An overview: of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section I

Chairman: Dr. Michal Petr

21st June at 09:45 – 10:45 by CET

Author(s)	Title & Abstract
Mária T. Patakyová/Comenius University in Bratislava	**Recodification of Competition Law in Slovakia – Missed Opportunity from Digital Markets Perspective?** Twenty years after the Act No. 136/2001 Coll. on Protection of Competition, as amended ("Previous Act") entered into force, it was recently replaced by the Act No. 187/2021 Coll. on Protection of Competition ("New Act"). The adoption of the New Act was closely related to the implementation of the ECN+ Directive, therefore, the New Act had been expected for some time before it entered into force. After quite turbulent preparatory works and complicated adoption process, the New Act is finally effective as of 1 June 2021. After briefly presenting the New Act, this contribution evaluates how the New Act is suitable for solving problems of the digital markets. In particular, the most significant amendments brought by the New Act are analysed in order to see whether they may contribute to the enforcement of competition law in digital environment, or rather the opposite. In sum, the contribution asks whether the New Act will facilitate the enforcement of competition law in digital sector. If not, the recodification of competition law in Slovakia may be seen as a missed opportunity from digital markets perspective.
Prabhpreet Singh, Vijaylaxmi Sharma /Manipal University Jaipur	**Competition law, policy and regulation in the digital era** During the round-table discussion on competition issues in the digital economy held during the eighteenth session of the Intergovernmental Group of Experts on Competition Law and Policy in 2019, many experts and enforcers expressed the view that existing competition laws and tools were adequate to address competition concerns arising from the market power of dominant digital platforms and that adapting the competition toolkit would be sufficient to address such problems. Since then, views have slightly changed in favor of legislative reforms and ex ante regulation. Digital platforms are essential elements of today's economy, in particular since the outbreak of the coronavirus disease of 2019 (COVID-19) pandemic, and are a key issue for Governments and competition authorities worldwide. Building upon previous discussions at UNCTAD on competition issues in the digital economy, this note provides an overview

	of the challenges faced by competition authorities in dealing with competition issues in digital markets and introduces recent competition cases involving online platforms, as well as legislative and regulatory initiatives undertaken in some jurisdictions. It provides a comparative analysis of recent initiatives taken by Governments worldwide and includes recommendations for developing countries in dealing with competition issues relevant to digital markets.
Michal Petr/Palacký University	**The role of competition policy in data privacy** Competition law is frequently called upon to intervene in areas where – arguably – it was originally not intended to apply. The German competition authority has recently decided that Facebook has abused its dominant position in the social networks market by imposing on its customers rules non in conformity with the data privacy ones. The fundamental question is not whether this conduct took place or whether the relevant market and Facebook's position in it was adequately analysed, but whether a breach of data privacy rules may at the same time constitute a breach of competition law. It will be argued that competition authorities should take utmost care when arguing like this. Alternatively, depending on your preferences and on the conference's ultimate agenda, I may propose an alternative topic: Will the use of autonomous pricing algorithms amount to reinterpretation of concerted practices under competition law? The employment of autonomous Artificial Intelligence pricing algorithms brings several challenges for competition policy. Crucial among them is the question whether such algorithms may increase the prices above competitive levels. Should it be regarded as a form of collusion, prohibited by competition law? Or a form of parallel conduct, which is outside its scope? It will be argued that the notion of tacit collusion might be in need of re-interpretation.

An overview of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section II

Chairman: Adj. Prof. Dr. Ondrej Hamuľák

21st June at 11:00 – 12:45 by CET

Author(s)	**Title & Abstract**
Alexander Antonov/TalTech	**Omnes Cives Europei Sumus in Digital Aetatem: The Charter of Fundamental Rights of the European Union as the Core Framework for the Protection of the Rights to Privacy and Freedom of Expression?** In the context of a contested digital environment, recent decisions rendered by the Court of Justice of the European Union demonstrate the growing importance of the Charter of Fundamental Rights of the EU in harmonizing the national human rights framework of EU Member States and thus in shaping European values, digital sovereignty and eventually European identity. With Digital Rights Ireland, Google Spain and Schrems I, scepticism abated that the CJEU as a Court non-specialized in human rights questions favoured the protection of Fundamental Freedoms of the Single Market over Fundamental Rights of EU citizens. Based on Art. 7 and 8 of the Charter and in reference to GDPR principles, the CJEU has gradually expounded the obligations of both EU institutions and EU Member States acting as EU agents vis-à-vis EU citizens in the area of privacy protection, eventually contributing to harmonizing the interpretation of digital privacy rights with a view to achieving a high level of fundamental rights protection in the EU. These recent developments are specifically relevant against the backdrop of the latest horizontal legislative proposal for the Digital Services Act, aimed to address the growing fragmentation in legislating content moderation practices in EU Member States and to define the legal obligations of information society services, particularly of very large digital platforms in i.a. preserving the fundamental right of freedom of expression. In addition to scrutinizing jurisprudence on the right to privacy, the second dimension thus examines the CJEU's decisions in Glawischig-Piesczek, Netlog and Scarlet, to assess the implications of algorithmicbased content moderation practises on the fundamental right of the freedom of expression, enshrined in Art. 11 of the Charter. As such, furthering the understanding of how to achieve an open, fair and safe Digital Single Market one the one side with the element of competition in mind on the other, the presentation examines recent case law by the CJEU evaluating the assumption

	of the Charter of Fundamental Rights of the EU as to gradually developing into the main framework for the protection of the rights to privacy and freedom of expression of EU citizens in the digital age. *Keywords:* Digital Single Market, Digital Services Act, Charter of Fundamental Rights of the European Union, Right to Privacy, Freedom of Expression
Oleksandr Pastukhov/University of Malta	**A Case for Statutory Damages under EU Data Protection Law** The right to privacy is one of the key 'digital' rights. It is also an important non-pecuniary right whose infringement is actionable in private law. However, the General Data Protection Regulation is preoccupied with administrative measures against the violators of its rules rather than with arming the victims of privacy intrusions with effective and efficient rules on privacy torts/delicts. The paper addresses the issue of the underutilization of the right of private action under EU data protection law by identifying deficiencies of the rules on damages contained in the Regulation and arguing for their reinforcement with provisions on statutory damages. In search for guidance, it looks into the application of statutory damages in intellectual property law, examines their potentially punitive effect and, on the basis of the privacy case law of the European Court of Human Rights, offers indications of possible amounts of the statutory damages being proposed.
Adam Máčaj/Comenius University in Bratislava	**Big Tech and Private Oversight in the Digital Age – Effective Remedy or a Merry-Go-Round?** Policing the Big Tech operating on digital markets globally proves to be a considerable regulatory challenge time and again. Activities of contemporary transnational corporations (TNCs) bring considerable opportunities into regions, as well as policy areas that have remained on the outskirts of public interest before the rise of the so-called Big Tech. Yet for all the progress and globalization, one cannot omit recalling the plethora of areas where individuals' human rights were at odds with operations of TNCs. Whether caused intentionally for corporate gains, or as a result of bona fide actions aimed at balancing various competing interests, individuals often face interferences with their fundamental rights, particularly in the digital era, and even suffer violations thereof. In tackling the power of Big Tech and the prospective abuse of its power, recent cases of attempts to secure compliance and set standards for corporate behaviour include voluntary oversight initiatives acknowledged by the corporations themselves. Illustrative case in point is the Oversight Board's decision on ban of the then-president Donald Trump from Facebook. Utilization of these private oversight bodies, with potential for global reach surpassing state-centric regulatory scope, nevertheless comes with its own set of consequential implications. The aim of this paper is to examine in particular whether these initiatives can

	be considered an alternative to judiciary, especially in serving as an effective remedy required by international human rights law. Based on this objective, the research then seeks to establish whether such remedies can supersede judicial process in securing human rights, or whether further improvements of the system are required to provide effective safeguard of human rights. *Keywords:* transnational corporations, Big Tech, business and human rights, freedom of expression, effective remedy
Lusine Vardanyan, Hovsep Kocharyan/ Palacký University	**The GDPR and the DGA proposal: are they in controversial relationship?** At the end of 2020, the European Commission published a new European data strategy, which aims to create a new legal framework to promote the development of a single European data market. As part of the new European strategy, the EU is already submitting proposals for new regulations. Along with the Digital Services Act[1] and the Digital Markets Act [2], the European Commission has proposed the Data Governance Act project, which aims to strengthen the governance mechanism to facilitate data exchange and introduce new instruments to implement the European data strategy. Even a cursory analysis of these proposals shows an attempt by the EU to become an active player in promoting the monetization of personal data. This is a radical shift in the EU's focus from the protection of privacy of the person to the promotion of data sharing. However, this shift strictly raises the question of the correct balance between the new regulations that will be adopted on the basis of the new strategy and the EU regulations that have already been adopted. Of particular importance is the problem of coordinating the GDPR and the DGA proposal[3], as indicated in the joint opinion of the EDPB and the EDP.[4] The most important concern is the possibility of weakening the level of protection of personal data and further application of the GDPR as the most influential legal instrument providing the enhanced protection of personal privacy. In this paper we aim to analyze the provisions of the GDPR and the DGA proposal in order to identify the main possible inconsistencies between these legislative acts and their effect for the individuals' control over their personal information. We also examine the relevant case-law of the CJEU regarding the application and interpretation of the

[1] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final

[2] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[4] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2021).p. 14

	GDPR to identify the possible existence of the judicial approach that can make the application of the DGA and the achievement of its goal difficult. We will try to find the answers for the following questions: Are there any inconsistencies between the DGA proposal and the GDPR, as well as in the relevant case-law of the CJEU, and if so, which are the main ones? Will the DGA really weaken the individual's control over their personal information compared to the GDPR? In this research we show that the EU legislation adopted before the New European Strategy did not sufficiently stimulate the creation of a data market and extensive data exchange, which was also connected with the CJEU's attitude to prioritize the protection of personal data over the free flow of data. Besides, it shows that the realization of the shift in the EU's focus from the potection of human privacy to the promotion of data sharing can be seriously affected by the already existing case-law of the CJEU and the latter may become an obstacle to the full application of the DGA and the achivement of its goal. The uncertainty of the legal concepts used in the DGA proposal, such as, for example, "data altruism", or the problematic relationship of consent models used in the GDPR and the DGA proposal can make possible to circumvent the strict provisions of the GDPR, weakening the guarantees for the implementation of the informational self-determination of the person and reducing of the level of the individual's control over the use of his/her personal data. A more precise legislative definition of the conceptual framework used or the consolidation of appropriate criteria for evaluating of the broad legal categories could be a significant step towards a clearer relationship between the GDPR and the DGA. *Keywords:* DGA proposal, GDPR, personal data, data exchange, free flow of data.
Sára Kiššová/ Comenius University in Bratislava	**Internet Intermediaries Liability** The article deals with the responsibility of internet intermediaries in the legislation of the European Union and the USA. The article analyzes the development of this regulation in the European Union and at the same time compares the expected legislation (The Digital Services Act package) with the US legislation and focuses on the concept of "good samaritan" in both jurisdictions.

An overview: of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section III

Chairman: Dr. Blanka Vítová

21st June at 13:15 – 14:45 by CET

Author(s)	**Title & Abstract**
Viktorija Soņeca	**The Digital Markets Act – is this a new saver?** Large platforms have emerged benefitting from characteristics of the sector such as strong network effects, often embedded in their own platform ecosystems, and these platforms represent key structuring elements of today's digital economy, intermediating the majority of transactions between end users and business users. A few large platforms increasingly act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation of conglomerate ecosystems around their core platform services, which reinforces existing entry barriers. As such, these gatekeepers have a major impact on, have substantial control over the access to, and are entrenched in digital markets, leading to significant dependencies of many business users on these gatekeepers, which leads, in certain cases, to unfair behavior vis-à-vis these business users. Member States apply or are considering to apply divergent national rules to address the problems arising from the significant degree of dependency of business users on core platform services provided by gatekeepers and the consequent problems arising from their unfair conduct vis-à-vis their business users. For example, Facebook targeted potential competitive threats to its dominance by buying WhatsApp. Facebook chose to buy an emerging threat rather than compete, and announced an agreement in February 2014 to acquire WhatsApp for USD 19 billion. Another example is Australia where, due to disputes between Australia and digital platforms such as Facebook and Google, the country began to develop a News Media and Digital Platforms Mandatory Bargaining Code (hereinafter referred to as "the Code"). For the Australian legislature to abandon the idea of the Code, Facebook prevented Australian press publishers, news media and users from sharing/viewing Australian as well as international news content, including blocking information from government agencies. Such action demonstrated how large digital

	platforms can affect the flow of information, in order to encourage the state and its legislature to change their position. This is all the more so because Australia eventually made adjustments to the Code in order to find a compromise with the digital platform and to enable the digital platforms to reach an agreement with the publishers in the first instance. Given the intrinsic cross-border nature of the core platform services provided by gatekeepers, regulatory fragmentation will seriously undermine the functioning of the Single Market for digital services as well as the functioning of digital markets at large. Therefore, in December 2020, the European Commission proposed the Digital Markets Act to regulate the gatekeepers of the digital world by imposing direct restrictions on the behavior of tech giants. However, will the Digital Market Act solve this problem? Will that be enough? What exactly is the Digital Markets Act proposing? Answers from these questions' author will be given in the paper.
Javad Keypour	**Smart Grids: A Technical Solution or a Legal Challenge for Carbon Abatement in EU Energy Sector?** Digitalisation has received a great deal of attention in most EU policy areas over the past decade. At the same time, since energy is one of the EU's shared competencies, the Commission has pursued various initiatives to achieve its goals in this area, including the Energy Union. The adoption of Directive 2018/844 urged alignment of the Energy Union goals, i.e. Single Energy Market and decarbonisation, with the Digital Single Market. Since then, promoting smart meters and smart grids have been sought for creating this convergence, practically. However, the legal challenges of using smart meters and smart grids have received less attention. In this study, these challenges are scrutinised into three levels: individual, state and the EU. The results show that while legal concerns about data security and customers' privacy are debatable at the first level, competition law infringement matters in establishing smart grid management e-platforms which interact with the prosumers. Finally, the efficient development of smart grids necessitates creating cross-border energy transmission infrastructure across the EU. This is known as the central part of the Energy Union plan, which is a time-consuming and costly task. Even if implemented, the unification of the energy tax system and the unified recognition mechanisms for the guarantee of origin across the EU are essential for prosumers to safeguard nondiscriminative energy trade. The implication of these challenges shows that the establishment of smart grids can be perceived as a technical solution to decarbonisation and digitalisation of the EU energy sector. In contrast, its legal challenges should be still addressed and resolved by EU legislative bodies.
Tea Kookma	**Challenges to consumer protection in the digital economy and how to overcome them?**

	Consumer protection is becoming increasingly challenging in the digital economy. In the digital economy, consumers can engage in transactions from any place in the world. In order to protect their rights, consumer protection laws stipulate respective obligations on traders. However, in a digitalized society, coupled with the phenomenon of consumer empowerment, compliance with and enforcement of these obligations has become challenging. The presentation will focus on the challenges of providing information to consumers about the goods and services they are purchasing; as well as on the challenges faced by traders and regulators regarding consumer data protection.
Blanka Vítová	**Personalised pricing as one of the unfair commercial practice** Price discrimination is not a new phenomenon, but in today's digital world it is more sophisticated, simpler and faster thanks to artificial intelligence. Personalised pricing - as opposed to mass advertising and uniform pricing - leads to higher profits for businesses. Price discrimination is a strategy in the sale of goods or services whereby a business charges customers different prices for the same product or service, and economics distinguishes between several degrees of price discrimination. In pure price discrimination, the seller or service provider charges each customer the maximum price that the seller believes the customer will be willing to pay. Whilst there is a relatively big amount of case law on price discrimination against consumers by businesses in 'bricks and mortar' shops, the rapid development of digital technology and online shopping has allowed for a proliferation of practices that are relatively new and still evolving in the field of consumer protection. The more sophisticated computer algorithms become, the more sophisticated practices businesses will be able to use against consumers and the more difficult it will be to detect and combat them. In a way, we are thus back at the beginning of the creation of consumer protection law, because we are creating protection in a new (online) environment.

An overview of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section IV

Chairmen: Prof. Dr. Thomas Hoffmann and PhD student Melita Sogomonjan

21st June at 15:00 – 16:15 by CET

Author(s)	**Title & Abstract**
Zoltán Gyurász	**(Artificially) Intelligent Healthcare - The ambitions and limitations of Artificial Intelligence in healthcare** New technologies and their applications in practice are experiencing an unprecedented boom. Technology-driven disruption is happening faster than we could have ever expected, reshaping the way we live and work. The digital revolution of the 20th century made information available everywhere and anytime. Our society has moved from its primary development from a collection-oriented economy, through production to current mass production. Industrialization also meant a shift of society to the so-called knowledge society, a society where goods and services are based on information.[1] Information thus began to be a very valuable asset and contributed to the dynamic development of technology. It is technologies based on the collection and analysis of information that is the driving force of current social events. From the creation of policies of private companies and their strategic decisions, through the prediction of future crime to the profiling of individuals for marketing purposes. Natural persons gradually became data hubs generating so-called information (behavioral) surplus, which can then be used for various purposes and often by commercialization.[2] This statement is doubly true of information about our state of health, which does not collect only qualified provision of healthcare as was the case in the past. It is the providers of various applications that regulate the diet of individuals or monitor their biometric functions that have legitimate and individual access to data on the health status of users. Gradually, a completely new type of market has emerged, which is based on monitoring and analyzing health information to users to provide various services. Examples include smart bracelets or various mobile phone applications.

[1] ZUBOFF, S.: *The Age of Surveillance Capitalism*. 1. vydanie. New York: PublicAffairs, 2019.

[2] See. *Umelá inteligencia ako hrozba pre ľudstvo? Vedci varujú pred katastrofou*. Denník Pravda [online]. [01-06-2021]. Available at: https://vat.pravda.sk/technologie/clanok/439268-umela-inteligencia-ako-hrozba-pre-ludstvo-vedci-varuju-pred-katastrofou/.

	Right now, you can see the entry of new technology into the game. Technology that has the potential to further influence the paradigms of our lives. Artificial intelligence has already entered the daily existence of society in various forms. For millennia, law have ordered society, kept people safe and promoted commerce and prosperity. The rise of artificial intelligence presents novel issues for which current legal systems are only partially equipped. If we are to live alongside artificial intelligence, we need to address these issues.[3] For this reason the topic of regulation of AI is the subject of a lively academic,[4] political debate, and these debates will soon bear concrete fruit outlined in strategic documents, especially at the European Union level).[5] The application of artificial intelligence has not been avoided even in the field of healthcare. Whether we are talking about AI as a diagnostic tool or a tool that will increase the accuracy and computational capacity of medical devices or drones that can transport drugs or medical devices to inaccessible or affected areas, healthcare AI use is growing exponentially with technology. The last stage of the use of AI is the cases when the technology itself provides health care or when using it, there is no element of human intervention. As the World Health Organization (WHO) has pragmatically stated, the AI application for healthcare raises legal, ethical, and associative issues regarding accountability, accessibility, prejudice, or privacy,[6] but with the promise of fundamentally improving health care. As indicated above, regulatory issues of AI healthcare cannot be overlooked as the right to healthcare is core part of several international treaties and national legal orders[7]. In view of the above, it is natural that we ask ourselves whether our society and our legislation is ready for the use of AI in the field of healthcare. The question is interesting, but no less complicated. For this reason, we consider it appropriate in this introduction to the outline of the content and methodology used in this publication. This abstract is to be followed by three chapters, the first of which shall introduce the basic concepts and basic legal framework of AI regulation with a specific focus on health care. Integral part of it shall be a definition of the basic concepts such as artificial intelligence, machine learning or deep learning. Understanding these concepts is an integral part of the study of the issue, and the source of the definition of the terms in question is primarily the doctrine and non-

[3]TURNER, J: Robot Rules: Regulating Artificial intelligence 2018 Available: https://www.law.kuleuven.be/citip/en/docs/hot-news/j-turner-robot-rules-regulating-artificial.pdf

[4] See. KAMALNATH, A.: Rethinking Liability and Licensing for Doctors in the Era of AI: Insights from Company Law, 2018 Or WARTMAN, S. – COMBS, D.: Medical education must move from the information age to the age of artificial intelligence, 2018. Available at: https://pubmed.ncbi.nlm.nih.gov/29095704/. Or GOMÉZ-GONZÁLES, E. - GÓMEZ, E.: Artificial Intelligence in Medicine and Healthcare: applications, availability, and societal impact. EUR 30197 EN. Publications Office of the European Union, Luxembourg, 2020.

[5]See. Proposal for a Regulation laying down harmonized rules on artificial intelligence, 2021 Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence?fbclid=IwAR3yDBx9z4dEDmXDJk0Vq03_PNV-bKRltOMPpgt_4EBarft_giV6m2SbJd8

[6] WORLD HEALTH ORGANIZATION: *Big data and artificial intelligence*. World Health Organization [online]. [01-06-2021]. Available at: https://www.who.int/ethics/topics/big-data-artificial-intelligence/en/.

[7] Article 40 of the Constitution of the Slovak Republic explicitly provides that everyone has the right to protection of health. Under health insurance, citizens have the right to free health care and medical supplies under the conditions laid down by law."

	binding documents adopted at the EU level. In the second chapter, we will outline the legal framework for AI regulation as planned by the legislator at the EU level, focusing in detail on the conclusions regarding the application in the field of healthcare. The third chapter introduces the fundamental ethical and legal problems of AI. Specifically, we will focus on the institutes of legal subjectivity, responsibility and outlining the ambitions and limitations of artificial Intelligence in healthcare. Given that information forms the basis and necessity of the AI used, special focus shall be on the issues of data processing regarding legislation and the creation of a data ecosystem, from which the AI could benefit.
Nick Guldemond	**Implications for health professionals in the context of a post-pandemic healthcare and future challenges of health systems** The current pandemic has accelerated the existing structural problems and underlying weaknesses of health and social care systems across the globe. Besides the necessary health system reforms, digitalisation in health and social care is seen as a major development to make related services better accessible, more efficient, and cost-effective. The current health and social care systems are professionally, organisational and financially fragmented. While usually the digital infrastructures and related information exchange are alike disintegrated with serious consequences for the health and social system performance and patient safety. This presentation poses the question how a redesign and alignment of regulation might help to facilitate EU citizen centred, digital enabled, health and social care services, considering the needs and challenges presented.
Ondřej Filipec	**e-Health in the Czech Republic: When Politics Meets Law** Covid-19 had a significant impact on the digitalization of healthcare in the Czech Republic and provided the final impetus for enacting new regulation in the area of e-health. However, the final proposal of the "E-health Act" is minimalistic with many political challenges ahead. Notably decentralized implementation may create future barriers and lead to systemic gaps limiting the accessibility and effectiveness of healthcare. Moreover, there is also a lack of the technical standards or dependency on the other pieces of related legislation. As a result, hospitals in the Czech Republic are building e-healthcare in their own way .with all positive and negative implications. The main aim of this contribution is to critically analyse possible impacts and challenges related to very new legislation in the Czech Republic which was aimed to bridge the gap vastly extended over the last 20 years, mainly due to political reasons.

Thomas Hoffmann	**Digital healthcare and AI** The practice of medicine today is dominated by heuristics and rule-based systems - matters which both will be outpowered by AI in near future. Still, five main levels remain where also sophisticated AI-run systems may decide erroneously, causing complex liability entanglements and thus considerable legal controversies. This short presentation will leave mistakes based on technical malfunction (i.e. hardware defects) aside and focus on the impact of an AI's malfunctioning software on the legal rights and duties of patients, doctors and further healthcare personnel, software engineers and the respective intermediaries (hospital management, service providers) as well as on possible challenges arising in future, when AI may have to take into account far more parameters than merely the pathological state of the patient (for instance limited resources and non-discrimination).

An overview of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section V

Chairman: Dr. Agnes Kaspar

22nd June at 11:00 – 12:30 by CET

Author(s)	**Title & Abstract**
Jozef Andraško/Comenius University in Bratislava	**QUO VADIS CYBERSECURITY?** NIS Directive as the EU's first cross-cutting regulatory tool in the area of cybersecurity has proven its limitations and has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. The low level of cyber resilience of businesses operating in the EU, the inconsistent resilience across Member States and sectors and the low level of joint situational awareness and lack of joint crisis response are the main issues identified by the evaluation on the functioning of the NIS Directive, conducted for the purposes of the Impact Assessment. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) aims at elimination aforementioned issues. Furthermore, the NIS 2 Directive should modernise the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. First of all, the author focuses on new categories of entities falling within the scope of the NIS 2 Directive, in particular essential and important entities. The author will compare the identification process used in NIS Directive with a uniform criterion that determines the entities falling within the scope of application of NIS 2 Directive (size-cap rule). Secondly, the author will compare the scope of risk management requirements and reporting obligations applied in NIS 2 Directive with risk management requirements and reporting obligations applied in NIS Directive. Furthermore, the author will critically point out the problematic provisions that concern reporting obligations.

	Last but not least, the author deals with competent authorities' new supervision powers as well as new administrative sanctions for breach of the cybersecurity risk management and reporting obligations that can be applied.
Aleksi Kajander/TalTech	**National Legal Framework for Smart City Software Security Vulnerabilities** A central feature of 'smart' cities is the utilization of interconnected ICT technologies such as an extensive sensor network to collect vast amounts of data to become more sustainable, competitive and improve welfare. However, such a vast interconnected network of devices also presents an unprecedentedly large multi-faceted attack surface for cyberattacks. In a complex smart city network, a cyberattack could easily have a cascading effect throughout the smart city's systems, causing multiple critical infrastructure systems to fail simultaneously. Critical infrastructure is already alarmingly regularly targeted by cyberattacks, such as the city of San Diego reported in 2016 that their systems are subject to on average 60 000 cyberattacks a day[1], which sometimes do succeed as demonstrated by power being denied to 250 000 people in Ukraine also in 2016[2] due to a successful cyberattack. Consequently, there is an abundance of reason to believe that a smart city network will be targeted and perhaps make for a more inviting target owing to the possibility of a single attack having a devastating effect on multiple critical systems. While there are multiple ways of exploiting vulnerabilities in systems, in cybersecurity there is often made a distinction between human, procedural and technology weaknesses. In this article the focus will be on tech security vulnerabilities, as software systems are at the heart of smart city digital infrastructures. As it is estimated that every 1000 lines of code will contain about 30 exploitable errors[3], it is reasonable to conclude that smart city software will inevitably contain exploitable weaknesses. Owing to the possibility of addressing software as goods, services, a mix of both or sui generis in legislation, there is a host of different legislation types that could address vulnerabilities therein such as consumer law, B2B regulation or cybersecurity-related legal acts.

[1] Anand, P. 'The 'mind-boggling' risks your city faces from cyber attackers'<https://www.marketwatch.com/story/the-mind-boggling-risks-your-city-faces-from-cyber-attackers-2016-01-04> Accessed 04.06.2021.
[2] Zetter, K. 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>, Accessed 04.06.2021.
[3] Kitchin, R., Dodge, M. (2019). 'The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention'. *Journal of Urban Technology*, Vol 26 (2), 49.

	Therefore, this article will chart and analyse the national legal framework in Estonia and Finland that addresses software security vulnerabilities, which is then contextualized for smart cities. The reason behind choosing Estonian and Finnish national laws is due to the cross-border smart city co-operation between the two capitals, Tallinn, and Helsinki. For Helsinki and Tallinn specifically an urban operating system has been proposed which would form a real-time cross-border link between the two cities4. Consequently, considering any software vulnerabilities would potentially be shared also between the two participants, the compatibility or lack thereof of their national legislations on the topic of software vulnerabilities as may be applicable for smart cities is an incredibly relevant question. In a twin smart city if the network that connects the two smart cities is compromised the cascading effect could potentially affect critical infrastructure in both cities and thus, both countries. As a result, a joint software system vulnerability management is a definite need for such a twin smart city project, which requires a compatible legal framework which this article aims to examine.
Tomáš Gábriš/Palacký University/Slovak Academy of Sciences	**An exercise in digital sovereignty: The long run of amendment to Slovak Cybersecurity Act** The Slovak Cybersecurity Act is in the longlasting process of its amending which started in mid2020, so as to meet the challenges of the 5G EU Toolbox. Despite numerous rounds of criticism and re-evaluations, the process is still not finished. It seems that the major contradiction and clash of interests lies in the search for proportionality between private business interests and national (and supranational) sovereignty, albeit issues of privacy and data protection come into play as well. The final battle is taking place these days, when the Slovak Parliament is debating the final wording of the amendment, together with accompanying proposals for additional changes, submitted by the members of the parliament. The "rational legislator" is thus to take his final word in the debate, based on which it will be possible to assess to what extent the public and private interests managed to be reconciled and to what extent the aim of securing digital sovereignty with regard to 5G networks was successful in Slovakia.
Agnes Kaspar/TalTech	**The emerging duty of care principle in EU cybersecurity** The overall idea of ’duty of care’ principle was first formulated in the EU’s Cybersecurity Strategies in 2017. It is based on the fact that there are no guarantees for 100% security, however the well-known and

[4] Soe, R-M. (2017). Smart Twin Cities via Urban Operating System. ICEGOV’17: Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance, 394.

	well-documented defects and vulnerabilities in software and hardware provide an ample attack surface that can be exploited by malicious actors, therefore it is desirable to take steps to reduce these vulnerabilities. While not all defects are critical from cybersecurity perspective, there are more than abundant examples when they have been exploited causing global outcry and led to international face-offs between countries.[5] The problem is exacerbated by the growing interdependence between information systems, and the proliferation of Internet of Things (which are often notoriously insecure), where a weak link in a system can open the gateway and have knock-on effect on linked critical systems. The EU has promoted the 'security by design' approach to address the issue, however, given the dynamic nature of information systems, this is a static solution[6] which should be accompanied by additional technical, legal and policy measures. The 2020 EU Cybersecurity Strategy promises new rules for software manufacturers to address vulnerabilities, including not only at the design phase, but also continued updates until end of life. Some steps are already taken before in the field of consumer protection in this regard, however if such enterprise is to succeed more broadly, the precise rules on vulnerability detection and disclosure need to be clarified. There are open questions in both regards. Ethical hacker, who may be more than instrumental in detecting vulnerabilities without having the intention to exploit them can be deterred by narrowly formulated criminal provisions (some based on Directive 2013/40/EU) and the disclosure of vulnerabilities have no EU level coordination – therefore it is up to national rules whether and when a vulnerability is such that it requires some action on the part of the manufacturer or the entity using the software. ENISA, the EU Cybersecurity Agency has published a call (tender) earlier this year, and „aims to procure supporting services to take stock of existing policies and good practices on Coordinated Vulnerability Disclosure (CVD), in the EU Member States and outside the EU, as well as taking stock of the existing national, regional and global vulnerability registers and databases and the formats, metrics, procedures used in these registers and databases".[7] The building of such database (which may or may not compete with existing databases) raises the question about its purpose and potential role in the EU legal system. For example, under the new Directive (EU) 2019/770 traders will have to ensure that consumers are informed of and supplied with security updates, however it is not clear when these security updates needed to be made. When, if there is an obligation to update a software, if it is not provided by contract? To certain extent, the Network and Information Security (NIS) Directive gives guidelines to a limited circle of actors,

[5] Mention could be about Wannacry, Petya, Non-Petya, or the most recent SolarWinds incidents.
[6] Ilves and Osula, The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out, available at https://m.guardtime.com/files/Ilves_Osula.pdf
[7] https://www.enisa.europa.eu/procurement/vulnerability-disclosure-policies-and-vulnerability-databases

	which need to observe 'state of the art', and the proposed NIS2 Directive (if adopted) may extend this requirement to more actors, even small enterprises. GDPR is also 'choice of weapon' on occasions when long-known vulnerabilities are exploited and the result is compromise of personal data (see for example Gloucester City Council fine[8] or the Digi fine in Hungary[9]). However, this concerns only issues with personal data, and vulnerability information may not qualify as such. Duty of care principle is now starting to shape, the framework's bits and pieces are starting to find their places, yet there are still many links missing. This research aims to cross some t's and dot some i's, focusing on legal issues relating to software vulnerabilities detection and disclosure, and their potential legal effect in the EU's cybersecurity-related legal ecosystem, and eventually, contribute to a clearer formulation of the duty of care principle in EU cybersecurity. *Keywords:* software vulnerability, vulnerability disclosure, cybercrime, duty of care, cybersecurity

[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/gloucester-city-council-fined-by-ico-for-leaving-personal-information-vulnerable-to-attack/
[9] https://www.twobirds.com/en/news/articles/2020/hungary/record-breaking-gdpr-fine-imposed-in-hungary-as-a-result-of-a-website-security-vulnerability

An overview of abstracts selected for the conference ***'The European Digital Single Market: Current and Future Challenges in the European Union law' on-line: 21st – 22nd June 2021'***

Section VI

Chairman: PhD researcher Pablo Martínez-Ramil

22nd June at 13:15 – 14:30 by CET

Author(s)	**Title & Abstract**
Matúš Mesarčík/Comenius University in Bratislava	**Transparency of algorithms: Current issues and future challenges** Regulation of artificial intelligence is one of the cornerstones of the ongoing agenda of the European Commission. Recently published proposal for the Artificial Intelligence Act complements the goal and stimulates political and academic discussions. The often-discussed issue of artificial intelligence is transparency or explainability (XAI) as a prerequisite for trustworthiness, ethics, and enforcement of individual rights. The aim of the transparency is either the explanation of individual decisions made by algorithms or a description of the logic behind the algorithm. However, these purposes are not always distinguished by legislation and their legislative expression is unclear. On the other hand, publishing information concerning the functioning of the algorithm clashes with the intellectual property rights of the developers and may cause the gaming of the algorithms by users. These aspects shall be carefully considered when legally requiring transparency of algorithms. The presentation discusses current legislation concerning algorithmic transparency. The special focus is on Article 22 of the EU General Data Protection Regulation provisioning automated decisions making. The scope of the article is still unclear and its obligations regarding transparency are blurry. Furthermore, the specific requirement of ranking provisioned in the regulation on fairness and transparency for business users of online intermediation services (2019/1150) is discussed. The ranking provides a certain level of transparency mainly for business users but is often valuable to data subjects as well. However, a strong emphasis on transparency may result in gaming. Finally, the proposed Artificial Intelligence Act also presents specific obligations regarding transparency. How it will fit the current regulation of algorithmic transparency? The presentation provides a critical analysis of the current and future transparency obligations of artificial intelligence

	and proposes a holistic approach considering various stakeholders and different goals of legislative requirements.
Gizem Gültekin-Várkonyi/University of Szeged	**Personal data, personal robots, personal services: Technical, legal, and practical challenges** Recent developments in artificial intelligence (AI) and robotics point a close future collaboration between human and machines. Even though use of personal robots is not yet a phenomenon, findings in technical and legal literature point several possible risks in processing personal data by such robots from the technical, legal and practical point of views. The technical risks belong to the nature of data processing conducted by algorithms based on Big Data and refer to the probability for unpredictability of the outputs generated. Furthermore, potential bias and discrimination issues shall be raised as part of the technical risks. Finally, the Uncanny Valley concept should be discussed from the point that it may encourage people to disclose more information about themselves. The applicability of the General Data Protection Regulation (GDPR) on AI technologies consist the legal aspects of the potential risks. At this point, invalid consent practices could be brought to the table as it would be potential legal basis for data controllers operating personal robots. The last part of the discussions would refer to the risks related to practical aspects that are, for example, the intersection of an average user in consumer law, consent in the GDPR and the actual use cases. In the end, some solutions will be raised aiming to contribute in better application of the GDPR on AI technologies in personal use, and a short evaluation on the proposed so-called AI Regulation would be presented.
Pablo Martínez-Ramil/Palacký University	**Is the EU human rights legal framework able to cope with discriminatory AI?** The challenges possessed by AI for the EU anti-discrimination legal framework have been a wide discussed topic among the doctrine. In the light of the 20th anniversary of the EU Charter of Fundamental Rights, the Commission released a regulatory proposal to tackle AI. Thus, this presentation seeks to determine whether the proposal successfully addresses the existent pitfalls of the EU framework. First, an analysis of the functioning of AI systems that employ machine learning techniques and determines how discrimination takes place. Second, intellectual property rights are examined as one of the main barriers for accountability and redressal for violations committed by an AI system. Third, the state of the discussion concerning the pitfalls of the existent EU approach towards non-discrimination is addressed. The available academic literature suggests that discriminatory outputs produced by an AI will amount to indirect discrimination in most scenarios.

	In this sense, cases of indirect proxy discrimination will likely pass the proportionality test, therefore justifying the discriminatory output. The last section of this article studies the Commission' regulatory proposal. Although the document seems to effectively tackle discrimination caused by biased training data sets, this paper concludes that intellectual property rights and proxy discrimination still constitute significant barriers for the enforcement of anti-discrimination law.