TIPC 2021, 16 JUNE

(10:00 – 16:05, AMSTERDAM)

PROGRAM

10:00-10:30 room 1:	**Opening:** Bo Zhao, TILT, Tilburg University **KEYNOTE:** RONALD LEENES, TILT, TILBURG UNIVERSITY *ARTIFICIAL INTELLIGENCE, LAISSEZ FAIRE, REGULATE OR WHAT?*
10:30-11:30	**Session 1:**
room 2	Law and Economics CHAIR : Bo Zhao, TILT, Tilburg University
10:30-10:50	**Olena Demchenko**, University of Pecs *Transactions with loot boxes in video games. European approach to the gambling regulations in the gaming industry* DISCUSSANT: Inge Graef, TILT, TILEC, Tilburg University
10:50-11:10	**Jamelia Anderson-Princen**, Tilburg University *Cloud outsourcing in the financial sector: An assessment of internal governance strategies on a cloud transaction between bank and a leading cloud service provider* DISCUSSANT: Konrad Borowicz, TILT, TILEC, Tilburg University
11:10-11:30	**Shashi Kant Yadav**, Central European University *Precautionary approaches towards fracking-related water risks in multilevel legal systems of the US, India, and EU* DISCUSSANT: Gert Meyers, TILT, Tilburg University
room 3	Regulating AI (1) CHAIR : Charmian Lim, TILT, Tilburg University
10:30-10:50	**Kelly Blount,** University of Luxembourg *Bridging the regulation gap in artificial intelligence technologies for law enforcement* DISCUSSANT: Floris Bex, TILT, Tilburg University

10:50-11:10	**Gijs van Maanen,** Tilburg University *Governance of algorithms requires attention to representation* DISCUSSANT: Tineke Broer, TILT, Tilburg University
11:10-11:30	**Francesca Palmiotto,** European University Institute *Transparency or explainability? Different solutions for regulating AI* DISCUSSANT: Linnet Taylor, TILT, Tilburg University
11:30-11:40 room 1	10 minutes break
11:40-12:40	Session 2:
room 2	Data and privacy protection (1) CHAIR : Tjasa Petrocnik, TILT, Tilburg University
11:40-12:00	**Eyup Kun ,** KU Leuven Centre for IT and IP Law (CiTiP) *Strengthening the supervision in the EU cybersecurity law: are all organizational measures created equally?* DISCUSSANT: Emmanuel.C.J. Pernot-LePlay, TILT, Tilburg University
12:00-12:20	**Athena Christofi** , KU Leuven, CiTiP *Smart cities and the challenge of aggregated effects: searching for macro-balancing tests* DISCUSSANT: Emmanuel.C.J. Pernot-LePlay, TILT, Tilburg University
12:20-12:40	**Maja Nisevic ,** University of Verona *A study on the personal data processing and the UCPD focused on case law of Italy, Germany and UK* DISCUSSANT: Emmanuel.C.J. Pernot-LePlay, TILT, Tilburg University
room 3	Regulating AI (2) CHAIR : Gijs van Maanen, Tilburg University
11:40-12:00	**Elisabeth Paar**, University of Vienna *Artificial Intelligence and judicial independence - An exemplary constitutional analysis regarding the hearing of witnesses*

	DISCUSSANT: Marijke Roosen, TILT, Tilburg University
12:00-12:20	**Maarten Herbosch,** KU Leuven *The precontractual use of AI systems: legal opportunities and challenges* DISCUSSANT: Marijke Roosen, TILT, Tilburg University
12:20-12:40	Antonella Zarra, Hamburg University, Institute of Law and Economics *The cost of AI-driven accidents* DISCUSSANT: Bo Zhao, TILT, Tilburg University
12:40-13:40 **Zoom room 1**	1h Lunch break
13:40-14:40	**Session 3:**
room 2	Data and Privacy Protection (2) CHAIR : Gargi Sharma, TILT, Tilburg University
13:40-14:00	Beril Boz , University of Oxford, Faculty of Law *Social media and children 'working' under surveillance* DISCUSSANT: Tanya Krupiy, TILT, Tilburg University
14:00-14:20	**Samir Jarjoui,** University of Dallas *People, process, and technology: A novel framework for big data governance* DISCUSSANT: Tanya Krupiy, TILT, Tilburg University
14:20-14:40	**Tjasa Petrocnik** , TILT, Tilburg University *Informed consent in the age of iLeviathan* DISCUSSANT: Bo Zhao, TILT, Tilburg University
room 3	Regulating AI (3) CHAIR : Charmian Lim, TILT, Tilburg University

13:40-14:00	**David Hadwick,** Universiteit Antwerpen *Deus tax machine: How should the use of artificial intelligence by tax administrations be regulated in the EU?* DISCUSSANT: Marijke Roosen, TILT, Tilburg University
14:00-14:20	Marthe Goudsmit, University of Oxford *Regulating user-generated image-based sexual abuse on online platforms : exploring criminal law and artificial intelligence-based web crawlers options* DISCUSSANT: Marijke Roosen, TILT, Tilburg University
14:20-14:40	Rachele Carli, University of Bologna *Criticalities and future challenges of social robotics: a focus on deception in human-robot interaction* DISCUSSANT: Dovilė Petkevičiūtė Barysienė, Vilnius University
14:40-14:50 room 1	10 minutes break
14:50-15:50	Session 4:
room 2	Energy and Environmental law CHAIR : Brenda Espinosa Apráez, TILT, TILEC, Tilburg University
14:50-15:10	**Asieh Haieri Yazdi** CEPMLP, University of Dundee *Nuclear energy in uncertain times of the Persian gulf* DISCUSSANT: Leonie Reins, TILT, Tilburg University
15:10-15:30	**Liebrich Hiemstra**, Tilburg University *Energy trading and data disclosure: the legal basis of information exchange between supervisory agencies* DISCUSSANT: Saskia Lavrijssen, TILT, TILEC, Tilburg University
15:30-15:50	Manon Simon, University of Tasmania *Adaptive governance for solar radiation management* DISCUSSANT: Leonie Reins, TILT, Tilburg University

room 3	Data and Privacy Protection (3) CHAIR : Gargi Sharma, TILT, Tilburg University
14:50-15:10	Hannah Smith , University of Oxford *The role of the citizen in legitimising reuses of administrative data in research* DISCUSSANT: Bo Zhao, TILT, Tilburg University
15:10-15:30	Florence D'Ath , Université de Luxembourg *Data protection law as a tool to neutralize discriminatory outcomes in the context of e-recruiting practices* DISCUSSANT: Bo Zhao, TILT, Tilburg University
15:50-16:05 room 1	15 Min. Conclusion

ABSTRACTS

SESSION 1: 10:30-11:30

LAW AND ECONOMICS ROOM 2

TRANSACTIONS WITH LOOT BOXES IN VIDEO GAMES. EUROPEAN APPROACH TO THE GAMBLING REGULATIONS IN THE GAMING INDUSTRY

The present paper explains possible ways of the legal approach to the transactions with loot boxes in free-to-play video games, particularly, focusing on the monetary value involved in operations with loot boxes. Current research examines online gambling definition accepted in the European Union and its application to the in-game transactions connected to the loot boxes trade both at internal and external platforms. The present paper focuses on gaps in existing legal procedures regulating (or not regulating) transactions on virtual items, stresses on the necessity of new legal models application in the gaming industry and underlines the importance of amendments to current European legislation with the focus on video games commoditisation in order to protect consumer rights, free movement of digital goods and to secure European public policy.

AUTHOR: **OLENA DEMCHENKO,** UNIVERSITY OF PECS

CLOUD OUTSOURCING IN THE FINANCIAL SECTOR: AN ASSESSMENT OF INTERNAL GOVERNANCE STRATEGIES ON A CLOUD TRANSACTION BETWEEN BANK AND A LEADING CLOUD SERVICE PROVIDER

Cloud applications are becoming central and critical to core operations, and delivery of financial services. For financial institutions, two main concerns are the increased exposure to transaction risks, and devising appropriate internal governance strategies, especially in light of their accountability for cloud failures. The study examines the effectiveness of internal governance strategies applied on a cloud outsourcing transaction between a Bank and Cloud service provider. The study applies a unique data set from a Banks' cloud risk register, to a structural modelling equation (SEM), and simple linear regression to test for transaction misalignment and causes of governance inefficiencies in the risk mitigation process. The tests on our structural model are positive for misalignment indicating governance inefficiencies. We find that, the inefficiencies on the SEM model, can be best explained by weaknesses in the design of the Banks' internal control framework. In particular, I illustrate that some of the most critical and important cloud risks, are not only driven by agency costs, but also by firm specific risks which contribute to significant transaction uncertainties and governance inefficiencies.

AUTHOR: **JAMELIA ANDERSON-PRINCEN**, TILBURG UNIVERSITY

PRECAUTIONARY APPROACHES TOWARDS FRACKING-RELATED WATER RISKS IN MULTILEVEL LEGAL SYSTEMS OF THE US, INDIA, AND EU

Differences in legal systems can play an imperative role in regulating 'risks' and 'uncertainties' posed by emerging technologies. A pro-innovation, light-touch regulatory approach may interfere with the citizens' constitutional right to a clean environment, access to water, among others. On the contrary, triggering the precautionary principle (PP) on low-level uncertain risks may discourage scientific innovation eventually halting innovation and market growth.

In any case, it is important to identify the 'safe levels' of resource exploitation. These safe levels are 'minimum plausible threshold' that enables only genuinely hazardous impacts of a technology to trigger precautionary actions. Although the current literature highlights the various components of a legal system that influence the regulation of environmental risk through PP, it does not comparatively analyse these components. A comparative analysis of how different multilevel legal systems trigger the PP is important to ensure that "safe levels" of resource exploitation is determined in a scientific, rationally (or proportionally), and decentralised (bottom-up) manner.

This research proposes to comparatively analyse how differences in the multilevel legal systems of the US, the EU, and India influence the application of the PP on the similar water risks related to hydraulic fracturing (fracking), a water-intensive technique of extracting unconventional natural (shale) gas by horizontally injecting millions of gallons of pressurised water into deep sedimentary rocks.

This case study, under the comparative method approach, will test the hypothesis that differences in the systemic distribution of legislative and regulatory powers between national and subnational units, in a multilevel legal system with shared competence on environmental matters, affect the application of the PP. In this context the three comparators (the US, the EU, and India) have (1) different level of shared competence over environmental matters in their multilevel governing system, (2) implemented fracking and triggered different precautionary actions against similar fracking-specific risks, (3) adopted PP with different interpretations.

AUTHOR: **SHASHI KANT YADAV**, CENTRAL EUROPEAN UNIVERSITY

REGULATING AI — ROOM 3

BRIDGING THE REGULATION GAP IN ARTIFICIAL INTELLIGENCE TECHNOLOGIES FOR LAW ENFORCEMENT

The application of artificial intelligence (AI) across every aspect of our lives has earned AI a reputation as 'disruptive technology.' Though it may not be readily apparent in the field of criminal law, the permeation of AI into this area of public life holds very important implications for fundamental rights. The development of AI technologies is increasingly regulated, as is the use of AI by law enforcement authorities (LEA). This paper posits that there is a public policy gap between the two bodies of regulation and addresses the public-private interaction between companies developing and supplying AI technologies and LEAs utilizing them. The paper will argue for a regulatory scheme that addresses the lack of transparency in procurement, licensing, and contractual relationship between AI developers and law enforcement authorities.

AI reliant technologies allow LEAs to better allocate their resources, and more effectively prevent and control crime. However these technologies often bring uncertainty as regards potentially propagating biases and the magnitude of potential errors. Many LEAs not only lack the knowledge to address these issues, but developers are unwilling to share proprietary information. Further, it is unclear whether the LEA or company dictates where data is stored and which entity acts as controller. Finally is the actual procurement process, by which LEAs contract or license with AI developers. This paper aims to demonstrate the need for transparency in the bidding process and subsequent contractual relationship. Though policing authorities are well scrutinized, and AI developers increasingly regulated, the bridging of the two is less studied. The paper will argue that by putting forward a regulatory approach that takes into account these peripheral factors, a transparent and mutually beneficial public-private interaction may occur.

AUTHOR: **KELLY BLOUNT,** UNIVERSITY OF LUXEMBOURG

GOVERNANCE OF ALGORITHMS REQUIRES ATTENTION TO REPRESENTATION

The perceived potential of computers to outperform people at a variety of tasks has led to the increasing usage of algorithms in the public and private sector. At the same time, the fallibility of algorithms has been demonstrated by numerous high-profile incidents. In response, many have called for governance of algorithms. While algorithmic accountability is considered one way to operationalize algorithmic governance, it is met with its own share of challenges. First, it remains unclear what algorithmic accountability should entail (Wieringa 2020). Second, there's ambiguity in how best to characterize algorithms. Dourish (2016) argues we should adopt the terminology used by the those working on algorithms. Seaver (2017) by contrast, argues that algorithms are 'multiple': a software engineer may 'enact' an algorithm through "mathematical analysis", while an anthropologist may enact them as "rangy sociotechnical systems".

In this paper we engage with these two challenges and contribute to the academic literature on algorithms and the governance of algorithms by foregrounding the epistemic and political representational qualities of algorithms. We analyze representational claims present in the Ofqual, SAFFIER II and SyRI algorithms, to illustrate their enactment of different and often clashing epistemic and political representational norms.

In respect to the academic debate, characterizations of algorithms that diametrically oppose technical enactments run the risk of alienating more 'technical' scholars from 'social' scholars and designers from critics (Barocas & boyd 2017). Such enactments have their place but seek to oppose and resist rather than to discuss and compromise. Our approach presents a middle ground that is neither "high-brow humanities" nor "techno-optimist" and provides common ground for debate. We argue that a more diverse academic discussion and public debate resulting from a sensitivity to representational claims is a precondition for the effective governance of algorithms.

AUTHORS: **GIJS VAN MAANEN,** TILBURG UNIVERSITY & DAAN KOLKMAN, EINDHOVEN UNIVERSITY OF TECHNOLOGY

TRANSPARENCY OR EXPLAINABILITY? DIFFERENT SOLUTIONS FOR REGULATING AI

In the past years, AI applications have grown exponentially, permeating every aspect of our everyday life. These systems are used for firing, hiring, profiling, targeting, ranking, and even for taking crucial decisions for individuals' lives. At the same time, many concerns have been raised, particularly regarding their reliability. Research has shown, for instance, that Amazon's AI recruiting tool was biased against women and that facial recognition may be less accurate when identifying black people. However, in a worrying trend, these tools are still concealed in secrecy and opacity, preventing individuals from understanding how their output has been generated.

In light of these concerns, the literature advocates for the development of transparent and explainable AI systems. Likewise, several EU's guidelines consider transparency and explainability of the system as key requirements for developing trustworthy AI. However, notwithstanding these European documents and scholarly work produced on this topic, the difference between the two options remains unclear. Which one is the most appropriate? How to choose between these two requirements? Or should both be demanded in any case?

This paper aims at addressing these questions by proposing a conceptual framework that provides guidance in the choice between transparency and explainability of AI systems. This debate is particularly timely, as a regulatory proposal by the Commission is expected by the end of this year. The Commission's primary goal is to safeguard fundamental EU values and rights by setting requirements related to trustworthiness for high-risk AI systems. Hence, a clarification on the differences between these two solutions is needed.

The paper argues that, when choosing between the two, one should consider the type of knowledge production's process that best fits the context. Hence, the main guiding question is: can I trust the explainer, or do I need to verify first-hand?

To test this hypothesis, the last part of the paper provides an analysis of two case studies: firing software in work relationships and risk-assessment software in criminal proceedings.

AUTHOR: **FRANCESCA PALMIOTTO,** EUROPEAN UNIVERSITY INSTITUTE

SESSION 2: 11:40-12:40

DATA AND PRIVACY PROTECTION (2) ROOM 2

STRENGTHENING THE SUPERVISION IN THE EU CYBERSECURITY LAW: ARE ALL ORGANIZATIONAL MEASURES CREATED EQUALLY?

The Directive on Security of Network and Information Systems (NIS I Directive) provides that operators of essential services and digital service providers (regulated entities) shall take appropriate technical and organizational measures to manage the risks arising from cyber-attacks on their network and information systems. However, it has been stated that they might externalize these risks to their users or society in the absence of appropriate regulatory supervision. Therefore, they might be reluctant to comply with the requirements under NIS I Directive. Despite discussions in the literature about the extent to which the supervision mechanism under the NIS I Directive can ensure effective compliance, the role of specific organizational measures in ensuring the supervision in this Directive and proposed NIS II Directive has not been explored.

After pointing out the shortcomings of the current supervisory mechanism, this paper aims to demonstrate that the insertion of specific organizational measures to the proposed NIS II Directive should be required to strengthen the supervision over the regulated entities. To support this claim, this paper examines the supervision mechanisms available under both NIS I and the proposed NIS II. Moreover, it investigates how organizational measures can help supervisory authorities oversee the risk management activities of these entities. The question of how security impact assessment and information security officers can improve supervision as organizational measures if they are provided under law is specifically addressed. While analyzing these measures, the reason why these measures can have a specific function in the supervision of those entities will be closely analyzed to justify the explicit insertion of these measures. During this analysis, the relevant provisions of the General Data Protection Regulation on data protection impact assessment and data protection officers are discussed to demonstrate how these organizational measures improve the supervision of regulated entities in enhancing compliance with cybersecurity requirements.

AUTHOR: **EYUP KUN,** KU LEUVEN CENTRE FOR IT AND IP LAW (CITIP)

SMART CITIES AND THE CHALLENGE OF AGGREGATED EFFECTS: SEARCHING FOR MACRO-BALANCING TESTS

Smart cities denote the gradual datafication of urban environments and urban governance, in ways that promise to produce important benefits in the public interest yet bring risks to the fundamental rights of city dwellers. The protection of rights should thus be effectively balanced with the public interests at stake. Balancing mechanisms can be found in the conditions for limitations of fundamental rights found in the EU Charter and ECHR, and principles like legality and proportionality. Then, EU data protection law provides even more fine-grained tools for balancing in the form of the Data Protection Impact Assessment (DPIA).
This paper discusses the limitations of these balancing mechanisms in the smart city context. Fundamental rights

and other interests are usually balanced in the framework of specific projects and processing operations. Yet, in the smart city this micro-/ project-focused approach might be insufficient in its own. While individual smart city projects may present limited risks, the paper stresses the need to consider and assess the aggregated effects of different projects. The change towards smart cities happens gradually, and it is the accumulation of several projects that could be most problematic from a fundamental rights perspective. Should a macro-balancing test be introduced in addition to the project-specific balancing mechanisms? How could aggregated effects be accounted for methodologically in DPIAs dealing with smart city projects?
The paper probes these questions, in particular by investigating whether parallels could be drawn from the assessment of environmental harms, where cumulative risks arising from a combination of industrial developments are also pertinent. As impact assessments in the environmental field have a longer history than their data protection counterpart, it looks into strategic environmental assessments and cumulative effects assessments to see if (methodological) tools found therein could be useful to address aggregated effects on fundamental rights in smart cities.

AUTHOR: **ATHENA CHRISTOFI,** KU LEUVEN, CITIP

A STUDY ON THE PERSONAL DATA PROCESSING AND THE UCPD FOCUSED ON CASE LAW OF ITALY, GERMANY AND UK

Today, personal data are considered a counter-performance for “free” digital services or discounts for online products and services. A primary concern of personal data processing is data collection or data manipulation, intending to produce new information about individuals. Considering the General Data Protection Regulation (GDPR), data processing means a wide range of operations performed on personal data, including manual or automated means. It includes collecting, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. Furthermore, manipulation with Big Data Analytics allows commercial exploitation of individuals based on unfair commercial practices. Traders use unfair commercial practices to attract consumers in order to buy their products or use their services online. Consequently, consumer protection concepts are essential in a data-driven economy and central issues to effective individuals’ protection in the Big Data Age. Although the field of consumer protection and data protection in the European Union (EU) have been developed separately, there is an unambiguous relationship between them. While the GDPR plays a crucial role in individuals’ data protection in the case of personal data processing, the Directive 2005/29/EC (UCPD) plays a crucial role in regulating an individual’s protection from unfair commercial practice when it comes to personal data processing. A vital aspect of the UCPD is the enforcement of issues related to consumer privacy. However, a much-debated question is whether the UCPD is fully effective or not for personal data processing.
This aritcle examines consumer protection from unfair commercial practice when it comes to personal data processing. Besides, this paper examines case law examples on WhatsApp and Facebook in Italy, Germany, and the United Kingdom. In the end, this paper is aiming to give a comprehensive conclusion on the issue, referring to the applicability of the rules on unfair commercial practice when it comes to data processing.

AUTHOR: **MAJA NISEVIC,** UNIVERSITY OF VERONA

ARTIFICIAL INTELLIGENCE AND JUDICIAL INDEPENDENCE - AN EXEMPLARY CONSTITUTIONAL ANALYSIS REGARDING THE HEARING OF WITNESSES

The use of Artificial Intelligence (AI) has initiated a disruptive process in the legal sector, which will also affect state institutions such as courts. As of today, it has already been pointed out that AI could take over tasks of the finding of justice in the near future. This discussion is often limited to the use of AI in legal assessment. However, a judge´s field of activity does not only comprise the legal assessment of established facts, but also the determination of the facts themselves. This second aspect essentially consists of the hearing and consideration of evidence. It should not be overlooked that recourse to AI is also conceivable in the course of dealing with these factual elements of the judicial basis for a decision; the question of (constitutional) admissibility arises equally.
The latter aspect is the subject of my proposed contribution, whereby the legal analysis will be carried out exemplarily on the basis of the hearing of witnesses and its assessment in the context of civil proceedings. Even within this specific stage of the procedure, potential application fields for AI are numerous. Due to this, a further restriction is necessary. The focus will be on three use cases: speech processing, the analysis of facial expression as a form of optical emotion recognition and the analysis of prosody as a form of acoustic emotion recognition. Building on these potential fields of application, it shall be examined whether the current constitutional law sets limits for the use of AIs in the hearing and assessment of evidence which obviate the need for explicit limitation. This constitutional analysis will be carried out exemplarily on the basis of judicial independence as a central structural principle of all constitutions based on the rule of law.

AUTHOR: **ELISABETH PAAR,** UNIVERSITY OF VIENNA

THE PRECONTRACTUAL USE OF AI SYSTEMS: LEGAL OPPORTUNITIES AND CHALLENGES

Artificial intelligence (AI) systems are used increasingly often in a precontractual context. They are not only used as a source of information, but in some instances, even contract negotiation and formation are delegated to these systems. This can be problematic, as the existing legal framework is highly centred around humans. This is exemplified by notions such as ‘consent’, ‘diligence’ and ‘fault’. The autonomy that characterises modern AI systems based on machine learning hinders the straightforward application of these concepts to the system’s user. Resultingly, it is unclear how the existing legal framework should be applied when parties use these systems. The resulting legal uncertainty gives rise to the question whether an adapted ‘intelligent’ contract law framework is required.
This contribution focuses on the difficulties encountered when a contract is concluded on the basis of incorrect information, provided by an AI system. It also examines the situation where the contract formation is delegated to an AI system. In both instances, it is examined how the use of an AI system may impact the existence and the validity of the resulting contract.

AUTHOR: **MAARTEN HERBOSCH,** KU LEUVEN

THE COST OF AI-DRIVEN ACCIDENTS

Current applications of artificial intelligence (AI) are far from being fully autonomous. As a matter of fact, human intervention is still required in most circumstances to take final decisions or to avoid system failures. The degree of interaction between human beings and machines brings about important consequences for the attribution of

liability when an accident occurs. For instance, the deployment of semi-automated vehicles, where a safety driver is required to relinquish control if needed, may induce over-reliance on the technology, resulting in an increased level of negligence by the operator. Evidence from other sectors (e.g. aviation) that have already witnessed a shift to full automation suggest that human operators might become the "moral crumple zone" (Elish, 2019) of accidents involving AI, being consistently blamed for negligence even in cases where their control on the machine is limited.

Against this backdrop, it is worth asking how liability should be attributed when a technology is automated but not autonomous and, in turn, how adequate levels of safety and innovation can be ensured. This paper first surveys possible liability frameworks applicable to AI systems and then reflects on the largely discussed hypothesis of attributing legal personality to algorithmic agents. It argues that the "human in the loop" should be considered when analyzing the level of precautions and activity. Furthermore, it contends that the type of liability regime and the consequent choice of remedies is shaped by how lawmakers conceive AI in the first place. In this respect, regulators should envisage specific mechanisms for partially autonomous technologies where human negligence persists, which would incentivize the adoption of adequate levels of precaution without stifling firms' investments in innovation.

AUTHOR: **ANTONELLA ZARRA,** HAMBURG UNIVERSITY, INSTITUTE OF LAW AND ECONOMICS

SESSION 3: 13:40-14:40

DATA AND PRIVACY PROTECTION (3) ROOM 2

SOCIAL MEDIA AND CHILDREN 'WORKING' UNDER SURVEILLANCE

While it is often discussed whether adults comprehend the adverse effects of technology eg social media platforms and render valid 'consent', there seems to be an oversight on the aspects of this incomprehension for decisions rendered by adults for children. Children seem to be mirroring their parents/guardians' behaviours and adopting this new social phenomenon too fast, before having the psychological necessities and legal tools to exercise autonomy. Social media accounts managed by parents (sharenting) seem to (i) disregard that children are aware that they are constantly under surveillance and tailor their behaviours accordingly; (ii) impose a sense of obligation to act in a certain way for the approvals of their parents and 'others'; (iii) expose children to social moulding too soon without necessary support and guidance. Legal frameworks acknowledge that children need supervision, protection and care, thus empower parents/guardians to exercise certain rights in line with that. However, these social media accounts run by the parents/guardians seem to make children 'work'. They 'work' to receive as many 'likes' and advertisement deals as they can. This is reminiscent of child TV stars. However, the two are quite different, both context and applicable regulations wise. TV stars are subject to stricter health and safety regulations eg hour-limitations and psychological support. Those who work on social media showcase their own lives, true identities and enable the followers/audience to mould their aspirations and perhaps characters. This article will compare the two work types, and their applicable legal frameworks (ie the GDPR and the E.U. frameworks on young people at work). It will then examine whether similar safeguards in place for TV work could be extended to social media and protect children from activities that are conducted beyond their free choice, which is yet to emerge.

AUTHOR: **BERIL BOZ,** UNIVERSITY OF OXFORD, FACULTY OF LAW

PEOPLE, PROCESS, AND TECHNOLOGY: A NOVEL FRAMEWORK FOR BIG DATA GOVERNANCE

While many companies maintain a system of internal controls and board-level experts for financial reporting, these checks and balances are less stringent for IT implementations. An MIT study in 2019 found that only 24% of boards were digitally savvy and abreast with technology transformation initiatives.
Many organizations harness big data capabilities to create value through innovations that improve competitiveness. While there is hardly any doubt among scholars and practitioners regarding the importance of big data, there is sparse guidance on how to holistically mitigate the risks inherent in big data technologies. Some of these risks are related to data privacy considerations, algorithmic biases, and intellectual property rights. As a result, big data stewardship continues to lag with inconsistent applications across organizations due to the lack of an end-to-end governance approach.
Leaning on the agency theory of the firm, we propose a governance model for big data capabilities within organizations. Although prior scholars have introduced governance frameworks that address big data challenges, these artifacts are limited in scope and do not synthesize the critical role of oversight structures and culture with other downstream governance activities.
In this paper, we outline a multi-layered governance model with several lines of defense to improve big data governance and accountability through an end-to-end approach of people, process, and technology. We emphasize the important role of organizational culture in the development of technology oversight and advance the notion that big data governance should commence at the board level, with clear risk management expectations. We contour three lines of governance oversight structures which include board of directors, independent reviews, and organizational controls. We also introduce three domains of big data governance activities which comprise technology investment measures, data life-cycle controls, and analytical optimization.

AUTHOR: **SAMIR JARJOUI,** UNIVERSITY OF DALLAS

REGULATING AI (3) ROOM 3

DEUS TAX MACHINE: HOW SHOULD THE USE OF ARTIFICIAL INTELLIGENCE BY TAX ADMINISTRATIONS BE REGULATED IN THE EU?

This research aims to bring to the Colloquium a discussion on the regulation of AI tools used by tax administrations. In 2019, the OECD reported that more than 40 tax administrations are making use of AI or planning to do so in the near future. In the EU, States such as Belgium, France, Germany, Poland or Spain all possess AI-driven solutions to perform some of their fiscal prerogatives. Due to the increase of e-commerce and the exponential growth in data flows, tax administrations have to process billions of documents every year, which places tax administrations in a strategic position to pilot such programs. Yet, the cases of SyRI and the toeslagenaffaire in The Netherlands, or RoboDebt in Australia show that AI governance tools bring a number of inherent risks to taxpayers' fundamental rights.
A lot of uncertainty remains around what tools are used by EU States to collect and analyse taxpayer data or to detect fraud, and how data protection provisions apply to these tools. This research identifies all AI tools used by tax administrations in the EU and classifies these tools in a function-based taxonomy. Informed by CJEU and ECtHR case-law, this research develops an analytical framework to assess infringements of taxpayers' privacy and data protection rights. The framework is then applied in a multiple case-study design, deriving data from multiple sources, including semi-structured interviews with tax officials and members of the DPA of several EU Member States. A comparative legal review is conducted to assess whether Member States' norms regulating the use of AI tax governance tools are appropriate to safeguard taxpayers' rights. The purpose of this research is ultimately to

develop qualitative requirements for the protection of taxpayers' privacy and data protection rights and the regulation of AI tax governance tools.

AUTHOR: **DAVID HADWICK,** UNIVERSITEIT ANTWERPEN

REGULATING USER-GENERATED IMAGE-BASED SEXUAL ABUSE ON ONLINE PLATFORMS : EXPLORING CRIMINAL LAW AND ARTIFICIAL INTELLIGENCE-BASED WEB CRAWLERS OPTIONS

Worldwide, there are over 3000 websites dedicated to hosting 'revenge porn' and countless forums on which images are traded 'like Pokémon cards'. Although image-based sexual abuse ('ibsa') is not new, its criminalisation only started when ibsa moved online. However, criminal laws addressing ibsa focus only on individual offenders. Platforms hosting and enabling non-consensual disclosure of private, sexual images, are not subject to regulations regarding this harmful content. Platforms have no legal obligation to comply with victims' take-down requests. This paper explores options for regulating digital platforms' facilitation of ibsa.
Firstly, I consider criminal law regulation. The criminal law may be especially helpful for regulating 'dedicated revenge porn sites', as those host exclusively illegal content. Platforms that have legitimate purposes beyond facilitating ibsa would be less easily criminalised: it could be an unreasonable infringement of free speech rights. Secondly, I address non-criminal legal remedies. I focus on what obligations may be put on platforms to ensure no illegal content is hosted by them. I consider promising possibilities for artificial intelligence-based web crawlers, which could help ensure no offending image will be (re-)published. Past attempts at automatically searching the web for illegal images have been challenged by the limits of technology: cropping an image would make it unrecognisable to a crawler. However, artificial intelligence-based software moves beyond those limitations. Software such as Clearview AI would work even with partial images, so that victims would not be required to upload the complete abusive image (as Facebook asked users to do in the past), thus increasing their safety. Anyone subsequently attempting to hosting the image could be alerted to its nature and prevent its renewed publication. I consider the legal feasibility of demanding platforms use such software and adhere to its restrictions. I conclude that the severity of ibsa warrants such regulations.

AUTHOR: **MARTHE GOUDSMIT,** UNIVERSITY OF OXFORD

CRITICALITIES AND FUTURE CHALLENGES OF SOCIAL ROBOTICS: A FOCUS ON DECEPTION IN HUMAN-ROBOT INTERACTION

The so called "forth revolution" is increasingly focused on the development of Artificial Intelligence (henceforth AI) devices, designed to directly interact with users, to collaborate with them and even to act in a human-centred environment – such is the case of robots characterised by a physical body – with different degrees of automatization. In order to encourage acceptability and trust, AI devices are structured as so to lever the human tendency to anthropomorphise what they interact with. It follows that some machines are able to simulate the feeling of genuine emotions or empathy, to appear needy of help, to pretend to have an own personality and – more in general – to induce the user to think that they are something more than mere objects. Thus, it may be argued that such interaction could lead to forms of manipulation that fall within the remit of a deceptive dynamic. This analysis investigates what is meant by "deception" in the human-robot interaction context, through an anthropocentric perspective and in line with principles and values expressed in the European Union legal framework.
To this end, a brief review of hypothetical scenarios of interaction is presented and discussed with regard to its possible long-term consequences, with the aim to draw a line between beneficial and harmful effects.

Therefore, both ethical and legal perspectives are reconstructed, with the attempt to try to distinguish their respective scope and to emphasise their fruitful integration in addressing these issues.
Finally, the possible relevance of fundamental human rights in human-robot interaction dynamics is discussed, due to their ability to reconcile ethical demands with the binding feature of legal norms.

AUTHOR: **RACHELE CARLI**, UNIVERSITY OF BOLOGNA

SESSION 4: 14:40-14:50

ENERGY AND ENVIRONMENTAL LAW — ROOM 2

NUCLEAR ENERGY IN UNCERTAIN TIMES OF THE PERSIAN GULF

The global nuclear energy scene is changing rapidly. Some countries are phasing out of nuclear technology. Some of the other countries are in the nuclear renaissance, planning to promote the most ambitious new nuclear construction programme. The statemen make the proper decision in nuclear policy striking the best balance of domestic energy policies, energy-concerned foreign policies, and the dynamism of international relations. This study tries to analyse the political aspects of nuclear programmes in foreign policies and international relations in the Persian Gulf region.
This project examines the reasons why oil & gas producer states want to acquire nuclear energy/weapons. The research examines policymaking processes in the Kingdom of Saudi Arabia, the United Arab Emirates, and Iran. Different states' power and different perceptions of the international system allow for explaining different role players in foreign policy and energy politics.
The theoretical starting point of this thesis is the Neoclassical Realism in the literature of international relations. This theory is a prominent context as a set of key beliefs and assumptions that affects or guides method selection. It offers good avenues for the analysis of energy resources in foreign policy. The theory concentrates on material power and underlines the importance of state domestic structure, as well as statesmen’s perception of the international system. These aspects create the opportunity to explain the different positions of energy resources in foreign policies of different states.
Empirically, the case-study findings have been synthesized into three key variables in which neoclassical realist linkages are particularly significant in cause and effect approach: the level of external vulnerability of the countries as the independent variable, the foreign policy induced by the distribution of power as the dependent variable, and ideological support for collective hegemony impacts on decision-makers as an intervening variable. Using three disparate neighbour cases in the Persian Gulf provides the lessons from which have formed the basis of comparative analysis.

AUTHOR: **ASIEH HAIERI YAZDI CEPMLP**, UNIVERSITY OF DUNDEE

ENERGY TRADING AND DATA DISCLOSURE: THE LEGAL BASIS OF INFORMATION EXCHANGE BETWEEN SUPERVISORY AGENCIES

Market participants trading in derivatives with a value based on an energy product (“Energy Trading”) are subjected to several legal obligations to disclose commercially sensitive data regarding their trades to supervisory agencies. It appears that supervision and enforcement benefit if such information is shared between supervisors on both a cross-border and a cross-sectoral level. This triggers questions on the legality, accountability and legitimacy of such information sharing activities and on rights and remedies market participants may have against

unlawful or unwanted disclosure.
This paper describes data disclosure from market participants active in Energy Trading to regulatory agencies at a European level in the context of cooperation between supervisory agencies. The process can be divided into two sections; the disclosure of data which relates to sector-wide market information and on the other hand data on Energy Trading activities from individuals which may relate to market abuse. The central question is which role the normative concepts of legality and legitimacy play in information sharing in the field of Energy Trading. After information sharing is explained in the light of these principles, competition law will be used as a benchmark to describe remedies for market participants against unwanted or unlawful disclosure.

AUTHOR: **LIEBRICH HIEMSTRA**, TILBURG UNIVERSITY

ADAPTIVE GOVERNANCE FOR SOLAR RADIATION MANAGEMENT

Solar Radiation Management (SRM) is a set of climate intervention techniques that are designed to increase the reflectivity of the planet, to diminish the absorption of solar radiation in the atmosphere and decrease global temperatures. These techniques are proposed as solutions to global warming but raise their own set of environmental and social issues. Because SRM schemes are likely to carry serious unintended side effects on the environment and human societies, scholars are calling for governance mechanisms to be developed. The development of governance arrangements for SRM, however, must overcome a number of challenges that traditional systems of governance appear inadequate to address. Therefore, a growing number of scholars suggest that new governance approaches are needed for SRM. 'Adaptive Governance' is one such approach for managing complex socio-ecological systems in the face of environmental change and offers a useful framework for governing the risks and uncertainties behind SRM. This paper addresses the opportunities and limits of adaptive SRM governance.

AUTHOR: **MANON SIMON**, UNIVERSITY OF TASMANIA

DATA AND PRIVACY PROTECTION (1) ROOM 3

THE ROLE OF THE CITIZEN IN LEGITIMISING REUSES OF ADMINISTRATIVE DATA IN RESEARCH

Keen to capitalise on advances in data analytics, governments are increasingly opening up their administrative data to researchers. In recognition of the new opportunities and risks fostered by such innovations, the GDPR and the UK's Digital Economy Act govern this reuse of data. These instruments justify their approach by references to the 'public interest' in such data reuse and societal expectations towards the benefits of increased knowledge. What remains unclear, however, is how far citizens share theses understandings of the 'public interest' within the law. My legislative analysis and my preliminary findings from a survey created to investigate citizens' views suggests there are divergences in the legal approach and citizens' expectations.
I argue such divergences undermine the legitimacy of these laws, due to the reliance placed on societal expectations and attitudes to justify their approach. Whilst citizens were given a role in the legislative processes of the GDPR and DEA 2017, my analysis suggests subsequent practices and more powerful actors shifted the legislative approach away from citizens' views towards a more permissive approach to data reuse. This finding is reinforced by my empirical findings, which indicate differences between what is legally permissible and societally acceptable.
In light of this, I advocate for more inclusive and responsive governance processes to better facilitate citizens'

views in determining appropriate data sharing practices. This does not entail the law completely mirroring societal views, due to the challenges of legislating when societal norms are incipient. Instead, I support processes which better include citizens in the decision-making processes that determine the permissibility of data reuse. Notions such as the 'public interest' could operate as a usefully flexible vehicle to accommodate the evolution of societal views, helping to secure the continued legitimacy of the law. This approach serves to best promote innovation whilst respecting citizens' interests.

AUTHOR: **HANNAH SMITH,** UNIVERSITY OF OXFORD

INFORMED CONSENT IN THE AGE OF ILEVIATHAN

In modern medicine, giving informed consent is an important and internationally recognized principle, intended to avoid violations of individual's autonomy and bodily integrity. As such, it is an important legal, ethical, and clinical requirement, protecting the vulnerable party, preventing harms, and cultivating trust. In this paper, I analyse whether the entry of big tech corporations into healthcare (Sharon, 2018) challenges the notion of informed consent by using a case study of Amazon's recent efforts in the sphere of health. These include Amazon's voice assistant Alexa giving out medical advice and Amazon launching its prescription drug delivery service as well as a direct-to-consumer telehealth platform offering on-demand access to a clinician. For my analysis, the concept of iLeviathan (Prainsack, 2019), which is defined as a big corporate entity to which individuals "submit some of their natural freedoms /…/ to receive something back that they consider essential", is relied upon. The paper demonstrates that the entry of big tech once again reshuffles the power in medical decision-making (Tancredi and Barsky, 1974), by making informed consent valu(at)ed less than appropriate to it (Anderson, 1990; Sharon, 2020 and 2021). This allows me to conclude that the notion of informed consent, as constructed and applied in the age of iLeviathan, is not fulfilling its functions sufficiently, namely in line with the underlying principles of medical ethics, which can transform healthcare provision in ways that could be considered problematic.

AUTHOR: **TJAŠA PETROČNIK**, TILT, TILBURG UNIVERSITY

DATA PROTECTION LAW AS A TOOL TO NEUTRALIZE DISCRIMINATORY OUTCOMES IN THE CONTEXT OF E-RECRUITING PRACTICES

In December 2000, the right to personal data protection was enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (the Charter). At that time, the impact of that 'novel' right remained relatively obscure. Over the last 20 years however, the substance of Article 8 of the Charter has grown together with the case law of the CJEU and legislative reforms in the field of data protection. The adoption of the General Data Protection Regulation (GDPR) has been yet another step in this direction. In parallel, new data-driven technologies (DDT), including algorithms developed to support or replace human-decision making, have become part of our daily life. DDT offer many opportunities for improvement in various fields, such as medical care, justice or employment. However, both old and recent scandals have also shown that, when poorly designed or badly employed, these DDT can be harmful to individuals' fundamental rights or freedoms. This paper argues that data protection legislation offers various tools to combat these harmful effects, and may thus ultimately be instrumentalised to (r)e(i)nforce other fundamental rights that are vulnerable to DDT, including the right not to be discriminated. To illustrate this point, this paper will rely on a case study on the use of automated decision-making in the field of recruitment and analyze to what extent data protection may prevent discriminatory outcomes.

AUTHOR: **FLORENCE D'ATH,** UNIVERSITÉ DE LUXEMBOURG