prof. dr hab. Stanisław Hoc

em. Uniwersytet Opolski

Recenzja rozprawy doktorskiej

mgr Krystiana Bartosza pt. „Zwalczanie cyberprzestępczości na przykładzie oszustwa komputerowego - problemy dogmatyczne i dowodowe w postępowaniu przygotowawczym". Rzeszów 2026, s.465

I. Uwagi ogólne

1. Autor w charakterze wstępu zawarł uwagi wprowadzające (s. 12-15/), w których wyjaśnia motywację podjęcia tematu rozprawy doktorskiej. Mając na uwadze rozwój cyberprzestępczości autor dostrzega lukę pomiędzy czynnościami przygotowawczymi a momentem ingerencji prawa karnego, co w praktyce oznacza, że organy ścigania często uzyskują możliwość reakcji dopiero wówczas, gdy szkoda została już wyrządzona (s. 12).

Zdaniem autora celem rozprawy jest kompleksowa analiza oszustwa komputerowego jako zjawiska prawnego i kryminologicznego, ze szczególnym uwzględnieniem relacji pomiędzy fazą przygotowawczą a momentem dokonania czynu. Wybór tematu jest trafny, zwłaszcza, że autor zamierza odnosić się do rozwoju nowych technologii w kontekście oszustwa komputerowego.

Główna hipoteza rozprawy zakłada, że obowiązujący model penalizacji oszustwa komputerowego, oparty na klasycznej konstrukcji czynu dokonanego nie w pełni odpowiada współczesnym realiom przestępczości cyfrowej. Hipotezy szczegółowe odnoszą się natomiast do wpływu nowych technologii na strukturę oszustw komputerowych, skuteczności wykrywania, standardów dowodowych oraz możliwości modyfikacji obowiązujących rozwiązań normatywnych (s. 14). Metody badawcze wykorzystane przez autora to: metody dogmatyczne, analiza orzecznictwa, badania empiryczne oraz elementy interdyscyplinarne, a także wykorzystanie literatury przedmiotu i wywiady.

2. Rozprawa składa się z wykazu skrótów, spisów wykorzystanych w pracy obrazów i tabel, uwag wprowadzających, dziewięciu rozdziałów merytorycznych, wniosków końcowych i bibliografii.

II. Uwagi szczegółowe

1. Rozdział I został zatytułowany „część podstawowa", może to budzić pewne uwagi, których autor nie wyjaśnia, aczkolwiek treść tego rozdziału wiąże się z regulacjami normatywnymi (s.15-73), z tym, że strona 73 jest pusta? Autor rozpoczyna swoje rozważania od wyjaśnienia definicji cyberprzestrzeni, cyberprzestępczości (s. 15 in.), wykorzystując znajomość literatury przedmiotu, w tym obcej. Podejmuje następnie próbę przedstawienia własnej autorskiej definicji cyberprzestrzeni: „Cyberprzestrzeń to dynamiczna, wirtualno-technologiczna przestrzeń funkcjonowania jednostek, instytucji i państw, tworzona przez współdziałające systemy teleinformatyczne, infrastrukturę sieciową, dane oraz użytkowników, w której dochodzi do komunikacji, wymiany informacji, realizacji procesów społecznych, gospodarczych i prawnych, a także do konfliktów i działań przestępczych, wywołujących realne skutki w świecie rzeczywistym" (s. 21).

Następnie analizuje pojęcie cyberprzestępczości (s. 21 in.), wskazując na stosunek UE do zagrożeń cybernetycznych (s. 24 in.), czyni to szczegółowo i kompetentnie. Zwraca uwagę na pojęcie przestępczości komputerowej i brak jej definicji (s. 41 in.). Posiłkuje się przy tym literaturą przedmiotu, aczkolwiek wybraną dość dowolnie. Warto zwrócić uwagę autorowi na np. następujące opracowania, które pominął: M. Nawrocki, O poszerzeniu jurysdykcji sądów karnych w sprawach o cyberprzestępstwa (uwagi w związku z art. 112a k.k.). „Państwo i Prawo" 2024, z. 9, C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2018, Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości red. M. Wielec, Warszawa 2023, A. Dana, R. Kaniecki, T. Tomczyk, H. Topolewski, Cyberprzestępstwo - problematyka czasu i miejsca popełnienia przestępstwa „Polityka i Społeczeństwo" 2023, nr 3.

Autor przechodzi do analizowania wybranych przestępstw, poczynając od art. 287 k.k. - oszustwo komputerowe (s. 45 in.). Warto zwrócić uwagę, że autor dość często używa określenia „zapis" (s. 54 i inne), jest ono właściwe dla zapisu windykacyjnego i zapisu na sąd polubowny. Na uwagę zasługuje chęć autora do podejmowania polemik, z innymi autorami np. z M.

Siwickim (s. 54). Omawia następnie hacking - art. 267 k.k. (s.56 in.), odwołując się m.in. do mojego poglądu (s.61). Widzi potrzebę doprecyzowania treści art. 267 § 2 k.k. (s. 62).

Autor analizuje treść art. 268 § 2 k.k. (s. 63 in.), a także art. 268a k.k. (s. 66 in.) oraz art. 269 k.k. (s. 67 in.), odnosząc się do wybranej literatury. Zajmuje się także treścią art. 269b k.k. (s. 70 in.). Nie mógł autor odnieść się do nowelizacji k.k. z 15 maja 2026 r., że w art. 269b w § 1 wyrazy "art. 267 § 3 zastępuje się wyrazami "art. 267 § 1-3" - Dz. U. poz. 902.

2. W rozdziale II autor zajmuje się sposobami popełniania przestępstw w cyberprzestrzeni (s.74-123) odnosząc się szczegółowo do: hackingu, crackingu, sniffingu, phishingu, warezu, skimmingu, ransomware, cryptojacingu. Autor stara się wykorzystać w miarę szeroko dostępną literaturę przedmiotu, wiele uwagi poświęcając publikacji A. Behana (s. 77), którą wysoko ocenia.

Mało zrozumiały jest przypis 188 (s. 84) w kontekście zdania: „W obecnym brzmieniu art. 267 k.k. penalizowane jest już samo uzyskanie dostępu do informacji, co jest obligatoryjne przy nieuprawnionym uzyskaniu do systemu lub do jego części. Nie jest konieczne uzyskanie władztwa nad informacją bądź wskazanie, że sprawca z taką informacją się zapoznał". Autor dostrzegając opracowanie D. Pożaroszczyka, kontrowersyjne - moim zdaniem - nie dostrzega opracowania: M. Kościelniak-Marszał, Wpływ oprogramowania typu Pegasus na korzystanie w procesie karnym z materiałów zabezpieczonych z urządzeń mobilnych. Prawo w Działaniu Sprawy karne, 2025, tom 63, a także innych autorów podejmujących ten temat.

Zdaniem autora przeprowadzona przez niego analiza prowadzi do wniosku, że hacking w ujęciu prawnokarnym nie stanowi jednorodnego typu zachowania, lecz obejmuje szerokie spektrum działań - od prostego, nieuprawnionego dostępu do informacji, po złożone operacje techniczne o charakterze przygotowawczym, realizowane przy użyciu wyspecjalizowanych narzędzi informatycznych (s. 92). Pozostałe kwestie podnoszone w rozdziale II nie nasuwają uwag, mają one przede wszystkim wymiar informacyjny, w którym autor porusza się swobodnie. Przy nazwisku R. Kędziora (s. 114) zabrakło przypisu, drobna uwaga techniczna.

3. W rozdziale III autor zajmuje się cyberprzestępstwami w regulacjach wybranych systemów prawnych ze szczególnym uwzględnieniem oszustw komputerowych (s. 124-183), nie wyjaśnia dlaczego dokonał takiego wyboru państw (Stany Zjednoczone, Wielka Brytania, Czechy, Włochy, Francja, Hiszpania, Japonia, Niemcy). Są to niewątpliwie interesujące rozważania

prawnoporównawcze, powstałe przy dobrej znajomości głównie literatury przedmiotu i innych materiałów, podnoszące wartości poznawcze rozprawy. W rozważaniach dotyczących czeskiego kodeksu karnego, autor używa zamiennie § 209 lub art. 209 (s. 135 in.) oraz obiektywna strona przestępstwa, dlaczego nie strona przedmiotowa? Razi określenie: „oszustwo komputerowe jest przestępstwem swobodnym" (s. 155), w kontekście włoskiego kodeksu karnego. Odnośnie niemieckiego kodeksu karnego (s. 174) istnieje w Polsce tłumaczenie tego kodeksu, publikowane. Vide: Ewa Tuora-Schwierskott, Niemiecki kodeks karny w tłumaczeniu na język polski, Wydawnictwo De lure, 2018.

4. W rozdziale IV autor zajmuje się stanem Rzeczypospolitej Polskiej oraz Unii Europejskiej w walce z cyberprzestępczością na podstawie raportu Najwyższej Izby Kontroli, CERT Polska i ENIS Threat Landscape (s. 184-211). Rozważania zawarte w rozdziale IV poddające analizie raporty o stanie bezpieczeństwa RP na polu zagrożeń cybernetycznych oraz analiza porównawcza z problemami, które dotyczą wspólnoty europejskiej mają przede wszystkim wymiar informacyjny, wzbogacający wartości poznawcze rozprawy. Należało dokładniej informować o ustawie z dnia 5 lipca 2018 r. (z 2026 r.) o krajowym systemie bezpieczeństwa (Dz.U. z 2026 r. poz. 200) -s.195, którą autor omawia, czy wykorzystał w pełni literaturę przedmiotu?

Autor oceniając krajowy system cyberbezpieczeństwa ocenia, że model ten koncentruje się przede wszystkim na reagowaniu na incydenty, a nie na ich zapobieganiu (s. 204). Przy rozważaniach o raporcie ENISA (s. 210) autor nie ustrzegł się powtórzenia.

5. W rozdziale V autor zajmuje się incydentami bezpieczeństwa i zagrożeniami na polu cybernetycznym (s. 212-239), odnosząc się szczegółowo do przeprowadzonych kampanii phisingowych, ataków ransomware, malware - złośliwe oprogramowanie, ataków DDoS, zainteresowań Linusem, ataków na portfele kryptowalutowe. Rozważania mające charakter przede wszystkim informacyjny, niewątpliwie podnoszą wartości poznawcze rozprawy, świadczą o poważnym zainteresowaniu autora, wykraczającym poza tytuł pracy. Autor swoje wywody wzmacnia obrazami.

6. W rozdziale VI autor zajmuje się perspektywą zmian ustawowych oszustwa komputerowego (s. 240-274), odnosząc się do propozycji zmian ustawowych dotyczących kradzieży tożsamości, rozważań możliwości wprowadzenia karalności przygotowania przestępstwa komputerowego, możliwości rozszerzenia zapisów (!) zawartych w artykule 287 k.k. o tryb kwalifikowany.

W pierwszej kolejności autor analizuje propozycje zmian ustawowych dotyczących kradzieży tożsamości (art. 190a k.k.) - s. 240 in. Omawia wymienione przestępstwo, ale bardzo skąpo odnosi się do literatury. Głównym zarzutem autora do wymienionego przestępstwa jest fakt, że kradzież tożsamości i stalking to odmienne zjawiska, jednak polski ustawodawca dokonał pewnej syntezy poprzez kryminalizację kradzieży tożsamości jako specyficznej odmiany stalkingu. Dlatego też - zdaniem autora - umieszczenie obu tych czynów zabronionych w jednym przepisie określić należy co najmniej jako „niefortunne" (s. 243). Stąd propozycja autora (s. 243), dość lakoniczna, czy nie należało jej szerzej uzasadnić?

Razi określenie „zgodnie z literaturą prawną" (s. 247), następnie autor używa określenia: „w literaturze prawniczej oraz informatycznej" (s. 248). Inne określenie rażące: „...rodzi u autora tekstu wiele wątpliwości" (s. 249). Autor dochodzi do wniosku, że istnieje systemowa luka ochronna pomiędzy przepisami penalizującymi kradzież tożsamości a przepisami dotyczącymi oszustwa, która w warunkach masowych oszustw teleinformatycznych (nowe pojęcie autora) wymaga ponownej oceny zakresu penalizacji oraz rozważenia zmian de lege ferenda (s. 250). Razi także określenie: „Wykorzystanie cudzych danych osobowych oraz wizerunków w świetle art. 190a § 2 k.k. rodzi u autora tekstu wiele wątpliwości na stopniu dogmatycznym" (s. 251).

Autor uważa, że należy rozważyć wprowadzenie do kodeksu karnego przepisów penalizujących tworzenie i rozpowszechnianie materiałów deepfke, które wprowadzają w błąd co do tożsamości osoby /s.253/. Propozycja interesująca, ale dostępna jest szersza literatura okołoprawna dotycząca materiałów deepfake. Interesujące są rozważania autora odnoszące się do możliwości wprowadzenia karalności przygotowania przestępstwa oszustwa komputerowego (s. 254 in.). Autor jest zwolennikiem takiej zmiany którą szczegółowo uzasadnia, ale dostrzega również mankamenty.

Niezbyt jasny jest pogląd autora: „W konsekwencji, choć część działań przygotowawczych może podpadać pod istniejące przepisy, luka penalizacyjna dotycząca najwcześniejszych etapów operacji ransomware pozostaje istotą. Właśnie dlatego wprowadzenie karalności przygotowania do oszustwa komputerowego odpowiednio zawężonej i opartej na przesłance zamiaru kierunkowego - byłoby rozwiązaniem spójnym systemowo i znacząco wzmacniałoby ochronę prawną przed tymi atakami" (s. 258). Autor niejako przy okazji analizuje przepisy innych państw pod kątem penalizacji czynności przygotowawczych. Proponuje on dodanie § 4 do art. 287,

penalizującego przygotowanie do przestępstwa z art. 287 k.k. (s. 260), uzasadniając swoją propozycję. Autor dostrzega także ewentualne zagrożenia związane z wprowadzeniem jego propozycji, ryzyko nadmiernego ograniczenia swobód obywatelskich (s. 264). Pomimo podnoszonych wątpliwości, autor stara się być gorącym zwolennikiem proponowanych zmian legislacyjnych, raz jeszcze posiłkując się rozwiązaniami obcymi, np. niemieckimi (s. 266 in.).

Dalej, ale już nieco chaotycznie, autor powraca do ewentualnych zagrożeń wynikających z wprowadzenia jego propozycji, twierdząc, że kolejnym argumentem przeciwko wprowadzeniu karalności przygotowania do oszustwa komputerowego jest ryzyko nadmiernego obciążenia systemu wymiaru sprawiedliwości (s. 266). Następnie autor rozważa możliwość rozszerzenia zapisów (!) zawartych w artykule 287 k.k. o tryb kwalifikowany (s. 267 in.). Autor odwołuje się początkowo do anonimowych autorów (s. 268), należało bardziej precyzyjnie się odnieść to użytego określenia. Tryb kwalifikowany autor ocenia na podstawie uregulowań obcych (s. 268 in.). Wskazuje także na argumenty przemawiające za wprowadzeniem trybu kwalifikowanego w Polsce (s. 268). Autor proponuje wprowadzenie trybu kwalifikowanego w § 4-7 (s. 271 in.). Swoją propozycję wnikliwie uzasadnia, będąc jej gorącym zwolennikiem, uważając, że wprowadzenie trybu kwalifikowanego do art. 287 k.k. jawi się jako rozwiązanie najbardziej adekwatne, proporcjonalne i funkcjonalne, spójne dogmatycznie i odpowiadające współczesnym wyzwaniom cyberprzestępczości (s. 274).

7. W rozdziale VII autor zajmuje się poszerzeniem uprawnień organów ścigania w zakresie czynności pozaprocesowych umożliwiających ustalanie tożsamości sprawców (s. 275-299), nie wyróżnia uwag wstępnych do treści rozdziału, odnosi się do: obecnego stanu prawnego i wyzwań, czynności pozaprocesowych a efektywności ustalania tożsamości, propozycji poszerzenia uprawnień de lege ferenda, zabezpieczenia przed nadużyciami, wykorzystania nowych technologii w identyfikacji sprawców.

Autor tajemniczo powołuje się na literaturę (s. 276) bez egzemplifikacji. Mam pytanie do autora, czym różni się kontrola operacyjna od podsłuchów (s. 276). Co to oznacza „długi czas potrzebny na uzyskanie zgody sądu na kontrolę operacyjną"? (s. 276). Postulat autora dotyczy wprowadzenia mechanizmu, który pozwalałby organom ścigania - przy zachowaniu kontroli następczej oraz ograniczeniu katalogu przestępstw - na dostęp do metadanych w czasie rzeczywistym, bez konieczności przechodzenia przez wieloetapową procedurę retencyjną /s.278/.

Jednocześnie autor zauważa, że proponowana przez niego zmiana opiera się na założeniu, że skuteczność ścigania przestępstw wymaga dostosowania trybu pozyskiwania metadanych do realiów cyberprzestrzeni, a nie modyfikacji granic ingerencji w sferę prywatności (s. 279). Widzi możliwość wprowadzenia do polskiego porządku prawnego regulacji wzorowanych na europejskich rozwiązaniach dotyczących E-Evidence oraz Digital Services Act (s. 280). Autor widzi także konieczność szerszego wykorzystania danych biometrycznych jako narzędzia służącego identyfikacji sprawców, a także stworzenia ram prawnych dla legalnej infiltracji przestrzeni Dark Web (s. 281). Trafnie zauważa, że każde rozszerzenie uprawnień organów ścigania wiąże się z ryzykiem nadużyć i naruszenia praw obywateli, w tym prawa do prywatności, dlatego proponuje określone zabezpieczenia (s. 283).

Wiele uwagi autor poświęca wykorzystaniu nowych technologii w identyfikacji sprawców (s. 283 in.). Uważa, że w kontekście art.287 k.k. oraz proponowanego rozszerzenia uprawnień organów ścigania w zakresie czynności pozaprocesowych, następujące technologie są bardzo ważne: sztuczna inteligencja, blockchain, analiza big data i narzędzia biometryczne, gdyż pełnią ważną rolę w wykrywaniu i identyfikacji sprawców (s. 283). Następnie autor odnosi się szczegółowo do wymienionych technologii, podkreślając konieczność dokonania zmian legislacyjnych. Jednocześnie ma na uwadze w swoich rozważaniach ryzyko naruszenia praw obywatelskich (s. 288). Szerzej zajmuje się zagadnieniami sztucznej inteligencji, np. w postępowaniu przygotowawczym (s. 292 in.), zauważa przy tym, że kodeks postępowania karnego nie zawiera przepisów regulujących stosowania sztucznej inteligencji (s. 294).

Autor przygotował propozycje de lege ferenda w zakresie stosowania sztucznej inteligencji w postępowaniu przygotowawczym (s. 296 in.), które omawia, niewątpliwie mogą one być interesujące i godne rozważenia. Proponowaną regulację autor rozszerza na inne kwestie związane z nowymi technologiami.

8. W rozdziale VIII autor zajmuje się metodologicznymi podstawami badań (s. 300-313), odnosząc się do: sytuacji problemowej, przedmiotu badań, metody, techniki i narzędzi badawczych. Autor wyjaśnia ramy metodologiczne prowadzonych badań (s. 300), powyższe uwagi nie nasuwają uwag, są one poprawne. Podkreśla, że przyjął założenie, że rzetelne poznanie zjawiska oszustw komputerowych wymaga synergii wiedzy teoretycznej, badań empirycznych oraz doświadczenia praktycznego (s. 301).

Autor wychodzi z założenia, że przyjęty model w art. 287 k.k. oszustwa komputerowego nie przystaje w pełni do realiów współczesnych zagrożeń cyberprzestępczych (s. 392). Stąd widzi on lukę prawną (s. 303), którą stara się zapełnić w swoich wywodach. Przedmiot jego badań odnosi się do wymiarów: materialnoprawnego, procesowego i empirycznego (s. 304).

Autor stawia główny problem i hipotezę badawczą (s. 305), a także szczegółowe problemy i hipotezy badawcze (s. 305), problemów badawczych i hipotez badawczych wymienia jedenaście. Jako metodę badawczą, o czym sygnalizował autor we wprowadzeniu, wymienia: metodę dogmatycznoprawną, prawoporównawczą empiryczną i interdyscyplinarną (s. 308). Przygotowanie metodologiczne autora jest prawidłowe, zna ważne pozycje z literatury przedmiotu, ale nie dostrzega dorobku M. Zielińskiego. Do technik badawczych zalicza: pogłębione wywiady eksperckie z funkcjonariuszami Policji i biegłymi sądowymi oraz analizę statystyk przestępczości, studium przypadku wybranych spraw (s. 311). Jako narzędzia badawcze autor wymienia: kwestionariusze wywiadów półustrukturyzowanych, zestawienia statystyczne, analizę dokumentów normatywnych i raportów (s. 311). Zastosował w swoich badaniach techniki badań jakościowych i ilościowych o charakterze komplementarnym (s. 311), co zasługuje na uwagę, świadomie natomiast zrezygnował z badań akt sądowych.

9. W rozdziale IX autor omawia przeprowadzone badania (s. 314-430), jest to obszerna część rozprawy, świadcząca o dużym wysiłku badawczym, co należy podkreślić. Rozpoczyna swoje rozważania od wywiadów z funkcjonariuszami CBZC, nie podaje z iloma, ale z dalszych wywodów wynika, że dwoma, czy jest to liczba wystarczająca? Autor omawia szczegółowo pytania i odpowiedzi, stwierdzając, że odpowiedzi funkcjonariuszy zostały znacząco rozbudowane, aby dostarczyć dogłębnej analizy i przykładów, ale moje pytanie - przez kogo?, czy przez autora? (s. 314 in.). Pierwszy funkcjonariusz udzielił odpowiedzi na 19 pytań, a drugi na 20 pytań. Lektura tych pytań i uzyskanych odpowiedzi jest interesująca, godna wielu przemyśleń.

Autor stara się dokonać analizy przeprowadzonych przez siebie wywiadów (s. 335 in.). W analizie zwraca uwagę na osiem aspektów (s. 336) przy uwzględnieniu różnic między uzyskanymi odpowiedziami. Następnie przedstawia siedem wniosków z przeprowadzonej analizy (s. 341), z których wylicza pięć rekomendacji (s. 342) dla dalszych badań. Nie wiem czy można postawić następującą tezę: „Wyniki analizy wskazują na pilną potrzebę reform systemowych, aby

sprostać rosnącym zagrożeniom w cyberprzestrzeni" (s. 342), chyba jednak zbyt szczupły materiał badawczy do takiego stwierdzenia.

Autor przeprowadził także dwa wywiady z biegłymi sądowymi w zakresie informatyki śledczej (s. 342 in.), pierwszy biegły udzielił odpowiedzi na dwadzieścia pytań otwartych (s. 343 in.), a drugi również na dwadzieścia pytań (s. 349 in.). Autor dokonuje analizy otrzymanych odpowiedzi (s. 355 in.), na ich podstawie wymienia pięć wniosków (s. 357). Podejmuje także próbę oceny skali cyberprzestępczości ze szczególnym uwzględnieniem oszustw komputerowych w odniesieniu do danych policyjnych (s. 357 in.). Bardzo szeroko omawia dane policyjne otrzymane z KGP (s. 359 in.), dokonując analizy tych danych (s. 364), to ważna część rozprawy. Następnie autor omawia dane otrzymane z Prokuratury Krajowej (s. 384 in.). Kolejnym zagadnieniem badawczym jest analiza porównawcza danych Policji i Prokuratury Krajowej dotyczących cyberprzestępczości w latach 2014-2024 (s. 416 in.). Autor wskazuje także na dynamikę oszustw komputerowych w Polsce w kontekście europejskim.

10. Rozważania merytoryczne autor kończy wnioskami końcowymi (s. 430-433), są one syntetyczne, ale wynikające z przeprowadzonego wywodu.

Uważa, że jego założenia badawcze zostały zrealizowane i upoważniają go do realizacji zaproponowanych rozwiązań legislacyjnych. Uważam, że propozycje de lege ferenda wymieniane w tekście, nie zawsze precyzyjnie, powinny być wyeksponowane w punktach we wnioskach końcowych.

11. Bibliografia jest w zasadzie obfita, ale nie wyczerpująca, zabrakło wielu pozycji literatury polskiej, dlaczego autor przy niektórych pozycjach wymienia numery stron? Autor wymienia również akty prawne, w sposób niezbyt uporządkowany, brak tekstów jednolitych, chronologia aktów prawnych, do aktów prawnych autor zalicza wyroki sądowe!, bogate źródła internetowe.

III. Uwagi końcowe

1. Autor podjął temat interesujący, podejmowany już w literaturze przedmiotu, raczej incydentalnie, jego podejście do tematu zasługuje na uwagę. Trud badawczy był pracochłonny, autor wykazał wnikliwe zainteresowanie problematyką oszustwa komputerowego (szeroko pojętego), w temacie porusza się swobodnie, posiadając szeroką wiedzę, którą stara się podzielić z czytelnikiem, niektóre rozważania wykraczają poza temat główny, nie jest to zarzut.

2. Język rozprawy jest czytelny, dobry, korekta rzetelna, a wywód logiczny.

3. Poziom wyszkolenia metodologicznego autora jest wysoki, być może niektóre kwestie dogmatyki nauk prawnych wymagają jego dalszego studiowania, to taka luźna uwaga.

3. Rozprawa doktorska ma charakter wartościowy, świadczy o dużym stopniu wiedzy merytorycznej autora, który chciał ją przekazać w nadmiarze. Rozprawa zawiera w sobie znaczny ładunek krytycznej analizy i samodzielności autora - niewątpliwie zasługuje na pozytywną ocenę.

4. Rozprawa mgr Krystiana Bartosza pt. „Zwalczanie cyberprzestępczości na przykładzie oszustwa komputerowego -problemy dogmatyczne i dowodowe w postępowaniu przygotowawczym" stanowi oryginalne rozwiązanie problemu naukowego, spełnia więc wymogi rozprawy doktorskiej określone w art.187 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2024 r .poz.1571 ze zm.) i może stanowić podstawę do przeprowadzenia czynności w postępowaniu o nadanie stopnia doktora w dziedzinie nauk społecznych w dyscyplinie nauki prawne.

10.08.2026 r.