STRESZCZENIE ROZPRAWY DOKTORSKIEJ

„Zwalczanie cyberprzestępczości na przykładzie oszustwa komputerowego - problemy dogmatyczne i dowodowe w postępowaniu przygotowawczym" - autorstwa mgr Krystiana Bartosza

Przedmiotem rozprawy doktorskiej jest kompleksowa analiza zjawiska cyberprzestępczości ze szczególnym uwzględnieniem przestępstwa oszustwa komputerowego, ujętego w art. 287 Kodeksu karnego, a także ocena skuteczności obowiązujących regulacji prawnych oraz praktyki organów ścigania w zakresie przeciwdziałania temu zjawisku. Celem pracy jest nie tylko charakterystyka współczesnych zagrożeń w cyberprzestrzeni, lecz również sformułowanie postulatów *de lege ferenda* zmierzających do zwiększenia efektywności zwalczania cyberprzestępczości.

W pierwszej części rozprawy przedstawiono podstawy teoretyczne badanej problematyki, obejmujące definicje cyberprzestrzeni oraz cyberprzestępczości, a także analizę przestępstw przeciwko bezpieczeństwu cybernetycznemu ujętych w polskim Kodeksie karnym. Szczególną uwagę poświęcono przestępstwu oszustwa komputerowego (art. 287 k.k.), jak również czynom zabronionym związanym z nieuprawnionym dostępem do informacji (art. 267 k.k.), utrudnianiem dostępu do danych (art. 268 i 268a k.k.) oraz sabotażem komputerowym i przestępstwami związanymi z tworzeniem narzędzi przestępczych (art. 269 i 269b k.k.). Analiza ta pozwoliła na identyfikację luk oraz problemów interpretacyjnych w obowiązującym stanie prawnym.

W dalszej części pracy omówiono najczęściej występujące sposoby popełniania przestępstw w cyberprzestrzeni, w tym hacking, cracking, sniffing, phishing, skimming, ransomware oraz cryptojacking. Przedstawiono ich mechanizmy działania, skalę występowania oraz znaczenie dla praktyki ścigania przestępstw, wskazując na dynamiczny rozwój technik wykorzystywanych przez sprawców.

Istotnym elementem rozprawy jest analiza porównawcza regulacji prawnych dotyczących cyberprzestępczości w wybranych systemach prawnych, takich jak Stany Zjednoczone, Wielka Brytania, Czechy, Włochy, Francja, Hiszpania, Japonia oraz Niemcy. Przeprowadzone badania komparatystyczne umożliwiły ocenę rozwiązań przyjętych w Polsce na tle innych państw oraz identyfikację potencjalnych kierunków zmian legislacyjnych.

W pracy dokonano również oceny stanu cyberbezpieczeństwa w Polsce i Unii Europejskiej na podstawie raportów Najwyższej Izby Kontroli, CERT Polska oraz ENISA Threat Landscape. Analiza ta została uzupełniona o omówienie konkretnych incydentów cyberbezpieczeństwa, takich jak kampanie phishingowe, ataki ransomware, wykorzystanie złośliwego oprogramowania, ataki DDoS czy ataki na portfele kryptowalutowe. Pozwoliło to na zobrazowanie rzeczywistej skali i charakteru zagrożeń.

Kluczową część rozprawy stanowią rozważania dotyczące kierunków zmian legislacyjnych w zakresie przestępstwa oszustwa komputerowego. Zaproponowano m.in. wprowadzenie karalności przygotowania do tego przestępstwa, rozszerzenie zakresu kryminalizacji w art. 287 k.k. poprzez wprowadzenie typu kwalifikowanego, a także zmiany dotyczące penalizacji kradzieży tożsamości. Równolegle podjęto analizę możliwości rozszerzenia uprawnień organów ścigania w zakresie czynności pozaprocesowych, przy jednoczesnym wskazaniu konieczności wprowadzenia mechanizmów zabezpieczających przed nadużyciami.

W części metodologicznej określono problem badawczy, hipotezy oraz zastosowane metody i techniki badawcze. Badania empiryczne obejmowały wywiady z funkcjonariuszami Centralnego Biura Zwalczania Cyberprzestępczości oraz biegłymi sądowymi z zakresu informatyki śledczej. Uzupełnieniem badań była analiza danych statystycznych pochodzących z Policji oraz prokuratury, obejmujących lata 2014–2024, co pozwoliło na ocenę dynamiki cyberprzestępczości, w szczególności oszustw komputerowych, w ujęciu krajowym, europejskim i globalnym.

Przeprowadzone badania potwierdziły, że obowiązujące regulacje prawne nie w pełni odpowiadają na wyzwania związane z rozwojem cyberprzestępczości, a skuteczność działań organów ścigania jest ograniczona m.in. przez trudności w identyfikacji sprawców oraz niedostosowanie narzędzi prawnych do współczesnych realiów technologicznych. Wnioski płynące z rozprawy wskazują na konieczność wprowadzenia zmian legislacyjnych oraz zwiększenia wykorzystania nowoczesnych technologii w procesie wykrywania i ścigania przestępstw.

Rozprawa stanowi próbę kompleksowego ujęcia problematyki oszustw komputerowych w kontekście współczesnych zagrożeń cybernetycznych oraz stanowi podstawę do dalszych badań nad doskonaleniem systemu prawnego i praktyki jego stosowania w obszarze cyberprzestępczości.