

Wrocław, dnia 26 lutego 2021 r.

Streszczenie rozprawy doktorskiej mgr Wojciecha Bijasa
napisanej pod kierunkiem promotora prof. dra hab. Dariusza Adamskiego
pt. „Rozpowszechnianie i posiadanie w przestępstwach komputerowych”

Wraz z rozwojem technologii, w prawie karnym pojawił się nowy rodzaj czynów zabronionych – przestępstwa komputerowe. Znaczna część norm prawnych, dotychczas dotycząca jedynie przestępstw „tradycyjnych”, rozszerzyła swój zakres zastosowania także na zachowania dokonywane w świecie wirtualnym. Nie inaczej było z przestępstwami polegającymi na rozpowszechnianiu i posiadaniu, gdyż wielu sprawców zaczęło udostępniać i przechowywać treści w postaci cyfrowej. Dostrzeżono przy tym, że sądy powszechne wykazują znaczne trudności z dokonywaniem oceny, czy do rozpowszechniania doszło, gdy czyn jest popełniany *online*. Nadto, wystąpiły wątpliwości, czy możliwe jest posiadanie treści cyfrowej bez władania nośnikiem danych (przedmiotem materialnym), co – wobec powszechności serwisów hostingowych – stanowi dla praktyki orzeczniczej ważkie zagadnienie. Na podstawie poczynionych obserwacji, połączonych ze znajomością funkcjonowania mediów elektronicznych, sformułowano dziewięć tez. Twierdzenia te zarówno ustalają przyczyny rzeczonych problemów, jak i dążą do ich rozwiązania. Konieczne było jednak ich udowodnienie poprzez przeprowadzenie dogłębnej analizy ich zasadności, czemu służyła rozprawa doktorska.

Tezy były dowodzone przy użyciu metody dogmatycznej, niejednokrotnie z zastosowaniem podejścia interdyscyplinarnego. Analizie poddano normy obowiązującego prawa, poglądy interpretacyjne doktryny prawniczej i judykatury (Sądu Najwyższego oraz sądów powszechnych). Praca, ze względu na charakter badanego tematu, zawiera elementy interdyscyplinarne, łączące prawo z naukami technicznymi, w szczególności informatyką. Porusza ona także zagadnienia z punktu widzenia różnych specjalizacji prawa karnego, a w szczególności prawa karnego materialnego, prawa karnego procesowego, kryminalistyki i kryminologii. Badania miały charakter jakościowy. Wystąpiły również elementy aktywistyczne, wyrażające się w utworzeniu nowych przesłanek rozpowszechniania i posiadania, a także w sformułowaniu postulatów *de lege ferenda* oraz *de lege lata*.

Przeprowadzono także studium (hipotetycznych) przypadków, celem wsparcia praktyki orzeczniczej i ukazania sposobu funkcjonowania utworzonych narzędzi interpretacyjnych.

Treść pracy – nie licząc wprowadzenia i zakończenia – została podzielona na sześć rozdziałów. Pierwsza część została poświęcona przybliżeniu pojęcia przestępstwa komputerowego oraz podziałowi przestępstw komputerowych na przestępstwa komputerowe *sensu stricto* i *sensu largo*. W drugim oraz trzecim rozdziale temat został skoncentrowany wokół tych czynów zabronionych, które wśród swych znamion zawierają pojęcie rozpowszechniania (rozdział 2) lub posiadania (rozdział 3) i mogą zostać popełnione przy użyciu komputera. Przeprowadzono w tym miejscu analizę każdego z tych przestępstw z osobna pod kątem rozumienia rzeczonych pojęć przez doktrynę prawniczą i Sąd Najwyższy. Jej celem było ustalenie, czy terminy te są rozumiane jednolicie bez względu na to, w jakim przepisie (przestępstwie) występują oraz czy występują rozbieżności interpretacyjne w ich obrębie. Finalnie wyabstrahowano ogólny obraz pojęcia rozpowszechniania, posiadania i posiadania w celu rozpowszechniania, stworzony przez doktrynę prawniczą i judykaturę Sądu Najwyższego, na gruncie analizowanych przepisów. Tak utworzone definicje – w końcowej części każdego z rozdziałów - poddano umotywowanej ocenie, podczas dokonywania której wskazano, za którymi poglądami opowiada się autor pracy oraz z jakiego względu. W tej części dowodzono dwóch tez. Pierwsza z nich zakłada, że przez pojęcie rozpowszechniania należy rozumieć uczynienie treści powszechnie dostępnej, tj. jako działanie wobec nieokreślonego kręgu osób i nieoznaczonej ich liczby, a nadto termin ten należy interpretować jednolicie, niezależnie od przestępstwa, które zawiera go w swoich znamionach. Należy mieć jednak na względzie, że przesłanka nieoznaczonej liczby osób nie ma charakteru bezwzględnego, albowiem w pewnych wąskich stanach faktycznych może nie wystąpić, pomimo zaistnienia rozpowszechniania. Ustalenie jej braku będzie jednak niezbędne do wykluczenia rozpowszechniania. Druga teza zakłada natomiast, że posiadanie – wbrew dotychczasowym poglądom doktryny prawniczej – należy odnosić do treści, nie zaś do nośnika treści, a tym samym możliwe jest posiadanie penalizowanych treści bez jednoczesnego władania nośnikiem danych, na której się znajdują. Doprecyzowane w ten sposób pojęcia rozpowszechniania oraz posiadania zostały zestawione z innymi pojęciami bliskoznacznymi używanymi przez ustawodawcę, celem zweryfikowania ich poprawności i uzyskania pełnej klarowności.

Tak wypracowane interpretacje posłużyły do przeprowadzenia analizy orzeczeń sądów powszechnych dotyczących przestępstw komputerowych polegających na rozpowszechnianiu i posiadaniu, czego dokonano w rozdziale czwartym. Uzasadniona w tym miejscu została teza,

zgodnie z którą sądy mają trudności z dokonywaniem subsumpcji w przypadku przestępstw komputerowych (polegających na rozpowszechnianiu i posiadaniu), pomimo, że w przypadku przestępstw „tradycyjnych” ustalenie kwalifikacji prawnej nie stanowi problemu (teza trzecia). W tym celu przedstawione zostało osiem założeń formułowanych przez judykaturę, z którymi trudno się autorowi zgodzić. Ukazane zostały także przyczyny, dla których pomimo relatywnie jednolitych poglądów doktryny prawniczej i orzecznictwa Sądu Najwyższego, stosowanie prawa w tym zakresie napotyka znaczne trudności. Wśród nich, pierwszorzędne znaczenie mają problemy z dokonywaniem subsumpcji oraz ustalaniem stanu faktycznego, będące częstokroć wynikiem niewystarczającej znajomości systemów informatycznych (teza czwarta). Co istotne, sądom znane były poglądy doktryny i orzeczenia Sądu Najwyższego, lecz często były stosowane nieprawidłowo, czego przyczyną była najprawdopodobniej nieprecyzyjność wykształconych przesłanek. W tej części pracy podjęto również próbę dowiedzenia, że sądy – podobnie jak doktryna prawnicza – odnoszą posiadanie do władania nośnikiem danych, nie zaś treści (teza piąta).

Dostrzeżone komplikacje, związane ze stosowaniem przepisów dotyczących przestępstw polegających na rozpowszechnianiu i posiadaniu dowiodły prawidłowości założenia, że konieczne jest sformułowanie nowych, dodatkowych przesłanek uznania określonego zachowania za rozpowszechnianie (teza szósta) oraz wytworzenie determinant, na podstawie których należy ustalać posiadacza treści cyfrowej w sieci internetowej (teza siódma). Przesłanki te zostały utworzone i przedstawione w rozdziale piątym. Ich zwieńczeniem było wytworzenie „testu rozpowszechniania” oraz „testu posiadania”, które to narzędzia poprzez odpowiedzi na kilka pytań, mają pomóc sądom w dokonywaniu subsumpcji, a tym samym wesprzeć praktykę orzecniczą. Ta część będzie stanowiła *meritum* pracy doktorskiej.

Rozdział szósty przeznaczony został na przeprowadzenie studium (hipotetycznych) przypadków. Przeanalizowano najpopularniejsze metody rozpowszechniania i posiadania plików w sieci internetowej. W obrębie każdej z nich wskazano jakie sytuacje należy uznać za rozpowszechnianie lub posiadanie, a jakim powinno się odmówić tego przymiotu. Szczegółowa weryfikacja dowiodła jeszcze jednej tezy w zakresie rozpowszechniania – zakładającej, że systemy informatyczne cechują się bardzo dużą różnorodnością, a tym samym czynienie w tym zakresie uogólnień jest niewskazane (teza ósma). Dowiedzione również zostało, że podczas ustalania osoby sprawcy posiadania w sieci internetowej kluczowe jest zweryfikowanie, czy podejrzany miał uprawnienia władcze w stosunku do treści oraz, czy był świadomy władania nimi (teza dziewiąta).

Finalnie zostały sformułowane postulaty *de lege ferenda* i *de lege lata*. Część aktualnie obowiązujących przepisów wymaga bowiem – w ocenie autora - korekcji, mogącej wyeliminować trudności związane z ich stosowaniem. Konieczne było również zwrócenie uwagi na sposób przeprowadzania przez sądy procesu orzekania, w szczególności poprzez podkreślenie znaczenia rzetelnej analizy działania systemów informatycznych, którymi posługiwał się sprawca oraz zachęcenie do częstszego sięgania po dowód z opinii biegłych informatyków. Pracę zwięźczo przedstawieniem konkluzji, poczynionych na podstawie badań przeprowadzonych na potrzeby stworzenia niniejszej pracy.

Handwritten signature of Wojciech Bijas in cursive script, followed by a dotted line.

mgr Wojciech Bijas