



## WYDZIAŁ PRAWA i ADMINISTRACJI

Uniwersytet Łódzki

### Ramowy program studiów podyplomowych „Prawo nowych technologii – obsługa biznesu i sektora publicznego”

#### Moduł I. Otoczenie regulacyjne nowych technologii i podstawy IT dla prawników

##### 14 godzin

- 1) Charakterystyka regulacji z zakresu nowych technologii w prawie unijnym i w prawie krajowym
- 2) Prawo prywatne międzynarodowe w sektorze IT
- 3) Prawnik w świecie IT – podstawowe pojęcia ze sfery technologii
- 4) LegalResearch i LegalTech - technologie wspierające pracę prawnika, digitalizacja, narzędzia informatyczne, wdrożenie oprogramowania
- 5) Technologie zwiększające prywatność i bezpieczeństwo
- 6) Doręczenia elektroniczne

#### Moduł II Prawne aspekty korzystania z nowych technologii

##### 73 godziny

- 1) Prawna ochrona programów komputerowych
- 2) Umowy dotyczące programów komputerowych oraz wdrożenia systemów informatycznych
- 3) Prawne aspekty funkcjonowania aplikacji
- 4) Blockchain, Smart kontrakt, kontrola algorytmów
- 5) Tokenizacja, kryptowaluty
- 6) Praktyczne aspekty wykorzystania mediów społecznościowych oraz wolność wypowiedzi i dobra osobiste w Internecie
- 7) Praktyczne aspekty wykorzystania chmur obliczeniowych
- 8) Zamówienia na usługi chmurowe i dotyczące systemów informatycznych
- 9) Prawo autorskie przy prowadzeniu stron internetowych i kont w mediach społecznościowych
- 10) Prawne uwarunkowania obrotu dobrami wirtualnymi i obrót NFT
- 11) Prawo dronów
- 12) Nowe technologie w zatrudnieniu
- 13) Obsługa prawna procesu produkcji i dystrybucji gier oraz utrzymanie gry online
- 14) Prawne aspekty streamingu
- 15) Prawne aspekty metaversum
- 16) Ochrona dzieci w Internecie
- 17) Ochrona patentowa rozwiązań wykorzystujących nowe technologie
- 18) Ochrona danych osobowych, profilowanie, biometria, *privacy by design i privacy by default*, odpowiedzialność, transfery
- 19) Otwarte dane i Data Act

## **Moduł III Cyberbezpieczeństwo**

**35 godzin**

- 1) Mapowanie legislacji w zakresie cyberbezpieczeństwa
- 2) Podstawowe definicje z zakresu cyberbezpieczeństwa i cyberprzestępczości
- 3) NIS2, DORA, CRA – cyberbezpieczeństwo horyzontalne
- 4) Cyberprzestępstwa, oszustwa, przestępstwa komputerowe, odpowiedzialność, incydenty naruszające dostępność zasobów na przykładzie ataków DoS, DDoS, ransomware
- 5) Pranie pieniędzy pochodzących z przestępstwa
- 6) Pojęcie dowodów elektronicznych, zadania organów ścigania w sprawach z zakresu cyberprzestępczości
- 7) Wykorzystanie sztucznej inteligencji i innych technologii przełomowych w sprawach z zakresu cyberprzestępczości
- 8) Warsztat hakera - jak wyglądają i do czego służą urządzenia hakerskie
- 9) Tło standaryzacyjne w cyberbezpieczeństwie – kluczowe standardy i normy dotyczące cyberbezpieczeństwa na poziomie krajowym i międzynarodowym
- 10) Cyberbezpieczeństwo w sektorach regulowanych (finansowy, medyczny, energetyczny, itd.)
- 11) 5G, AI, IoT oraz inne wyzwania dla cyberbezpieczeństwa
- 12) Zarządzanie i zgłaszanie incydentów cyberbezpieczeństwa

## **Moduł IV Sztuczna inteligencja w obsłudze biznesu i sektora publicznego**

**50 godzin**

- 1) Wstęp do sztucznej inteligencji i otoczenie prawno-regulacyjne
- 2) Obszar etyczny stosowania AI
- 3) Przejrzystość i wyjaśnialność AI
- 4) Analiza ryzyka w związku z wdrożeniem, AI wysokiego ryzyka, zarządzanie ryzykiem AI na przykładzie NIST AI RMF
- 5) Dane (osobowe i nieosobowe) w systemach AI
- 6) Obowiązki dostawców i użytkowników systemów AI
- 7) Zakazane praktyki w zakresie sztucznej inteligencji
- 8) Normy, ocena zgodności, certyfikaty rejestracja, AI Governance – jak bezpiecznie zarządzać systemami sztucznej inteligencji na przykładzie normy ISO 42001:2033
- 9) Compliance korzystającego z systemów AI i dostawcy narzędzi
- 10) Prowadzenie dokumentacji związanej z wykorzystywaniem systemów AI
- 11) Sztuczna inteligencja a prawa własności intelektualnej
- 12) Zasady odpowiedzialności za działania sztucznej inteligencji
- 13) Wykorzystanie sztucznej inteligencji w ochronie danych osobowych - aspekty prawne, techniczne i organizacyjne
- 14) Wykorzystanie sztucznej inteligencji w administracji publicznej
- 15) Sztuczna inteligencja w zatrudnieniu, sztuczna inteligencja w działalności sądów, w sektorze bankowym i ubezpieczeniowym oraz w sektorze medycznym

## **Moduł V Prawo platform internetowych oraz prawne aspekty handlu elektronicznego i digital marketingu**

**40 godzin**

- 1) Europejskie i krajowe podstawy prawne handlu elektronicznego i regulacje dotyczące platform internetowych
- 2) Prawne aspekty działania platform internetowych w akcie o usługach cyfrowych oraz w akcie o rynkach cyfrowych

- 3) Nieuczciwe praktyki rynkowe w handlu elektronicznym, dark patterns
- 4) Płatności elektroniczne i usługi fin-tech
- 5) Modele e-sprzedaży i obowiązki e-sprzedawcy, umowy w e-handlu i ich wpływ na treść zobowiązania, ograniczenia (produkty sensytywne)
- 6) Ochrona konsumentów w handlu elektronicznym
- 7) E-marketing i telemarketing (użycie e-maila, SMS/MMS, telefonu i automatycznych systemów wywołujących dla celów marketingu bezpośredniego i przesyłania informacji handlowych)
- 8) Reklama internetowa, przejrzystość, plasowanie, systemy rekomendacji na tle nowych regulacji - DSA i DMA, dyrektywy cyfrowej i Omnibus
- 9) Dane osobowe, pliki cookies, narzędzia analityczne i marketingowe, systemy śledzące



# WYDZIAŁ PRAWA i ADMINISTRACJI

## Uniwersytet Łódzki