



Course Syllabus

Course Code LAW-320	Course Title Internet Law	ECTS Credits 6
Prerequisites N/A	Department Law	Semester Fall or Spring
Type of Course Elective	Field Law	Language of Instruction English
Level of Course 1 st Cycle	Lecturer Dr Costas Stratilatis	Year of Study 3 rd or 4 th
Mode of Delivery Conventional	Work Placement N/A	Corequisites N/A

Course Objectives:

The main objectives of the course are to:

- Introduce the students to the technological, societal and political background of the Information Society.
- Analyze the challenges that the rapid development of Information Technologies poses for law and for governance.
- Present the problematization regarding the protection (and balancing) of freedom of speech, of privacy and of other fundamental rights in the Internet.
- Clarify the legal status and the level of the legal responsibilities of the various intermediaries within the online environment.
- Provide adequate knowledge of the principles and rules of special fields of Internet regulation (such as copyright and intellectual property, electronic commerce, cybercrime, data protection, surveillance and interception, defamation and hate speech) under UK and EU law.

Learning Outcomes:

After completion of the course students are expected to be able to:

- Understand and reproduce the main challenges for law in the Information Society.

- Comprehend and appraise the problem of balancing freedom of speech with privacy and with other fundamental rights within the online environment.
- Explain and discuss the immunities of intermediaries in online regulation.
- Identify core issues which are relevant with the protection of copyright and of intellectual property in the Internet; cite, analyze and apply the relevant rules.
- Recognize the implications of e-commerce and of online contracting; cite the relevant rules.
- Assess the justificatory foundations of a specific right to data protection; cite, analyze and apply the principles, rules and rights of the data protection regime.
- Classify the types and forms of computer-related crime and of cybercrime; illustrate the legal attempts for combating cybercrime.
- Cite, analyze and apply the principles regulating lawful interception of electronic communications; identify and describe the development of the data retention regime in EU and in the UK; cite the relevant jurisprudence of the CJEU.
- Illustrate the principles and standards of the ECtHR regarding the limitation of freedom of online speech vis-a-vis the right to protection of reputation and of private life; appraise the intensity of the need to limit online hate speech.

Course Content:

1. Introducing the Internet - The Information Society and Law: aspects, challenges and perspectives – Freedom of speech, privacy, and other fundamental rights in the Internet.
2. Regulating Information Technologies: International, European and national legal frameworks – Legal harmonization – The problems of competence and of enforcement - Internet Governance.
3. Intermediaries within online regulation – The immunities under the Electronic Commerce Directive – US intermediaries immunities – The involvement of intermediaries in regulation.
4. Copyright and the Internet – Hyperlinks – Search engines - File sharing – Domain names – Trade marks.
5. Intellectual property rights in software – The Software Directive and its implementation – Patents and computer related inventions – Intellectual property rights in databases.
6. Electronic Commerce - International and European initiatives in e-commerce – Online contracting – Electronic signatures.
7. Privacy and data protection - The emergence of data protection – The European data protection regime and the EU General Data Protection Regulation – Basic concepts and fundamental principles of the data protection regime.

8. Data protection: Individual rights and remedies - Sectoral aspects of data protection – Supervision - Transborder data flows.
9. The phenomenon of computer-related crime - Cybercrime typology – The Budapest Convention - Computer forgery and fraud – Hacking - The Internet and computer pornography - Detecting and prosecuting computer crime.
10. Surveillance and interception – The problem of Internet anonymity - Data retention –The emergence and the ‘fall’ of the EU data retention regime - The Regulation of Investigatory Powers Act of 2000 – The jurisprudence of the European Court of Human Rights - Basic principles regarding interception.
11. Cyber-speech – Social media, websites, and internet news portals – Freedom of speech and its limits in the Internet – Basic principles of the European Court of Human Rights regarding defamation and protection of private life.
12. Hate speech in the Internet – The *Delfi* case in the European Court of Human Rights – Standards regarding the responsibility of news portals for comments of visitors.

Learning Activities and Teaching Methods:

Lectures, student participation, individual and group work

Assessment Methods:

Final exams, midterm exams, student participation, assignment(s)

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Information Technology Law (5 th edition)	Diane Rowland, Uta Kohl, Andrew Charlesworth	Routledge	2016	978-0415870160
Information Technology Law (8 th edition)	Ian J. Loyd	Oxford University Press	2017	978-0198787556

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Information Technology Law: The Law and Society (3 rd edition)	Andrew Murray	Oxford University Press	2016	978-0198732464
EU Internet Law (2 nd edition)	Andrej Savin	Edward Elgar Publishing Ltd	2018	978-1784717957
EU Internet Law: Regulation and Enforcement	Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou (eds)	Springer	2017	978-3319649542