Course Leader

Orla Lynskey is an Assistant Professor in the Law Department at the LSE, where she teaches in the fields of Digital Rights and IT law. Her primary area of research interest is EU data protection law. Her monograph, The Foundations of EU Data Protection Law, was published with Oxford University Press in 2015. Orla is an editor of International Data Privacy Law and the European Law Blog, an Editorial Committee member of the Modern Law Review and on the Editorial Board of European Data Protection Law Review. Orla holds an LLB in Law and French from Trinity College Dublin, an LLM in EU law from the College of Europe (Bruges) and a PhD in EU law from the University of Cambridge. Before entering academia, she worked as a Competition lawyer in Brussels and as a teaching assistant at the College of Europe.

Course Outline

The Internet is a global medium for communications and commerce. As such, there has been a longstanding debate about whether it is possible to regulate the Internet and, if so, who should be responsible for such regulation and what the most appropriate form of regulation is. This issue becomes particularly contentious when nation states seek to apply their Constitutional norms and cultural values to Internet-based activities. This course will examine, through a comparative lens, how the rights to privacy, data protection and freedom of expression have been applied to the Internet. The course will take as its starting point the European Union legal framework for data protection and privacy, which has been used as a blueprint for over 100 data protection regimes worldwide, and examine alternative regimes including that in China and in the United States. The protection offered by the US First Amendment for freedom of speech will be used as a benchmark to compare the legal protection offered by the European Convention on Human Rights. Participants will be asked to draw on their own experience and knowledge of the domestic legal framework in China for comparative courses. The course will conclude by considering future perspectives for convergence between domestic legal frameworks and the challenges of internet fragmentation.
In recent years, this course has attracted students with a wide range of interests. I think this seminar would be of interest to those in private legal practice (given the extra-territorial reach of the EU’s data protection rules, entering into force in May 2018), working in government (as China has yet to develop a comprehensive legal framework for personal data processing, which may be necessary to ensure data flows between the EU and China) and civil society representatives and students interested in human rights more broadly. It may also be of interest to those working in the technology industry or at relevant regulators, although those with other backgrounds would also be welcome to attend.

**Learning Outcomes**

*By the end of this seminar, participants should have:*

- An understanding of the principles underpinning cyber-regulation and the challenges cyber-regulations entail from a legal and policy perspective
- Knowledge of the substantive legal framework applicable to communications and data processing in the digital sphere
- The ability to engage critically with the substantive legal framework (examining, for instance, whether it is desirable to regulate all personal data processing, or to distinguish between forms of permissible/impermissible speech).

**Assessment**

Assessment will be based on an assignment as a mid-term examination (worth 50% of final mark) and a final examination 2 questions in 2 hours (worth 50% of final mark).

**Topic Session Titles**

Day 1: Introduction to Cyberlaw – Who Controls the Internet and How?
Day 2: Freedom of Expression – Conflicting Visions of Free Speech (example: Defamation)
Day 3: Freedom of Expression – The Challenges of Content Regulation (Pornography; Hate and Extremism; and the role of Internet intermediaries)
Day 4: Data Protection and Privacy – An Introduction to the Legal Frameworks (EU and US)
Day 5: Data Protection and Privacy – The Right to be Forgotten and the Right to Data Portability
Day 6: Data Protection and Privacy – Profiling and Automated Decision-Making
Day 7: Data Protection and Privacy – Regulating International Data Flows (APEC comparison)
Day 8: Data Protection and Privacy – State surveillance and data retention (the Snowden revelations and beyond)
Day 9: The Role of Non-State Actors in Internet Governance
Day 10: The Fragmentation of the Internet – a challenge or inevitability?

**Main texts/ essential reading**


© LSE-PKU Summer School 2018