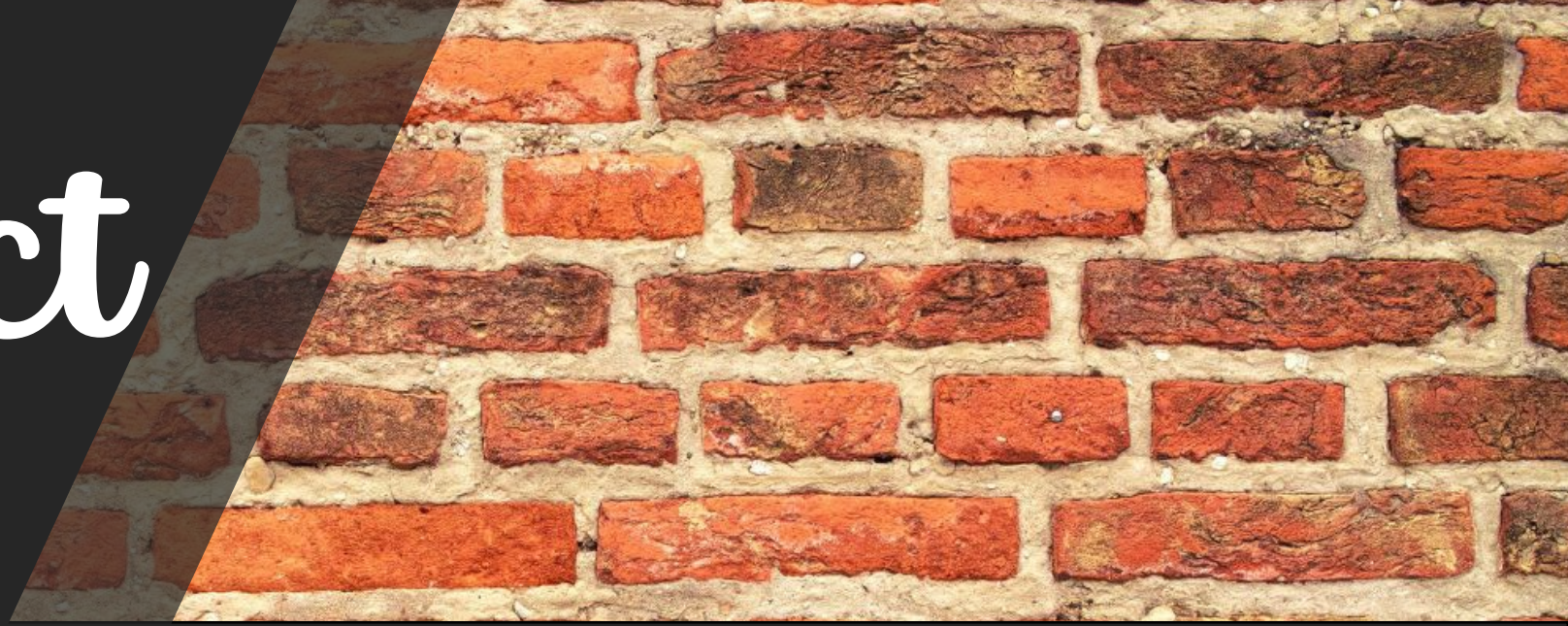
Abstract Book



International Scientific Conference

„The Right to Privacy - View of Young Researchers"

The event is organised as part of the **Central European Professors' Network**,

CENTRAL EUROPEAN PROFESSORS' NETWORK

WYDZIAŁ PRAWA I ADMINISTRACJI UKSW
Fides et Ius

IWS
INSTYTUT WYMIARU SPRAWIEDLIWOŚCI

KNPKP
Koło Naukowe Prawa Karnego Procesowego

CEA
CENTRAL EUROPEAN ACADEMY

coordinated by the University of Miskolc - Central European Academy

Scientific Committee

1. Prof. Dr. Dusan Popovic
2. Prof. Dr. hab. András Koltay
3. Ass Prof. Dr. David Sehnálek
4. Assis Prof Dr. Matija Damjan
5. prof. Zoltan J. Toth
6. prof. Aleksandra Syryt
7. dr hab. Marcin Wielec, prof. UKSW
8. JUDr. PhDr. Lilla Garayova, PhD

Dr. András Koltay

Dr. András Koltay

Dr. András Koltay is the research professor of the University of Public Service (Budapest). He is also professor of law at Pázmány Péter Catholic University Faculty of Law and Political Sciences in Budapest, Hungary. He received LL.M. degree in public law at the University College London in 2006, and PhD degree in law at the Pázmány Péter Catholic University in 2008. Between 2018 and 2021, he served as rector of the University of Public Service. He has been the president of the National Media and Infocommunications Authority of Hungary since 2021. His principal research has been concerned with freedom of speech, personality rights and media regulations, but he also deals with other constitutional questions. He is the author of more than 400 publications, and numerous monographs on freedom of speech; in English: *Freedom of Speech – the Unreachable Mirage* (Wolters Kluwer 2013), *The Troubled Relationship between Religions and the State. Freedom of Expression and Freedom of Religion* (Whitelocke 2017) and *New Media and Freedom of Expression* (Hart 2019). He was a speaker in more than 125 conferences in several countries.

Ass Prof. Dr.
David Sehnálek

Ass Prof. Dr. David Sehnálek

Associate professor and a vice dean at Faculty of Law, Masaryk University in Brno. Teacher of European Union Law, organizator of every year Autumn School of Global Legal Skills for the students in region covering primarily the Czech Rep. And Australia. Its aim is to promote the legal skills in system of education and introduce students to diffrent methods of legal thinking and argumentation. Project leader on the project about development and introduction of the first distance learning program in law studies in Czech Rep.

dr hab.
Marcin Wielec,
prof. UKSW

dr hab. Marcin Wielec, prof. UKSW

A graduate of the Faculty of Law and Administration at the Cardinal Stefan Wyszyński University in Warsaw. Professor of the Cardinal Wyszyński University in Warsaw. Currently, at this Faculty, he is also Vice-Dean for Student Affairs in the field of "Law", as well as "Man in Cyberspace" and the Head of the Department of Criminal Procedure of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw.
A graduate of the MBA program – Top Public Executive at IESE Business School University of Navarra in Barcelona and the Lech Kaczyński National School of Public Administration. Director of the Institute of Justice in Warsaw.

Vice-chairman of the Scientific Council of the Institute of Forensic Expertise Prof. J. Sehna in Kraków, Member of the Council of the Lech Kaczyński National School of Public Administration. Member of many program bodies of scientific journals in Poland and abroad, including: Chief editor of the quarterly "Law in Action" published by the Institute of Justice in Warsaw, Member of the Scientific Council of the journal "Probacja" published by the Ministry of Justice, Member of the Program Board of the international scientific journal "Central European Journal of Comparative Law" published by the Ferenc Mádl Institute of Comparative Law in Budapest, Member of the Program Board of the international scientific journal "Law, Identity and Values" published by Central European Academic in Hungary, Member of the Program and Scientific Council of the scientific journal "Law and Climate" published by the Ministry of Climate and Environment. Member of the Central European Professor Network, co-founder of an international research project called the Polish-Hungarian Research Platform conducted by the Institute of Justice in Warsaw, President of the Polish Association of Comparative Law and a member of the Central European Association of Comparative Law based in Miskolc (Hungary).

Author of many scientific studies in the field of criminal law and procedure, disciplinary law and proceedings, executive criminal law, axiology of law, etc.

Assis Prof Dr.
Matija Damjan

Assis Prof Dr. Matija Damjan

Dr Matija Damjan an Assistant Professor for civil and commercial law at University of Ljubljana, Faculty of Law, and Secretary General of the Institute for Comparative Law attached to the Faculty of Law, where he is also active as a research fellow. He passed the State Examination in Law in 2005, after having worked for two years at the Higher Court in Ljubljana as a judicial trainee. He obtained his PhD at the Faculty of Law, University in Ljubljana in 2007 and has been active in the scientific legal research since then. In his work, he primarily focuses on the areas of civil law, intellectual property law and information society law, and has authored and co-authored more than thirty scientific articles and monographs discussing issues in these fields. He is currently engaged in long-term research projects on the legal challenges of the information society and on the impact of the European regulation of electronic communications and competition law on the legal position of telecommunications networks. Since 2020, he has been a member of the Data Governance Working Group at the Global Partnership on Artificial Intelligence.

Prof. **Zoltan J. Toth**

Prof. Dr. Zoltan J. Toth

Prof. Dr. Zoltan J. Toth has graduated in law from University of Szeged, Hungary in 2002. From 2002 until recently he has been working in the Faculty of Law at Károli Gáspár University, Budapest; at present, he is a full professor in the Deparment of Jurisprudence and History of Law. Besides this, he serves as a chief counsellor to the Constitutional Court of Hungary. He is a member of the Central European Professors' Network, member of the Scientific Council of the Eötvös Loránd Research Network, Hungary, and vice president of the Hungarian Association of Law and Political Sciences. Previously, his main research topic was the matter of capital punishment; now he studies the theoretical and practical aspects of constitutional adjudication and the issue of constitutional and statutory interpretation. Altogether he has published 15 books as author or co-author; his latest monograph is 'Changing Attitudes Towards the Death Penalty: Hungary's Renewed Support for Capital Punishment' (Palgrave Macmillan, 2020); his latest edited book is 'Constitutional Reasoning and Constitutional Interpretation: Analysis on Certain Central European Countries' (Ferenc Mádl Institute of Comparative Law – Central European Academic Publishing, 2021). E-mail: toth.zoltan@kre.hu.

Prof. Dr.
Dusan Popovic

Prof. Dr. Dusan Popovic

Dr. Dušan Popović is a Full Professor of Intellectual Property Law, Competition Law and Internet Law at the University of Belgrade Faculty of Law. He holds a PhD degree from the University Paris-Nanterre, LLM degree from the University of Nancy and LLB degree from the University of Belgrade. He was visiting researcher at the University Panthéon-Assas (2019), Max Planck Institute for Innovation and Competition (2014, 2010), CEIPI – University of Strasbourg (2012, 2011, 2010) and University of Salzburg (2008). He was a visiting professor at the University of Lyon III Jean Moulin (2018/2019) and University of Skopje (2014-2016) and held a number of guest lectures at different European universities. Dr. Dušan Popović served as a Jean Monnet Module Leader within the Erasmus+ project “Free trade agreements and European integration of SEE countries” (2017-2020).

JUDr. PhDr.
Lilla Garayova,
PhD

JUDr. PhDr. Lilla Garayova, PhD

Lilla Garayova is an international lawyer and an associate professor of International Law. She defended her doctoral dissertation in English in 2017 at the Faculty of Law of the Pan-European University with the title: "Torture as a means to prevent terrorism?". In parallel with her legal studies, she also studied Japanese language and intercultural communication at the Faculty of Arts of Comenius University. She is affiliated with the Institute of International and European Law of the Pan-European University. She speaks 9 foreign languages and regularly publishes and lectures in them. Her professional and publishing practice focuses on international law and the protection of human rights. She is a member of the Scientific Council of the Faculty of Law of the Pan-European University, the Slovak Association of European Law and the Central European Society of Administrative Science. She is a member of the editorial boards of several national and international scientific journals, including the Central European Journal of Comparative Law; Institutiones Administrationis - Journal of Administrative Sciences and Paneurópske právnické listy. Currently, she is one of the experts of the Central European Professors' Network. Since October 2020, she has been serving as Vice Dean for Bachelor and Master Studies and International Relations of the Faculty of Law of the Pan-European University.

Prof. **Aleksandra Syryt**

Prof. Aleksandra Syryt

Aleksandra Syryt, dr hab. assistant professor at the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw. Her research focuses on the field of constitutional law, including the principles of the system and the protection of human rights, the systemic foundations of local government, as well as legislation, the knowledge-based economy and the impact of technological changes and digital progress on the law. She has experience in managing and participating in research programmes, including interdisciplinary projects.

Speakers

1. Assist. Aljoša Polajžar
2. Tomasz Bojanowski
3. Agata Wróbel
4. M. Sc. Matjaž Drev
5. Klaudia Łuniewska
6. JUDr. Ing. Dominika Moravcová
7. JUDr. Edita Filadelfiová
8. Igor Popovic
9. Bartłomiej Oręziak
10. Assis Prof Dr. Matija Damjan
11. Ass Prof. Dr. David Sehnálek

Assist.
Aljoša Polajžar

Assist. Aljoša Polajžar

Assistant Aljoša Polajžar is a Young Research Fellow, Academic Assistant and PhD candidate at the University of Maribor, Faculty of Law - under mentorship of Full Professor Darja Senčur Peček, Ph.D. He commenced employment in October 2020 (period of study 2015-2020). He defended his Master's thesis in law on the topic of employee privacy protection at the workplace in the digital era (fields of Labour law, Data Protection law, Human Rights law and EU law). His PhD research is focused on (collective) labour law aspects of platform work. He is the author of numerous scientific and professional articles in the field of Law in English and Slovenian (see COBISS and SICRIS). He is the assistant of the LeXonomica journal (WoS) Editorial board – international scientific journal for the fields of Law and Economics. He serves as the faculty coordinator of the international Moot Court and Model United Nations (MUN) competitions, which he himself attended as a competitor and co-mentor during his studies (European law moot court competition, etc.). He is a co-author of the Commentary on the Slovenian Public Sector Salary System Act (ZSPJS) and the Public Employees Act (ZJU).

Assist. Aljoša Polajžar

The Right to Privacy at the Workplace: the ECHR and EU law Perspective

The development of information and communications technology (ICT) has brought new possibilities for workplace surveillance. As an organizer of the working process and the owner of the working equipment, the employer has the interest that his ICT equipment is used for work-related purposes. Due to the possibility that a working computer, internet, e-mail, etc. are used for private purposes, the employer has the interest to monitor the employee's use of the ICT equipment. The problem is to determine the legal limits of admissible workplace monitoring. The cases and conditions under which this kind of surveillance is permissible are not specifically denoted in the law.
The limits of permissible workplace surveillance are delineated by weighing the directly applicable fundamental rights of the employee and employer's legitimate interests via the method of practical concordance. Workplace monitoring is an interference into employee's rights to protection of (communications, information) privacy, and personal data.
The fundamental rights in question are protected within the framework of the national Constitutions, the EU Charter, and the ECHR. Under EU law, the limits of permissible surveillance are delineated by the General Data Protection Regulation (GDPR), which must be interpreted in light of the EU Charter. It also follows from the guidelines of the Article 29 Data Protection Working Party that monitoring can only be carried out in compliance with the principles of the GDPR, namely transparency, proportionality, and lawfulness of the processing. Due to the employee's position as a weaker party in an employment relationship, his consent will in general not be an appropriate legal basis for the surveillance.
It follows from ECtHR case law that in order to determine the limits of permissible surveillance, it is essential to assess whether the employee had a reasonable expectation of privacy in connection to the use of the work-related ICT equipment, and whether the employer had sufficiently substantiated interests to exercise the surveillance. Conducting workplace monitoring should be ultima ratio. Regarding the enaction of special statutory rules, the GDPR contains the possibility to regulate workplace monitoring with special statutory rules or with bilateral autonomous rules. Moreover, it would be appropriate that employers would lay down detailed organizational rules in general acts - specifying the obligations of employees and setting the limits of permissible use of the ICT equipment for private purposes.

Tomasz Bojanowski

Tomasz Bojanowski

student of Law at the Faculty of Law and Administration of Cardinal Stefan Wyszyński University.
Scholarship holder of the Minister of Education and Science for significant achievements for the academic year 2021/2022 and scholarship holder of the President of the City of Warsaw named after John Paul II for the academic year 2018/2019. Author of scientific articles and participant of research projects. Speaker and organiser of national and international scientific conferences.

Main areas of scientific interest are: criminal law and process, legal protection bodies, protection of human rights, administrative law, constitutional law and history of law.

Tomasz Bojanowski

Criminal pre-trial is closely linked to the issue of so-called investigative operations

At this point it should be emphasised that the literature has developed many definitions of investigative operations, but none of them has primacy over the others However, it is possible to list some features which are repeated in most definitions:
1) the competence for investigative operations. should result from universally binding provisions, at least of the rank of a act of Parliament;
2) in the framework of investigative operations., information is obtained or confirmed, which can be used as evidence in a criminal trial;
3) the main objective of investigative operations. should be the detection and prevention of crime
4) investigative operations are of a secret nature;
5) investigative operations may be conducted only by authorised bodies;

It is also necessary to add one more important feature that investigative operations are controlled by the judiciary, and more specifically by the locally competent regional courts, which was not indicated by the above-mentioned.

On this basis we can define investigative operations. as activities of authorised legal protection bodies, which result from generally binding regulations, are secret in nature, aim at obtaining or confirming information for the needs of a future criminal trial, and their main purpose is to detect and counteract crime and socially harmful behaviour.

It is clear from this that investigative operations interfere with the right to privacy.

The right to privacy is one of the fundamental human rights which stems, inter alia, from Article 12 of the Universal Declaration of Human Rights ('PDHR') , Article 17 of the International Covenant on Civil and Political Rights ('ICCPR') , Article 8 of the European Convention on Human Rights ('ECHR') and Article 47 of the Constitution of the Republic of Poland . The strong embedding of the human right in question confirms that it stems directly from human dignity and is one of the elements that allows a person to self-define.

The issue of investigative operations have been the subject of jurisprudence of the Polish Constitutional Tribunal in the context of the right to privacy.

Investigative operations are undoubtedly a violation of fundamental rights and freedoms anchored in the Constitution of the Republic of Poland, but they are admissible from the perspective of the necessity of their limitation on the basis of the general limiting clause established in Article 31 par 3 of the Constitution of the Republic of Poland as admissibility of violating the essence of freedoms and rights.

Despite the broad protection of rights and freedoms, Investigative operations are admissible on constitutional grounds, but each of their forms must be considered on the constitutional and purpose-related level as intertwined issues of activities in the process of criminal prosecution carried out by an authorised body. On this basis it may be concluded that investigative operations are consistent with the Constitution, if they fulfil a number of specific conditions. Firstly, as a restriction of human rights and freedoms they must comply with the previously mentioned principle of proportionality expressed in Article 31 par. 3 of the Constitution of the Republic of Poland. Investigative operations may be provided for only by act of Parliament and only when they are necessary in a democratic state of law for its security or public order, or for the protection of the environment, health and public morals, or freedoms and rights of other persons.
At this point, it should be pointed out that due to technological development and social processes, both the Europeans and nationals courts rulings in specific cases are on the side of individual rights,. in a way endorsing the right to privacy. In such circumstances one should reflect on the progressive interference with the right to privacy and anonymity through Investigative operations. In the previous I mentioned that Constitutional Court in Poland, under strict conditions, allow interference with the right to privacy through Investigative operations, which is intensified by recent legislative changes and technological development, digitisation and equipment of services authorised to conduct operational work, such as the Pegasus system.
In the reality of the information society, we need to consider whether the right to privacy or anonymity is not a normative fiction. In fact, we consent to being deprived of these rights through the use of modern technologies. In the context of this issue, the development of legislation and case law lines on the admissibility of Investigative operations and the right to privacy should be closely observed. Both issues are on a collision course and the current trend in national and international case law (ECtHR and CJEU) leads to an inevitable conflict that will eventually have to be resolved. This is likely to be the task facing the European Court of Human Rights, and its decision will be crucial to the perception of human rights from the perspective of the modern rule of law and Investigative operations

Agata Wróbel

Agata Wróbel

Law student at the Faculty of Law and Administration of the Cardinal Stefan Wyszynski University in Warsaw, member of the board of the Scientific Circle of Criminal Procedure of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, recipient of the Rector's Scholarship for the best students for 2020/2021, organizer of international and national scientific conferences, member of international and national scientific projects.

Main interests: public international law, criminal procedure, European Union law, human rights

Agata Wróbel
Protecting privacy on the Internet - an analysis of selected virtual privacy violations

Cybercrime is an area that Polish law has only recently begun to address. The coronavirus epidemic, which has determined in many cases remote work in various areas of social life, has also shown much need here. In Polish law there is no legal definition of this phenomenon, so for the purpose of my speech I will adopt a very broad definition,
according to which cybercrime is a type of crime in which a computer is either an instrument or an object of crime. The term covers all kinds of crimes committed with the help of computer or ICT networks.
The speech is about legal regulations and specifics of privacy rights violations in the form of:

- **phishing** (a security cracking technique used to obtain personal and confidential information for the purpose of identity theft by sending fake emails that resemble misleadingly authentic messages),
- **spyware** (spyware is a type of so-called "malware" that infects a computer or mobile device and gathers information about the user and their browsing habits on the web and Internet usage. This includes capturing keystrokes, screenshots, credentials, personal email addresses),
- **sniffing** (a form of privacy violation in which the perpetrator. does not interfere with the content of the data stored on the victim's computer, but "snoops" on what is happening),
- **e-mail worm** (is a malware that causes massive attacks on a user's device and accounts by gaining control and email inbox and sending massive amounts of virus emails),
- **spam** (privacy on the Internet can be violated not only by unauthorized gaining of information about a person, but also by imposing on user’s content, which the user not agreed to receive before),
- **nigerian fraud** (it is most often inducted by contacting a potential victim via e-mail and offering him the opportunity to obtain substantial funds in exchange for "assistance" in recovering them by, for example, setting up and confirming bank account login data, paying a bribe).

Although the Criminal Code provides protection in many cases of cybercrimes, the Polish doctrine still needs modernization in this regard. I think the starting point should be a defining broad definition of cybercrime. Such a definition should address in its essence issues not yet regulated by law, such as hate speech or the crime of fake news.

M. Sc.

Matjaž Drev

M. Sc. Matjaž Drev

Matjaž Drev, MSc., is an information security consultant at the National Institute of Public Health. He has been professionally involved in the field of personal data protection and information privacy for more than a decade, first as a system administrator, then as a state supervisor for personal data protection at the Information Commissioner of the Republic of Slovenia. As a part of his publishing activities, he has published several articles in peer-reviewed journals. He is also a co-author of the commentary on the General Data Protection Regulation (GDPR) and a long-time lecturer. Currently, he is doing a Ph.D. at the Faculty of Information Studies, Novo Mesto, on the topic of privacy by design.

M.Sc. Matjaž Drev

Integrating privacy in personal data processing operations

The use of the internet and related smart devices encourages mass processing of an individual`s personal data, which commonly leads to a reduction in privacy. In the European Union legislators faced this challenge decisively in 2018, when the General Data Protection Regulation (GDPR) was enforced. Through the idea of *data protection by design and by default*, GDPR seeks to direct the development and use of information communication technology in a way in which personal data processing, taking into account the legitimate interest of the public and private sector, interferes as little as possible with the privacy of individuals.

The purpose of the research done was to find out how the GDPR understands *data protection by design and by default*, to compare different approaches of other relevant authors, and to offer guidelines for a conceptual model of *privacy by design* covering all key elements of data protection by design and by default. The proposed conceptual model was then tested on the information system of the national health organization (NHO). The whole process of implementation included gathering sufficient information, doing gap analysis by comparing the actual state of data processing with GDPR requirements and (optimized) *data protection by design and by default* criteria, and producing the final report.

Results showed that the concept of *privacy by design* can be clearly defined, which includes the identification of common building blocks. The analysis enabled the conceptualization of a model that was general enough to be implemented in a variety of personal data processing operations, while also specific enough to ensure a clear understanding of how to implement it. However, a few research questions remained unanswered. Was the proposed conceptual model better than alternatives, either other models or an ad hoc unsystematic approach? Was the implementation procedure optimal? Would it be feasible to empirically measure both the effectiveness and efficiency of the conceptual model when applied to personal data processing operations? These questions could, at least to some extent, be answered in further (comparative) research.

M. Sc. **Klaudia Łuniewska**

M. Sc. Klaudia Łuniewska

polish lawyer. A graduate of law at the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw. Research and technical specialist at the Institute of Justice. Author of several dozen legal studies (scientific articles, chapters, glosses, etc.). Member of a number of national and international research projects.
Speaker and organizer of national and international scientific conferences, as well as scientific events. Multiple scholarship holder of the Rector's scholarship for the best students. Laureate of the XLVIII. International Seminar of Scientific Circles, awarded for the best speech during a legal and political panel. President and Vice-President of the Scientific Circle of Criminal Trial Law at the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University, President and Vice-President of the Scientific Circle of International Law and Human Rights. Member of the Teaching Committee at the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw on behalf of students. Main interests focus on issues related to criminal law and criminal procedure, new technologies law, human rights protection, public international law, European Union law, and international relations, as well as internal security.

M. Sc. Klaudia Łuniewska

The right to privacy and the need to ensure the internal security of the state by public authorities - analysis of selected legal issues

The aim of the paper is to show the correlation of the right to privacy and the need to ensure state security by public authorities.
As part of the presentation, the issue of the right to privacy will be presented in opposition to the powers of Polish state authorities in the scope of the possibility of surveillance of citizens and interference in the life of an individual. The most important issues regarding Polish legislation in this area will also be presented, as well as statistics on the use of tools for surveillance of citizens by state authorities. It should be noted that the right to privacy has been guaranteed by a number of documents, both international and national. It has also been regulated in the Polish legal system at the constitutional and statutory level. This right gives everyone the right to the protection of private and family life, honor and good name and the right to decide about their personal life. However, the right to privacy is not absolute and may be limited. Currently, most countries, in justified cases, after meeting the conditions set out by law, allow the possibility of interference by state bodies with the right to privacy of the citizen. This may occur in the event of a threat, inter alia, public order, health, public morality or the freedom and rights of others. The interference and attempt to limit the right to privacy must be legal and proportionate. The interference of public authorities in the private sphere of an individual may take place, inter alia, in through the use of telecommunications data control, operational control, the use of control and recording the content of telephone calls (process wiretaps), as well as a number of other activities. As part of the presentation, the issue of the right to privacy will be presented in opposition to the powers of Polish state authorities in the scope of the possibility of surveillance of citizens. Specialized state authorities may obtain classified data about citizens, including, inter alia, telecommunications data (including subscriber and billing data, geolocation data, data from websites), as well as materials in the field of operational control (including out-of-process wiretaps). landline, cellular and satellite telephony, wiretapping of people and rooms, GPS, electronic wiretapping, acquisition and recording of the content of correspondence, access and control of the contents of parcels). Modern technologies have created a number of possibilities to control citizens. Often people themselves provide information about themselves necessary to state authorities, and sometimes white intelligence is not enough, and then operational work by special services and law enforcement agencies is needed. As part of the presentation, the most important issues regarding Polish legislation in this area will be presented, as well as statistics on the use of citizen surveillance tools by state authorities.

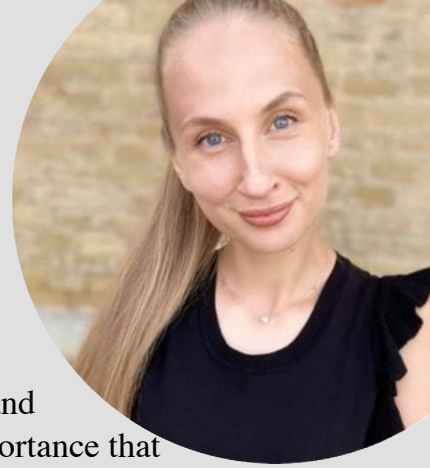
JUDr. Ing. **Dominika Moravcová**, MBA

JUDr. Ing. Dominika Moravcová, MBA

PhD student at the Faculty of Law of the Pan-European University in Bratislava, Slovak Republic. Her thesis work at the Faculty of Law and participation in conferences focuses primarily on judicial cooperation in civil matters within the EU. The topic of her dissertation comes from the sphere of the EU internal market and focuses on the area of recognition of professional qualifications. She graduated in law (JUDr.) and economics (Ing.) at the Pan-European University, Slovak Republic.

JUDr. Edita Filadelfiová / JUDr. Ing. Dominika Moravcová

Data protection on the Internet in EU and in Slovakia



The COVID-19 pandemic has led to a significant increase in online shopping across the EU and it is for this reason that we have chosen the topic of our paper from the online environment. The pandemic, in general, has also highlighted the need for greater security in the digital world. Not only e-commerce but also the use of online banking and various other online activities are essentially part of our daily lives, so we should be aware of how our data is protected on the Internet. Our paper focuses on the data protection on the Internet within the EU. The paper is dedicated to dealing with the general EU legal framework in this field and then subsequently with the specifics of the Slovak legislation. The European Union has a clear interest in the highest possible level of data protection. Legislation in this field ensures that our data is adequately protected whenever it is collected. A characteristic feature of the data protection on the Internet in the EU is that it also applies to companies based outside the EU, as long as they provide services in the EU market (e.g. social networking sites, foreign e-commerce sites, etc.).

In order to ensure the right to respect for private and family life, home and correspondence in the online environment, it was necessary to coordinate the collection and processing of data also on the Internet. A key source of law at the EU level is the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), which sets out, among other things, the detailed situations in which companies are able to collect and process personal data. It establishes rules for the protection of people in the processing of personal data in order to protect them. In the sphere of the Internet, we consider one of the main elements to be consent to the processing of personal data, which is often misunderstood as a necessarily marked disagreement and not as explicit consent.

We would like to draw companies' attention to the website GDPR.eu. This page provides a great deal of useful information to help companies harmonize their GDPR terms and conditions with current legislation. The mere fact that the GDPR is a regulation that is binding in its entirety and directly applicable in all Member States, underlines the importance that the EU places on this subject. On the Internet we often come across the term „cookies“. These are small text files that web applications store on the user's device via the browser. Here, it is necessary to distinguish the nature of the cookies, as not all of them are subject to our consent. This also brings us to another key source of EU law in the area under analysis, the so-called ePrivacy Directive. Although it has been in force for about 20 years, it underwent a comprehensive amendment in 2009 to reflect current needs. The Directive aims to harmonize legislation in the Member States to ensure an adequate level of protection of fundamental rights and freedoms with regard to the processing of personal data in the electronic communication sector. It is a Directive, which means it is a legally binding act of secondary EU law, but which the Member States have to implement in their own legal systems. It sets a minimum standard for the regulation of cookies, while the Member States are naturally free to go beyond the protection set out in the Directive. It is also necessary to mention an independent European body, The European Data Protection Board (EDPB), which contributes to the uniform application of data protection rules throughout the European Union. In addition to the sources of secondary law, we extract a great deal of information on this field from the case-law of the Court of Justice of the EU, which, through its interpretation in selected preliminary rulings, completes the legislative framework in this area.

JUDr. **Edita Filadelfiová,** PhD **student**

JUDr. Edita Filadelfiová, PhD student, Bratislava, Slovakia

PhD student at Pan-european University, Edita Filadelfiová is a student of doctorate degree at Faculty of Law in the field of international law with the focus on European law. She started a PhD degree in 2021 and her research is mainly focused on public procurement in the European Union. In addition to her university studies, she is working in the field of human resources, labor and business law in the world of IT technology. Prior to university, she studied at foreign schools in France and Belgium, thanks to which she is fluent in French and English. She is interested in international diplomatic and economic relations, migration and deepening of European integrity.

JUDr. Edita Filadelfiová / JUDr. Ing. Dominika Moravcová
Data protection on the Internet in EU and in Slovakia

In the second part of the presentation, the authors focus on the Slovak legislation in the area of personal data protection on the Internet. Within the Slovak legislation, the EU acts have been transposed into the Slovak Act Act no. 452/2021 Coll. on Electronic Communications. The latter has been recently amended and is effective from 1 February 2022. The term associated with data protection on the Internet is undoubtedly "cookies". The Slovak legislation does not recognize the term "cookies" as such, but works with the definition: "whoever stores or accesses information stored on the user's terminal device is entitled to do so only if the user concerned has given demonstrable consent." The new law, in contrast to the old one, does not include the ability to give consent through the settings of the web browser. The amendment responded to a questionable inconsistency with the ePrivacy Directive as well as the GDPR. The law also regulates the formal requirements for the so-called "Cookie bar" as well as its content page. The Slovak Republic considers the issue of personal data protection on the Internet, especially in relation to consumers, to be very important. Changes by lawmakers since February are also a fact. The Electronic Communications Act regulates the maximum fine for breach of duty and, unlike the GDPR regulation (4% of turnover), according to the Slovak legislation, it can reach up to 10% of turnover for the previous calendar year.

Igor Popovic,
LL.M. senior
assistant

Igor Popovic, LL.M. senior assistant

Igor is a senior teaching and research assistant at the Faculty of Law of Banjaluka University (International Law Chair) in Bosnia and Herzegovina, where he earned his LL.B as the best student of his generation. He has an LL.M. from the University of Belgrade and is pursuing a Ph.D. at the same university (researching on freedom of expression and the Internet). Igor is a legal researcher for the Columbia Global Freedom of Expression Project and the Artistic Freedom Initiative's legal counsel for Western Balkans. In 2020, he passed the bar exam.

Igor is a supervisor at the "Institutio Oratoria" Centre for Public Speaking, where he teaches students about public speaking and coaches students on the faculty's moot-court squad for human rights competitions. He works with international organizations and NGOs such as the Council of Europe and the OSCE Mission in Bosnia and Herzegovina, and is on the OSCE's list of local experts on the European Convention on Human Rights.

Igor acted as an adviser or a counsel in several cases before local courts and the ECtHR related to human rights and constitutional law. The areas of his research are human rights, the ECHR, and international law in general.

Igor Popovic

Online Privacy and Freedom of Expression - ECtHR's approach

The European Court of Human Rights ("ECtHR" or "Court") has not been left out of the Internet era and it issued some significant rulings referring to the relationship between freedom of expression and private life (privacy) on the Internet. I will focus on two aspects of online speech and privacy (privacy) in three 2021 cases: (i) the right to be forgotten (RTBF) and (ii) anonymization and media.

In *Hurbain v. Belgium*, domestic courts ordered an online newspaper to anonymize a story about Mr. G.'s conviction for a tragic car accident that occurred twenty years earlier. The article was first published in print sixteen years before the request for anonymization. Belgium courts pleased Mr. G.'s request for anonymization under the right to be forgotten. The first significant feature of the case is that the Court followed the traditional five-part (defamation) test (*Axel Springer/von Hannover* criteria) and found no breach of Article 10. This test, however, is for defamation issues rather than the RTBF. Second, the ECtHR has accepted the domestic courts' findings that the RTBF could be invoked against primary sources (online news sites) rather than only search engines. Finally, RTBF the beneficiaries can be legal persons according to the domestic courts and the ECtHR. The Grand Chamber has opted to review the Chamber's judgment, therefore we shall hear from the Court on this matter once more.

The ECtHR altered its approach partially in the case of *Biancardi v. Italy*, which was determined only a few months after the *Hurbain* decision. This case included the RTBF as well, but only to a limited extent, because the applicant (a person who runs an internet news site) was held liable before domestic courts for failing to *de-index* (rather than anonymize) an article containing the names of two brothers involved in a restaurant fighting. At the time of rendering the last domestic decision, the criminal proceeding was still pending. The ECtHR found no violation of Article 10. However, unlike in *Hurbain*, the Court did not use the traditional five-part test and instead introduced a "new tripartite test". In the Chamber's opinion the "[s]pecial attention should be paid […] to (i) the length of time for which the article was kept online – particularly in the light of the purposes for which V.X.'s data was originally processed; (ii) the sensitiveness of the data at issue and (iii) the gravity of the sanction imposed on the applicant". In comparison to *Hurbain* (and earlier cases), this is a considerable step forward as the Court acknowledged that cases involving the online conflict between Articles 8 and 10 require a new method different from the traditional test. However, the Court's elaboration of these three elements is far from judicial excellency.

In addition, the Court might consider adducing other factors to the test, taking into account the press role in a society. In sum, one can only hope that the Grand Chamber might remedy the mentioned criticism of *Hurbain* and *Biancardi* judgments. While the previous two cases depict a clash between anonymization and privacy, and freedom of expression, the case of *Standard Verlagsgesellschaft mbH v. Austria (no. 3)* portrays compatibility of anonymization and freedom of expression. Austrian courts ordered the applicant (a company that runs a website) to disclose personal information about authors of online comments which were offensive for certain Austrian politicians. The comments were posted on the applicant's website. The applicant lodged the application and the Court found violation of the right to freedom of expression. The first significant judgment's conclusion is that governments interfere with journalistic freedom simply by requiring the identification of commentators. According to the ECtHR "anonymity would not be effective if the applicant company could not defend it by its own means." Second, the Austrian courts failed to examine the nature of speech claiming that it was only relevant to potential lawsuits brought by politicians against the commentators. Nonetheless, the ECtHR believes that national courts should assess the nature of expression in these types of cases, at least on a prima facie basis.

One could make several conclusions about the recent ECtHR's case-law on online privacy and freedom of expression:

- The Court, as international forum, will *regularly* accept domestic courts' views on new concepts arising from the Internet use. It is through these lenses that we should interpret the court's stance that the RTBF can be used against primary sources and that even legal persons may exercise such right.
- The ECtHR faces difficulties with fitting the existing standards concerning the relationship between Articles 8 and 10 in online environment. *Biancardi* has demonstrated that it is necessary to introduce a new test for certain online cases, i.e. RTBF cases. Yet, the *Biancardi* rationale does not seem persuasive regarding the RTBF.
- The ECtHR reaffirmed its previous views that in cases of interference with freedom of speech, the *nature of speech* should *always* be considered (at least in the *prima facie* manner);
- Lastly, an order to the online media to reveal the identity of anonymous commentators represents an interference with that media's freedom of speech.

M. Sc. **Bartłomiej Oręziak**

M. Sc. Bartłomiej Oręziak

Coordinator of the Center for Strategic Analyzes of Institute of Justice, researcher in the Central European Professors' Network 2021 (Research group „The Impact of Digital Platforms and Social Media on Freedom of Expression and Pluralism"), researcher in the Central European Professors' Network 2022 (Research group „The Right to Privacy"), PhD student at the Faculty of Law and Administration of the Cardinal Stefan Wyszynski University in Warsaw, laureate of the Minister of Science and Higher Education Scholarship for outstanding achievements in science for the academic year 2017/2018, winner of the DOCUP 2020 competition, Representative of the Institute of Justice in the Artificial Intelligence Working Group at the Chancellery of the President Council of Ministers, author of several dozen scientific texts (articles, chapters, glosses, etc.), manager and member of international and national research projects, as well as a speaker and organizer of international and national scientific conferences. Main interests: new technologies law, human rights protection, intellectual property law, public international law and criminal law and trial.

M. Sc. Bartłomiej Oręziak

The Right to Privacy as part of the New Technologies Law

This paper concerns the presentation of the right to privacy as part of the new technologies law. Currently noticeable technical and civilization progress changes the perception of traditional solutions. This progress has also created a new non -material space of human activity. We can see here many benefits and this is rather undeniable.

Nevertheless, at the same time it is obvious that this is associated with numerous threats. If cyberspace is a new space for human actions, it must also be a space for the rights and freedoms of each individual. Basically, the entire human rights protection system developed over the years should apply in cyberspace.

One of the more sensitive rights of the individual in this respect is the right to privacy. The paper is aimed at showing this right as an important element requiring increased protection in the digital world. As part of the presentation, an example range of new technologies for practical use will be shown as segments in which the right to privacy should be treated extremely seriously.

Finally, there will be a short summary with conclusions for the future.

Assis Prof Dr.

Matija Damjan

Assis Prof Dr. Matija Damjan
The protection of locational privacy in the digital age

Locational privacy covers the information on the individual's current or past location and movements in physical space. Before the advent of the digital age, covert surveillance used to be complex and costly activity that could easily cross the threshold of legality. Today's digital devices invariably include the location tracking function using different technologies. Additionally, individuals' location can be tracked electronically through various touch points. Hence, locational information is now collected quietly and cheaply. Location tracking is increasingly used in many software applications, which transmit the location data to the service provider to adapt the service to the user's location. From the user's perspective, this is often quite convenient: navigation services show us immediately where we are, Google search results are adapted to our location, drivers of taxi services know immediately where the customer is situated, and the service can tell when they will arrive there. During the Covid-19 crisis, similar apps have been used for contact tracing. Businesses also use location tracking to follow their employees' movements.

The bulk of locational information can reveal a lot about the private and even intimate life of any individual: the location of your home, your work place, whether you have visited a doctor, where you do your shopping, who you might be dating, etc. Tagging of people in geo-located photos shared on social networks interferes even with locational privacy of third parties. By analysing the collected locational data, service providers can build profiles of users' behaviour and preferences, which are then be used for personalised marketing. Service providers then sell, use or analyse the data to cater to advertisers. This can interfere with individuals' privacy. The collected locational data can also be hacked by third parties or misused by law enforcement to avoid the legal constraints connected with traditional surveillance. Businesses that collect locational data claim not to violate privacy because users' data is anonymous as they are interested in consumer preferences, not identities. However, the access to raw locational data often allows easy identification of persons without their permission.

Today's location tracking is part of individual's information privacy. The GDPR treats location data as personal data, so app users must specifically agree to location tracking, which they in fact do in exchange for free services. This legal solution is not satisfactory as most people never read data policies and cannot fully understand their legalistic language. Additionally, there is often hardly any alternative service that does not collect users' data. A better solution would be to regulate the technical infrastructure for the collection of locational data, so as to prevent or limit the centralised collection of locational data and keep the information on the users' devices.

Ass Prof. Dr.
David Sehnálek

Ass Prof. Dr. David Sehnálek

Interpretation of the Right to Privacy in Relation to the Possibility of Using Secretly Made Recordings as Evidence in Court Proceedings

The “conflict” between the possibilities that offers the digital technology and the right to privacy is particularly relevant in the area of evidence in court proceedings. According to both Czech Criminal Procedure Act and Civil Procedure Act, evidence can be anything, thus also audio or visual recordings. Their advantage is that they are able to provide a range of data not only the image or sound itself but also location, time atc.) and reliably prove a certain fact. It would therefore be a pity not to take advantage of the possibilities offered by modern technology.

Nevertheless, from a privacy perspective, situations where recordings are made without the knowledge of the person being recorded are problematic. However, it is precisely such recordings that can be of the highest probative value and sometimes, they are also the only direct evidence a court has.

Both the Czech Civil and Criminal law do allow, under certain circumstance, the use of such recordings. The contribution will explore conditions, as well as limits of such use. Particular attention will be dedicate also to the use of evidence, that was provided by a private person originally in his or her favor, but later was used against him/her.

Organizational team

Agata Wróbel

M. Sc. Bartłomiej Oręziak