University of Gdańsk

Subject card

Subject name and code	Seminar III - ROJSZCZAK Marcin , PG_00171649		
Field of study	Law		
Date of commencement of studies	October 2022	Academic year of realisation of subject	2026/2027
Education level	uniform Master's studies	Subject group	Optional subject group
Mode of study	full-time studies	Mode of delivery	at the university
Year of study	5	Language of instruction	Polish
Semester of study	10	ECTS credits	18.0
Learning profile	academic	Assessment form	credit
Conducting unit	Department of Legal Informatics -> Faculty of Law and Administration -> Rector		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. Marcin Rojszczak	
	Teachers	dr hab. Marcin Rojszczak	

Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	0.0	0.0	0.0	0.0	30.0	30
	E-learning hours included: 0.0						

Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan	Participation in consultation hours	Self-study	SUM
	Number of study hours	30	0.0	420.0	450

Subject objectives

The aim of the seminar is to deepen the student's knowledge of new technology law and to develop the ability to independently analyse and solve complex legal problems arising from the use and development of digital technologies.

The seminar focuses in particular on cybersecurity law, the regulation of artificial intelligence and other emerging technologies, data protection and privacy, the regulation of digital services and platforms, cybercrime, and the legal aspects of electronic surveillance.

The course also aims to develop the research and legal writing skills necessary to prepare a master's thesis on a topic selected in accordance with the diploma procedure applicable to the Law programme. The student develops the ability to formulate legal problems, search for and critically analyse sources, interpret legal provisions, analyse case law, construct legal arguments, and independently prepare written legal analyses.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[PRAWOJ5_WK12] He/she has knowledge of occupational health and safety in public administration institutions	The student knows the basic principles of occupational health and safety relevant to professional and research activities in public administration institutions, in particular in relation to the use of digital systems and tools.	[SW1] oral statement/ conversation/discussion
[PRAWOJ5_UW07] He/she has the skills in understanding and analyzing social phenomena and utilizing this analysis in his/her professional work.	The student is able to analyse the social consequences of the development and use of digital technologies and apply the results of that analysis to the assessment of existing and proposed legal solutions.	[SU1] oral statement/conversation/ discussion
[PRAWOJ5_WG04] He/she knows the system of Polish law, mutual connections within the system and connections of Polish law with the European Union law and international law	The student understands the relationship between Polish law, European Union law, and international law in the regulation of digital technologies and is able to determine its relevance to specific legal problems.	[SW5] implementation of a problem task
[PRAWOJ5_UW03] The graduate demonstrates deepened skills of using complex theoretical points of view to analyze, interpret and plan strategies of legal activities; solves concrete problems connected with the creation, application and interpretation of legal regulations, anticipates the course of their solution and predicts the effects of planned activities	The student is able to apply advanced theoretical approaches and legal methods to problems of new technology law, propose possible legal solutions, and assess their potential consequences.	[SU3] text preparation/written work
[PRAWOJ5_KK02] He/she is aware of the necessity to widen professional competences and qualifications, to improve skills, is able to indicate the direction of own development and education independently in widened and deepened way	The student is able to identify areas requiring further study and independently determine directions for the development of their competences in the field of new technology law.	[SK5] implementation of a problem task
[PRAWOJ5_WG05] The graduate demonstrates systematic knowledge about the types of legal relations and the governing regularities	The student has structured knowledge of legal relationships arising in the digital environment, in particular between users, providers of services and technologies, businesses, and public authorities.	[SW5] implementation of a problem task
[PRAWOJ5_WG02] He/she knows wide terminology and concepts in the scope of law and connected disciplines	The student knows and correctly uses terminology relevant to new technology law, in particular cybersecurity law, data protection and privacy, artificial intelligence regulation, and digital services law.	[SW2] presentation/project/paper/ report
[PRAWOJ5_UW02] The graduate utilizes theoretical knowledge in legal science and the connected academic disciplines to analyze and interpret complex legal issues	The student is able to integrate knowledge from different branches of law and related disciplines in order to analyse and interpret complex legal problems concerning digital technologies.	[SU2] presentation/project/paper/ report
[PRAWOJ5_KR07] The graduate is ready to take up professional challenges, takes up efforts and is persistent in the implementation of individual and group activities in the creation, application or interpretation of legal regulations and related sciences	The student is prepared to independently and systematically undertake complex analytical tasks in the field of new technology law and to participate in discussions and work on legal problems requiring in-depth analysis.	[SK2] presentation/project/paper/ report
[PRAWOJ5_UK08] The graduate has wide skills to prepare written works connected with the work of a lawyer in Polish and foreign language	The student is able to prepare well-structured and substantively sound written legal analyses and academic papers on new technology law, using both Polish- and foreign-language sources.	[SU3] text preparation/written work
[PRAWOJ5_KK01] The graduate is deeply aware of the level of his/her knowledge and skills, and also understands the need of lifelong learning	The student is able to critically assess their own knowledge and skills and understands the need for their continuous development in response to rapid technological and regulatory change.	[SK1] oral statement/conversation/ discussion

Course outcome	Subject outcome	Method of verification
[PRAWOJ5_WG01] The graduate demonstrates deepened and systematic knowledge about the character of legal science, its place in the system of sciences and mutual relations.	The student has in-depth knowledge of the nature of new technology law, its place within legal sciences, and its links with other disciplines, in particular computer science, security studies, and social sciences.	[SW1] oral statement/ conversation/discussion
[PRAWOJ5_UW01] He/she has advanced skills in observation and interpretation of social phenomena, analyzes their connections with various areas, activity of legal science and the related disciplines	The student is able to identify and interpret social and technological phenomena associated with digitalisation and analyse their links with different branches of law and other academic disciplines.	[SU5] implementation of a problem task
[PRAWOJ5_WG07] The graduate knows methods and tools, including techniques of data and information acquisition, as well as research methods appropriate for the field of study and the related disciplines	The student knows research methods appropriate to legal studies and tools for obtaining and analysing information used in research on new technology law, including methods for analysing legal acts, case law, and academic literature.	[SW5] implementation of a problem task

Subject contents

The seminar focuses on the legal aspects of the development and use of digital technologies and on the evolution of the contemporary regulatory framework for the information society.

The course covers, in particular: the system and sources of new technology law; the relationship between national law, European Union law and international law in the regulation of the digital environment; EU and national cybersecurity law; the security of digital products and services; the regulation of artificial intelligence and other emerging technologies; privacy and data protection; the regulation of digital services and platforms; liability for illegal online content; legal aspects of cybercrime and electronic evidence; confidentiality of communications and encryption; electronic surveillance; and the protection of fundamental rights in the digital environment.

The seminar also covers legal research skills and methodology, including the formulation of research problems; application of research methods appropriate to legal studies; searching for, selecting and critically analysing academic literature, legal acts, official documents and case law; use of national, EU and international legal and academic databases; legal interpretation and construction of legal arguments; preparation of problem-oriented analyses and other academic texts; principles of citation and source documentation; and academic integrity, including the appropriate use of artificial intelligence tools.

As part of preparation for the diploma process, the seminar also addresses the principles of independently preparing a master's thesis on an assigned topic, including identifying the relevant legal problem, selecting appropriate source materials, developing the structure of the thesis, formulating arguments and conclusions, and organising the research process.

Prerequisites and co-requisites

Knowledge of the fundamental legal institutions and of the functioning of the Polish and European Union legal systems, in particular the basics of constitutional law, European Union law, administrative law, civil law and criminal law. Ability to independently search for and analyse legal acts, case law and legal literature.

A command of English sufficient to use academic literature, European Union law, European case law and materials published by international institutions is recommended.

Specialist technical knowledge of computer science or cybersecurity is not required; relevant technical issues are discussed to the extent necessary for the proper analysis of legal problems.

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Timely completion of seminar assignments in accordance with the instructor's requirements, including in particular the preparation of legal analyses, completion of problem-based tasks, presentation of selected issues and participation in substantive discussions.	51.0%	100.0%

<table>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td>1. C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, wyd. 2, Wolters Kluwer, Warszawa 2023.
2. K. Flaga-Gieruszyńska, J. Gołaczyński (red.), Prawo nowych technologii, Wolters Kluwer, Warszawa 2021.
3. D. Lubasz, M. Namysłowska (red.), Akt o usługach cyfrowych. Komentarz, Wolters Kluwer, Warszawa 2024.
4. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra (red.), AI Act. Akt w sprawie sztucznej inteligencji. Komentarz, Wolters Kluwer, Warszawa 2025.
5. A. Murray, Information Technology Law: The Law and Society, 5th ed., Oxford University Press, 2023.
6. M.G. Porcedda, Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, Hart Publishing, 2022.</td></tr>
<tr><td>Supplementary literature</td><td>1. B. Fischer, A. Pązik, M. Świerczyński (red.), Prawo sztucznej inteligencji i nowych technologii 3, Wolters Kluwer, Warszawa 2024.
2. F. Wilman, S.L. Kalėda, P.-J. Loewenthal, The EU Digital Services Act, Oxford University Press, 2024.
3. M. Finck, The EU Artificial Intelligence Act: A Commentary, Oxford University Press, 2026.
4. M. Rojszczak, Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective, Routledge, 2024.
5. M. Rojszczak, Beyond Hate Speech: Clearly Unlawful Content in EU Digital Law, Routledge, 2026.
6. Current legal acts, case law of the CJEU and the ECHR, documents issued by European Union institutions, and up-to-date academic literature concerning the topics discussed during the seminar.</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="2">Examples of research areas:

1. The architecture of EU digital law: the relationship between the AI Act, Digital Services Act, Digital Markets Act, Data Act, NIS2 and Cyber Resilience Act.
2. The European cybersecurity regulatory model after NIS2: the relationship between horizontal and sector-specific regulation.
3. NIS2 in the Polish cybersecurity system: regulatory obligations, supervision and liability.
4. Cybersecurity by design and manufacturers' responsibility for the security of products with digital elements under the Cyber Resilience Act.
5. European cybersecurity certification under the Cybersecurity Act: legal nature, functions and future development.
6. The risk-based model of artificial intelligence regulation: the AI Act, fundamental rights and innovation.
7. General-purpose AI (GPAI) models: providers' obligations and the regulation of systemic risk under the AI Act.
8. Artificial intelligence and copyright law: the use of protected works for model training and the legal status of AI-generated content.
9. Liability of intermediary service providers and the moderation of illegal content under the Digital Services Act.
10. Systemic risks of online platforms, freedom of expression and the protection of fundamental rights under the DSA.
11. Regulation of gatekeepers under the Digital Markets Act: between competition law and ex ante regulation of digital markets.
12. Access to and use of data under the Data Act: new limits of control over data generated by connected products.
13. The relationship between the GDPR and the AI Act: personal data protection, profiling and automated decision-making.
14. Confidentiality of electronic communications, data retention and electronic surveillance under EU law and the ECHR.
15. Cross-border access to electronic evidence and user data - the e-Evidence framework and fundamental rights.
16. End-to-end encryption and the state's obligations to combat serious crime and protect individual rights.
17. Cybercrime under Polish, EU and international law: jurisdictional challenges and effective prosecution of cross-border offences.
18. Quantum computing and legal obligations concerning migration to post-quantum cryptography.</td></tr>
<tr><td>Work placement</td><td colspan="2">Not applicable</td></tr>
</table>

Document generated electronically. Does not require a seal or signature.