dr hab. Wojciech Filipkowski, prof. UwB
Katedra Prawa Karnego i Kryminologii
Wydział Prawa
Uniwersytet w Białymstoku

Recenzja rozprawy doktorskiej mgr Krystiana Bartosza
pt. „Zwalczanie cyberprzestępczości na przykładzie oszustwa komputerowego – problemy dogmatyczne i dowodowe w postępowaniu przygotowawczym"

Przedstawioną do oceny rozprawę doktorską mgr Krystiana Bartosza oceniam pozytywnie. W związku z tym, może ona stanowić podstawę podejmowania dalszych procedur w jego przewodzie doktorskim.

I. Ocena wyboru tematu rozprawy doktorskiej

Wybór tematu należy ocenić pozytywnie. Zgodnie z art. 187 ust. 1–2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, rozprawa doktorska musi prezentować ogólną wiedzę teoretyczną kandydata w dyscyplinie, umiejętność samodzielnego prowadzenia pracy naukowej oraz stanowić oryginalne rozwiązanie problemu naukowego. Podkreśla się także, że oryginalność odnosi się nie do samego problemu, lecz do sposobu jego rozwiązania – problem może być znany, jednak metoda i wynik jego rozstrzygnięcia muszą wnosić nową wartość poznawczą. Z taką sytuację mamy do czynienia w przypadku tej rozprawy. Analizowany temat spełnia ten warunek formalny: przestępstwo oszustwa komputerowego (art. 287 k.k.) jest przedmiotem znanym doktrynie od lat, natomiast Doktorant proponuje nowe podejście – ujęcie oszustwa komputerowego jako procesu wieloetapowego, rozłożonego i w czasie, i pod względem podmiotowym, a nie zdarzenia punktowego. Ponadto, uzupełnia tę perspektywę o funkcjonowanie lub wykorzystanie systemów sztucznej inteligencji (SI) przez przestępców, jak i organy ścigania i wymiar sprawiedliwości.

Na gruncie polskim temat oszustwa komputerowego (art. 287 k.k.) był już przedmiotem opracowań dogmatycznych (artykułów, komentarzy do kodeksu karnego), jednak przegląd aktualnej literatury nie wskazuje na istnienie porównywalnie

kompleksowej pracy łączącej analizę dogmatyczną, prawnoporównawczą (wykorzystano regulacje ośmiu jurysdykcji), dane statystyczne Policji i Prokuratury z dekady 2014–2024 oraz badania jakościowe z praktykami organów ścigania i biegłymi. Tym samym temat, choć nie jest nowy w wymiarze przedmiotowym, jest innowacyjny w wymiarze metodologicznym – stanowi to zgodne z wymogiem ustawowym „oryginalne rozwiązanie problemu naukowego" rozumiane jako nowość metody, a nie przedmiotu. Szczególnie nowatorski jest wątek dotyczący wpływu sztucznej inteligencji na mechanizmy oszustw komputerowych oraz na proces dowodowy (problem wykorzystania systemów opartych i tzw. *black box*), który w polskiej doktrynie karnistycznej wciąż pozostaje słabo zbadany w porównaniu do prawa cywilnego czy administracyjnego.

Międzynarodowa literatura z lat 2024–2026 intensywnie eksploruje problematykę odpowiedzialności karnej za oszustwa wspomagane sztuczną inteligencją, co potwierdza aktualność i trafność wyboru tematu przez Doktoranta. Prace takie jak analiza F. Zhanga zawarta w artykule pt. *The Dilemma and Solutions in Applying Criminal Law to Generative AI Fraud Crimes: The Case of Sora* z 2025 r. dotycząca oszustw generowanych przez SI lub badania nad odpowiedzialnością wielopodmiotową w automatyzowanych oszustwach (np. opracowanie Z. Zhou pt. *Criminal Law Responses to Artificial Intelligence Fraud Crimes: Research on Practical Dilemmas and Regulatory Paths* z 2025 r.) wskazują na globalny trend przesuwania debaty od pytania „czy SI może być podmiotem odpowiedzialności?" do pytania bardziej praktycznego i osadzonego w obowiązującym prawie karnym: „jak rozłożyć odpowiedzialność w całym ekosystemie przestępczym". Recenzowana rozprawa wpisuje się w ten nurt (hipoteza III i IV rozprawy dotyczącą rozproszenia sprawstwa), co świadczy o jej aktualności.

Podobnie temat standardów dowodowych wobec dowodów cyfrowych generowanych przez SI jest przedmiotem aktualnego raportu Eurojustu (*Cybercrime Judicial Monitor*, wydanie 10 z 2025 r.), który stwierdza brak specyficznych barier prawnych dla wykorzystania dowodów SI w postępowaniach karnych, lecz podkreśla konieczność zachowania standardów rzetelności, wiarygodności i łańcucha dowodowego. Ponownie, Doktorant trafnie identyfikuje aktualne linie sporu naukowego, jednak w ograniczonym zakresie odnosi się wprost do najnowszych (2025–2026) prac zagranicznych dotyczących modeli odpowiedzialności wielopodmiotowej za tzw. *AI-*

fraud, co stanowi istotny obszar do uzupełnienia bibliografii w przypadku publikacji rozprawy.

Główna konkluzja o istnieniu systemowej luki ochronnej między fazą przygotowawczą a dokonaniem oszustwa komputerowego koresponduje z aktualnym nurtem światowej debaty o potrzebie regulacji proaktywnej, wyprzedającej wymierzonej w infrastrukturę przestępczą (a w zasadzie w poszczególne elementy całego ekosystemu przestępczego), co czyni wnioski aktualnymi i osadzonymi w rzeczywistej dynamice współczesnych cyberzagrożeń i cyberprzestępczości.

W tym miejscu należy jednak zgłosić uwagę o charakterze polemicznym. Tytuł deklaruje trzy elementy: zwalczanie cyberprzestępczości jako kategorię ogólną, oszustwo komputerowe jako egzemplifikację oraz problemy dogmatyczne i dowodowe jako perspektywę analityczną. Lektura rozprawy potwierdza, że wszystkie trzy elementy znajdują odzwierciedlenie w strukturze rozprawy – Rozdziały I–II i VI dotyczą dogmatyki, Rozdziały VIII–IX oraz fragmenty VII dotyczą kwestii dowodowych i metodologicznych, a Rozdziały III–V realizują szeroko rozumiane „zwalczanie cyberprzestępczości" w wymiarze instytucjonalnym i międzynarodowym. Zastrzeżenie budzi jednak fraza „na przykładzie" – sugeruje ona, że oszustwo komputerowe ma funkcję ilustracyjną wobec szerszego zjawiska cyberprzestępczości, podczas gdy w rzeczywistości art. 287 k.k. wydaje się być jednak centralnym, samodzielnym przedmiotem badań, a nie jedynie przykładem. Cyberprzestęopczość jest pokazywana jako tło rozważań. W tym przypadku bardziej precyzyjne byłoby odwrócenie akcentu głównego na oszustwo komputerowe z cyberprzestępczością jako punktem odniesienia, co lepiej odpowiadałoby proporcjom objętościowym rozprawy (rozdziały poświęcone bezpośrednio i wyłącznie oszustwu komputerowemu – 1.2.1, VI, VII, IX – stanowią łącznie większość materiału opisowego, analitycznego i empirycznego).

Konkludując tę część recenzji należy stwierdzić, iż temat rozprawy w pełni spełnia wymogi ustawowe jako oryginalne (metodologicznie i merytorycznie) rozwiązanie aktualnego problemu naukowego, osadzone w rzetelnym warsztacie teoretycznym i wykazujące samodzielność badawczą Doktoranta. Temat jest również wysoce aktualny na tle literatury zagranicznej i innowacyjny względem literatury krajowej.

II. Ocena warsztatu badawczego

Uwagi wprowadzające wraz z Rozdziałem VIII i Wnioskami końcowymi stanowią ramę metodologiczną rozprawy. Zastanawia jednak fakt, iż rozdział metodologiczny jest dopiero ósmy w kolejności, mimo iż zawiera opisy odnoszące się do założeń z obszaru prawa i metody dogmatyczne, a nie jedynie empirycznego aspektu. Zdaniem Recenzenta rozdział ten powinien być pierwszy w kolejności tuż za Uwagami wprowadzającymi.

Analiza wykazuje, że cel i przedmiot badań są wzajemnie w pełni komplementarne – cel określa kierunek poznawczy (relacja przygotowanie–dokonanie), a przedmiot precyzuje jego zakres teoretyczny (materialnoprawny, procesowy) i empiryczny. Tak jak już zostało to zauważone, tytuł rozprawy wydaje się być nieco inny niż faktyczny zakres celu i przedmiotu, gdyż np. nie odnosi się do sztucznej inteligencji, która w celu badań figuruje *explicite* („rola sztucznej inteligencji w mechanizmach popełniania, wykrywania i dowodzenia"). Zgodnie ze standardami metodologii nauk prawnych tytuł rozprawy powinien być najwęższym, ale w pełni reprezentatywnym odzwierciedleniem jej celu i przedmiotu – w tym przypadku zachodzi częściowa niespójność wymagająca korekty tytułu lub jego rozszerzenia (np. przez podtytuł sygnalizujący wątek technologiczny).

Główny problem badawczy jest sformułowany w postaci pytania otwartego (czy i w jakim zakresie model penalizacji zapewnia ochronę), a hipoteza główna stanowi jednoznaczną, zamkniętą odpowiedź przecząca na to pytanie. Jest to poprawna logicznie konstrukcja metodologiczna – hipoteza powinna być odpowiedzią przewidywaną na problem badawczy, podlegającą weryfikacji, a nie jego powtórzeniem. We Wnioskach końcowych Doktorant konsekwentnie stwierdza, że „główny problem badawczy został rozstrzygnięty negatywnie", co jest logicznie zgodne z pierwotnym sformułowaniem hipotezy głównej – stanowi to istotny walor spójności wewnętrznej całej konstrukcji badawczej.

Wszystkie jedenaście problemów szczegółowych stanowią dekompozycję problemu głównego na wymiary: ilościowy (I, XI), dogmatyczny (II, VII, VIII, X), kryminologiczny (III, IV), instytucjonalny (V) oraz procesowy (VI, IX). Taka dekompozycja jest metodologicznie uzasadniona, jednak trzy problemy (II, VII, X) w istocie stawiają to samo pytanie o nieadekwatność art. 287 k.k. z różnych perspektyw (kwalifikacja, moment ingerencji, potrzeba nowelizacji). W ocenie Recenzenta powinny zostać scalone

w jeden złożony problem badawczy z trzema poziomami analizy, co zwiększyłoby przejrzystość konstrukcji bez utraty wartości poznawczej.

W szczególności analiza treści jedenastu par problem–hipoteza wykazuje, że można je pogrupować w pięć obszarów tematycznych:

1. dynamika i charakter zjawiska (I, XI),
2. dogmatyczna nieadekwatność art. 287 k.k. (II, VII, VIII, X),
3. wpływ technologii/SI na model sprawcy i skuteczność czynu (III, IV),
4. zdolności instytucjonalne organów ścigania (V) oraz
5. standardy dowodowe, w tym dowody generowane przez SI (VI, IX).

Obszar drugi jest szczególnie przeładowany – cztery odrębne hipotezy (II, VII, VIII, X) w istocie stawiają to samo pytanie o niedopasowanie art. 287 k.k. do rzeczywistości cyberprzestępczości, jedynie z różnych punktów wejścia (kwalifikacja prawna, moment ingerencji, karalność przygotowania, potrzeba nowelizacji) – jest to swego rodzaju nadmierność w treści, a nie realna wielowymiarowość problemu.

Dobór metod (dogmatyczno-prawna, prawnoporównawcza, empiryczna, interdyscyplinarna) jest w pełni adekwatny do celu i przedmiotu badań, a jego uzasadnienie teoretyczne jest metodologicznie poprawne i dobrze umotywowane. Doktorant trafnie broni tezy, że w obszarze dynamicznie zmieniających się zjawisk technologicznych analiza tekstu prawnego wymaga wzbogacenia o dane empiryczne, powołując się na stanowisko, iż sama analiza tekstu prawnego może okazać się niewystarczająca dla pełnego uchwycenia funkcji i skutków regulacji.

Samo stosowanie metody dogmatycznej jest poprawne. Słabością tej części jest jednak brak przełożenia ogólnego uzasadnienia teoretycznego na konkretną operacjonalizację metody empirycznej. Nie można na przykład odnaleźć opisu, czy zastosowana metoda prawnoporównacza (Rozdział III) ma charakter funkcjonalny (tj. czy Doktorant systematycznie odnosi rozwiązania zagraniczne do własnych hipotez badawczych, zwłaszcza dotyczących karalności przygotowania), czy pozostaje głównie deskrypcją poszczególnych systemów bez spójnej ramy porównawczej (tzn. jednolitych kryteriów porównania).

Ponadto, w żadnej z części rozprawy nie sprecyzowano doboru respondentów wywiadów (jedynie w przypadku biegłych możemy się tego dowiedzieć pośrednio poprzez charakterystykę ich działalności zawodowej), co jest istotnym niedostatkiem w

świetle wymogu przejrzystości i powtarzalności metody (i w konsekwencji całości badań). Poza tym, wywiady z funkcjonariuszami Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) budzą pewne zastrzeżenia. Odpowiedzi są nienaturalnie rozbudowane, nasycone precyzyjnymi liczbami, nazwami systemów (np. Palantir Gotham, PredPol), przykładami międzynarodowymi (np. WannaCry, Colonial Pipeline, SolarWinds) i strukturą, która nie przypomina spontanicznej wypowiedzi (tak jak jest to w przypadku wywiadu z biegłymi) anonimowego funkcjonariusza. Sam Doktorant zresztą zaznacza we wstępie do tego podrozdziału, że „odpowiedzi funkcjonariuszy zostały znacząco rozbudowane, aby dostarczyć dogłębnej analizy" bez wskazania szczegółów metodologicznych tej „rozbudowy". Z drugiej strony wywiady z biegłymi sądowymi mają cechy autentycznego materiału jakościowego: odpowiedzi są zróżnicowane, momentami niepewne lub ograniczone przez kompetencje respondenta, a analiza porównawcza w podrozdziale 9.4 poprawnie identyfikuje zarówno zbieżności, jak i rozbieżności stanowisk. Jest to metodologicznie wiarygodne i zgodne z deklarowaną techniką wywiadu częściowo ustrukturyzowanego.

Doktorant powołuje się na klasyków polskiej teorii prawa oraz metodologii nauk społecznych, umiejętnie łącząc je z własną koncepcją triangulacji metod. Świadczy to o dobrym poziomie dojrzałości warsztatowej, choć warto zauważyć, że część przywołanej literatury metodologicznej ma charakter ogólny i podręcznikowy, a nie specyficzny dla nauk prawnych czy kryminologii (np. *digital criminology*, *cybercriminology*). Recenzent oczekiwałby szerszego odwołania do metodologii badań nad cyberprzestępczością (np. dokumentów Europolu IOCTA, ENISA *Threat Landscape*) już na etapie uzasadnienia metodologicznego, a nie tylko jako materiału empirycznego w rozdziałach IV–V. Należy także podkreślić, iż raporty Europolu i ENISA dotyczą spojrzenia strategicznego na obszar Unii Europejskiej, ale bliżej im jednak do analiz kryminologicznych. Raporty te mają inną perspektywę. O ile Europol opisuje w IOCTA swoją roczną pracę w zakresie koordynacji zwalczania cyberprzestępczości na poziomie unijnym, to ENISA posługuje się pojęciami i kategoriami typowymi dla cyberbezpieczeństwa (czyli incydentami, a nie przestępstwami lub czynami zabronionymi).

Opisanie danych z Komendy Głównej Policji i Prokuratury Krajowej za lata 2014–2024 jest metodologicznie solidne. Doktorant prawidłowo dokumentuje źródło danych, prezentuje dane w formie tabelarycznej i stosuje analizę porównawczą rok do roku oraz

analizę trendu długookresowego. Wartościowe jest również wyjaśnienie ograniczeń tej metody (ciemna liczba przestępczości, niejednolite praktyki kwalifikacyjne), co świadczy o metodologicznej samoświadomości Doktoranta.

Wnioski końcowe stwierdzają, że główny problem badawczy został rozstrzygnięty negatywnie – obowiązujący model penalizacji oszustwa komputerowego nie zapewnia pełnej i adekwatnej ochrony dóbr prawnych wobec procesowego, wieloetapowego charakteru współczesnych oszustw komputerowych. Jednakże Doktorant nie określił w precyzyjny sposób, jakie przyjął kryteria oceny skuteczności: czy miałyby to być, np. zdolność zapobiegania szkodzie, szybkość wykrycia zdarzenia, identyfikację sprawcy, możliwość procesowego udowodnienia winy oraz odzyskanie mienia lub kompensację szkody? Hipoteza główna oraz hipotezy dotyczące jakościowego charakteru wzrostu przestępczości, zmiany modelu sprawcy na rozproszone struktury sieciowe oraz wpływu sztucznej inteligencji na skuteczność oszustw zostały w pełni potwierdzone; hipoteza dotycząca zdolności organów ścigania potwierdzona częściowo, a hipoteza o linearnym, nieprzerwanym wzroście cyberprzestępczości została obalona na podstawie danych z lat 2014–2024, które wykazały dynamikę falową. Doktorant konkluduje, że skuteczna ochrona dóbr majątkowych wymaga odejścia od reaktywnego modelu prawa karnego na rzecz modelu uwzględniającego charakter tej kategorii przestępstw jako wieloetapowego procesu i złożonego pod względem podmiotowym, z zastrzeżeniem, że ewentualna penalizacja fazy przygotowawczej powinna mieć charakter wąski i proporcjonalny, wykluczający kryminalizację działań neutralnych, takich jak legalne testowanie zabezpieczeń.

Podsumowując tę część recenzji należy ocenić ją pozytywnie mimo zgłaszanych licznych uwag. Konstrukcja metodologiczna rozprawy wykazuje wysoki poziom wewnętrznej logiki na poziomie makro (cel–przedmiot–problem główny–hipoteza główna–wnioski końcowe), co stanowi jej istotny walor naukowy. Na poziomie mikro (problemy i hipotezy szczegółowe, operacjonalizacja metod) występują jednak nadmierna złożoność i częściowa redundancja, które – w celu spełnienia najwyższych standardów rozprawy doktorskiej – wymagają konsolidacji hipotez szczegółowych oraz bardziej szczegółowego uzupełnienia opisu procedur badawczych w rozdziale metodologicznym.

III. Ocena struktury rozprawy doktorskiej

Analiza rozprawy pod względem wewnętrznej spójności ujawnia zróżnicowany poziom precyzji nazewniczej. Rozdziały I, VI, VII, VIII i IX mają tytuły na ogół precyzyjne odpowiadające ich treści i są logicznie skorelowane z problematyką dogmatyczną i dowodową zadeklarowaną w tytule głównym. Nie zawsze jednak trafnie oddają treść (np. w podpunkcie 1.1.4 wbrew tytułowi nie porusza on kwestii definicyjnych). Natomiast Rozdziały II–V mają charakter bardziej deskryptywny niż analityczny, co ujawnia się już na poziomie tytułów – „Sposoby popełniania przestępstw w cyberprzestrzeni", „Cyberprzestępstwa w regulacjach wybranych systemów prawnych", „Stan Rzeczypospolitej Polskiej oraz Unii Europejskiej [...] na podstawie raportu NIK, CERT Polska i ENISA" oraz „Incydenty bezpieczeństwa i zagrożenia" sugerują raczej syntezę wiedzy zastanej niż własną analizę problemową. Standardy metodologiczne rozpraw doktorskich w naukach prawnych wymagają, by część teoretyczna prezentowała stan wiedzy związany z tematyką rozprawy, jednak w proporcji odpowiadającej wadze części empirycznej i analitycznej. W analizowanym przypadku tytuły rozdziałów II–V wskazują na dominację funkcji opisowej, sprawozdawczej.

Rozprawa ma charakter zdecydowanie interdyscyplinarny, jednak z dominującym rdzeniem w dyscyplinie prawa – konkretnie prawa karnego materialnego i procesowego – co potwierdza już samo sformułowanie przedmiotu badań jako prawnokarnej analizy oszustwa komputerowego jako zjawiska normatywnego i praktycznego. Metodologia oparta na dorobku klasyków polskiej teorii i dogmatyki prawa, jednoznacznie sytuuje rozprawę w paradygmacie nauk prawnych, a nie kryminologii jako dyscypliny autonomicznej. Jednocześnie Doktorant wyraźnie deklaruje w Uwagach wprowadzających cel jako analizę oszustwa komputerowego jako zjawiska prawnego i kryminologicznego, co wskazuje na świadome, choć nie w pełni zoperacjonalizowane, osadzenie rozprawy również w kryminologii – zwłaszcza w obszarze sprawcy, struktur sieciowych i dynamiki zjawiska kryminalnego w czasie (dane 2014–2024). Trzecim komponentem dyscyplinarnym jest kryminalistyka, obecna w warstwie dotyczącej informatyki śledczej, dowodów cyfrowych, funkcjonowania biegłych sądowych oraz metod wykrywania i dokumentowania przestępstw. Rozprawa potwierdza silny akcent kryminalistyczny w części empirycznej.

Tym samym, można stwierdzić, że rozprawa reprezentuje model badań łączonych (*law and technology, law and society*), typowy dla współczesnych rozpraw z zakresu cyberprzestępczości, przy czym oś centralna – analiza dogmatyczna art. 287 k.k. i postulaty *de lege ferenda* – przynależy jednoznacznie do prawa karnego, natomiast kryminologia i kryminalistyka funkcjonują jako dyscypliny wspomagające, dostarczające materiału empirycznego do weryfikacji hipotez prawnych. Warto zauważyć, że tak skonstruowany model badawczy jest w pełni zgodny z tym, co Doktorant deklaruje w Rozdziale VIII, powołując się na konieczność synergii wiedzy teoretycznej, badań empirycznych oraz doświadczenia praktycznego – deklaracja ta jest spójna z rzeczywistym doborem dyscyplin. Można odnieść jednak wrażenie, że interdyscyplinarne podejście stanowiło dla Doktoranta wyzwanie w konsekwentnym stosowaniu tych samych lub podobnych pojęć wraz z ich znaczeniem typowym dla prawa, kryminologii i informatyki (lub raczej cyberbezpieczeństwa).

Recenzowana rozprawa obejmuje dziewięć rozdziałów o łącznej objętości 422 stron, poprzedzonych wykazem skrótów, spisem wykorzystanych obrazów i tabel oraz Bibliografią. Jej pierwsza jednostka techniczna prezentuje transformację przestępczości przeciwko mieniu pod wpływem cyfryzacji ze szczególnym naciskiem na oszustwo komputerowe jako zjawisko, które przechodzi od jednorazowego działania sprawcy do złożonego, wieloetapowego procesu w całym ekosystemie przestępczym w sieci. Doktorant analizuje konstrukcję art. 287 k.k., wskazując na lukę między fazą przygotowawczą a momentem ingerencji prawa karnego, oraz osadza problematykę w zasadach proporcjonalności, subsydiarności i *ultima ratio*. Sformułowano tu cel rozprawy, przedmiot badań, hipotezę główną oraz zarys metod badawczych (dogmatycznoprawna, orzecznictwo, badania empiryczne, elementy interdyscyplinarne).

Rozdział I („Część podstawowa") obejmuje definicję cyberprzestrzeni i cyberprzestępczości oraz przegląd przestępstw przeciwko bezpieczeństwu cybernetycznemu w polskim kodeksie karnym: oszustwo komputerowe (art. 287), hacking (art. 267), utrudnianie zapoznania się z informacją (art. 268), niszczenie danych informatycznych (art. 268a), sabotaż komputerowy (art. 269) i wytwarzanie programów komputerowych (art. 269b). Rozdział II opisuje sposoby popełniania przestępstw w cyberprzestrzeni: *hacking*, *cracking*, *sniffing*, *phishing*, *warez*, *skimming*, *ransomware* i

cryptojacking. Rozdział III prezentuje regulacje cyberprzestępczości w ośmiu systemach prawnych: Stanach Zjednoczonych, Wielkiej Brytanii, Czechach, Włoszech, Francji, Hiszpanii, Japonii i Niemczech, ze szczególnym uwzględnieniem oszustw komputerowych. Rozdział IV analizuje stan walki z cyberprzestępczością w Polsce i UE na podstawie raportów Najwyższej Izby Kontroli, CERT Polska oraz ENISA Threat Landscape, w tym Krajowego Systemu Cyberbezpieczeństwa. Rozdział V opisuje incydenty bezpieczeństwa i zagrożenia: kampanie phishingowe, ataki *ransomware*, *malware*, ataki DDoS w kontekście politycznym oraz ataki na portfele kryptowalutowe. Rozdział VI przedstawia perspektywę zmian ustawowych dotyczących oszustwa komputerowego w Polsce, obejmując propozycje zmian w zakresie kradzieży tożsamości, rozważenie karalności przygotowania do oszustwa komputerowego oraz możliwość wprowadzenia trybu kwalifikowanego w art. 287 k.k.. Rozdział VII dotyczy poszerzenia uprawnień organów ścigania w zakresie czynności pozaprocesowych umożliwiających ustalanie tożsamości sprawców, w tym propozycji *de lege ferenda*, zabezpieczeń przed nadużyciami oraz wykorzystania nowych technologii w identyfikacji sprawców. Rozdział IX prezentuje wyniki badań empirycznych: wywiady z funkcjonariuszami CBZC i ich analizę, wywiady z biegłymi sądowymi z zakresu informatyki śledczej i ich analizę porównawczą, a także obszerną analizę skali cyberprzestępczości na podstawie danych Komendy Głównej Policji i Prokuratury Krajowej, w tym analizę porównawczą tych danych za lata 2014–2024 oraz dynamikę oszustw komputerowych w kontekście europejskim, globalnym i azjatyckim.

Należy zauważyć, iż w momencie złożenia rozprawy nie weszła w życie najnowsza nowelizacja z lipca 2026 r. ustawy o krajowym systemie cyberbezpieczeństwa implementująca Dyrektywę NIS2. Dlatego też częściowo treści tam zawarte są już nieaktualne.

IV. Ocena formalnej strony rozprawy

Styl rozprawy jest typowy dla dysertacji z zakresu nauk prawnych – formalny, bezosobowy, z częstym stosowaniem konstrukcji pasywnych i nominalizacji („przystępując do analizy...", „na tle tych przemian szczególnego znaczenia nabiera..."). Jednak w kilku miejscach styl staje się nadmiernie rozbudowany składniowo, co utrudnia percepcję – przykładem jest zdanie z Uwag wprowadzających: „Mechanizmy te

powodują, że granica pomiędzy etapem przygotowania, a momentem dokonania przestępstwa ulega zatarciu, a kluczowe elementy decydujące o powodzeniu czynu zabronionego realizowane są często na długo przed wystąpieniem skutku w postaci szkody majątkowej". Zdanie to, choć poprawne gramatycznie, kumuluje trzy niezależne myśli, co może obniżać czytelność wywodu. Standardy pisania rozpraw doktorskich w naukach prawnych rekomendują większą dyscyplinę składniową i unikanie zdań wielokrotnie złożonych, szczególnie w partiach o kluczowym znaczeniu metodologicznym.

Pozytywnie należy ocenić konsekwentne stosowanie przez Doktoranta struktury argumentacyjnej „teza – uzasadnienie – odniesienie do literatury", co widoczne jest szczególnie w Rozdziale VIII, gdzie każda deklaracja metodologiczna jest natychmiast poparta przypisem do konkretnej i adekwatnej pozycji bibliograficznej. Jest to wysoko oceniana praktyka przy recenzowaniu rozpraw doktorskich, świadcząca o rzetelności warsztatu naukowego i unikaniu twierdzeń niepopartych źródłami. Jednocześnie należy jednak podnieść, iż są obszerne fragmenty w rozprawie bez przypisów lub powołujące się na źródła internetowe o różnym poziomie wiarygodności (np. oficjalne strony instytucji państwowych lub międzynarodowych, ale i serwisy informacyjne, strony dostawców oprogramowania lub usług w sieci, kancelarii) w miejsce źródeł typowo naukowych.

Analiza słownictwa wykazuje dobre opanowanie terminologii z trzech obszarów: dogmatyki prawa karnego (np. „znamiona czynu zabronionego", „niekorzystne rozporządzenie mieniem", „subsydiarność", *„ultima ratio"*), informatyki śledczej i cyberbezpieczeństwa (np. *„wallet drainer"*, *„black box problem"*, *„Cybercrime-as-a-Service"*, *„Phishing-as-a-Service"*) oraz metodologii badań społecznych (np. „triangulacja metodologiczna", „operacjonalizacja hipotez"). Doktorant sprawnie posługuje się anglicyzmami branżowymi (CaaS, PaaS, RaaS, MaaS), co jest uzasadnione ich powszechnym stosowaniem w literaturze przedmiotu i brakiem utrwalonych polskich odpowiedników.

Pewne zastrzeżenia może budzić widoczna miejscami niekonsekwencja w stosowaniu niektórych pojęć kluczowych dla rozprawy. Termin „luka ochronna" używany jest zamiennie z „luką penalizacyjną" oraz „systemową luką" bez wyraźnego zdefiniowania, czy są to synonimy czy pojęcia o różnym zakresie znaczeniowym. We

Wnioskach końcowych występuje sformułowanie „istnienie wyraźnej systemowej luki ochronnej", podczas gdy w Hipotezie X mówi się o „luce penalizacyjnej". Trafniejsze byłoby wskazywanie, czy chodzi w danym miejscu o np. niedostatki ochrony prawnej, ograniczenia konstrukcji art. 287 k.k., deficyty dowodowe czy bariery organizacyjne organów ścigania. Taka korekta zwiększyłaby precyzję dogmatyczną rozprawy i zapobiegłaby nieuprawnionemu przechodzeniu od diagnozy słabości praktyki ścigania do postulatu rozszerzenia odpowiedzialności karnej. Rozprawa z zakresu dogmatyki prawa karnego powinna precyzyjnie rozgraniczać te pojęcia.

Podobna niejednoznaczność dotyczy pojęcia „proces przestępczy" – używanego jako kategoria opisowa („oszustwa komputerowe mają charakter procesowy, wieloetapowy i infrastrukturalny"), bez wyraźnego osadzenia w klasycznej dogmatyce form stadialnych przestępstwa (klasyczny pochód przestępstwa: przygotowanie – usiłowanie – dokonanie). Doktorant posługuje się tym terminem w sposób zbliżony do języka kryminologicznego (opis dynamiki zjawiska pod względem powiązanych ze sobą funkcjonalnie wielu zdarzeń, w których bierze udział wiele osób w różnych rolach), jednak w kontekście dogmatycznoprawnym (gdzie ma znaczenie dla momentu penalizacji) wymagałoby to jednoznacznego zdefiniowania na wstępie rozprawy, czy „proces przestępczy" jest kategorią opisową (kryminologiczną) czy normatywną (dogmatyczną) – w obecnej formie pojęcie to funkcjonuje dwuznacznie.

W obszarze terminologii informatyczno-kryminalistycznej odnotować należy poprawne, zgodne ze stanem wiedzy stosowanie pojęć takich jak *phishing*, *ransomware*, *cryptojacking*, *skimming* – ich rozdzielenie na osobne podrozdziały w Rozdziale II świadczy o systematyzującym podejściu do taksonomii cyberprzestępczości. Wątpliwość budzi jednak umieszczenie „Zainteresowania Linuxem" jako osobnego podrozdziału (5.5) na równi z takimi kategoriami jak ataki DDoS czy ataki na portfele kryptowalutowe. Tytuł ten nie jest terminem technicznym ani kategorią zagrożenia, lecz sformułowaniem potocznym, niejasnym analitycznie; rekomendowane byłoby albo dookreślenie tego podrozdziału (np. „Podatności systemów Linux jako wektor ataków"), albo jego przeformułowanie zgodnie z konwencją terminologiczną pozostałych podrozdziałów.

Natomiast nie da się pominąć niekonsekwencji technicznych w numeracji jednostek technicznych rozprawy, które świadczą o niedopracowaniu redakcyjnym

spisu treści: dwukrotne oznaczenie punktu „1.2.5" (Sabotaż komputerowy i Wytwarzanie programów komputerowych), nielogiczna kolejność podpunktów 2.3–2.6 w Rozdziale II (numeracja 2.2, 2.4, 2.5, 2.3, 2.6 – *Cracking*, *Sniffing*, *Phishing*, *Warez*, *Skimming* w nieuporządkowanej sekwencji) oraz dwukrotne „8.3.1" w Rozdziale VIII. Powyższe błędy techniczne powinny zostać skorygowane przed oddaniem rozprawy, gdyż w obecnej formie mogą sugerować niedostateczną kontrolę nad redakcją całości.

Zestawienie źródeł bibliograficznych, na których oparto rozprawę wykazuje silne jej osadzenie w dogmatyce prawa karnego przy jednoczesnym niedostatecznym nasyceniu literaturą specjalistyczną z zakresu kryminologii, cyberprzestępczości oraz prawa nowych technologii (w szczególności prawnokarnych aspektów SI, np. J. Giezek, *Sztuczna inteligencja a fundamenty odpowiedzialności karnej państwa demokratycznego*, Studia nad Autorytaryzmem i Totalitaryzmem 2025, nr 46 wraz z cytowaną tam literaturę), które stanowią deklarowany, ważny wątek badawczy rozprawy. Rekomendowane jest znaczące wzmocnienie bibliografii w segmencie: kryminologia sieciowa i strukturalna (*network criminology*), odpowiedzialność karna za *AI-fraud* w literaturze międzynarodowej z lat 2024–2026, oraz standardy dowodowe wobec dowodów cyfrowych generowanych przez systemy (przykładowe z nich wymienione na początku recenzji).

Doktorant nie wspomniał (nawet z perspektywy historycznej lub punkt odniesienia dla autorskich analiz) o trzech artykułach opublikowanych w Studiach prawniczych (nr 4 z 2006 r.) zawierających następujące opracowania: B. Kunicka-Michalska, *Oszustwo komputerowe. Regulacje prawa polskiego*; R. A. Stefański, *Oszustwa komputerowe w praktyce polskich organów ścigania* oraz B. Świątkiewicz, *Oszustwo komputerowe - techniki dochodzeniowe*; a także nowszego autorstwa A. Kania, *Rozwój nowych technologii a kryminalizacja oszustwa komputerowego*, Wojskowy Przegląd Prawniczy 2017, nr 1, s. 110-124.

Należy także podnieść, iż rozprawa ma mankamenty natury technicznej związanej z redagowaniem tekstu: liczne wypunktowania, różne style prowadzenia analiz oraz braki w konsekwentnym tworzeniu opisu tabel, diagramów i wykresów (zwłaszcza ich tytułów i źródeł). Nie zawsze zasadne jest tworzenie skromnych tabel (s. 136, 369). Zdarzają się też powtórzenia fragmentów tekstu (s. 210), czy odmienny sposób cytowania nawet tych samych pozycji w przypisach dolnych i w Bibliografii (np. przypis nr 176 i 179 dotyczą tej

samej pozycji A. Behan, rozbieżność opisu pozycji K. Buczkowskiego w przypisie nr 76 i w Bibliografii). Czasami opis pozycji bibliograficznej jest na tyle skrótowy, że trudno zweryfikować jej prawdziwość i wartość naukową (np. Roger M., E. Lopez, C. Martin, *Digital Sovereignty in the European Union: Challenges and Opportunities*, 2025, s. 9–13). Brak opisu stron internetowych utrudnia ocenę ich wiarygodności. Ponadto, należałoby jednak oddzielnie umieścić wykaz literatury naukowej od np. dokumentów i raportów instytucji krajowych i międzynarodowych, a także orzecznictwa wykorzystanego w rozprawie (zamiast umieszczać go w podpunkcie zatytułowanym II. Akty prawne).

Dobra praktyką jest także zamieszczanie wzoru narzędzia badawczego jako załącznika do rozprawy. Doktorant nie zawarł kwestionariuszy wywiadów wykorzystanych we własnych badaniach metodą sondażu diagnostycznego. Częściowo jest to rekompensowane faktem, iż rozprawa zawiera dokładną (słowo w słowo) transkrypcję wywiadów wraz z pytaniami. Jeżeli Doktorant chciał wykazać się wiarygodnością swoich badań empirycznych, to powinien przenieść treść wywiadów jako załączniki na koniec rozprawy. Natomiast w Rozdziale IX. pozostawić syntetyzującą analizę ich wyników w poszczególnych obszarach tematycznych. W ten sposób utrzymana zostałaby spójność i płynność prezentacji wyników przeprowadzonych badań. Podobny zabieg powinien zostać zastosowany względem prezentacji treści korespondencji z organami państwowymi, celem pozyskania danych statystycznych.

Zdaniem Recenzenta aspekt formalno-techniczny jest najsłabszą stroną rozprawy spośród pozostałych.

V. Wnioski końcowe

Konkludując przytoczone w niniejszej recenzji uwagi, pozwalają one dojść do przekonania, że przedstawiona do recenzji rozprawa doktorska mgr Krystiana Bartosza spełnia wymagania określone w ustawie z dnia 20 lipca 2018 r. roku Prawo o szkolnictwie wyższym i nauce (tekst jednolity Dz.U. z 2024 r., poz. 1571 t.j. ze zm.) i może być podstawą dalszego postępowania w przewodzie doktorskim.

Natomiast lektura rozprawy skłania do zadania następujących pytań:

1. W jaki sposób należy rozgraniczyć instytucje współsprawstwa i pomocnictwa na gruncie doktryny polskiego prawa karnego, aby skutecznie pociągnąć do

odpowiedzialności sprawców działających w poszczególnych elementach przestępczego ekosystemu *Cybercrime-as-a-Service*?

2. Jakie konkretnie minimalne kryteria metodologiczne i techniczne musiałby spełniać systemy sztucznej inteligencji, aby pozyskany za jego pomocą dowód mógł zostać uznany za dopuszczalny w postępowaniu karnym? W jaki sposób ocenić jego wartość dowodową?



Białystok, dnia 31 sierpnia 2026 r.