INSTITUTE OF CRIMINOLOGY
at the Faculty of law Ljubljana

BIG DATA:
NEW CHALLENGES FOR LAW AND ETHICS

International scientific conference

22 - 23 May 2017

Faculty of Law, University of Ljubljana

Poljanski nasip 2, Ljubljana, Slovenia

FACULTAS IURIDICA UNIVERSITAS LABACENSIS
Pravna fakulteta
Univerza v Ljubljani

Slovenian
Research
Agency

Table of Contents

About the Conference

“Big Data” is a phrase that has been used pervasively by the media and the lay public in the last several years. Amongst many other fields, social control and crime control in particular have become one of the key emerging use cases of big data. For example, police predictive software produce probability reports on criminality and assure us that by using this, societies will reduce crime. Other programs are looking for patterns that would help us predict a terrorist attack. Criminal justice systems are using technological solution too, for instance, to predict future crimes of those applying for bail or those to be sent on a parole. Underlying these and many other potential uses of big data in crime control, however, are a series of legal and ethical challenges relating to, among other things to privacy, discrimination, and presumption of innocence.

The leading questions the conference speaker will tackle are:

- how the operations of society, political systems, and, in particular, social control and crime control, is changing due to large data bases and algorithmic data mining and predicting powers?
- Will computers decide who to prosecute and who should be sent to jail?
- Which programmes and systems of algorithmic predictions are already in place in the criminal justice systems around the globe?
- Why this can be dangerous in terms of fundamental human rights and fundamental principles of democratic societies?
- Is the new GDPR a suitable framework for »algocracy«, i.e. rule by the algorithm?
- How can we propose solutions that may not hinder the development of the technology, but enable more nuanced, ethically and legally sound solutions to be developed in the future?

We invite paper proposals from scholars across the ***social sciences*** and ***humanities*** studying big data challenges for law and ethics.

Themes of interest include (tentative list):

- big data and crime control
- predictive policing
- automated justice
- big data and discrimination
- big data and social sorting
- ethical dilemmas and predictive analytics
- big data and international law
- big data and personal data protection law
- big data and cyber espionage
- big data and citizen empowerment

Keynote speakers

- Dean Wilson, University of Sussex, Brighton, UK
- Nadya Purtova, TILT, Tilburg University, The Netherlands
- Joanna J. Bryson, University of Bath, UK, and affil. at The Center for Information Technology Policy, Princeton University, USA
- Marko Grobelnik, Jozef Stefan Institute, Slovenia
- Tjerk Timan, TILT/ University of Tilburg
- Alexander Czadilek, Christof Tschohl and Walter Hötzendorfer, epicenter.works, Research Institute Vienna
- Renata Salecl, Institute of Criminology at the Faculty of Law, Slovenia
- Aleš Završnik, Institute of Criminology at the Faculty of Law, Slovenia

Dean Wilson was a lecturer and then senior lecturer in criminology at Monash University, Melbourne, Australia between 2003 and 2010 and a Reader in Criminology at the University of Plymouth prior to joining the University of Sussex in 2015, where he is Professor of Criminology in the Department of Sociology, School of Law, Politics and Sociology. Dean's key research interests are in surveillance and policing, and he has published widely in the areas of histories of urban policing, contemporary policing, surveillance and most recently pre-emption and criminal justice. His most recent publication (with Jude McCulloch*) Pre-Crime: Pre-emption, precaution and the future* was published by Routledge in 2016. Dean is also Co-Director of the international Surveillance Studies Network, and an Associate Editor of the journal *Surveillance & Society*.

Nadya Purtova is an Assistant Professor at Tilburg Institute for Law, Technology, and Society, Tilburg University, where she does research on data protection and informational privacy law, property rights in personal data and economic analysis of data protection law. Nadya obtained her PhD in law (cum laude) in 2011 from Tilburg University. Her dissertation on property rights in personal data (Tilburg University Best Doctoral Dissertation Award for 2010/11) is published by Kluwer Law International. In 2016 she was awarded the European Research Council (ERC) Starting Grant to conduct a five-year research project aimed to reconfigure legal protection of people against information-induced harms based on better understanding of information rooted in law, economics, and information studies (ERC-2016-StG-716971 INFO-LEG).

Joanna J. Bryson is a transdisciplinary researcher on the structure and dynamics of human- and animal-like intelligence. Her research covers topics ranging from artificial intelligence, through autonomy and robot ethics, and on to human cooperation. Bryson's first degree is in Behavioural Science (non-clinical psychology) from Chicago (1986), she also holds an MSc in Artificial Intelligence and an MPhil in Psychology from Edinburgh (1992, 2000) and a PhD in Artificial Intelligence from MIT (2001).

Bryson joined Bath in 2002 in their Department of Computer Science, where she was promoted to Reader (tenured associate professor) in 2010. She founded and for several years lead their Intelligent Systems research group, and is affiliated with Bath's Institutes for Policy Research and Mathematical Innovation, as well as their Centres for Networks and Collective Behaviour and for Digital Entertainment. She has held visiting academic positions with Princeton's Center for Information Technology Policy (where she is still affiliated), the Mannheim Centre for Social Science Research (MZES, 2011-2014), the Department of Anthropology Oxford (Harvey Whitehouse's Explaining Religion project, 2010-2011), The Methods & Data Institute at Nottingham (agent-based modelling in political science 2007-2008), and the Konrad Lorenz Institute for Evolution & Cognition Research in Austria (on the biological origins of culture, 2007- 2009). Before coming to Bath, she conducted academic research in Edinburgh's Human Communication Research Centre (1999-2000), and Harvard's Department of Psychology (2001-2002). Additionally, she has professional experience in Chicago's financial industry (1986-1991), international organization management consultancy (1993-1994), and industrial AI research (for LEGO, 1995, 1998).

Bryson has served on the Senate, Council, and Court for the University of Bath, representing the Academic Assembly. She is presently a member of the College of the British Engineering and Physical Sciences Research Council (EPSRC) and serves as a member of the editorial board for several academic journals, including Adaptive Behaviour, AI & Society, Connection Science, and The International Journal of Synthetic Emotions.

Marko Grobelnik is a researcher in the field of Artificial Intelligence (AI). Focused areas of expertise are Machine Learning, Data/Text/Web Mining, Network Analysis, Semantic Technologies, Deep Text Understanding, and Data Visualization. Marko co-leads Artificial Intelligence Lab at Jozef Stefan Institute and is the CEO of Quintelligence.com specialized in solving complex AI problems for the commercial world. He collaborates with major European academic institutions and major industries such as Bloomberg, British Telecom, European Commission, Microsoft Research, New York Times. Marko is co-author of several books, co-founder of several start-ups and is/was involved into over 50 EU funded research projects on various fields of Artificial Intelligence. In 2016 Marko became Digital Champion of Slovenia at European Commission.

Tjerk Timan is a postdoc researcher on surveillance and privacy in the VICI project of prof. Bert-Jaap Koops at Tilburg Institute for Law, Technology, and Society / University of Tilburg.

Christof Tschohl is ICT engineer and lawyer and serves since 2012 as Scientific Director of the Research Institute – Digital Human Rights Center in Vienna. He is primarily in charge of the development of research projects and publications on Human Rights and Information Technology and has been employed many years as a legal researcher for the Ludwig Boltzmann Institute of Human Rights and as post-doc Project Assistant at the University of Vienna. Mr. Tschohl is furthermore the chairman of epicenter.works, formerly “working party on data retention” (AKVorrat.at). This NGO took action against the comprehensive blanket data retention of traffic data records of all public communication services and successfully conducted a lawsuit, supported by 11.167 people, at the Austrian constitutional court in this case. Together with a preliminary request from Ireland this lead to the abolition of the Data Retention Directive by the European Court of Justice (CJEU) in April 2014.

Walter Hötzendorfer is Senior Researcher and Senior Consultant at the Research Institute, Board Member of the Austrian Computer Society (OCG) and Co-Chair of the OCG Forum Privacy. He has degrees in law as well as in business informatics (information systems) and experience in research, legal counselling and software engineering. From 2011 to 2016 he was a Researcher at the University of Vienna Centre for Computers and Law, where he has worked in several national and international research projects and did a PhD on Data Protection and Privacy by Design in Federated Identity Management. Walter’s research interests span data protection law, privacy by design, privacy engineering, electronic identities, public security, information security, cloud computing, telecommunication and the legal aspects of these and other fields of ICT.

Alexander Czadilek is since 2015 lawyer at epicenter.works (formerly AKVorrat.at) in Vienna, which is, since its successful campaign for the anullment of the data retention directive, commited to the fight against mass surveillance. In addition to this he is a legal reasearcher at Research Institute – Digital Human Rights Center and consultant at ky-center, a think tank for social media law (Vaduz, Vienna, Munich). He deals with data protection law for more than ten years and is author and speaker in the fields of data protection law, privacy and surveillance. He is commited to the preservation of freedom rights and a pluralistic society.

The Research Institute (RI) is a young private research and consulting centre at the cutting point of technology, law and society, which covers questions about human rights in a digital society through a multi- and interdisciplinary perspective. This covers technological and legal aspects of data protection and data security as well as technological impact assessment, cybercrime and political strategies.

Renata Salecl is a Slovene philosopher, sociologist and legal theorist. She is a senior researcher at the Institute of Criminology, Faculty of Law at the University of Ljubljana, and holds a professorship at Birkbeck College, University of London. She has been a visiting professor at London School of Economics, lecturing on the topic of emotions and law. Every year she lectures at Benjamin N. Cardozo School of Law (New York), on Psychoanalysis and Law, and she has also been teaching courses on neuroscience and law. From 2012, furthermore, she is visiting professor at the Department of Social Science, Heath and Medicine at King's College London. Her books include: Salecl, R. (2000). *Sexuation*. Durham, North Carolina: Duke University Press; Salecl, R. (2004). *On anxiety*. London New York: Routledge; and Salecl, R. (2010). *Choice*. London: Profile. The books have been translated into thirteen languages.

Aleš Završnik, Doctor of Law (LL.D.), is a Senior Research Fellow at the Institute of Criminology at the Faculty of Law in Ljubljana and Associate Professor at the Faculty of Law University of Ljubljana. He was a postdoctoral fellow at the University of Oslo (2012) and at the Max-Planck-Institute für ausländisches und internationals Strafrecht, Freiburg i. Br. (2009), and is starting with Visiting Fellowship at the Collegium Helveticum Zürich, a joint initiative of the ETH Zürich and the University of Zürich (2017-18). He collaborated in several European Cooperation in Science and Technology (COST) Actions, e.g. *Living in Surveillance Societies*. In his latest research Završnik focused on surveillance implications of drones in the book he edited *Drones and Unmanned Aerial systems: Legal and Social Implications for Security and Surveillance*. He also co-edited a book *Crime and Transition in Central and Eastern Europe* that was awarded for the best scientific achievement in criminology by the Slovenian Research Agency in 2012. He has extensively researched and published on cybercrime, IT-law, surveillance, crime control and technology. Završnik conducts ethical analysis for security and ICT projects, e.g. he is an independent Ethics Expert with REA, the research arm of the European Commission, for Horizon 2020 projects. Among others, he led a research project *Law in the Age of Big Data: Regulating Privacy, Transparency, Secrecy and Other Competing Values in the 21st Century* (funded by the Slovenian Research Agency, No. J5-6823). E-mail: ales.zavrsnik@pf.uni-lj.si.

Contact Information and Registration

The conference is organized within the research project »Law in the age of big data: Regulating privacy, transparency, secrecy and other competing values in the 21st century« carried out at the Institute of Criminology at the Faculty of Law Ljubljana and Faculty of Law University of Ljubljana, and coordinated by Assoc. Professor Aleš Završnik. It is funded by the Slovenian Research Agency.

Venue
Faculty of Law, University of Ljubljana,
Poljanski nasip 2, SI-1000 Ljubljana, Slovenia

Chair of the Program Committee

Aleš Završnik, LL.D., Assoc. Professor

Program Committee

- Professor Frank Pasquale, University of Maryland, Baltimore, USA
- Professor Renata Salecl, Institute of Criminology at the Faculty of Law, Slovenia
- Professor Katja Šugman Stubbs, Faculty of Law, University of Ljubljana, Slovenia
- Associate Professor Primož Gorkič, Faculty of Law, University of Ljubljana, Slovenia

Organising Committee

- mag. Maruša Veber
- mag. Maša Kovič-Dine
- dr. Mojca M. Plesničar
- Katja Simončič, Junior Researcher
- Miha Hafner, Junior Researcher
- Lara Brecelj
- Klara Cvar
- Maša Gril
- Neja Domnik

Contact
Aleš Završnik, LL.D., Assist. Prof., E: ales.zavrsnik@pf.uni-lj.si
Institute of Criminology at the Faculty of Law Ljubljana, E: inst.crim@pf.uni-lj.si phone: +386 (0) 1 4203 242

Conference fees
Participants of the conference, i.e. speakers and delegates not presenting a paper, have to pay a conference fee; unless invited or students (in the latter case, please provide proof).

The following conference fees apply:

- full pass - speakers: 100 EUR
- full pass - delegates (not presenting a paper): 70 EUR
- full pass - VIPs (invited, upon an appointment): FREE
- students: free of charge *(proof must be provided)*
- Early bird (until April 22, 2017): 75 EUR for speakers; 40 EUR for delegates.

Delegates and students can register via e-mail: inst.crim@pf.uni-lj.si

Please pay by bank transfer to IBAN: SI56 0201 4025 3359 987, SWIFT/BIC: LJBASI2X (Nova ljubljanska banka d.d., Trg republike 2, 1520 Ljubljana, Slovenija). Account holder: *Institute of Criminology at the Faculty of Law Ljubljana*, Poljanski nasip 2, 1000 Ljubljana, Slovenia. You agree that your personal data will be collected and processed for the conference purposes. The bank transfer is the only payment method available. At the conference, you must provide the proof of payment.

Programme

MONDAY 22nd MAY

Hour		Lecture hall
8:30 – 9:00	**REGISTRATION**	**Gold**

Hour	INTRODUCITON AND WELCOME	Lecture hall
9:00 – 9:30	**Prof. Matjaž Jager,** Director of the Institute of Criminology at the Faculty of Law **Prof. Miha Juhart,** Dean of the Faculty of Law, University of Ljubljana	**Gold**
	Keynote session 1 Chair: Aleš Završnik	
9:30 – 11:00	Marko Grobelnik: **Limits of the current state of Artificial Intelligence for Law** Dean Wilson: **Algorithmic Patrol: The Futures of Predictive Policing**	**Gold**
11:00 – 11:30	Coffee break	
11:30 – 13:00	Keynote session 2 Chair: Aleš Završnik	
	Nadya Purtova: **Personal data for common good: how to profit from Big Data sustainably** Alexander Czadilek, Christof Tschohl and Walter Hötzendorfer: **We don't know what the Questions are, but we know we're gonna find the Answers**	**Gold**
13:00 – 14:00	Lunch	

MONDAY 22nd MAY

BIG DATA AND PERSONAL DATA PROTECTION

BIG DATA AND CRIMINAL PROCEDURE

Hour	Session 1 Seminar room 4 Chair: Mojca M. Plesničar
14:00 – 15:30	1. Helena Uršič: **Individual control over personal data in the data-driven economy** 2. Lilian Edwards and Michael Veale: **Slave to the Algo-rhythm? Legal and technological sticking points concerning machine learning and the GDPR** 3. Wenlong Li: **Big Data, Data Protection and Citizen Empowerment** 4. Maša Galič: **Living labs and big data in practice: Stratumseind 2.0 - A discussion of a living lab in the Netherlands**

Session 2 Seminar room 5 Chair: Katja Simončič
1. Sabina Zgaga: **Slovenian criminal intelligence activity and protection of privacy** 2. Primož Gorkič: **Judicial oversight of (mass) collecting and processing of personal data** 3. Carolina Are: **How Are the Australian Metadata Laws Affecting the Average Social Media User?** 4. Begüm Bulak Uygu: **Databases and Due Process with regard to European Court of Human Rights' Case-Law**

15:30 – 16:00	Coffee break

HUMAN RIGHTS, CRIMINAL JUSTICE AND BIG DATA

Hour	Session 3 Seminar room 4 Chair: Primož Gorkič
16:00 – 17:30	1. Sorina Ioana Doroga: **Protecting Individual Rights With Basic Tools in the High-Tech Era** 2. Mojca M. Plesničar: **The alluring promise of objectivity: Big data in criminal justice** 3. Gavin Robinson: **(Anti)Discrimination and Big Data Consumer Credit Risk Analysis** 4. Uwe Ewald: **Big Data in Criminal Justice – Few Chances and Serious Risks**

BIG DATA POLICING

Session 4 Seminar room 5 Chair: Miha Hafner
1. Gregor Urbas: **Automated Cybercrime Investigations: The example of "Sweetie 2.0"** 2. Stanislaw Tosza: **Cross-border exchange of big data - innovative technology meets outdated legal framework** 3. Federico Costantini: **Social network, social profiling, predictive policing. Current Issues and future perspectives** 4. Lydia Morgan: **Reconfiguring freedom: Big data, the Investigatory Powers Act 2016 and the construction of liberty in the UK's security state**

Hour		
17:30 –	**WELCOME RECEPTION – FACULTY OF LAW**	**Main Hall**

TUESDAY 23rd MAY

Hour		Lecture hall
8:30 – 9:00	**REGISTRATION**	**Red**

Hour	Keynote session 3 Chair: Mojca M. Plesničar	Lecture hall
9:00 – 10:30	Joanna J. Bryson: **Five Reasons Not to Personify AI** Renata Salecl: **Big Data – Big Ignorance**	**Red**
10:30 – 11:00	Coffee break	
11:00 – 12:30	Keynote session 4 Chair: Mojca M. Plesničar	Lecture hall
	Tjerk Timan: **“But I used quotation marks”: data science methods and misinterpretations** Aleš Završnik: **Algorithmic prediction in crime control**	**Red**
12:30 – 13:30	Lunch	

TUESDAY 23rd MAY

BIG DATA KNOWLEDGE

Hour	Session 5 Seminar room 4 Chair: Miha Hafner
13:30 – 15:00	1. Michael Veale: **How do public sector values get into public sector machine learning systems, if at all?** 2. Matej Kovačič, Aljaž Košmerlj: **Anonymisation of judicial decisions with machine learning** 3. Janez Štebe, Sonja Bezjak, Irena Bolko and Ana Slavec**: Personal Data Protection in Social Sciences in Big Data Era** 4. Gašper Fele-Žorž, Andrej Brodnik: **Hiding large amounts of data in virtual disk images**

BIG CYBER DATA AND INTERNATIONAL LAW

Session 6 Seminar room 5 Chair: Katja Simončič
1. Vasilka Sancin: **State's Due Diligence in Cyberspace in the Era of Big Data** 2. Mitko Bogdanoski and Metodi Hadji-Janev: **Finding the right balance between security and privacy: NATO and the big data analyses** 3. Maruša T. Veber: **Big Data and Economic Cyber Espionage: an International Law Perspective** 4. Maša Kovič Dine: **Economic Cyber Espionage and Regulation of Big Data Theft at the International Level**

15:00 – 15:30	Coffee break

SOCIAL, ECONOMIC & HEALTH ASPECTS OF BIG DATA

Hour	Session 7 Red lecture hall Chair: Maruša T. Veber
15:30 – 17:00	**1.** Zoran Kanduč: **Dispensable humans and indispensable machines in the context of class and social control** **2.** Gianclaudio Malgieri**: Pricing (big) data: the right to know the value of our own personal data** **3.** Friderik Klampfer, Bojan Musil, Nenad Čuš Babič and Domen Bajde: **Big Data, Psychodiagnostics and Threats to Personal Autonomy** **4.** Tjaša Zapušek: **Healthcare Robots and the Right to Privacy**

Hour	Red lecture hall Chair: Aleš Završnik
17.00-17.15	**CONCLUDING REMARKS**

***** Changes to the program can be made in the run-up to the conference. All the changes will be displayed in the program published on the conference web page. The organizers shall not be liable for any loss, liability, damage or expenses suffered or incurred by any person due to the changes.

Abstracts

"But I used quotation marks" - data science methods and misinterpretations

Tjerk Timan
TILT/ University of Tilburg

Whereas Big Data in itself is a debatable term (for computer science it means data that is too large to compute by a single machine, where for social science it means data is too large to analyze by one human researcher), it is also a decontextualized one, and therefor it leads to many hyped and confusing promises in society. Questions rise about big data by whom and for whom. As STS researchers, we have to ask what kind of impact BD has, or can have, on society, but also what kind of reflection BD is giving of society. Where the natural sciences have already adapted to a computational and often quantitative way of working, many social sciences are now confronted with not only a stronger focus on quantitative methods of working (also more and more as the sole accepted method of working!), but also have to deal with larger heaps of data.

In an extreme scenario, the promise of real-life data means the end of social science (one can analyze “everything” realtime with real data). However, many disciplines in social science and therefor many types of knowledge are still inductive (not deductive). While machines can make data into other forms of data and possibly even can translate data into forms of information, this information still needs humans and contexts in order to produce some form of an added value. In that sense, this new possible real-time quantitative turn is nothing new; its just more. This also means that if social science want to remain relevant, it needs to be able to counter purely quantitative claims and understand a thing or two about data science methods. One way of doing so is to create new alliances - where before it was math and stats, now its data scientist and programmers - and get into some data science methods and tills themselves (yes, this also holds for lawyers!).

In this talk I will briefly go into some theoretical assumptions on Big Data / data science and via data science practices and examples, I will show how misinterpretation and decontextualisation of data lead to non-sensical analysis and strange representations of people via skewed data doubles. I will conclude by attempting a make connection between technical and legal understandings of what personal data can be.

(Anti)Discrimination and Big Data Consumer Credit Risk Analysis

Gavin Robinson
University of Luxembourg

Recent UK legislation facilitating the credit scoring of SMEs using Big Data techniques and Open Data sources threatens to hollow out information management norms and data subject rights enshrined in privacy and data protection law just as it is gathering unprecedented momentum in courts and, with the impending application of the General Data Protection Regulation, in practice across the EU. At the national level, and however Brexit may pan out, it is doubtful that the regulatory re-shuffling and privacy-related safeguards bundled into the legislative stimulus for SME credit risk scoring are likely to address adequately the serious accuracy, transparency and accountability concerns of individual data subjects whose life chances it alters. Would the effective, full enforcement of data protection principles and data subject rights really cripple the credit reference industry to the detriment of the nascent economic recovery, or is there a middle path and will the GDPR provide it?

This paper proposes to tackle a particularly thorny aspect of that debate: the relationship between credit risk analysis and antidiscrimination. It begins by surveying the cutting-edge of consumer credit risk tools, products for which “all data is credit data”: their sources, processes and (unforeseen) impacts on citizens. The latter, oft-neglected aspect is then unpacked with the emphasis placed on the compatibility of such tools with the letter and the spirit of antidiscrimination laws on the books in the US and the EU. This in turn implies a review of the recent, abundant (mainly US) literature on discrimination in the “scored society” (Zarsky), “black boxes” (Pasquale) and disparate impact (Barocas & Selbst), but also of its far scarcer European counterpart – and this in the light of EU-level antidiscrimination norms (e.g. Article 21, Charter of Fundamental Rights of the European Union). Is ever-more-granular Big Data-powered credit risk analysis at all compatible with such values? What might be the impact of the GDPR in this regard? How ought its much-vaunted provisions on profiling be interpreted in order to increase the transparency of credit scorers vis-à-vis the scored – and how are they likely to be interpreted?

Algorithmic Patrol: The Futures of Predictive Policing

Dean Wilson
University of Sussex

‘Predictive Policing’ has emerged as the key buzz term of contemporary policing. Engaging predictive analytics drawn from such diverse domains as disaster prediction, combat situations and supply-chain management, predictive policing extends the promise of anticipating crime prior to its actualization. Marketing materials are replete with strident claims of future crimes that are calculable, knowable and targetable before they transpire. Additionally, predictive policing is promoted as the ideal policing technology for a climate of fiscal austerity, with the capacity to direct police operations in a cost-effective fashion – removing the necessity for ‘costly’ measures such as community engagement. This chapter interrogates the claims of predictive policing, contextualizing them against the longer trajectory of information technology within police organizations. Predictive policing also emerges within a context of security commodification where astute marketing has advanced the view that future criminal acts – and persons – can be rendered visible and actionable in the present. In common with the central tenets of dataism, there is also an underlying logic that predictions will be rendered evermore precise through the accumulation and integration of an ever-expanding array of data sets. While acknowledging that the outcomes of predictive policing are likely to be highly contingent, both organizationally and geographically, it is argued that it represents a potentially disturbing trend in contemporary policing. The limited evaluation evidence to date suggests an elective affinity between predictive policing and the ‘criminologies of everyday life’ such as rational choice and routine activities theory, that privilege asocial technical solutions. The integration of SOCMINT (Social Media Intelligence) also presages forms of algorithmically guided ‘real-time’ anticipatory policing – the consequences of which remain uncertain. Nevertheless, it is argued that patterns of discriminatory policing and their attendant militaristic logics may well escalate, while simultaneously remaining obscured beneath the sheen of algorithmic calculation.

Algorithmic prediction in crime control

Aleš Završnik
Institute of Criminology at the Faculty of Law

The paper will present several existent uses of big data in the criminal justice system, for example, for the prevention of payment card fraud by means of skimming; for the prediction of crime with predictive software; the use of algorithms to predict the recidivism of parolees. Such knowledge, built on a large amount of seemingly unrelated data, whose credibility is based on complex mathematical algorithms, may legitimise increased social control, limit privacy and undermine the basic principles of criminal procedure. Taking into consideration the benefits of algorithmic service, the paper will claim that our society will have to find a balance between the benefits of using big data and the disturbing effects it may pose for society (e.g. abuse through data fishing, loss and theft of personal data, etc.). It will present the pitfalls of reliance on big data predictions used by law enforcement and criminal justice agencies and the risks big data carries as regards encroachment on fundamental liberties.

Anonymisation of judicial decisions with machine learning

Matej Kovačič, Aljaž Košmerlj
Jozef Stefan Institute

Slovenian Constitution determines that court proceedings are public. This means that court hearings (except when there are some special reasons, for instance involved minors, government secrets, etc.) shall be public, and judgments shall be pronounced publicly. Therefore public has the right to know the decisions of judiciary branch of power. However, publishing court decisions is also believed to create a push towards unification of jurisprudence.

These are main reasons why Slovenian ministry of justice wants to publish all court decisions on the Internet. However, Slovenian Constitution also protects personal data, so court decisions should be published on the Internet in anonymous form.

Before public release, all personal data or other data from which persons involved in trial could be identified, should be removed from court decision

In a presentation we will present a tool Tacita, which helps in this anonymisation process. Tool was developed at Jožef Stefan Institute and uses machine learning to predict which part of a court decision should be removed (anonymised) with a high probability. Tacita is not working completely automatic, but helps in otherwise time-consuming manual process of anonymisation. We will also show how the tool has been developed and which tools for analyzing natural language has been used.

Automated Cybercrime Investigations: The example of "Sweetie 2.0"

Gregor Urbas
University of Canberra

Dutch non-government organisation Terre des Hommes in 2013 identified over a thousand predators seeking to engage in Webcam Child Sex Tourism from some 65 countries over a period of about 10 weeks. These were among 20,000 requests directed to a fictitious 10-year-old Filipina girl, really a 3-D avatar called "Sweetie", operated by a team of Terre des Hommes researchers. Numerous referrals to police and prosecutions followed, the first resulting conviction being that of an Australian citizen in 2014. A more sophisticated and automated version of the virtual girl, "Sweetie 2.0", now operates independently as a chatbot with enhanced detection functionality to recognise indecent online behaviour and chat characteristics associated with individuals, which can be stored and analysed for matching with chat records held or obtained by law enforcement or third parties. These developments illustrate the expanding scope for automated detection of cybercrime, including online child exploitation that might be an important element of future policing. However, most legal systems are not yet ready for automated surveillance devices such as "Sweetie" to be used by law enforcement, with open questions about the legality of their use and the admissibility of evidence thereby obtained. The presentation discusses the findings of the 2016 report entitled 'Legal Aspects of Sweetie 2.0' commissioned by Terre des Hommes comparing the laws of nearly twenty countries, against the substantive and procedural frameworks of their domestic legal systems as well as key international agreements such as the Council of Europe's Convention on Cybercrime and the Lanzarote Convention.

Big Data – Big Ignorance

Renata Salecl
Institute of Criminology at the Faculty of Law

In today's society, people are monitoring and collecting data related to themselves. As people with the help of various applications dutifully record their daily lives, they allow companies to use their data for marketing and surveillance purposes. The paper first looks at the psychological mechanisms that are behind the desire for self-monitoring. Second, it looks at the way corporations exploit these desires. And third, it addresses the question of why people often ignore the fact that data that is collected about their lives can easily be used to their disadvantage.

Big Data and Economic Cyber Espionage: an International Law Perspective

Maruša T. Veber
Faculty of Law, University of Ljubljana

The value and power of economic big data is increasingly being recognised as an important asset of States in their endeavours at the competitive and globalised economic markets. Against this background various methods to gather massive amounts of secret, publicly unavailable economic information of third States are being used. In this respect, cyber space has become an ultimate tool enabling relatively easy, sophisticated and quick access to large amounts of confidential information, essential for the performance and operation of businesses and economic stability of States. This presentation will focus on economic cyber espionage among States and assesses the legality of such activities under international law. It will provide a general overview of three relevant international legal frameworks governing economic cyber espionage: bilateral agreements between States, general international law rules on non-intervention and trade policy tools. It will argue that economically motivated cyber espionage activities by States and their status under international law should be differentiated from other forms of traditional espionage conducted for military, strategic and security reasons. While the legality of traditional espionage activities at the international level remain uncertain, we are witnessing important legal developments in the area of economic cyber espionage.

Big Data in Criminal Justice – Few Chances and Serious Risks

Uwe Ewald
Ruhr-Universität Bochum in Germany

Starting from the Foucauldian concept of the “regime of truth” in criminal justice this paper will present findings of a case study analyzing a complex organized crime case in Germany were huge amounts of digital data have been introduced into evidence. As findings show Big Data Evidence (BDE) are about to alter the traditional way professionals in law enforcement and criminal justice act in the evidentiary process.

First, some light will be shed on the BDE challenges for the investigation and analysis of serious criminal cases and possible shortcomings of training and practice of crime analysts in, e.g., Computer-Aided Qualitative Data Analysis (CAQDAS) to reliably assess the probative value.

Second, the new situation for lawyers at trial will be considered. Most current lawyers (in Germany) have a blind spot when it comes to empirical analysis of digital evidentiary mass data retrieved from ICT-devices or collected by means of electronic surveillance. There is in particular no clear understanding regarding the way how information is produced from these digital data, eventually forming evidentiary knowledge and needed to apply substantive law in a credible manner.

Third, serious risks will be discussed which arise in light of BDE from the mismatch of criminal procedural frameworks and practical requirements in the analysis by legal experts. Moreover, BDE tends to create what data science calls “ambient intelligence” which jeopardizes basic principles of modern criminal law such as “presumption of innocence”, “equality of arms” or “public trial” – if not handled properly at the levels of legal education, judicial practice and law-making.

Finally, some suggestions should be offered on how to conceptualize truth-finding and BDE and how to limit the risks for a fundamental human rights and rule of law centered approach in criminal justice.

Big Data, Data Protection and Citizen Empowerment: The Revival of Individual Participation Principle as a Response to New Technological Challenges

Wenlong Li
The University of Edinburgh

The individual’s participation in protecting personal data was greatly respected and considered a major principle while modern data protection rules were taking shape in the 1980s. During the following decades, however, the principle has been largely underutilised for the reason that individuals oftentimes find it difficult to get involved in such undertaking. This has been further deteriorated when big data analytics formulate an unpredictable data dynamic that creates a wide range of economic, cognitive and operational obstacles for individuals to stay relevant.

This paper attempts to examine to what extent can data protection law accommodate and achieve the idea of ‘citizen empowerment’ and focuses on the role of an individual in minimising the risks and harms of big data analytics. It principally looks at the legislative efforts in the EU reform of data protection law, aside from the emergence of decentralised technologies that assist individuals in fully controlling their personal data.

The paper begins by tracing back to the foundation of data protection law – the OCED Privacy Framework. It takes the individual participation principle it creates as an entry point and examines its compatibility with the idea of citizen empowerment. Particularly, the paper argues the importance of individual checks among a majority of paternalistic and corporate-centric rules and explores the legal basis for achieving citizen empowerment and user-centric rules in the context of data protection. Further, it examines the flexibility of individual participation principle in the era of big data and looks at the European approach to user control, taking the newly created right to data portability as a case study. Notably, this right is considered a critical step to formulate a new dynamic featuring ‘individual centricity’, thus enabling individuals to take advantage of personal data for their own good and ultimately share the enormous benefits of big data.

Big Data, Psychodiagnostics and Threats to Personal Autonomy

Friderik Klampfer, Bojan Musil, Nenad Čuš Babič and Domen Bajde
University of Maribor

Experts and institutions have warned of the threat that big data analysis poses to our right to privacy, the challenge it raises to our traditional notions of criminal responsibility and justice, as well as concerns about the rising levels of invisible and unaccountable social control (EDPS 2015). And yet, surprisingly little has been written so far about its damaging potential for our personal autonomy as consumers and citizens. This is even more surprising given the psychodiagnostic research that has been conducted and developed in recent years (Kosinski et al 2013, Youyou et al 2015, Park et al 2015, Musil et al 2017), which is also being aggressively marketed to, and used by, economic and political stakeholders as well as political parties and organizations, as a powerful tool of non-rational persuasion.

In the paper, we first provide an overview and an assessment of those psychodiagnostic and psychoprognostic computing tools that are currently making headlines. We try to dispel the fog of self-promotion and spin to see its real, not merely imagined or hyped-up, diagnostic potential. How accurate are “psychograms” based on an analysis of people’s seemingly innocuous online activities? Is there any substance to the claim that computer algorithms can know us better than we know ourselves? Next, we assess the bold promises that the knowledge of a variety of psycho-social facts about individual users of ICT enables us to match every particular message to a particular addressee’s emotions, needs, and preferences to an extent that was unimaginable a decade ago. Can we really, by means of this new technology, manipulate people’s minds, choices and behavior much more efficiently than ever before? And what implications does this have for our self-understanding as rational and autonomous beings, not to mention the elevated moral standing that comes with it?

Manipulation is one of the most familiar but also increasingly common threats to personal autonomy, which in turn is widely considered as worthy of, and even commanding, (almost) unconditional respect. Accordingly, every charge of manipulation needs to be taken seriously from the moral point of view. But does targeted, individualized commercial and political online advertising amount to vicious, morally problematic manipulation at all? In order to answer this, we provide a tentative definition of manipulative, as opposed to non-manipulative, attitudinal and behavioral influence. We then show targeted advertising exploitative of Internet users’ identified cognitive shortcomings and emotional vulnerabilities manipulative. We lament the commercialization of politics and offer an explanation of what renders manipulation of citizens’ choices particularly problematic, even compared to daily tampering with our consumerist choices.

Finally, for the purpose of policy recommendations, we envision three future scenarios: (a) pessimistic, (b) optimistic, and (c) balanced, arguing that while self-regulation and an opt-out option of data sharing may be sufficient for the second and the third, the onset of the first would require the passing of restrictive data-protection legislation if we are to preserve our core democratic values and institutions.

Big health data on social networking platforms: The legal and ethical questions

Maria Tzanou
Keele University

This contribution seeks to explore the legal and ethical questions that arise from the use of personal health data in online social media. Health data, which refers to information concerning an individual’s health or disability can be exchanged in a number of different ways in social media: i) through specific health-related networking platforms, such as Patientslikeme; ii) through general networking platforms, such as Facebook and Twitter; and, iii) through health and fitness applications, such as wearable devices, which collect data about the bodily functioning, including eating, sleeping, and other activity habits of the individual and can be integrated with social media and share this information in order to showcase the user’s personal performance statistics. Sharing of health data in social media raises major ethical and legal questions relating to privacy, data protection and personal autonomy and dignity as well as the issue of the surveillance of digital communities. The present contribution aims to investigate these challenges and critically evaluate the possibilities of the currently available legal and regulatory frameworks at the EU and the international level to effectively protect big health data from the widespread surveillance and monitoring of online communities by both government authorities (in order to fight terrorism and serious crime) and the private sector (private insurance companies, companies offering health products or services, marketing and advertising companies).

Cross-border exchange of big data - innovative technology meets outdated legal framework

Stanislaw Tosza
University of Liège

In order to effectively investigate and prosecute criminal offences, law enforcement must have access to digital data, which is mostly in possession of Internet service providers, often located abroad. The law of criminal procedure allows the authorities to access this data, while protecting suspects' procedural safeguards. However, when the service provider is located in another country or the data is stored abroad, law enforcement should in principle resort to mutual legal assistance (MLA) because their coercive powers are limited to their national territory.

MLA procedure is cumbersome and lengthy. In view of its deficiencies, authorities have a tendency to circumvent MLA rules in practice. For instance, they request data directly from the service providers or conduct digital searches in computers systems located abroad (e.g. by means of Trojan horses). The latter option is questionable as it consists in a unilateral, covert access to data on foreign territory. The first method puts at risk the rights of the persons affected. Furthermore, if a service provider refuses to cooperate, the problem arises as to how to enforce the cooperation request.

This conundrum becomes even more complex because of the use of cloud services or encryption. It becomes particularly challenging by the growing tendency and need to use big data by law enforcement. The latter problem has not been comprehensively addressed. This may presumably favour direct cooperation with service providers. Yet, it also requires protection of the rights of affected persons. The aim of this paper is to demonstrate how the technological developments and the needs of law enforcement challenge the existing legal framework and critically analyse from that perspective the solutions currently being discussed within the EU and the US.

Databases and Due Process with regard to European Court of Human Rights' Case-Law

Begüm Bulak Uygun
Yeditepe University

Security concerns are at the forefront of data storage. The increasing use of databases in the criminal procedure raises problems in terms of ensuring the respect and protection of fundamental rights. Databases are in widespread use in the criminal justice field across the world. These instruments have undoubted advantages: databases contribute considerably to the investigation of the crime, ensure rapid intervention at the investigation level, and allow the possibility of making an information exchange between countries. On the other hand, they have undoubtedly an impact on individual privacy. The use of this type of investigative tools creates a need for appropriate regulation for the use and storage of the data collected in order to safeguard the dissemination and access to personal data. Whilst the use of such measures by law enforcement agencies is common, mass surveillance as opposed to targeted surveillance constitutes an interference with the right to privacy and the rights of the defence such as the presumption of innocence. In particular, specific protection is needed to ensure the right protection for the individual's privacy. If the enforcement of the criminal laws requires the preservation of personal information greater awareness is needed of the threat to privacy implicit in the accumulation of vast amounts of personal information in data banks. Clearly, a high level of protection of the personal data of individuals would ensure effective judicial co-operation in criminal matters and police cooperation.

Further to an analysis of the legal framework that applies to the relationship between surveillance and data protection, this paper will try to figure out how to overcome the limits of privacy. While doing so, the main argument will not be just a question of balance between data protection and national security as such. Mass surveillance entails a challenge to core privacy principles for how personal data must be processed in a reasonable, correct and legitimate manner. Given that data retention in the field of telecommunication challenges the very foundations of the rule of law, the focus is instead on a larger scale being the impact of this conflict on due process rights in a democratic society.

This paper suggests an analysis of the recent case-law of the ECtHR on the issue. In particular, the privacy challenges associated with surveillance, primarily within the realm of the criminal justice databases will be highlighted. More specifically, this paper sketches the extent to which data protection laws interacts with the criminal procedural law in order to evaluate the effectiveness of police and judicial cooperation. When assessing the individual's privacy in the area of criminal law, the concern must be the extent to which criminal procedures are constrained by a respect for privacy. One of the basic issues is the admissibility of evidence from law enforcement-related databases.

Dispensable humans and indispensable machines in the context of class and social control

Zoran Kanduč
Institute of Criminology at the Faculty of Law

The paper deals with the use, or rather with the abuse, of (both “smart” and “stupid”) machines as the means controlling (and disciplining) working class (individuals who have to sell their working power to the private or public master in order to get the money they need for living), workers in (formal and informal) work places, consumers and citizens. In particular, we emphasize the role of “labour-saving” technology (as the result of modern science) in the class and imperialist (dubbed as “anti-terrorist”) war (in fine, in the war of the rich against “the rest of the world”), i.e. in the destructive and irrational capitalist economy (functioning as gigantic anonymous “automaton” or, in Marx's words, “automated subject”), and its reproduction and transformation. Obviously, machines can easily substitute humans, because they already function as quasi automata, personifications of specific economic categories and following the dominant type of rationality (“algorithms”) imposed on them by the capitalist social relationships and structures (existing in them in the form of personal dispositions, attitudes, desires, beliefs, and aspirations). Yet, humans – working in private enterprises (tyrannies) or repressive state apparatuses – are problematic because of their “all too human” characteristics, not just emotions, passions or vices (e.g. “laziness” or even allergy to work), but potentiality or actuality of disobedience, i.e. the possibility of saying “No!” to the masters or even to fight against them in order to destroy their economic, political, legal, and ideological (or cultural) power. Machines may have some deficiencies or imperfections, but they have one crucial quality. Namely, they are always obedient to the masters. Moreover, they are the increasingly important reason for fearful and shameful obedience (or even grotesque conformism) of formally and informally employed “voluntary slaves” (or rather “auto-mobiles”), many of whom, nevertheless, manage to find justifiable alibis in joys obtained from commercial goods, e.g. private cars, TV sets, personal computers, mobile phones, or legal and illegal psycho-active substances. Of course, the technology (even in its most advanced, “smart” or “intelligent” forms) is by no means invincible. And what is more, the rich – as the legal, but not legitimate rulers of the world – can be defeated even more easily. They, of course, have a lot of money (with which they can buy humans), but it is not really theirs. It is stolen, albeit legally. And it is or remains theirs primarily because of the state force and omnipresent economic and legal propaganda fulling “enough people enough time”. So the main problem seems to be human stupidity, not as inborn characteristic, but as socially constructed and permanently reproduced. Is it insuperable, so that there is really just one alternative?

Economic Cyber Espionage and Regulation of Big Data Theft at the International Level

Maša Kovič Dine

Faculty of Law, University of Ljubljana

Many governments are resorting to some sort of economic cyber espionage/exploitation for various reasons. With the development of Internet technologies, it has become easier and more inexpensive to carry out data theft. The benefits of such theft include important competitive advantages on the globalised market both for benefiting companies as for the sponsoring States. At the same time, such theft causes serious damage to the targeted company, mostly in the loss of profit and a loss of years of research and development. As the topic is a relatively new issue in international law, few attempts at regulation have been made. Mostly due to the fact that all states resort to some sort of espionage. However, the consequences of the failure to regulate economic cyber-exploitation are serious, rendering a need for its regulation at the international level. Economic cyber-exploitation is characteristically similar to pillage of natural resources. Thus the law on prohibition of pillage could provide a basis for designing the regulation on economic cyber-exploitation and prohibit such activities. Theft is theft, however it is carried out and whatever the information that is stolen. When economic cyber-exploitation is taking place among states, an international response is necessary.

Finding the right balance between security and privacy: NATO and the big data analyses

Mitko Bogdanoski, Metodi Hadji-Janev

Military academy “General Mihailo Apostolski-Skopje”

During its last Chief of transformation conference held in Norfolk in 2016 NATO’s chiefs of transformation have recognized that big data phenomenon has become one of the most promising and prevailing technology to predict future trends. Big data analyses may enable NATO to automatically process and extract valuable insights, predict patterns and enhance decision making. However, put in the context of NATO’s commitment to respect international law big data analyses raise serious concerns with regards to the individual freedoms in general and personal data protection in more specific sense.

The paper will briefly explain how big data analyzes may enhance NATO’s mission accomplishment. It will then evaluate how and why finding the right balance between security and individual freedoms (especially personal data protection) are essential for NATO’s mission accomplishment while employing big data analyses.

Five Reasons Not to Personify AI

Joanna J. Bryson

University of Bath and Center for Information Technology Policy at Princeton University

Artificial Intelligence is often treated as an alien force or an unruly, potentially dangerous child. In fact, AI is just a special case of computation being commodified, which is to say that the means by which AI is changing society are not trivial, but are less transparent than simple opposition. Intelligence is the triggering of appropriate actions in response to perceived events. Information technology has been allowing humans to enhance our capacity to do this arguably for thousands of years. It allows us to both remember and perceive more than we could as individuals, which in turn allows us to innovate at cooperate in unprecedented ways, sometimes at the expense of each other, other groups or the rest of the ecosystem.

In this talk I establish a clear, science-based, functionalist definition of intelligence, and artificial intelligence, demonstrating from this that concerns about artificial general intelligence and superintelligence are misguided, though in different ways. Then I will talk about efforts to regulate AI, with a focus on the British efforts going back six years now with the Principles of Robotics. Finally I will address why we should not

construct AI to be legal or moral agents – not because such construction is impossible, but because it is ill advised and easily avoided, at least for commercial products.

Healthcare Robots and the Right to Privacy

Tjaša Zapušek
University of Copenhagen, Faculty of Law

The paper reveals author's personal conclusions derived from the fact that an increasing autonomy of robots is not a science fiction, yet it presents a notorious feature of modern era that requires a comprehensive and systematic legal approach. However, a European Parliaments' recently issued recommendation to consider robots as electronic persons seems inappropriate from human rights perspective and may reflect in serious violations of fundamental rights attached to all human beings. This article focuses on negative aftermaths of automaton and the impact they have on health law and the right to privacy. The fundamental principle of healthcare ethics, a protection of patient's clinical records presents a cornerstone of doctor-patient confidential relationship. The latter is, due to its importance, protected not only by national health legislations, yet also by Article 8 of the European Convention on Human Rights, Right to privacy. Among the latest medical achievements is the revelation of the alternative to a person in a white coat, a robot that can perform the surgery completely on its own, has individual sessions with autistic persons etc. As already mentioned, medicine is a profession that requires a certain level of maintenance of secrecy of confidential information and according to the previous Court's decisions the secrecy is even more important in cases that involves psychiatric records. The robots' involvement in medical treatments on one hand and easy access to the information they gain during the treatment on the other, bring into question the effectiveness of the provisions of Article 8 of the European Convention on Human Rights. Law allows individuals, pledged to secrecy to bypass the provisions of Article 8(2) of the ECHR. The mentioned paragraph states, that any disclosure must be in accordance with the law and have legitimate purpose, moreover it has to be proportionate in accordance with the law and necessary pursuant to the democratic society.

The presence of robot doctors rises many questions such as, what kind of consequences will have the disclosure by robot doctors? Does it mean that robots are/will be capable of evaluating the importance of particular information and therefore will it possess a moral sense? Or, will a robot, due to its mechanical nature be used as a simple tool in order to gain some important information that have been saved on the its disc?

Current legislations in countries around the world do not put much attention on this particular area, even though the modern robotic approaches have already been introduced and also very well accepted.

Hiding large amounts of data in virtual disk images

Gašper Fele-Žorž, Andrej Brodnik,
Faculty of Computer and Information Science, University of Ljubljana

Over the past few decades, multiple methods for hiding data in on hard drives have been devised. Most of these depend on unallocated space either between or within filesystems.

Since methods for hiding data may also be used by criminals, they are of interest to digital forensic investigators. Tools used by investigators therefore usually support features which can be used to inspect data within places where data may be hidden, such as deleted files, unallocated sectors or alternate data streams.

Widely available virtualization of and on personal computers can be used to support old software which might otherwise not run on modern hardware. Virtualization is also essential in developing low-level software, such as operating systems, and is an essential component of all solutions for cloud computing. Virtualization technologies are therefore widely used and will likely remain popular in the foreseeable future. With virtual computers it is often more convenient to use files as virtual hard drives instead of physical disks. These files are typically large, so data could potentially be hidden within them, depending on the virtual disk image format.

We have analyzed the most popular virtual disk image file formats and devised three general approaches for hiding data within such files. Two of these approaches allow large amounts of data to be hidden. The hidden data is unlikely to be detected by current digital forensics tools. New techniques and procedures will have to be developed to detect such data.

We have implemented one of the approaches which can be used to store practically unlimited amounts of data in a library which is freely available.

How Are the Australian Metadata Laws Affecting the Average Social Media User?

Carolina Are
University of Sydney

This paper analyses the increased surveillance the Australian population has experienced after the terrorist attacks of 9/11. Examining the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 No. 39, 2015, also known as ‘metadata laws’, this research attempts to identify the reasons behind this increased surveillance in the era of Islamic State (ISIS)’s thorough use of social media platforms to incite and recruit new terrorists (Klausen 2015; Stern and Berger 2015). Examining the necessity and proportionality of the laws in accordance with the United Nations’ (UN) Universal Declaration of Human Rights (UDHR) (UN 1948), this paper sets out to establish how the average social media savvy citizen is likely to be affected by this restrictive and conservative turn in the Australian criminal justice and anti-terrorism landscape. It is expected that cracking down on average social network users in order to spot and punish terrorist organisations and their unlawful use of the internet and social media is likely to produce mixed, if not unsuccessful, results.

How do public sector values get into public sector machine learning systems, if at all?

Michael Veale
University College London

More machine learning algorithm–powered decision-support systems are piloted and deployed in the public sector each day to help detect individuals and corporate wrongdoing in areas such as taxation, child protection and policing. While some welcome this trend as the dawn of more evidence-based administrative decision-making, others worry that the opacity and perceived objectivity of such systems usher in unwanted biases through the back door just as they kick due process out.

Studies of these systems have primarily attempted to look-in or reverse-engineer them from the outside, missing the people that obtain, deploy and manage these technologies within diverse institutional contexts. To help fill this gap, 25 public servants and technologists from different sectors and countries involved in public sector machine learning projects were identified and interviewed. They were asked about their experiences with these technologies, focussing on how they understood and approached operational barriers and ethical issues they encountered. Analysis of these interviews shows promising roles for recent technological approaches to responsibility in this field such as ‘fairness-aware’ or interpretable machine learning systems. Yet these interviews also raise questions and issues that are both currently underemphasised and unlikely to be resolved by technical solutions alone. This research suggests that governance mechanisms for applied machine-learning must be more sensitive to on-the-ground pressures and contexts if they are to succeed in ensuring new data-driven decision-support systems are societally beneficial.

Individual control over personal data in the data-driven economy

Helena Uršič
Center for Law and Digital Technologies, Leiden Law School

Control over personal data processing is an integral part of the fundamental right to personal data protection. In the era of big data and growing digital economy, data subject control rights such as the right to erasure and the right to access face important challenges. It is disputable whether new circumstances still allow for meaningful control over personal data processing. To answer this question, the contribution at hand examines legal framework for commercial data use and reuse, paying special regard to the provisions on individual rights. Drawing on this analysis, it will be shown how the meaning of individual rights and their implications have been changing in the light of big data.

Judicial oversight of (mass) collecting and processing of personal data

Primož Gorkič
Faculty of Law, University of Ljubljana

The paper explores different approaches to securing judicial oversight of collecting and processing of personal data in a criminal justice system. It focuses on traffic communication and DNA data. A brief comparative overview show that the need to establish judicial oversight very much corresponds to the manner the right to privacy is conceptualised within a specific jurisdiction. On one side, the US relies heavily on the concept of reasonable expectation of privacy (privacy as secrecy, Solove). On the other side, European jurisdictions - although not uniformly - view privacy protection as an integral part of protecting one's personhood and dignity. The paper explores the clash of the two competing conceptions within US jurisdictions, particularly after the Snowden revelations. In general, the recognition of the need to provide judicial oversight is greater in jurisdictions that view privacy in the context of protecting one's personhood. In this sense, the level of procedural safeguards very much corresponds to the substantive understanding of the right to privacy.

Limits of the current state of Artificial Intelligence for Law

Marko Grobelnik
Jozef Stefan Institute

Artificial Intelligence (AI), despite its recent successes on several fronts, has still serious limitations when it comes to the problems related to the deep understanding the world. Law is an area, where mostly shallow AI probabilistic solutions are not useful. As a consequence, many of the standard routines, where humans are performing well, are still not solvable with the current AI techniques and systems. In the presentation we will touch what are the limits of the current AI and what is the reason for them. Recent successes and popularity of AI is often raising expectations what technology could do – in reality, many of the “impressive” technological solutions are based on shallow effects which machine learning (as a key today’s AI technology) can capture from the big data. But there is a serious problem on how the world and the context is perceived by the technology. We will present a thin line between what AI technology can do and what cannot do based on current developments and where this line can move on the future and how the law can benefit out of it.

Living labs and big data in practice: Stratumseind 2.0 - A discussion of a living lab in the Netherlands

Masa Galic

Tilburg Institute for Law, Technology and Society (Tilburg University)

Living lab projects are becoming common practice in (smart) cities around the world. They represent a platform and methodology for technology testing and experimentation, which relies on big data analysis and increasingly shapes life in the city. As a relatively recent phenomenon, however, they are underresearched, lacking a widely recognised definition and theoretical framework. The proliferation and growing importance of such urban technological projects demands a more thorough analysis and disentanglement of the practice and the concept. In order to address this need, this paper first presents a living lab in practice – the Stratumseind Living Lab (part of the Stratumseind 2.0 project) in Eindhoven, the Netherlands. The Stratumseind Living Lab, a smaller project in a middle-sized and upcoming European city, which includes local and global technology companies, serves as an illustrative example of a European living lab, its operation and its promises. The second part of this paper examines academic literature on living labs and briefly analyzes the operation of the Stratumseind Living Lab project in view of its promises, particularly those pertaining to the ideological rhetoric of big data. Based on the examination of theory and the practical example, the paper concludes that such technological projects carry with them a wide range of social, political, ethical and legal concerns, which the parties of the Stratumseind Living Lab project do not engage with seriously enough. The pace of development and rollout of living lab (and smart city) technologies in Eindhoven and beyond is proceeding well ahead of wider reflection, critique and regulation. Such activity is foolish and dangerous and does not lead to greater effectiveness and legitimacy of the vision.

NATO’s New Challenge: Synchronizing “Dots”, “Bullets” and “Skills”

Mitko Bogdanoski and Metodi Hadji-Janev

Military academy “General Mihailo Apostolski-Skopje”

Employing cyberspace to achieve strategic ends via a hybrid mode of the warfare state and non-state actors threaten NATO like never before. Understanding the evolving complex threat environment on 14 June 2016, NATO’s defense ministers agreed to recognize cyberspace as a domain at the upcoming Warsaw Summit. During the Warsaw Summit as an addition to the existing operational domains of air, sea and land, cyberspace was officially recognized as a new operational domain. Although this decision does not change NATO’s mission or mandate it requires significant diplomatic, economic, operational and informational efforts to synchronize the “dots”, “bullets” and “skills”. There are three reasons for this. First, not all NATO members, not to speak partner nations, have the same cyber capacities. Second, related to former, not all member states have the same perception when it comes to cyber threats. Third reason stems from the operational need.

The article will first explain the security threat landscape that NATO is facing from cyberspace and will provide evidences why NATO and partner nations need to consider cyber threats as a serious national security threat. Then, using the complex system analysis the article will explain the reasons strategic, legal and technical point of view for the main argument i.e. to synchronize the “dots”, “bullets” and “skills”. Particularly, the article will analyze the importance of building cyber defense capacities among the partner nations. Finally the article will provide some recommendation that need to be considered by NATO and partner nations.

Personal data for common good: how to profit from Big Data sustainably

Nadya Purtova

Tilburg Institute for Law, Technology, and Society, Tilburg University

The promises of Big Data Analytics are grand and tempting. Access to the large pools of data, much of which is personal, is said to be vital if the Big Data initiatives are to succeed. The resulting rhetoric is of data sharing. This talk exposes 'the other side' of data sharing which often remains in the dark when the Information Industry and researchers advocate for more relaxed rules of data access and use: namely, the talk frames the issue of personal data use in terms of the commons, a resource shared by a group of appropriators and therefore subject to social dilemmas that have to be addressed if the resource use is to be sustainable. The talk will argue that the uncontrolled use of the data commons will ultimately result in a number of the commons problems, and elaborates on the two problems in particular: disempowerment of the individual vis-à-vis the Information Industry, and the enclosure of data by a few Information Industry actors.

Personal Data Protection in Social Sciences in Big Data Era

Janez Štebe, Sonja Bezjak, Irena Bolko and Ana Slavec

Arhiv družboslovnih podatkov

The development of digital technologies fosters new types of data, research approaches and methodologies as well as significantly increased the amount of data interesting for social sciences. However, it also raises severe legal, ethical and quality issues. The Social Science Data Archives at the University of Ljubljana (Arhiv družboslovnih podatkov - ADP) is involved in the SERISS (Synergies for Europe's research Infrastructure in the Social Sciences), international project that connects leading European research infrastructures. In one of the tasks the ADP together with project partners conducted the literature review on how social media data (Twitter, Facebook, Snapchat, etc.) is already used in social scientific research and how legal and ethical challenges are discussed in the field. Based on 20 years of experience in data curation and preservation we identified questions related to different phases of the research data lifecycle. Since social media data is not created for research purposes, one of the main issues is obtaining participants' informed consent to reuse data. Consent is no longer requested only by research ethics committees, but it will become a requirement with the implementation of the new GDPR. Although social media data is often publicly available, researchers don't have an explicit informed consent to collect and analyse their data nor that can they link it with other sources or reuse it beyond the original purpose of data collection. As a data archive, ADP is particularly interested in finding a legal solution for data to be stored, curated and disseminated in the long term. Several questions arise, from determining data ownership to time limits for data storage and documentation, as well as to enable researchers to link data from different provenance (e.g. official statistics, social media data, historical and health data). The research community needs to recognise the gap between research interests and laws and ethics policies, and find a balance between research freedom and the protection of respondents.

Pricing (big) data: the right to know the value of our own personal data

Gianclaudio Malgieri

Vrije Universiteit Brussel - LSTS research group

The commodification of digital identities is an emerging reality in our Big Data era: personal data of individuals have high value in the data-driven economy and are often considered a counter performance for "free" digital services or for "discounts" in insurances. An effort that can increase awareness and controllership of consumers/users on their own personal information could be making them aware of the "price" of their personal data, so that they can acquire higher awareness about their power in the digital market.

In order to find objective parameters for quantifying data, we propose to combine two methods: a) a top-down approach (the price of personal data “demand”), i.e. the price that companies generally pay for personal data of individuals (turnover from online ads); and a b) bottom-up approach (the price of personal data supply), based on a “reverse liability” paradigm, i.e. measuring the “value” of personal data in terms of damage to privacy or “loss of privacy” and also in terms of increase of consumer asymmetry.

Secondly, it is necessary to find how this “pricing” of personal data can be introduced in the digital market. We propose to add a new specific duty of information at article 13 of the EU General Data Protection Regulation: in each data processing where the value of customers’ personal data is relevant for the economic transaction, the price of these data (calculated on objective parameters) should be communicated to the consumer.

Actually, personal data do not have the same value for each individual. Subjects having a lower propensity to consume and presumably lower incomes have less “valuable” data than other consumers and could have worse contractual conditions.

Accordingly, in order to avoid discrimination based on the value of personal data, we propose to include the propensity to consume and the economic conditions of data subjects within the “special categories of data” at Art. 9 GDPR.

Protecting Individual Rights With Basic Tools in the High-Tech Era

Sorina Ioana Doroga

West University of Timisoara

In the era of ever-expanding digital markets and surprising advancements in technology, it is hardly surprising that law seems, at times, unable to keep up. With the increasing use of big data in a large number of sectors – both in the private, as well as in the governmental sphere – most transactions and operations take place in the absence of the concerned individuals whose data is actually being collected and processed. This raises issues relating not only to the insufficiency (or rather, inadequacy) of big data regulation, but also to the effectiveness of existing mechanisms of legal protection for data subjects. The present paper deals with concerns relating to the protection of individual rights in the context of data processing, by tackling the issues of informed consent, as well as effective remedies available to data subjects under international human rights instruments. While it is acknowledged that specific rules available at national and EU level might prove at times to be insufficiently precise (or flexible, in some cases) so as to offer effective protection of rights such as privacy or freedom of expression of data subjects, we attempt to look back at the core principles under human rights instruments, which could be employed in order to cover existing regulatory gaps. To this end, a comparative analysis of the EU and US case-law concerning the interaction of big data with privacy and expression rights provides a useful tool in identifying the legal standards that could help strike a fair balance between the legitimate interests in the use of data and the protection of individual freedoms. The specificities of the interplay between the right to privacy and the freedom of expression in the European and US legal cultures also create a fertile ground for identifying potential solutions for improving existing data regulations.

Reconfiguring freedom: Big data, the Investigatory Powers Act 2016 and the construction of liberty in the UK’s security state.

Lydia Morgan

University of Birmingham

The UK’s Investigatory Powers Act 2016 puts a number of troubling powers on statutory footing and expands other already existing powers under the guise of legislative rationalisation. One of the principles at its core is a preventative rather than punitive approach terrorism and serious crime supported by the idea of security as

central to the national interest. Big data is gathered by and on behalf of the state and utilised to monitor, predict and prosecute preparatory activities. In so doing, a variety of forms of freedom are curtailed. This paper explores the ways in which this reconfigures the idea of freedom in the 21st century, blending approaches from public law and political theory. It suggests security is now privileged over freedom rather than being sought to pursue it. This unnecessarily restricts even negative liberty and has little recognition of the impact on autonomy and agency.

Slave to the Algo-rhythm? Legal and technological sticking points concerning machine learning and the GDPR

Lilian Edwards and Michael Veale
Strathclyde University, UCL

More machine learning algorithm–powered systems are deployed each day in areas that now include employment, policing, marketing, price discrimination, health intervention, online news curation, tax fraud prediction and child protection. Some welcome this trend of data-driven decision-making and decision-support, while others worry that the opacity and perceived objectivity of such systems usher in unwanted biases through the back door at the same time as they kick due process out. The GDPR offers a range of rights —some new, some simply rehashed — that many hope will help them navigate this new algorithmic governance society in the courts. Yet as this paper will discuss, when considering the GDPR in the context of machine learning using both a legal and a computer science lens these rights do not appear straightforward to understand or implement.

An alleged new "right to an explanation" (art 13)—which has actually existed in similar form in the DPD since 1995 —has both legal and technical caveats. Legally, there has always been a carve out from the right for the protection of trade secrets and intellectual property, which probably explains its lack of historical use in the EU. Recital 63 of the GDPR does however now counsel that this should not justify "a refusal to provide all information to the data subject" [emphasis added].

Providing "meaningful information about the logic" of advanced machine learning models is rarely technically possible. The main techniques proposed today by computer scientists to effectively 'explain' neural networks, their innards black-boxed even to their designers, wrap simpler models optimised for an explanation around more complex ones to estimate core logics: so-called 'pedagogical interpretation'. Yet such simple models are just that—simple—therefore often failing to 'explain' the fringe cases that are the most likely to lead individuals to call upon their GDPR rights.

The right to not be subject to algorithmic decision-making (art 22) – again not new but extended from an earlier right in the DPD, art 15 – seems promising, but is replete with exemptions and only valid (a) in cases of automated processing producing legal or similar significant effects and (b) where the effect was solely based on automated processing. Machine learning in high-stakes contexts is almost always deployed as decision-support rather than purely automated decision-making and the GDPR lacks the nuances necessary to establish whether a human was seriously 'in-the-loop'.

Similar issues arise around existing rights to a "right to data portability" (art 20) ,deletion and "to be forgotten" (erasure, art 17) with problems also foreseeable given the ongoing debate on when personal data ceases to be so by virtue of anonymization/pseudonymisation. . What right does a data subject have to these in respect of inferred data?

We conclude by asking if we are all condemned to be slaves to the algo-rhythm?

Slovenian criminal intelligence activity and protection of privacy

Sabina Zgaga
Constitutional Court of the Republic of Slovenia

Recently tendency could be noticed that the intelligence powers of not only national intelligence and security agencies, but that of regular police should be empowered, also with intent to gather evidence for subsequent criminal prosecution. This trend could be recognised also in Slovenia. It is connected to data mining, since the police intelligence activity includes the acquisition, assessment and analysis of personal and other data about criminal activity of natural and legal persons and criminal associations according to police legislation. Based on this, the process of decision-making and planning of police activity regarding crime prevention, detection and investigation should be made. In this framework, the Police can gather information from all public sources and with cooperation of persons, who voluntarily give the police operational information about criminal acts, perpetrators and other relevant activities. This increased police intelligence activity of course opens up also numerous legal issues and question. From the viewpoint of compatibility of with Criminal Procedure Act it is also of great significance, when this intelligence activity transforms into criminal procedure, in which stronger encroachments of privacy are allowed, but in which also the status of a suspect carries certain legal protection. And last, but not least; it is essential, whether the police is allowed to use its own - already existing - official records of personal data, or even the official records of personal data, kept by other state authorities, since the Slovenian personal data protection is relatively strict. This paper therefore explores data mining, conducted by the Police during its intelligence police activity in Slovenia, and its legal limits.

Social network, social profiling, predictive policing. Current issues and future perspectives

Federico Costantini
Università degli Studi di Udine

Network analysis is a powerful tool that is increasingly used not only to determine events that occurred in the past, but also to predict what may happen in the future. This contribute will discuss the perspective, far from being abstract or remote, that such methods may be adopted in order to anticipate crimes. Taking into account current technologies, present legal science and according to the recent “Onlife Manifesto”, here are tackled three issues, concerning respectively the epistemological, the legal-philosophical and the anthropological aspect. In the first place, the relevance of the information provided in a crime’s “prediction”, since it does not concern an event of the past. Secondly, the nature of responsibility ascribed on these grounds, as neither an “actus reo” nor a “mens rea” can be found in the case. Finally, the kind of punishment could be given to the supposed criminal, because free will should be doubted if his behaviour could be foreseen.

State’s Due Diligence in Cyberspace in the Era of Big Data

Vasilka Sancin
Faculty of Law, University of Ljubljana

Due diligence under international law explains what a responsible State ought to do under normal conditions in a situation with its best practicable and available means, with a view to fulfilling its international obligation, and thus refers to a level of judgement, care, prudence and, determination that a State would reasonably be expected to undertake under particular circumstances. The author aims to discuss States' due diligence in cyberspace in the era of big data through the three-fold obligation of States: to prevent, to investigate and to prosecute those responsible for cyber attacks. The analysis delves upon the paradigm shift in interpreting State's sovereignty in cyberspace. Some of the well-established principles in certain areas of international law,

such as due diligence in international environmental law relating to prevention of transboundary harm, are used mutatis mutandis as guiding principles for the application of due diligence in cyberspace. In discussing the contents of due diligence in cyberspace emphasis is given to the dilemmas surrounding the issues of threshold of emerging damage from the attack, actual and constructive knowledge of the state and possible measures that a State can take in response to a cyber attack.

The alluring promise of objectivity: Big data in criminal justice

Mojca Plesničar
Institute of Criminology at the Faculty of Law

Criminal justice systems have long aimed at preventing judges' subjectivity from having any impact on in the courtroom. A good, yet complex example is the case of sentencing, where an example of trying to minimise judges' subjectivity are the infamous sentencing grids, used by different USA jurisdictions, which have entered the sentencing stage promising to limit judicial discretion thus eliminating judges' subjectivity and consequently sentencing disparity. To say the promise was not quite kept is an understatement. Other systems, relying on less detailed guidelines or statutory regulation have left more room for the individualisation of sentences, but in parallel for subjectivity as well.

A modern option to tackle the issue has emerged with the developments in processing big data. Big data has so far entered criminal justice at three levels: bail, sentencing, and parole. They all utilise a large amount of previously decided cases to build a strong algorithm able to predict the best possible answer to the given question in a specific case. The outcomes they offer are data-driven probabilities of requested instances.

The clear answers such algorithms are able to produce are very alluring. They bring promises of a fairer system: informed decisions devoid of bias and any kind of subjectivity. There are many potential benefits of bringing together technological accuracy and human empathy: such decisions could be much more accurate and based on a sound analysis of predictive factors. Seen as more objective, such algorithms could instil the long-lost trust of the public in the fairness of the criminal justice system. Moreover, they may present an opportunity to purposefully re-shape the penal system in order to reflect progressive values and support a more humane outlook.

However, there are some important considerations to be made before embarking on the big-data-saviour-of-justice wagon which we will discuss in detail.

We don't know what the Questions are, but we know we're gonna find the Answers

Alexander Czadilek, Christof Tschohl and Walter Hötzendorfer
epicenter.works, Research Institute Vienna

Big Data has been discussed in the Data Protection Law community for several years now. However, the big questions still remain. In this paper, we discuss some of these questions. We strongly belief that data protection is not an end in itself but a catalyst to achieve more fundamental aims. Therefore, we will start from a fundamental (and fundamental rights) perspective, asking what the protective purpose of Data Protection Law actually is and what that means for Big Data. We will then delve into the new legislative acts of EU Data Protection Law, the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) and the Police and Criminal Justice Authorities Directive (Directive (EU) 2016/680) to analyse their implications on the use of Big Data. A key point here is the principle of purpose limitation and the new rules on further processing for compatible purposes (Art. 5(1)(b) and Art. 6(4) GDPR).

Another important issue is profiling and automated decision making for law enforcement, criminal justice and other purposes based on Big Data. Here, not only legal aspects but also the implications of factual psychological mechanisms have to be considered, such as an over-confident belief in the results calculated by software systems ("machines"). It must also be considered whether results, with both negative and positive consequences for a suspect, are taken up (principle of material truth).

Finally, we ask, whether and how the problems we described can be resolved. In our view, Privacy by Design will play a major role. Based on our experience both in research projects and commercial projects we show some practical examples.

About the Venue

Faculty of Law, University of Ljubljana
Poljanski nasip 2
SI-1000 Ljubljana

The Faculty of Law is situated in the center of Ljubljana, by the Dragon Bridge over river Ljubljanica.
Location on the map of the city

Link to the official web-site of the **Faculty of Law**:
W: http://www.pf.uni-lj.si/en/

The organizing institutions:

Institute of Criminology at the Faculty of Law Ljubljana and

Faculty of Law, University of Ljubljana

Poljanski nasip 2, 1000 Ljubljana, Slovenia

W: http://inst-krim.si/en/

On behalf of the organizer:

Associate Prof. Dr. Aleš Završnik

The city

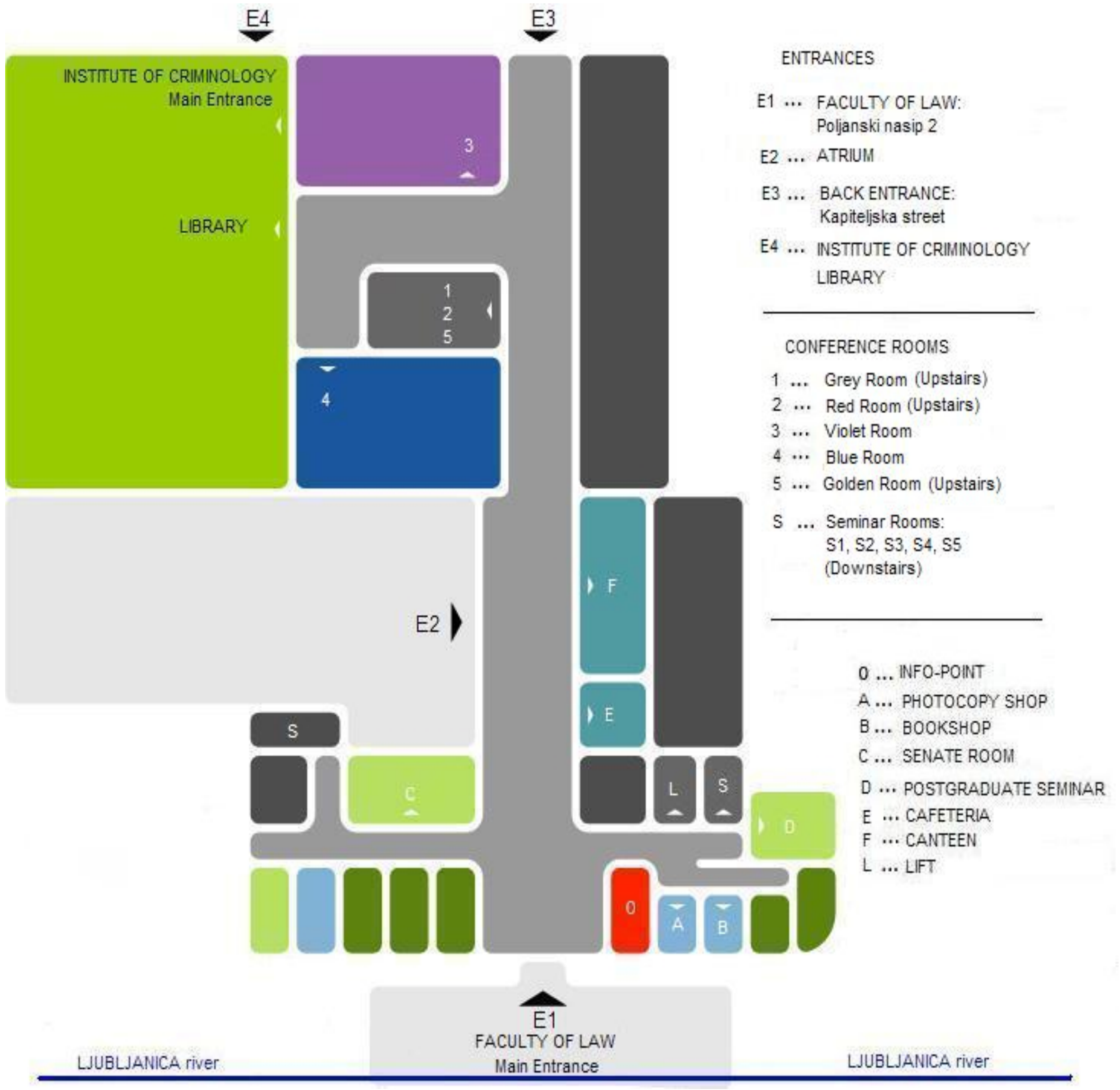
Ljubljana is the lovely capital of Slovenia. The charming city covers a surface area of 275 km2 and has a population of about 276,000. The city centre, abundant in cultural and architectural pearls can be explored by feet and the variety of pubs, bars and restaurants by the banks of the river Ljubljanica offer a pleasant experience at the end of the day.

For information on Ljubljana you may check the following:
http://www.ljubljana.info/
http://www.ljubljana-calling.com/ENG/index.asp

Slovenia

Slovenia is a young European country with the population of almost two million. In spite of its size it offers a mixture of geographical and cultural features, from the sunny Alps to the green Mediterranean, from the Pannonian fields to the Karst stones. Because of its size they are all within your arm's reach.
For information on Slovenia, please refer to the following web-sites:
http://www.slovenia.info/
http://en.wikipedia.org/wiki/Slovenia

Map of the Building of the Faculty of Law

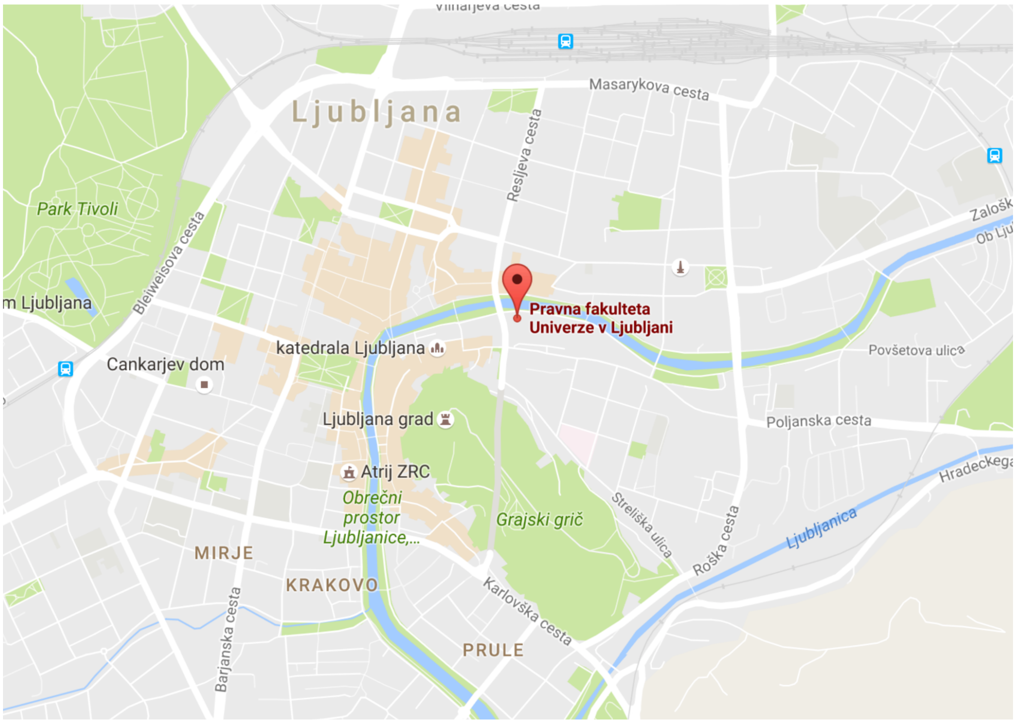


VENUE: Faculty of Law in Ljubljana

(Faculty of Law, University of Ljubljana, Poljanski nasip 2, 1000 Ljubljana, Slovenia)

The Faculty of Law, established in 1919, is one of the founding faculties of the University of Ljubljana and the largest law faculty in Slovenia. Ever since, the Faculty has offered its students an intellectually exciting learning environment with high academic standards at undergraduate and postgraduate levels, promoting both legal knowledge and critical thought. Today, it is not only the oldest but also the largest and – by any measure – the best law faculty in Slovenia. The Faculty boasts a large teaching staff working in nine departments, six further associated research institutes and the most extensive law library in the region. Graduates of the Ljubljana Faculty of Law go on to assume important positions in society and shape the Slovenian legal system and practice, but the Faculty also nurtures its international outlook and reputation. This is shown not only in the European, comparative and international focus embodied in study programmes, but also in the high mobility of students and teaching staff, frequent visiting lecturers and other distinguished guests, successful participation in international student competitions and a growing portfolio of international conferences and similar events taking place at the Faculty.

Venue: Faculty of Law, University of Ljubljana location



The conference will take place in the seminars and lecture rooms at the ground floor of the Faculty of Law. There will be indications at the entrance of the Faculty to indicate way for participants.

WIFI access

Free WIFI will be available to all participants of the Big data: New Challenges for Law and Ethics conference. All necessary information on this will be provided for when participants arrive to the venue. EDUROAM network is available.

Cafeteria

The organisers will provide for coffee breaks for the participants during breaks. The Faculty cafeteria is also available to participants, it is open from 8 am to 15 pm. There are also shops (e.g. Spar) nearby Faculty where participants will be able to purchase their own food.

Contact Information

For any further information write to inst.crim@pf.uni-lj.si .

HOST CITY: Ljubljana

(Source: http://www.ljubljana.guide/how-to-travel/travel-to-ljubljana/)

Ljubljana, the capital of Slovenia, is the political and cultural heart of the Slovenian nation. It is classified as a mid-sized European city, but has preserved its small-town friendliness and relaxed atmosphere while providing all the facilities of a modern capital. Ljubljana is a unique city dotted with pleasant picturesque places where you can expect all kinds of nice little surprises.
It is an important European commercial, business, exhibition and congressional centre as well as the transport, science and education centre of Slovenia.

Whether you're taking a stroll down the Congress square or alongside riverbanks you can feel and see the atmosphere that surrounds the beautiful but yet small city centre. Today scientists are drawn to the city because of its high-calibre institutes and university, of which especially law school and medical school are a top pick in the region, as are artists due to its world-famous graphic biennial, art academy and countless art galleries. International businessmen, economists and experts from all fields frequently attend the city's many business and congressional meetings, exhibitions and trade fairs.

Ljubljana is also a city of culture. It is home to numerous theatres, museums and galleries, and hosts one of the oldest philharmonic orchestras in the world. For the people of Ljubljana, culture is a way of living. Over 10,000 cultural events take place in the city every year, among which there are 10 international festivals.

For further information please visit: https://www.visitljubljana.com/en/visitors/

OTHER IMPORTANT INFORMATION

Currency

Slovenia is a European Union member state therefore the official currency is the euro (€). It was introduced at the beginning of 2007. Most shops across the country accept international credit and debit cards. Slovenia has a widespread cash machine network.

Medical Assistance

Pharmacies: In case of minor health problems such as colds, headaches, temperature above normal, and insect bites, medicines can be obtained from pharmacies also without a prescription. There are numerous pharmacies in Ljubljana, which are open from 8.00 am until 19.00 pm. The Lekarna pri Polikliniki duty pharmacy is open 24 hours a day, seven days a week (Address: Njegoševa cesta 6k, 1000 Ljubljana, tel.: +386 (0)1 230 61 00).

Emergency medical services:

- For rescue and emergency services, call the free phone number 112.
- 24-hour emergency GP services for adults are provided by the Emergency Unit of the Ljubljana University Medical Centre, entrance from the Bohoričeva ulica street, 1000 Ljubljana.

Notes