applications that are currently used. Locomotion and motion sickness solutions are the most frequent problems. Human body requires specific conditions to be meet in order to have a comfortable experience and even achieving the feeling of presence, or in other words, being in the virtual environment. Concrete solutions on how to build a virtual reality environment will be discussed including, psychological, design, technical and financial aspects of this task.

11:15 – 12:45 – Privacy and Surueillance – 025

chaired by **Aleš Završnik**

Lina Jasmontaite, Serge Gutwirth, Gloria Gonzalez-Fuster & Paul de Hert

Incorporating EU Data Protection Principles in Incident Notification under the Network Information Security Directive

The proposed Directive concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive") has been primarily seen as a remedy ensuring reliability and security of network and information systems and services. At the same time, it can be anticipated that once transposed into domestic laws of the Member States, the NIS Directive will have wider implications. In particular, the NIS Directive will affect the protection of individuals' rights to privacy and data protection when handling incident notifications. Incident notification to the NIS competent authority or the Computer Security Incident Response Teams will be a mandatory requirement in cases where an incident will have a substantial impact on the performance of operators of essential services. As explained by the European Data Protection Supervisor, it is highly likely that in the context of incident notification the processed data will include some types of personal data, such as IP addresses or names of contact persons of affected providers of essential services. Building on this observation, this contribution will analyze requirements listed in Article 16 of the NIS Directive in the light of the recently adopted General Data Protection Regulation. While both new regulatory measures call for a culture of risk management, to enhance legal certainty it is important to consider synergies between the two measures.

Adrienn Lukács

To Post, or Not to Post – That is the Question: Why Do Employees Use Facebook and Why Does the Employer Monitor It

Social media are omnipresent in every area of our lives. They are used for numerous objectives: self-expression, keeping in touch with acquaintances, communication or obtaining information about the latest events and news. During their use the individual shares a significant amount of data about himself/herself. This conduct can have serious implications on employment. The (prospective) employer is interested for several reasons in the surveillance of these sites as he/she can easily gain insight into the individual's private life and obtain, without costs, detailed information about him/her.

The aim of the presentation is to highlight the different user behaviours and conducts while explaining the effects of social networks on privacy and elaborate why the employer is interested in their surveillance. Then, I will present the collision of the employer's legal and economic interest and the employee's fundamental right to privacy. As an outcome of the presentation I will draw attention to the legal and ethical problems lying behind social network background checks. I will provide recommendations on how users can continue to use these sites while still preserving their privacy.

Jillisa Bronfman

I'm Ready for My Close-Up, Mr. Spielberg: Creating a Working Model for

Data Security and Personal Privacy in the Use Case of Unmanned Aerial Systems (UAS) in Film and Video Game Production

In the case study of drone development, necessity and innovation have driven the rise of new technologies and new uses of technologies. Lacking a comprehensive regulatory framework in the United States, companies in the film and video game production industries had to either petition the Federal Aviation Administration (FAA) for Unmanned Aerial Systems (UAS) use or venture abroad for more relaxed regulation and enforcement. This article will capture the nascent use of non-military small UAS for film and video games as a model for the promulgation of commercial drone use internationally. The research will address regulations of UAS/drones in the U.S. by the FAA and the National Telecommunications and Information Administration (NTIA), an agency of the United States Department of Commerce, industry attempts at self-regulation, and the regulations offered by myriad international, state, and local entities. The backlash against drone usage in personal and public spaces by privacy advocates and the public has generated debates over the nature of amateur versus professional media development, the definition of art, and the balance between speech and safety. Considering these competing concerns, this article will formulate a viable privacy and security regulatory design for commercial UAS usage that goes beyond a case-by-case analysis and into a workable solution that provides certainty for business operations and a measure of calm in the skies for the public.

13:45 – 15:15 – Cybersecurity, cybercrime – 214

chaired by **Václav Stupka, Jakub Harašta**

Dániel Eszteri & István Zsolt Máté

Identity Theft in the Virtual World: Analysis of a Copyright Crime in Second Life from Legal and IT Forensics Point of View

In Hungary, there is an active practice for inspecting crimes committed in information technology environments as well as crimes affecting intellectual property (the two areas often overlap). Moreover, the moment has recently come when a criminal infringement of copyright occurred in a very special environment: in the virtual world of Second Life.

In our paper we present the questions raised by the abovementioned case from a legal and IT forensic perspective, as well as the answers recommended by the authors.

The first half of the article will present the specialties of virtual world environments and how the criminal investigation started. We also discuss general criminal procedure norms governing IT forensics. We try to answer the question that how copyright law protects avatars or virtual items in Second Life and how can we assess the financial value of a virtual item. The second and main part of the paper will present in detail the IT forensic examination of a concrete criminal case where illegal copies of avatars appeared in Second Life. We discuss the question in detail that how digital evidences can be obtained from simulated virtual environments from a legal and IT forensic perspective.

The paper was written in order to stimulate interest in the special field of relationship between IT forensics, criminal law and virtual worlds because articles dealing with the aforementioned problem in scientific literature are barely found.

Sarah Markiewicz

Cybersecurity Law : join reading of the ISO 27001 norm, the NIS Directive and the French RGS

The purpose of this talk is to discuss the relations between different texts who try to regulate the computer systems and networks security. At the international level, there is the ISO 27001 norm called “Information Security Management Systems” which is an extralegal instrument drafted by the International Organization for Standardization, published in 2005 and reviewed in 2013. At the European scale, a European Directive on security of network an information systems has just been adopted on 6 July 2016 which will play the role of basic legal text all around the European Union. Eventually, at a national level, in France, the National Agency for Information Security Systems, independent administrative authority edited a toolkit in this field : the General Reference Document for Security (1st version : 2010, 2nd version : 2014). Despite all these texts have the same topic, their territorial application and normative power are different. This talk proposes to identify if by reading both of them, we can reach to some common foundations and principles which apply as cybersecurity law and maybe, point out some different approaches. Afterwards, we will analyze the relations between both of them with respect to their matter scope and application scope : Do they cover exactly the same area ? Can they apply together by successive layers ? Can we define a reading order between them : one can be considered as a more detailed or technical version of another one like an appendix ?

Walter Hötzendorfer, Christof Tschohl & Rolf-Dieter Kargl

The implications of the NIS Directive on CSIRTs

Cyberspace is facing a continuous increase of threats. Therefore, Computer Security Incident Response Teams (CSIRTs/CERTs) are becoming more important and more numerous, which demands an intensified communication between CSIRTs as well as with other stakeholders. In July 2016 the European Directive on security of network and information systems (NIS Directive) was enacted. We will introduce the content of the Directive and scrutinize the new legal framework, obligations and duties it puts in place specifically for CSIRTs. We will then focus on the direct and indirect implications the new Directive will have on the communication of CSIRTs amongst each-other and with other stakeholders. Finally we will discuss what the Directive leaves open for the national legislators in this field and propose options for implementing acts. This presentation will be based on results from the Austrian research project CERT-Komm II. In case similar papers are proposed, we are happy to coordinate with the other authors and focus on a more specific aspect of the topic.

13:45 – 15:15 – Ideas for Cyberspace – 215

chaired by **Herbert Hrachovec, Radim Polčák**

Damian Klimas

Marco Civil da Internet as a perfect (?) regulation of Internet

The Internet is an object of interest of Brazil government for a long time. Establishment of the Brazilian Internet Steering Committee (CGI.br) may be a good exemplification of such. The Committee was created in 1995 to coordinate and integrate all Internet initiatives in Brazil, as well as the promotion of high-quality technology and innovation.

Brazil is one of few countries with such far-reaching regulation of information society. This regulation solves important issues raised in the doctrine of the ICT law. It is certain, however, that this act caused quite a stir as well as it was very positively received by Internet users in Brazil. This

is, so far, the most mature private act regulating Internet.

Despite brazilian net neutrality in mid-2015 the Brazilian criminal court ordered the block of WhatsApp application for 48 hours. Lock was caused by a rejection of Facebook to provide the data from the WhatsApp account of a mobile phone. The user of this mobile phone was suspected of having committed a serious offense (was a gang member).

The news spread around the world very fast. Especially because 96% of smartphone holders in Brazil uses WhatsApp for communication.

The lecture will aim to present the privacy regulations of Marco Civil da Internet and summarize legal and social issues that this regulaton caused. These problems have become the basis for the judgement of Criminal Court de São Bernardo do Campo in August 2015 which background will also be presented.

Jakub Harašta

Technology neutrality - single concept or mythical beast?

Technological (or technology) neutrality has been often coined as a principle – principle governing the creation of new legislation or interpretative principle preventing hindrance of law by the new technology. Many authors approached the notion in many papers – often stating multifaceted nature of technological neutrality (Koops, 2006; Reed, 2007; Reed, 2010; Ohm, 2010; Birnhack, 2012; Hildebrandt/Tielemans, 2013; Craig, 2014). Some of the authors reached conclusion that this principle may not be the way forward (Ohm, 2010; Birnhack, 2012) because properly neutral legislation cannot be drafted – it is always based on the underlying idea of a particular technology (Bennett Moses, 2007; Birnhack, 2012; Olsen et al., 2016) or the law itself is embodied in specific technology of printing press that cannot be escaped (Hildebrandt, 2011).

The proposed paper aims to review these approaches in their underlying theoretical notions, since some of the approaches towards technology neutrality can be read as advocating various ways of purposive interpretation, while some seem to be calling for a specific legislation technique (such as use of general terms and future-proofing clauses) or for starting (at least to certain extent) over. Ultimate goal is to understand the extent to which the technology forms the law and vice versa, being it the technology-specific nature of law in general, technology-specific nature of specific laws or techno-regulation in the form of Lessig's Code.

References:

- Bennett Moses, 2005 – BENNETT MOSES, Lyria. The Legal Landscape Following Technological Change: Paths to Adaptation. Bulletin of Science, Technology & Society, 2007, vol. 27, no. 5, pp. 408-416.

- Koops, 2006 – KOOPS, Bert-Jaap. Should ICT Regulation be Technology-Neutral? In Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds.). Starting Points for ICT Regulation. Deconstructing Policy One-Liners. The Hague: T.M.C. Asser Press, 2006. Pp. 77-108.

- Reed, 2007 – REED, Chris. Taking Sides on Technology Neutrality. ScriptED, 2007, vol. 4, no. 3, pp. 263-284.

- Ohm, 2010 – OHM, Paul. The Argument Against Technology-Neutral Surveillance Laws. Texas Law Review, 2010, vol. 88, no. 7, pp. 1685-1713.

- Reed, 2010 – REED, Chris. Online and Offline Equivalence: Aspiration and Achievement. International Journal of Law and Information Technology, 2010, vol. 18, no. 3, pp. 248-273.

- Hildebrandt, 2011 – HILDEBRANDT, Mireille. Legal Protection by Design: Objections and Refutations. Legisprudence, 2011, vol. 5, no. 2, pp. 223-248.

- Birnhack, 2012 – BIRNHACK, Michael. Reverse Engineering Informational Privacy Law. Yale Journal of Law and Technology, 2012, vol. 15, no. 1, pp. 24-91.

- Hildebrandt/Tielemans, 2013 – HILDEBRANDT, Mireille and Laura TIELEMANS. Data protection by design and technology neutral law. Computer Law & Security Review, 2013, vol. 29, no. 5, pp. 509-521.

- Craig, 2014 – CRAIG, Carys J. Technological Neutrality: (Pre)Serving the Purposes of Copyright Law. In Michael Geist (ed.). The Copyright Pentalogy: How the Supreme Court of Canada Shook the Foundations of Canadian Copyright. Ottawa: University of Ottawa Press, 2013. Pp. 271-305.

- Olsen et al., 2016 – OLSEN, Matt, SCHNEIER, Bruce, ZITTRAIN, Jonathan et al. Don't Panic. Making Progress on the "Going Dark" Debate. Available at https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Tomáš Abelovský

Beyond a digital doubt: lucky chance in the cyberspace

Electronic stored information (ESI) represents data utilized in digital form, requiring the use of computer hardware and software. It doesn't matter if it is a picture, confidential document or log of an IP address, we often think about it as a tangible object in determined environment. When we talk about the evidence, we understand available body of facts or information signaling whether a hypothesis is true or false. Nevertheless, the signalization can be deceived by various factors such as a false ESI, procedural elements or our prior beliefs. Can we avoid these fallacies by probability method? There is comprehensive discussion of the role of evidence generalizations and hypotheses. When we evaluate data, we may also create the evaluated data. In another words, we involve elements of prior probabilities to our beliefs in framing our conclusions. The following paper argues that the ESI misinterpretation could be deciphered also by explanation of probabilistic and statistical reasoning next to the procedural law. The more alternative explanations there are for the evidence, the less plausible our beliefs are and vice versa (e.g., Bayes' theorem). We explain the role

of the chance and probability in the light of the electronic evidence/digital forensic.

Navid Khazanei

First amendment's homesickness, second amendment's homecoming: militia as "501(c)," arms as "code"

Hannah Arendt, Justice Kennedy, and Citizens United's critiques as well as the modern pro-gun movement all share the same homesickness: A First Amendment homesickness. The pro-gun movement's answer to this homesickness is a Second Amendment homecoming. However, the outcome of Defense Distributed v. U.S. Department of State, a recent case about 3D printable gun codes, illustrates why this pro-gun's answer is misguided.

Employing Arendt's thoughts, this paper argues that a proper answer for the current crisis in the jurisprudence of the First Amendment and the Second Amendment should entail the understanding that: (I) "freedom of speech" should only be protecting speech-action that concern public interest; and (II) "the security of a free State" requires adequate access to the infrastructures that make speech possible, thus, violence impossible.

As this paper concludes, by developing atomic weapons, the government has "constructively taken" the people's "right to keep and bear Arms." Accordingly, this paper suggests a model on how the government may provide a "just compensation" for this "taking" as required by the Fifth Amendment's "taking clause." The model demands that equal to a portion of the defense budget should be spent annually to publicly fund 501(c) organizations, the modern "well-regulated Militias."

13:45 – 15:15 – International Internet Law – 109

chaired by **Dan Jerker B. Svantesson**

Ravinder Kumar

Cyber Defamation in India

The term 'defamation' is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The defamation is both a crime and a civil wrong. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public. Cyber defamation is a new concept but the traditional definition of the term defamation is application to the cyber defamation as it involves defamation of a person through a new and a virtual medium. The widespread use of internet has also given a new face to the crime and a new medium to the bad elements to commit crime.

Thus, Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. Accordingly, if someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation. It is important to note that harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world. Therefore, Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim.

In India, Cyber Defamation results in Civil as well as Criminal proceedings against the offender. Some the Acts and rules that deals with Cyber Defamation are The Indian Penal Code, 1960, The Information Technology Act, 2000, The Code of Criminal Procedure, 1973 and The Indian Evidence Act, 1872. The Charging Act for prevention of Cyber Crimes in India is the Information Technology Act, 2000. Section 66A of the Information Technology Act, 2000 provides punishment for online Defamation.

Thus, the law of defamation requires a delicate balance between the right of person not to be defamed and the right of others to engage in free speech. However, it is harder to maintain in case of internet, which has been visualised by judicial approach in India over this issue. Following the Honourable Supreme court of India's decision over the issue, the researcher examines the recent developments in Cyber defamation law in India.

Anabela Susana de Sousa Gonçalves

Choice-of-court agreements in electronic international contracts

Regulation No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) establishes that the parties may agree in giving jurisdiction to a court or the courts of a Member State to settle any disputes in a particular legal relationship, under certain requirements. According to Article 23, and in addition to other requirements, the agreement shall be: in writing or evidenced in writing; or in a form which accords with practices established between the parties; or in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned. Section 2, of Article 23, determines that it will be equivalent to a writing agreement any communication by electronic means which provides a durable record of the agreement. The regulation No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

(Brussels I Recast) maintains the same wording in Article 25, section 2. This presentation will try to determine how should be interpreted the concept of any communication by electronic means which provides a durable record of the agreement in contracts concluded electronically, for example when click-wrapping occurs, taking into account the ECJ jurisprudence.

Veronika Křížová

The Future of International Business in the Light of GDPR and Modernization of the EU Copyright

The year 2016 brought several important changes in the area of international internet law. In May, the official texts of Regulation (EU) 2016/679 and Directive (EU) 2016/680 – the EU's General Data Protection Regulation (GDPR) – were published, discussion about DSM Strategy is still on-going and the second set of legislative proposals of the Commission was introduced in September. Additionally, the European Court of Justice has ruled in several important cases regarding the copyright law on the internet, such as GS Media v. Sanoma or Mc Fadden; and for the data protection enthusiast, there is the interesting development of the Schrems case, following the CJEU's decision last October. General discussion of the significant changes in legal regulation of Ecommerce has not developed evenly. On copyright related issues some industries were more active than others. Nevertheless, the current framework for modern EU copyright poses more questions than it provides answers with respect to the application of proposed directives and regulations. Even more important is the unsettling unpreparedness of companies and institutions to comply with the GDPR, which comes into effect as early as May 2018. The aim of this article is to show on several examples some of the expected changes in international business practice in light of the latest developments in EU legislation and case law of the European Court of Justice. The main focus of the article is on the GDPR compliance and the future of international business transactions concerning copyright protected digital content.

13:45 – 15:15 – New Media and Politics – 208

chaired by **Alena Macková**

Robert Imre

Populism and New Media: Hungary and Finland

The rise of populist political parties throughout Europe has been a major concern for analysts for some time now. The changing political landscape since the end of the Cold War and the subsequent expansion of the EU has changed political alignments on the European subcontinent. In both media studies as well as communication studies there have been significant treatments of populism as a political movement as well as specific populist political parties. In this paper I will compare recent developments in Finland and Hungary regarding populist political discourses. This paper also uses approaches from media studies as well as specific analytical standpoints from political communication studies. My concern here is to examine the messaging of 'populism' writ large via social media and mainstream media.

Both Finland and Hungary have appealed to versions of ethno-nationalism, limited resources, threats of political violence from nefarious outsiders, and being overrun by asylum-seekers and migrants. These populist discourses are quite amenable to social media constructs, as they can be extreme views, even by elected officials, and then subsequently 'watered down' in mainstream media to thus make it appear as if both far-right and populist political positions as officially stated are quite reasonable and centrist.

My paper here is concerned with the differences and similarities in the tactics and messages of populist movements as well as populist political parties in Finland and Hungary.

Norbert Merkovity

Trump and Others: The Emergence of Attentionbased Politics

This presentation will introduce the findings of two research projects on politicians' use of Twitter and Facebook in order to attract, maximize, and direct the attention of followers and journalists. The used communication techniques set the focus of analysis on the attention-based politics and the phenomena around it (network logic, self-mediatization, popularization and populist political communication). The main findings of the research are that ICTs do not create a further advanced 'public sphere' but rather guarantee unidirectionality of communication. The research results showed that Social Networking Sites are significantly more often used for informational (press conference like) communication. However, the politicians' behavior could change this picture (see Donald Trump's SNS campaign).

Altogether, the presentation will support the thought that the new ICTs will not revolutionize political communication, what we see is a 'spectacular' development, adaption to the information environment, which process is once faster, other times slower. This makes one feel that what has been well-functioning in political communication in the past few years is now becoming obsolete.

Michal Kus

Citizen journalism in Poland: actors and structures

Citizen journalism (CJ) is frequently defined as mode of public communication that fulfills the same tasks as professional journalism, i.e. the selection and dissemination of current topics for the self-monitoring of society. However, in the case of CJ, the relevant contents are produced by non-professional actors, mostly media users who avail themselves of the participatory potential of digital media (Lewis, Kaufhold, and Lasorsa 2010).

In Poland, the term "citizen journalism" was highly debated between 2007 and 2011, when different traditional media companies started their own "citizen" or "participatory" journalism platforms – but only few of them survived. On the other hand, independent CJ platforms and individual (or

small-team) CJ initiatives started to develop at the same time.

This paper focuses on historical and structural aspects of CJ in Poland, concentrating mostly on CJ landscape as well as on complex relationships between actors representing institutionalized media field (mainstream media) and those coming from outside institutionalized media field.

Research methods include: desk study (to map the field of CJ and highlight the most relevant examples) and semi-structured interviews with practitioners in the field (representing three different types of CJ, mentioned above).

Results of this study are part of a multi-national analysis in six European countries (UK, Germany, Austria, Switzerland, Italy, and Poland).

13:45 – 15:15 – Psychology of Cyberspace – 209

chaired by **David Šmahel**

Piergiovanni Mazzoli & Aurora Bobocea

Net Addiction in Preadolescence and its Prevention

Net addiction is becoming an increasingly worrisome issue especially amongst preadolescents and there is a widespread need to further explore its potential effects and its prevention. In 2015 we launched a research project on the use, abuse and dependence to the Internet. We examined a sample of 2900 preadolescents, with the age range of 11-15 years-old. For the analysis we used the UADI questionnaire. In the data cleaning phase, we discarded from the data analysis those questionnaires that had more than 5% missing or invalid responses, which left us with a sample of 2432.We proceeded with a first statistical analysis on this sample, followed by second analysis on a further reduced sample obtained by discarding those questionnaires with at least one null response (1723).Both samples were balanced to respect the gender distribution and their comparison allowed us to increase the reliability of the results. The analysis was focused on the following five factors which gave us a full picture of the Internet usage of the subjects: Compensatory Evasion (EVA), Impact (IMP),Experimentation (SPE),Dissociation (DIS),Dependence (DIP).Overall we found that a significant percentage of the sample(6.3%) is in a risk area, or has a clear dependence to the Internet(2.4%).Thus, we can say that the phenomenon is present and relevant to the extent of 8.7% of our sample. Based on these outcomes, we launched a prevention project based on EB prevention and targeted to parents and primary school teachers.

Lukáš Blinka & Anna Janů

Parental factors in adolescents' excessive internet use

The term excessive Internet use (EIU) is often associated with determining pathological extensive Internet usage, which could also be called "online addiction" and is usually defined by the following components used for determining other types of addictive behaviour: salience, withdrawal symptoms, tolerance, conflicts and relapse reinstatement and. The described behaviour may lead to the social, mental and also physical impairment of children and youth. A number of recent studies have provided insights into the prevalence and correlates of this phenomenon. Still, so far only a very limited amount of research has focused on excessive Internet use among adolescents in different but comparative cultural and national contexts.

In this presentation I will conclude findings from the EU Kids Online II project, which includes representative samples of adolescents aged 11 to 16 from 25 European countries (N = 18,709), the biggest pan-European project on social and psychological factors of children digital media use so far. A short five-item Excessive Internet Use Scale was used to measure the phenomena. In the presentation, I will provide methodological of the project and psychometric properties of the scale. Also, I will discuss problematics of identifying at-risk population, psychological, behavioural and social factors associated with EIU as well as cross-country and cultural differences.

Ondřej Ostrovský & Šárka Licehammerová

Dissociation among online players - case studies of live online gamblers

Beginning of gambling and dissociation research is possible to find in the early nineteen eighties, when Durand F. Jacobs began his work, which resulted in the formulation of General Theory of Addictions, published in 1986. It includes The Addictive Personality Syndrome (APS), which is a set of physiological (condition of chronic hyper or hypo arousal) and psychological (child experiencing trauma or rejection in childhood) predisposition to addiction. These are activated at the moment when a person with the APS encounters with the activity, which will provide dissociation experience. It is represented by feeling of absorption, trance, depersonalization, feeling that I am someone else or amnesia for gambling session.

Based on the gambling research, there is a justified assumption that certain games can associate with dissociation more than others. especially VLT and EGM (Griffiths, Wood, Parke & Parke, 2006; McCorriston, 2006). Considering the specific characteristics of online gambling it can be assumed that a high level of dissociation will also experience the players participating in online gambling.

The aim of the presentation is to link knowledge about the manifestations of dissociation by the online players from theory with concrete examples from case studies of gamblers - live online bookies. Research on the presence and quality of dissociation has the potential to provide an important source of knowledge for creating policy toward a preventive measures and treatment.

13:45 – 15:15 – Privacy and Surveillance – 025

chaired by **Aleš Završnik**

Michal Czerniawski

Territorial scope of the EU data protection regime in the age of an equipment-based society

Territorial scope of the EU data protection law is a very complex issue. Article 4 of the Data Protection Directive (DPD) is considered as 'arguably the most controversial, misunderstood and mysterious of the Directive's provisions'. According to Article 4(1)c of the DPD, EU data protection law applies to the processing of personal data where a data controller makes use of equipment situated on the territory of a Member State.

The notion of 'equipment' goes beyond computer servers, terminals or questionnaires – examples indicated by the drafters of the DPD. Today we can add to this list various kinds of electronic devices, such as smartphones, connected cars, wearables, smart TVs, fitness equipment or mobile applications. It is justified to say that the information society and the digital market rely on various kinds of equipment, used for processing of information and that the information society can be seen also as an 'equipment-based' society.

In this analysis I compare article 4(1)c of the DPD with Article 3(2) of the General Data Protection Regulation (GDPR). I conclude that the jurisdictional scope of the GDPR, based on targeting and market access trigger, seems to be more reasonable than 'use of equipment' criterion incorporated in Article 4(1)c of the DPD, as the latter, in the 'equipment-based' society we live in, results in lack of legal certainty and brings the risk of jurisdictional overreach.

Aleš Završnik

"Algorithmic cops": introduction to big data policing

The automatic generation of huge amounts and diverse sets of data used for data mining and processing by algorithms to be acted upon in decision-making processes has profound implications for crime control. It has been claimed by many that our world is running on artificial intelligence and data processing in many fields of our lives, as social networks suggest whom to befriend, algorithms trade our stocks, and computers help the military find its targets. This "revolution that will transform how we live, work, and think" (Mayer-Schönberger & Cukier 2014) is shifting power relations in the so-called "security and control" domain as well.

"Predictive policing" has quickly emerged as one of the buzzwords of contemporary Anglo-American policing. It was recently defined in a Rand Corporation report as "the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions" (Perry et al., 2013: xiii). Predictive policing software, such as IBM's Blue Crush program, produce probability reports on criminality. The TrapWire program looks for patterns that would help predict terrorist attacks. These analyses include information posted on social media and YouTube usage profiling, by using techniques such automatic sentiment analysis and emotion analysis techniques (e.g. SentiStrength) that produce understanding of how citizens behave online. There are number of ways for the police to monitor social media discussions and perform social media sentiment analysis ("Opinion mining").

Underlying these and many other potential uses of big data in crime control, however, are a series of legal and ethical challenges relating to, inter alia, privacy, discrimination, and the presumption of innocence, that the paper outlines.

Jan Tomíšek

Data transfers in cloud computing: does GDPR change the game?

General data protection regulation (GDPR) is the most significant change in the legal regulation of privacy since the adoption of the current Directive 95/46/EC on the protection of personal data. GDPR establishes adequacy decision, appropriate safeguards (such as binding corporate rules, standard contractual clauses, codes of conduct and certifications) and derogations as the tools for transfer of personal data outside the European Union. These tools also apply to data transfers that take place in course of provision of cloud computing services. As the share of cloud services on the IT market increases, the relevance of this topic also grows.

The paper will analyse instruments for data transfers under GDRP and how they apply to data transfers in cloud computing in the light of the decision of the Court of Justice of European Union in Case C-362/14 Maximillian Schrems against Data Protection Commissioner (with its requirement of "essential equivalence" applied to GDPR), adoption of Privacy Shield and standard contractual clauses decision expected to be challenged. It will be discussed what will be the impact of that GDPR brings in comparison to the Directive 95/46/EC to data transfers in cloud computing and what should be the best approach to regulation of these transfers in future

Jakub Míšek

Built-in filters in the Personal data protection system

One of the biggest problems with the current legal system of personal data protection is its incapability to react properly to everyday life situations. Even though this is mostly connected with information and communication technologies, it is a general problem. The system created by the European Directive 95/46/EC is set in a binary matter. Something is personal data, and thus all the duties of the controller must apply. Something is not personal data, and hence no duties apply. In connection with the broad definition of personal data can this situation lead to absurd conclusions that data controllers must fulfill duties, which just cannot be met in this technical reality. There are two ways out of this situation. The first one is narrowing the input of the system - definition of

personal data. The second one is an existence of granularity of duties within the system, and thus narrowing the output. It is an aim of this article to examine thoroughly possibilities for enhancing granularity of data controller duties which offers the General Data Protection Regulation (GDPR). In the first part, the article presents some examples of obvious failures of the system, e.g. internet search engines and IP addresses within cybersecurity context. The second part discusses possible solutions which can be found within the current system of the Directive 95/46/EC. The third part analyses GDPR and evaluates whether it helps to solve the discussed problem.

15:30 – 17:00 – Intellectual Property On-Line – 214

chaired by **Andreas Wiebe, Matěj Myška**

Aurelija Lukoseviciene

The changing concept of "author" in the context of EU copyright law

The ways people create and communicate their creations in different historical periods were always a result of interaction between culture, social/legal norms and technology in that specific place and time. Likewise, the understanding of what it means to be an author, what is the role of an author in the society, and what are her needs has also been different, ranging from mere servant of God's will to a craftsman, to solitary genius, and someone not needed at all after the work is created (the famous "death of the author" in post-modernist thinking).

Copyright laws have for a long time been in the centre of regulation of creation and distribution of culture and are the source of certain understanding of "author" while technological changes always called the rigid copyright concepts into question and forced them to change. Now after the new digital technological revolution we see some harsh discrepancies between the understanding of "author" in the legal and the digital contexts as well.

In my thesis and this presentation I want to expose several of these discrepancies between copyright laws in EU (including the legal systems of member states where there is no sufficient harmonisation) and the communities forming under so-called User Generated Content (UGC) phenomenon. What does it mean to be original in both of these contexts? What moral rights mean for these different "authors"? These are the questions I plan to address.

Martina Kotyková

Protection of graphical user interface, sequence of snapshots and animated icons

Industrial design protections for graphical user interface (GUI) and animated icons has already become mainstream, as many jurisdictions around the world regularly are granting Industrial design registration/ patents for GUI and animated icon design innovation.

In many of these jurisdictions, these types of designs are among the fastest growing and the types of industrial designs for which design protection is most frequently sought, both by local designers and designers from around the world.

This essay analyzes the options for protection of a graphic user interface (GUI), sequence of snapshots and animated icons by way of design registration at The Industrial Property Office of the Czech Republic (IPO CZ) and at the European Union Intellectual Property Office (EUIPO). There is a different attitude of IPO CZ and EUIPO to registration of GUI, sequence of snapshots and animated icons. From the perspective of the Czech Republic in case of registration of GUI, sequence of snapshots and animated icons as a design there is a problem of the product definition. Different attitude to that point is thus not given only by a different form of the representation requirement, but by different understanding of what is a "product" in accordance with the definition of EC Council Regulation no. 6/2002 on Community Designs. This essay highlights future development as a result of the harmonisation of processes throughout the EU.

This essay also mentions options for protection of GUI as a part of patents and utility models as well as the fact that copyright law may not adequately protect GUI.

Michaela MacDonald

Copyright Implications of Creative Uses of Video Games

Creative uses of video games, such as e-sports and live streaming, fan creations, mods, bots and emulators, or the issue of video game preservation all touch upon a wide range of exclusive rights of the copyright owner (the right of reproduction, display, making derivative works, public performance and so on). The issue is that current copyright law does not yet recognise a category for 'amateur creative expressions' and it is thus unclear what precisely the legal implications of transformative uses of video games are. Copyright owners often opt for the so-called 'tolerated use' policy and there is always a DMCA procedure available. Users, on the other hand, can argue that their use falls under the fair use defence. There is also the 'de minimis' argument, which is based on the premise that the copying is so trivial it does not meet the legal threshold for actionable copying. However, it is difficult, if not impossible, for a lay person to navigate the counter-notice procedure and other avenues in case that their content is taken down or to determine what qualifies as fair use. Moreover, ISPs such as YouTube or Twitch can unilaterally remove content or withdraw their services, leaving users with little or no recourse to pursue their rights. Developing new technologies that allow anyone to produce and circulate 'cultural' material demands that copyright law reconsiders the position of both owners and users of copyright-protected material.

15:30 – 17:00 – Legal Informatics – 215

(special track) chaired by **Erich Schweighofer**

Jakub Harašta, Matěj Myška, Pavel Loutocký, Jakub Míšek, Michal Malaník, Markéta Klusoňová, Monika Hanych & Jaroslav Šavelka

Citation analysis - understanding the citations in the Czech law

The research we intend to present aims towards creating resources for the complex citation analysis of the Czech case law. Complex citation analysis allows for more efficient information retrieval, cost savings on empirical legal research and more legal certainty. We plan to briefly elaborate on these underlying principles behind our methodological research.

We will focus on introducing the annotation manual as a resource allowing us to create the gold standard for complex and full scale citation analysis of case law of the Czech Constitutional Court, Supreme Court and Supreme Administrative Court. Despite our work being oriented specifically towards the Czech legal environment (and thus being language-specific), we believe many issues not to be bound to specific language and legal environment, and therefore being suited for discussion with international audience of the Cyberspace conference. Overall, we argue for the necessity of distinguishing of argumentative and procedural citations and descriptive and normative jurisprudence. We also include the law and literature movement.

Besides introducing the annotation manual as the final outcome of this research stage, we aim to discuss the future work arising from it, such as the coefficient for structuring vastly prevalent positive sentiment of citations.

Bernhard Waltl, Thomas Reschenhofer & Florian Matthes

Tool-supported Collaborative Design of Semantic and Executable Models from Normative Texts

The interpretation of normative texts, such as laws, or contracts, is a complex, knowledge-, time-, and mostly data-intensive task. Therefore, several attempts have been made to formalize this process, which have met rather less approval in legal science and practice.

Based on the modeling of the product liability act, this paper proposes a collaborative modeling environment to support the analysis and interpretation of normative texts. It implements state-of-the-art text mining technologies to assist legal experts during the modeling of norms by automatically detecting key concepts within normative texts, such as legal definitions, prohibitions, etc. This paper describes a collaborative application supporting the creation of semantic and executable models of norms by multiple users. In addition, main requirements for such a text mining environment are derived. The implementation extends an existing data science environment and describes a reference architecture and data model. Finally, the technological and methodological limitations are discussed.

15:30 – 17:00 – International Internet Law – 109

chaired by **Dan Jerker B. Svantesson**

Tereza Kyselovská

The Hague Conference "Judgments Project" and Principles on Choice of Law in International Commercial Contracts – "old wine in a new bottle" for online contracts?

The Hague Conference on Private International Law has for many years worked on several projects and proposals to harmonize the private international law rules for civil and commercial matters with cross-border element. The recent work is presented by the "Judgments Project" and the Principles on Choice of Law in International Commercial Contracts (Choice of Law Principles).

The "Judgments Project" on cross-border litigation in civil and commercial matters (jurisdiction and recognition and enforcement on judgments) was initiated in 1992. Later, due to several factors, it was abandoned. In recent years, the project was resurrected, and in 2016 work on proposed draft text Convention continues. The "Judgments Project" should certainly be welcomed. The rules on jurisdiction and recognition and enforcement of judgments are the core of private international law. Nevertheless, in the context of online activity, with emphasis on legal certainty and predictability, it is necessary to assess its provisions and their applicability to contracts concluded online.

The Choice of Law Principles is, in my opinion, less significant project of the Hague Conference. Their practical application and impact is very debatable. In my opinion, it will turn to be another merely "academic" project. Nevertheless, I would like to briefly analyze its relevant provisions in the context of online commercial contracts.

In my presentation, I would like to analyze relevant provisions of the two Hague Conference projects and critically asses their relevance, impact and application on online activity and online contracts. I would like to debate necessary changes and present ideas de lege ferenda.

Anna-Maria Osula

Notifying the other state about remote search and seizure: obligation or politeness?

With the general aim of respecting private life, home and correspondence, lawful search and seizure in domestic criminal procedure usually include the requirement of providing a notice of the search. If there are reasonable grounds for believing that compliance with such a requirement would unduly prejudice ongoing or subsequent investigations or endanger the safety of any person, the requirement may be postponed.

This presentation will move from domestic regulation to international and ask what is the role of notification in remote search and seizure procedures if domestic law enforcement is, during an investigation, accessing data that is not stored on domestic territory? Is such notification required by international law (e.g. to exclude a possible breach of territorial sovereignty) or is it merely a polite gesture introduced by a few states (e.g. Belgium which requires notifying the other state of remote search after the procedure has taken place)?

In circumstances where the location of the data can be identified, the obligation to notify the other state about transborder access has been discussed before; however, it was not included in the CoE Convention of Cybercrime Article 32(b) as a condition for transborder access. Given that the possible breach of territorial sovereignty is one of the central debates hindering an international agreement on transborder access, it should be examined whether a notification prior or after the search would exclude the breach and be thereby able to take the discussion forward. Another issue is whether such a notification should be a one-way formal declaration or should it also require a response from the other state (the latter would open up a number of additional challenges that are related to the current MLAT process such as non-responsive states).

Finally, the presentation will discuss alternatives to the requirement of notifying the state, given that determining the exact geographical location of the data (e.g. due to cloud computing) may not be feasible.

Nicholas J. Gervassis

From Delphi to DELFI – part 2: The Developing European jurisprudence in View of MTE v Hungary

Less than a year since the Grand Chamber's decision in the case of Delfi AS v Estonia (app. no. 64569/09), the Strasbourg court faced almost similar facts in MTE & Index.hu v Hungary (app. no. 22947/13). The latter ruling, however, looked in the opposite direction when answering the question of whether an ISP's Freedom of Expression has been violated following the imposition of liability over hosting defamatory comments by third parties.

While early predictions on the Delfi case's possible jurisprudential impact were correct in their instincts to downplay it – actually, to disregard it – there are still several questions unanswered, regarding the applied standards across Europe for regulating the operations of online intermediaries and the ways in which our contemporary judicial oracles understand both how society assimilates the use of new technologies and life in cyberspace.

This discussion observes the developing European outlooks in applied regulatory practices and judicial decision making; that is, way down the line after the introduction of the Directive 2000/31/EC on Electronic Commerce and certainly at a time when national and international appreciations of human rights and citizenship in online contexts should have matured and presented a more 'harmonious' picture. While MTE should have been seen as establishing a desirable order that Delfi almost disturbed, the background of facts and subsequent judicial utterances hint, we argue, that uncertainty still prevails.

15:30 – 17:00 – New Media and Politics – 208

chaired by **Monika Metyková, Jakub Macek**

Tonatiuh Lay

The criminalization of the on line social protest in Mexico

Mexico has two highlighted social movements for the use and appropriation of cyberspace , these are the Zapatismo, emerged in 1994 and #YoSoy132, in 2012. Although these movements continue to have some effect, the emergence of both occurred in different contexts, but taking similar feature as the establishment of its communication strategy and agenda on the Internet and virtual social networks. Similarly, other social movements have made use of these tools, reaching different goals and objectives.

However, the proliferation of these movements, along with their appropriation of cyberspace aroused suspicions and fears both the political class and the Mexican federal government, that`s why the federal legislators began to present initiatives to create or modify laws to restrict certain Internet applications and content through virtual social networks. Some of these proposals were rejected immediately, others are still under study, but some were approved and endorsed by the own Supreme Court of Justice.

The aim of this paper is to describe and analyze the social movements that have made use and appropriation of cyberspace and various tools associated with it, as well as legislative and government proposals to censor and criminalize these actions, which is, obviously, a decline in Mexican democracy and its institutions.

Zuzana Pešťanská & Magdaléna Petrjánošová

Social media and birth narratives: From sharing intimate experience to human rights activism

In this paper we will discuss the beginnings and current activities of a Slovak NGO focusing on reproductive, parental and patient´s rights. We will demonstrate how sharing of birth narratives through social media contributed to the start of the NGO in 2011 and how social media help spreading its (in Slovakia non-mainstream) ideas about pregnancy and childbirth specifically, and patient´s rights in general. We will corroborate our argument using ethnographic interviews conducted with the members of the NGO and other women who support its activities. Our analysis shows also how cooperation with human rights lawyers and social scientists was crucial on the path towards activism, because it gives the NGO´s activities political significance and the weight of expert knowledge.

Monika Hanych

Image of the Czech Contemporary Constitutional Court´s Judges in Online Media

It could be assumed that the Czech Constitutional Court judges and their decisions affect both the legal system and functioning of law in the Czech society to a significant extent. Moreover, the judges are not "anonymous", neither individuals mechanically deciding on submissions; they are publicly known and active subjects with certain characteristics, preferences, and attitudes. Therefore, it might be in the interest of the citizens to be informed not only about the results of the judicial proceeding but also about the ones who decide. The paper focuses in this regard on the image of the current Constitutional Court judges – as of public officials – as constructed by the Czech online media (currently the second most preferred source of news of the Czech media audiences). While in the US it is conceived regular to publicly inform about a judge both in terms of her personal and political standpoints and as well as her comments on judicial decisions, in the Czech Republic such practice has been so far avoided. In other words, this contribution draws upon an assumption that the Czech constitutional judges are reported in media only as "impartial" commentators of their own decisions, while any more complex representation of them as of individuals is omitted. The research employs a method of content analysis, inquiring selected Czech news portals in a period of six months during 2016.

15:30 – 17:00 – Religion in Cyberspace – 209

chaired by **Vít Šisler**

Seyedehbehnaz Hosseini

Transnational religious practices on Facebook: The ethnography study of the Yārsani and Ezidis community

Yārsani(A religious belief of Indo-Iranian origin that Majority of them are ethnically Kurd form Iran, Iraq inhabit different regions of Iran, North of Iraq, and some part of Europa, Canada) access to cyberspace has given them a platform for identity-making, which, in turn, has enabled them to challenge the existing geographic, political and cultural constraints in Iran. I am referring to Yarsani self-representation and presentation before the Internet. The Yārsani in Iran have to live with the threat of discrimination and even violence, on the internet, self-identification as Yārsani is practiced much more freely. The rise of a public Yārsani identity within Iran and in the diaspora are closely interconnected. The experience of persecution and of persistent libel and prejudice on the part of the Shia majority forced the Yārsani to adopt a distinctive practice. The Yārsanai have experienced problems on Facebook, too, so the creation of virtual communities has not free of negative consequences.

The great majority of Yārsani live in Iran, and most of the material hosted on Yārsani websites refers to that country. In general, the websites represent Yārsanism as a cultural or religious tradition that is tightly attached to the spatial, historical and cultural context of Iran. Many of websites 'participants intend to introduce Yārsanism and provide basic information. Organizational websites also have the task of giving information about Yārsanism. Most of the websites have a typical textual format. Some pages contain images, frequently pictures of their shrines in Kurdistan, Iran or their religious manuscripts. Most of these pages refer to Dalahoo as central location for reminiscing about their religion and rituals around the world. Yārsani people illustrate their own culture, voice their identity, oppose dominant cultural discourse, provide alternative cultural resources and reconstruct their distinctiveness through their representations. They create an imagined community that is broadly supported and supporting. Yārsani build their imagined community through Facebook activity and offer suggestions about opportunities for other Yārsani to get involved in propagation of their religious minority identity.

The Yārsāni group employs Facebook to introduce to the international community their religion as an independent one. They try to use Facebook to help with digital leveraging (via online appealing), protest campaigns, and risk awareness. They seek to structure support for their objectives. The central question of this article is why in recent years the Yārsāni community in and Iran has been willing to express their beliefs whereas in the past this group has hidden their identity from fear of persecution. Present research on Yārsāni would gain equally from ethnographies synthesized both offline and online. The rising presence of the Yārsani community on Face book has become a new context for social interaction, demonstrating a visual opportunity in digital media.

Throughout history, the Yārsani have been banned to talk about their religion, especially in Iran. They worshipped in secret due to social dominance during their history. On Yārsani pages, relationships are increasingly communicated between people through images, and these pages provide them with an opportunity to communicate and rethink people in a more significant fashion.

Based on the images of Yāri followers in Kurdistan, this part will discuss the building of identity through visual communication. By visually expressing themselves through pictures they put on Face book, Yārsanis on Face book show themselves through pictures of their sacred shrines or their territories, and "religious elders" manufacture their online cultural relation. The online efficiency of their own culture and religion is analyzed in the interaction of offline social to cultural desires on Face book to understand how Yārsanis using Face book define their identity, and how important Face book is for Yārsani, followers of the religion kept their beliefs and practices clandestine they regarded their faith as a serr, a secret that sealed the lips of those who knew it.

Monika Marta Przybysz

Christian mobile applications as a communicative tool of the Catholic Church

Mobile communication and mobile applications are the future of social communication. Smartphones have changed the character of the contemporary man's activity and the way of his/her communication. These devices have revolutionized the technological sphere, combining the capabilities of a personal computer with active mobility and they also created new user behaviours, the style of consumption and even the a life style. A contemporary smartphone user is constantly on the move and wants to have access to mobile technology at any place, also while performing other activities. This makes new challenges appear in the institutional communication. New behaviours and phenomena appear, such as multi-tasking of young users. As many as 99% of adult Poles own a mobile phone. Such communicative changes force firms and institutions to adapt to the contemporary communicative challenges and to create mobile applications for smartphones. Mobile communication is also a bigger and bigger challenge for the Church and religious institutions.

Questions arise about how to find, in the multitude of new tools and possibilities, the ones which will make it possible for the Catholic Church to effectively communicate her message? How to use the changeable communicative behaviours in a way which is modern as far as communication itself is concerned but does not change the content of the Gospel Message? How to communicate with the faithful, who turn away from the traditional media and at the same time not to lose the identity and be faithful to the Church teaching? Which ones among the presently available Christian mobile applications fulfil these requirements and which ones can be a communicative threat for the Church? What communicative challenges are there before the Church in the mobile communication through smartphone applications? The paper will answer these and also other research questions. The methodology applied here will be a quantitative analysis of the available mobile applications with Christian content in the Polish language.

Józef Kloch

Transgressing the Boundaries. The Creative Use of the Net Based on Real and Virtual Activity of the Churches

Tim Berners-Lee made a significant progress – he built the first web page and a graphic browser to use it. The Internet network and web browser were essential for the welfare of humanity, and also because of freedom and democracy. The idea was simple – any persons around the world could exchange information in real time. The internet crossed the borders, it broadened the scope of its impact, it was being used in more and more new areas of human activity and cyber-life.

One area which the Internet has also entered is religion. Various religious communities started to use digital communication on the Net in a creative way. Christian Churches in Europe, especially the Roman Catholic Church, began to use the Internet already in the 1990s. What is interesting, the Vatican was the front runner both in practical applications and in the theoretical sphere. It built a "laboratory of Web use" of a kind in Latin America (RIIAL project). On the foundations of these experiences the Vatican launched its own website and e-mail system. More numerous applications appeared when Web 2.0 came. Here another boundary was crossed – the Internet users became also authors of the content.

The article concerns the creative Web use through real and virtual religious communities. Many interesting phenomena happen on the borderline between the Net, religion and virtual reality. The openness of the Internet is matched with the openness of religious communities.

Vít Šisler

Who is Listening to Your Fatwas? Social Network Analysis of Islamic Sites' Audiences on Facebook

This paper presents an empirical study on Islamic social network sites providing normative content for Muslim minorities living in a non-Muslim context, particularly in Western Europe. It analyses the Facebook audiences of these sites and explores their similarities, differences, and affinities via social network analysis. The paper introduces a new quantitative method, Normalized Social Distance, that calculates the distances between various social groups, based on the intentional stances as expressed by these groups members' activities on social networks.

The emergence of social media have introduced substantial innovation in both production and consumption of Islamic knowledge, where established traditional Muslim authorities compete for audiences with charismatic satellite preachers and Internet-based muftis. This is particularly relevant to European Muslim communities, where experiences of cultural displacement and negotiations on hybridity and authenticity are at the heart of contemporary life. At the same time, the rise of social media along with the progress in computational tools that can process massive amounts of data makes possible a fundamentally new approach for the study of human beings and society.

This paper explores 80 Facebook sites providing specific 'Islamic' content to European Muslim minorities. By doing so, it analyzes publicly available data about more than 3,5 millions users of

these sites via Normalized Social Distance (NSD). In a nutshell, NSD is a formally defined method calculating the distance between social groups, based on the intentional stances as expressed by these groups members activities on social network sites. The resulting number expresses how 'far' or 'close' are the audiences of various sites to each other. The method provides an opportunity for a distant reading of social media, enabling us to formally represent and analyze the structural aspects of 'big social data'.

The empirical evidence indicates that there exist several tightly connected clusters of Islamic sites on Facebook, whose audiences are significantly 'close' to each other and share similar intentional stances. The users located in these clusters share similar media content and rarely reach out to different clusters. Furthermore, the findings indicate that a specific content, particularly related to the coexistence between Islamic law and European legal systems, gains a significant prominence on social networks by the actions of relatively small, yet coherent and active, audiences of predominantly Salafi sites. This elevation then subsequently influences the ways mainstream media and politicians prepare and promote their content on social network sites, shaping the public debate on Islam in Europe.

15:30 – 17:00 – Video Games and Society – 025

chaired by **Cyril Brom, Zdeněk Záhora**

Birgit Ursula Stetina, Natalie Rodax, Serkan Sertkan, Armin Klaps, Zuzana Kovacovsky & Helmut Hlavacs

"Purpose": Approaching Racism and Sexism within a Survival Serious Game

Racism and sexism are amongst the currently most relevant problems in our society. News present on a daily basis the cruel results of power ideas, "us-vs-them concepts", together with intense emotions, taboo, distancing and avoidance behavior (eg Diller, 2011). Defensive behaviors can easily be observed in daily life, the underlying racism and/or sexism might be unconscious.

"Purpose", a browser game, is based on currently famous survival gaming genre with the background story of a zombie apocalypse. Players have to build their virtual group of non-infected humans to reach a save place, which is indicated on a map. All survivors of the zombie apocalypse are presented with their skills and a picture. How is the decision making process regarding the group structure biased by stereotypical racist and sexist aspects?

In a mixed method design data of 10 participants were collected from a laboratory experiment with video analysis in combination with post-hoc semi-structured interviews for individual positioning. Analysis included content analysis and statistical procedures (eg cluster analysis).

In the presented exploratory study racist and sexist behaviors, cognitions and emotions could be triggered during the game in experienced and unexperienced gamers. A guided reflection process raised the problem awareness of underlying racist and sexist patterns in the gamers. Gamification to tackle this serious problem might be a low-threshold way to increase awareness.

Kateřina Lukavská

Immediate and longterm effects of time perspective on online gaming

The aim of the research was to verify the effect of Time Perspective (TP), measured by shortened version of Zimbardo Time Perspective Inventory (ZTPI-short), on online gaming (the time spent playing, problematic gaming symptoms). TP is a psychological phenomenon that reflects the ability of people to shift attention between memories (past frame), current stimulation (present frame) and plans and expectations (future frame). Some people have a tendency to focus on rather negative, unpleasant and painful aspects of each frame, which constitutes the Negative TP. We analyzed data from 377 MMORPG players revealing that the Negative TP (which consists of ZTPI scores of Past Negative, Present Fatalistic and Future Negative) influenced significantly either playing time or the presence of problematic gaming symptoms. Future positive TP (the focus on positive and constructive aspects of one's future) showed the opposite effect. Further we revealed that the effects of TP on gaming is partially mediated by gaming habits concerning starting and quitting gaming sessions under various circumstances. Habits were meassured by Cues Sensitivity Scale. Within 76 respondents from the original sample that were willing to participate in the follow-up, we examined the gaming usage patterns after 3 years. Data suggested that the intensity of gaming decreased over time. However, Negative TP was revealed as the significant antagonist of this decrease. Further analyses are in progress and will be presented at the conference.

Vítězslav Slíva

Computer Game Interface and Anthropologic Methods in Virtual Worlds

Even though some ethnologic studies focusing on virtual realities and MMORPGs has been published (Boellstorff, 2008, Nardi, 2010, Taylor, 2006), only little attention has been paid to the aspect of interfaces of those systems. In this work, we study how computer game interfaces influence user experience from methodological perspective. As most of the anthropological research is based on direct participant observation, we would like to revisit these methods with respect to the interface of aforementioned virtual realities, in particular, for a popular game Elder Scroll Online. We work with a hypothesis that observing a participant in virtual worlds differs from real world observation due to the interaction limits. In this work we propose adjustmets to the observation methodology which attempts to reflects these limits. On the example of the investigated game, we show reflexive outlook on the function of its interface and how it influences the participant observation.

17:15 – 18:45 – Research Data and Open Data – 215

(special track) chaired by **Michal Koščík**

Matěj Myška

Defining scientific research: a necessary prerequisite for application of the respective copyright and sui generis rights exceptions

The newly proposed Directive on copyright in the Digital Single Market introduces new exceptions to copyright and sui generis database rights for text and data mining for research organizations. Also the InfoSoc Directive provides for an exception to the reproduction and communication to the public right for scientific purposes in its Art. 5(3)(a). The Database Directive analogously exempts the extraction or re-utilization of substantial parts of the database for the purpose of scientific research in its Art. 9(b).

However a clear definition of "scientific research" - a necessary prerequisite for application of these exceptions - is missing.

The aim of this paper is to provide a descriptive analysis of the concept of "scientific research" as understood in the relevant policy and regulatory instruments on the European level as well as in the case law of the CJEU in order to alleviate the legal uncertainty surrounding this term. Based upon this analysis two characteristics of the respective activity (namely nature of the beneficiary and the objective and the method of implementation of the activity) potentially usable for its qualification as "scientific research" are critically discussed and evaluated.

Daniela Procházková

Implementation of the Database Directive: Lack of Bravery?

This paper is dealing with problems of implementation of the Directive 96/9/EC of the European Parliament and of the Council. Namely it is focuses on the absence of specific legal rules connected with the plurality of subjects of the sui generis right. The goal of this article is to highlight this problem and to offer examples of solution of this situation.

Firstly, the paper summarizes different types of legal protection of databases. It shortly recapitulates the copyright and the sui generis right protection as was established by the Database Directive.

Secondly, the paper is focused on the problem of plurality of right holders of these rights, especially in the case of holding both abovementioned rights simultaneously. This situation causes a lot of difficulties for the addressees of law due to the absence of specific legal rules in Czech Republic and other European countries. The paper discuses examples of legally problematic situations (e.g. licensing the rights to database). International aspect is also considered, e.g. one of the right holders comes from a different member state in European Union or from outside of the European Union.

In the third part of the paper a possible solution is offered based on theoretical grounds, practical aspects of everyday life and original purpose and main aims of the Database Directive.

Märten Veskimäe

Uptake of large e-services: example of e-prescribing adaption patterns in Estonia using system log data

A number of commercial e-prescribing services have emerged across the world, due to expected benefits in program administration, medication discharge and patient safety (Garfield et al. 2016, Kaushal et al. 2010, Grasso et al. 2002). The aim of this paper is to examine the adoption growth of such services for different user groups. Modeling such behavior allows us, first of all, to predict usage numbers, but more importantly, it gives us valuable insight about the possible impact of adapting e-prescribing services. In many cases, however, available data has not been sufficient for generating fully reliable inferences. Here, Estonia provides a compelling case, where a nationwide public e-prescribing service was set in motion in 2010. Log data from the Estonian e-prescribing infrastructure allows us to examine how different user groups (doctors, patients and pharmacies) have used this service over a six year period. Analysis shows strong seasonality in usage numbers, with significantly stronger demand during colder months. Data also indicates substantially different adaption patterns for patients and pharmacies. Considering the growing number of e-prescribing services, the results will be beneficial for policymakers and service providers in the given sector.

17:15 – 18:45 – New Media and Society – 208

chaired by **Jakub Macek**

Tomáš Karger

Frictionless Distribution and Community Building: The dual meaning of sharing in free and open source software

This study draws upon ethnographic research in a software development project belonging to the free and open source software movement. It conceptualizes licensing as a part of infrastructure providing means for public distribution of source code – for sharing it. However, it seems that in this context, the word “sharing” has a dual meaning. The preference of standard licenses is intentionally promoted in order for source code distribution to take place without interaction or negotiation. On the other hand, the term sharing points to establishing interpersonal ties among contributors to software development projects, providing an image of community building. In this way, the dual meaning of sharing corresponds to Nicholas A. John’s recently developed distinction between sharing as distribution and sharing as social exchange. A conflation of these two meanings of sharing could represent a starting point for critique of peer-production projects. The aim of this study is to provide differentiation between practices in which aspects of distribution or social exchange can be recognized and to attempt to generalize this differentiation in order to be applicable also to other

types of peer-production projects. This would allow us to see peer-production projects not simply as practicing sharing, but more precisely as using distinct types of sharing in their particular practices.

Bianca Balea, Anca Velicu & Monica Barbovschi

Adolescent's perception and awareness of personal data misuse. Qualitative data of the project Friends 2.0

In the context of recent studies (Barbovschi & Velicu, 2014; Smahel & Wright, 2014; Vincent & Haddon, 2014) reporting on the emergent risks of personal data misuse (PDM) when social networking sites are used (e.g. hacking of profiles, sharing or tagging other peers without permission, etc.), and considering Peter and Valkenburg''s argument (2011) around the importance of privacy and self presentation in the identity construction in adolescence, this paper will explore most up-to-date experiences and perceptions of PDM young Romanians experience and their awareness strategy for avoiding them. The data on which this study reports were collected in the first qualitative phase of the Friends 2.0 project (2015-2017; Romania) which aims to explore the meaning of friendship for adolescents in the context of social media use. The design of this stage of the research consist in 12 single-sex focus groups with young people aged 11-13, 14-15, 16-18, in two urban areas in Romania.

Åsa Borgström

Young people with intellectual disabilities and social media – a systematic review

Previous research has studied internet use in youth and adults in general, but little is known about how young people with intellectual disabilities use the internet and social media. The available research indicates that there are both dilemmas and opportunities to be found. While there are risks for victimization and bullying, there are also benefits such as new ways of communication and empowerment. The purpose of this study was to conduct a systematic review of the research field with a specific focus on dilemmas and opportunities.

A search strategy was designed in collaboration with the Gothenburg University library. The databases Scopus, Web of Science and Google Scholar was chosen due to their multi-disciplinary character. The search was limited to scientific journal articles and conference proceedings published in English. Search terms was chosen and combined with Boolean operators. The search was concluded in August 2016.

After articles off topic and cross references were removed, 22 of 104 publications remained. The preliminary analysis showed that most research was conducted in Europe, North America and Asia to an equal extent. The studies were primarily from social sciences, medical sciences and educational sciences. Almost half of the studies were published after 2015 indicating a rapidly growing field. Most studies were quantitative. The studies were grouped thematically based on content: bullying, self-disclosure, contact and engagement. Other central themes were access/participation and identity formation.

17:15 – 18:45 – Video Games and Society – 025

(special stream) chaired by **Cyril Brom, Zdeněk Záhora**

Discussion

How to teach game studies and game development in the Czech Republic (and beyond)

Game studies and game development finally became part of university study programmes; here, in the Czech Republic. What are the lessons learnt? What can be improved? How students and teachers view these study programs? What kind of jobs is available for graduates? You can have the unique opportunity to ask these and other questions in our 90 min long panel discussion with people from academia and beyond.