Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Seminarium I - ROJSZCZAK Marcin , PG_00171647		
Kierunek studiów	Prawo (O)		
Data rozpoczęcia studiów	październik 2022 r.	Rok akademicki realizacji przedmiotu	2025/2026
Poziom kształcenia	jednolite magisterskie	Grupa zajęć	Grupa zajęć fakultatywnych
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	4	Język wykładowy	polski
Semestr studiów	8	Liczba punktów ECTS	4.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji -> Katedra Informatyki Prawniczej		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. Marcin Rojszczak	
	Prowadzący zajęcia z przedmiotu	dr hab. Marcin Rojszczak	

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	0.0	0.0	0.0	0.0	30.0	30

W tym liczba godzin zajęć na odległość: 0.0

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	30	0.0	70.0	100

Cel przedmiotu

Celem seminarium jest pogłębienie wiedzy studenta z zakresu prawa nowych technologii oraz rozwijanie umiejętności samodzielnej analizy i rozwiązywania złożonych problemów prawnych związanych z funkcjonowaniem technologii cyfrowych.

Seminarium koncentruje się w szczególności na prawie cyberbezpieczeństwa, regulacji sztucznej inteligencji i innych technologii przełomowych, ochronie danych i prywatności, regulacji usług i platform cyfrowych, cyberprzestępczości oraz prawnych aspektach inwigilacji elektronicznej.

Celem zajęć jest również rozwijanie warsztatu badawczego i umiejętności pisarstwa prawniczego niezbędnych do przygotowania pracy magisterskiej na temat wyłoniony zgodnie z procedurą dyplomowania obowiązującą na kierunku Prawo. Student doskonali umiejętność formułowania problemów prawnych, wyszukiwania i krytycznej analizy źródeł, wykładni przepisów, analizy orzecznictwa, konstruowania argumentacji oraz samodzielnego przygotowywania pisemnych analiz prawnych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[PRAWOJ5_UK08] posiada pogłębioną umiejętność przygotowania różnych prac pisemnych w języku polskim i języku obcym związany z wykonywaną pracą zawodową	Student potrafi przygotowywać uporządkowane i poprawne merytorycznie pisemne analizy prawne i opracowania naukowe dotyczące problematyki prawa nowych technologii, z wykorzystaniem źródeł polsko- i obcojęzycznych.	[SU3] opracowanie tekstowe/ praca pisemna
[PRAWOJ5_KR07] jest gotowy do podejmowania wyzwań zawodowych, podejmuje trud i odznacza się wytrwałością w realizacji indywidualnych jak i zespołowych działań w zakresie prawa i nauk pokrewnych	Student jest gotowy do samodzielnego i systematycznego podejmowania złożonych zadań analitycznych z zakresu prawa nowych technologii oraz do udziału w dyskusji i pracy nad problemami prawnymi wymagającymi pogłębionej analizy.	[SK2] prezentacja/projekt/referat/ raport
[PRAWOJ5_UW02] potrafi wykorzystywać i integrować wiedzę teoretyczną z zakresu prawa oraz powiązanych z nią dyscyplin naukowych w celu analizowania i interpretowania złożonych problemów prawnych	Student potrafi łączyć wiedzę z różnych gałęzi prawa oraz dyscyplin powiązanych w celu analizy i interpretacji złożonych problemów prawnych dotyczących technologii cyfrowych.	[SU2] prezentacja/projekt/referat/ raport
[PRAWOJ5_WG02] zna terminologię oraz pojęcia z zakresu prawa i dziedzin z nim związanych w stopniu rozszerzonym	Student zna i prawidłowo posługuje się terminologią właściwą dla prawa nowych technologii, w szczególności prawa cyberbezpieczeństwa, ochrony danych i prywatności, regulacji sztucznej inteligencji oraz usług cyfrowych.	[SW2] prezentacja/projekt/referat/ raport
[PRAWOJ5_WG05] ma uporządkowaną wiedzę o rodzajach stosunków prawnych i o rządzących nimi prawidłowościami	Student ma uporządkowaną wiedzę o stosunkach prawnych powstających w środowisku cyfrowym, w szczególności między użytkownikami, dostawcami usług i technologii, przedsiębiorcami oraz organami władzy publicznej.	[SW5] realizacja zadania problemowego
[PRAWOJ5_WG07] zna metody i narzędzia, w tym techniki pozyskiwania danych i informacji oraz metody badawcze, właściwe dla nauk prawnych oraz innych powiązanych dyscyplin, w tym dyscyplin z zakresu innych dziedzin naukowych	Student zna metody badawcze właściwe dla nauk prawnych oraz narzędzia pozyskiwania i analizy informacji wykorzystywane w badaniach nad prawem nowych technologii, w tym metody analizy aktów prawnych, orzecznictwa i literatury naukowej.	[SW5] realizacja zadania problemowego
[PRAWOJ5_KK01] ma pogłębioną świadomość poziomu swojej wiedzy i umiejętności, a także rozumie potrzebę uczenia się przez całe życie	Student potrafi krytycznie oceniać poziom własnej wiedzy i umiejętności oraz rozumie potrzebę ich stałego rozwijania w związku z dynamicznymi zmianami technologii i regulacji prawnych.	[SK1] wypowiedź ustna/rozmowa/ dyskusja
[PRAWOJ5_KK02] ma świadomość konieczności poszerzania kompetencji i kwalifikacji zawodowych, jak również doskonali umiejętności, potrafi samodzielnie wyznaczać kierunki własnego rozwoju i kształcenia w stopniu rozszerzonym i pogłębionym	Student potrafi identyfikować obszary wymagające pogłębienia wiedzy oraz samodzielnie wyznaczać kierunki dalszego rozwoju kompetencji w zakresie prawa nowych technologii.	[SK5] realizacja zadania problemowego
[PRAWOJ5_WK12] ma wiedzę o bezpieczeństwie i higienie pracy w instytucjach administracji publicznej		
[PRAWOJ5_UW03] potrafi posługiwać się złożonymi ujęciami teoretycznymi w celu analizowania, interpretowania oraz projektowania strategii działań prawniczych; potrafi generować rozwiązania konkretnych problemów związanych z prawem oraz prognozować przebieg ich rozwiązania i przewidywać skutki planowanych działań	Student potrafi stosować pogłębione ujęcia teoretyczne i metody prawnicze do analizy problemów prawa nowych technologii, proponować możliwe rozwiązania prawne oraz oceniać ich potencjalne skutki.	[SU3] opracowanie tekstowe/ praca pisemna

	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[PRAWOJ5_WG01] ma pogłębioną i uporządkowaną wiedzę o charakterze nauk prawnych, ich miejscu w systemie nauk i relacjach do innych nauk	Student ma pogłębioną wiedzę o charakterze prawa nowych technologii, jego miejscu w systemie nauk prawnych oraz jego powiązaniach z innymi dyscyplinami, w szczególności informatyką, naukami o bezpieczeństwie i naukami społecznymi.	[SW1] wypowiedź ustna/rozmowa/ dyskusja
	[PRAWOJ5_UW01] posiada pogłębione umiejętności obserwacji i interpretacji zjawisk społecznych, analizuje ich powiązania z różnymi obszarami, gałęziami prawa i nauk pokrewnych	Student potrafi identyfikować i interpretować społeczne i technologiczne zjawiska związane z cyfryzacją oraz analizować ich powiązania z różnymi gałęziami prawa i innymi dyscyplinami naukowymi.	[SU5] realizacja zadania problemowego
	[PRAWOJ5_WG04] zna system polskiego prawa, wzajemne powiązania wewnątrz tego sytemu oraz powiązania polskiego prawa z prawem Unii Europejskiej i prawem międzynarodowym	Student zna relacje między prawem polskim, prawem Unii Europejskiej i prawem międzynarodowym w zakresie regulacji technologii cyfrowych oraz potrafi określić ich znaczenie dla rozwiązywania konkretnych problemów prawnych.	[SW5] realizacja zadania problemowego
	[PRAWOJ5_UW07] posiada rozwinięte umiejętność rozumienia i analizowania zjawisk społecznych oraz wykorzystywanie tej analizy w pracy zawodowej	Student potrafi analizować społeczne skutki rozwoju i stosowania technologii cyfrowych oraz wykorzystywać wyniki tej analizy do oceny obowiązujących i projektowanych rozwiązań prawnych.	[SU1] wypowiedź ustna/rozmowa/ dyskusja

Treści przedmiotu	Problematyka seminarium koncentruje się na prawnych aspektach rozwoju i stosowania technologii cyfrowych oraz kształtowaniu współczesnego modelu regulacji społeczeństwa informacyjnego. W ramach zajęć omawiane są w szczególności: system i źródła prawa nowych technologii; relacje między prawem krajowym, prawem Unii Europejskiej i prawem międzynarodowym w regulacji środowiska cyfrowego; unijne i krajowe prawo cyberbezpieczeństwa; bezpieczeństwo produktów i usług cyfrowych; regulacja sztucznej inteligencji i innych technologii przełomowych; ochrona prywatności i danych osobowych; regulacja usług i platform cyfrowych; odpowiedzialność za treści bezprawne w Internecie; prawne aspekty cyberprzestępczości i elektronicznego materiału dowodowego; poufność komunikacji i szyfrowanie; inwigilacja elektroniczna oraz ochrona praw podstawowych w środowisku cyfrowym. Seminarium obejmuje również zagadnienia warsztatu naukowego prawnika: formułowanie problemów badawczych; stosowanie metod badawczych właściwych dla nauk prawnych; wyszukiwanie, selekcję i krytyczną analizę literatury, aktów prawnych, dokumentów urzędowych i orzecznictwa; korzystanie z krajowych, unijnych i międzynarodowych baz informacji prawnej i naukowej; wykładnię prawa i konstruowanie argumentacji prawniczej; przygotowywanie analiz problemowych i innych tekstów naukowych; zasady cytowania i dokumentowania źródeł oraz zasady rzetelności naukowej, w tym właściwego wykorzystania narzędzi sztucznej inteligencji. W ramach przygotowania do procesu dyplomowania omawiane są również zasady samodzielnego opracowania pracy magisterskiej na zadany temat, w tym identyfikacja problemu prawnego, dobór materiału źródłowego, konstruowanie struktury pracy, formułowanie tez i wniosków oraz organizacja pracy badawczej.
Wymagania wstępne i dodatkowe	Znajomość podstawowych instytucji prawa oraz zasad funkcjonowania polskiego i unijnego systemu prawnego, w szczególności podstaw prawa konstytucyjnego, prawa Unii Europejskiej, prawa administracyjnego, cywilnego i karnego. Umiejętność samodzielnego wyszukiwania i analizy aktów prawnych, orzecznictwa i literatury prawniczej. Znajomość języka angielskiego umożliwiająca korzystanie z literatury naukowej, prawa Unii Europejskiej, orzecznictwa europejskiego oraz materiałów instytucji międzynarodowych jest zalecana. Nie jest wymagana specjalistyczna wiedza techniczna z zakresu informatyki lub cyberbezpieczeństwa; niezbędne zagadnienia techniczne omawiane są w zakresie koniecznym do prawidłowej analizy problemów prawnych.

<table>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="2"><table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Terminowa i zgodna z wymaganiami prowadzącego realizacja zadań seminaryjnych, obejmujących w szczególności przygotowanie analiz prawnych, realizację zadań problemowych, prezentację wybranych zagadnień oraz udział w dyskusji.</td><td>51.0%</td><td>100.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</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>Uzupełniająca lista lektur</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. Aktualne akty prawne, orzecznictwo TSUE i ETPC, dokumenty instytucji Unii Europejskiej oraz bieżąca literatura naukowa dotycząca problematyki omawianej podczas seminarium.</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
</table>

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Przykładowe obszary badawcze: **1. Architektura unijnego prawa cyfrowego**: wzajemne relacje AI Act, Digital Services Act, Digital Markets Act, Data Act, NIS2 i Cyber Resilience Act. **2. Europejski model regulacji cyberbezpieczeństwa po NIS2**: relacje między regulacją horyzontalną i sektorową. **3. NIS2 w polskim systemie cyberbezpieczeństwa**: zakres obowiązków regulacyjnych, nadzór i odpowiedzialność. **4. Cybersecurity by design** i odpowiedzialność producentów za bezpieczeństwo produktów z elementami cyfrowymi w świetle Cyber Resilience Act. **5. Europejska certyfikacja cyberbezpieczeństwa** w świetle Cybersecurity Act: charakter prawny, funkcje i kierunki rozwoju. **6. Model regulacji sztucznej inteligencji oparty na ryzyku**: AI Act a ochrona praw podstawowych i rozwój innowacji. **7. Modele sztucznej inteligencji ogólnego przeznaczenia (GPAI):** obowiązki dostawców i regulacja ryzyka systemowego w AI Act. **8. Sztuczna inteligencja a prawo autorskie**: wykorzystywanie chronionych utworów do trenowania modeli i status treści generowanych przez AI. **9. Odpowiedzialność dostawców usług pośrednich** oraz moderowanie treści bezprawnych w świetle Digital Services Act. **10. Ryzyka systemowe platform internetowych** a wolność wypowiedzi i ochrona praw podstawowych w świetle DSA. **11. Regulacja strażników dostępu (gatekeepers)** w Digital Markets Act: pomiędzy prawem konkurencji a regulacją ex ante rynków cyfrowych. **12. Dostęp do danych i zasady ich wykorzystywania w świetle Data Act**: nowe granice kontroli nad danymi generowanymi przez produkty połączone. **13. Relacje między RODO i AI Act**: ochrona danych osobowych, profilowanie i zautomatyzowane podejmowanie decyzji. **14. Poufność komunikacji elektronicznej**, retencja danych i inwigilacja elektroniczna w świetle standardów prawa Unii Europejskiej i EKPC. **15. Transgraniczny dostęp do dowodów elektronicznych i danych użytkowników** - system e-Evidence a prawa podstawowe. **16. Szyfrowanie end-to-end** a obowiązki państwa w zakresie zwalczania poważnej przestępczości i ochrony praw jednostki. **17. Cyberprzestępstwa w prawie polskim, unijnym i międzynarodowym**: problemy jurysdykcji i skutecznego ścigania czynów transgranicznych. **18. Rozwój komputerów kwantowych** a prawne obowiązki w zakresie migracji do kryptografii postkwantowej.
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.