Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych

Studium prawno-kryminalistyczne

Paweł Opitek

KRAJOWA SZKOŁA SĄDOWNICTWA I PROKURATURY

KWALIFIKACJA PRAWNA I OPIS ZNAMION PRZESTĘPSTW TELEINFORMATYCZNYCH

STUDIUM PRAWNO-KRYMINALISTYCZNE

PAWEŁ OPITEK

KRAKÓW 2023

RECENZENCI:
prof. dr hab. Tadeusz Tomaszewski
dr hab. Igor Zgoliński

WYDAWNICTWO KRAJOWEJ SZKOŁY SĄDOWNICTWA I PROKURATURY
Kierownik – dr Piotr Kosmaty
ADRES REDAKCJI
31-547 Kraków, ul. Przy Rondzie 5
tel. 12 617 96 39, fax 12 617 94 21
e-mail: redakcja@kssip.gov.pl

ISBN 978-83-952072-9-7
Nakład 500 egzemplarzy

Spis treści

Wstęp 5

Rozdział 1. Zagadnienia podstawowe 7
1.1. Uwagi wprowadzające 7
1.2. Metodologia przeprowadzonych badań 9
1.3. Opis znamion, kwalifikacja prawna czynu zabronionego i *modus operandi* 13

Rozdział 2. Przedmiot czynności wykonawczej w przestępstwach teleinformatycznych 22
2.1. „Informacje", „dane" i „dane informatyczne" 22
2.2. Subiektywna lub obiektywna ocena pojęć „informacje" i „dane informatyczne" 28
2.3. Hasła zabezpieczające dostęp do danych lub informacji 34

Rozdział 3. Przestępstwa przeciwko ochronie danych i informacji 39
3.1. Analiza spraw karnych dotyczących czynów z art. 267 § 1 k.k. 39
3.2. „Przełamanie" albo „ominięcie" zabezpieczenia informacji (art. 267 § 1 k.k.) 48
3.3. Różnica pomiędzy art. 267 § 1 k.k. a art. 267 § 2 k.k. 65
3.4. Analiza spraw karnych dotyczących czynów z art. 267 § 3 k.k. 76
3.5. Utrudnianie zapoznania się z informacją i niszczenie danych informatycznych (art. 268 k.k. i art. 268a k.k.) 91
3.6. Zakłócenie pracy systemu komputerowego (art. 269a k.k.) 106
3.7. Wytwarzanie programów komputerowych (art. 269b § 1 k.k.) 128

Rozdział 4. Przestępstwa ukierunkowane na bankowość elektroniczną 147
4.1. „Środek pieniężny zapisany na rachunku" 147
4.2. Własność środków zgromadzonych na rachunku i podmiot pokrzywdzony przestępstwem 153
4.3. Relacje pomiędzy art. 267 § 1-3 k.k., art. 278 § 1 k.k., art. 279 § 1 k.k. i art. 287 § 1 k.k. 160
4.4. Transakcje zbliżeniowe 178
4.5. Dodatkowe uwagi o kwalifikacji prawnej czynu z art. 287 § 1 k.k. 189
4.6. Oszustwa w cyberprzestrzeni (art. 286 § 1 k.k.) 202

Rozdział 5. Przestępstwa z wykorzystaniem kryptoaktywów **224**
5.1. Tokeny cyfrowe 224
5.2. Status prawny kryptoaktywów 230
5.3. „Kradzież" bitcoina 246
5.4. Pozostałe przestępstwa dokonywane z wykorzystaniem walut wirtualnych 257
5.5. Zabezpieczenie majątkowe na kryptowalutach 275
5.6. Cyfrowe artefakty w grach komputerowych 283
5.7. Nielegalny hazard z wykorzystaniem walut wirtualnych 288
5.8. Skiny (analiza przypadku) 297

Podsumowanie **303**

Bibliografia **317**

Wstęp

„Transakcje oszukańcze kartą płatniczą", „skimming w bankowości elektronicznej", „cyberprzestępczość w pracy prokuratora", „wykorzystanie kryptoaktywów do popełniania przestępstw" – to zagadnienia, które stanowiły przedmiot moich wcześniejszych książek. Monografia pt. *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawno-kryminalistyczne* konsekwentnie wpisuje się w realizowany od 2016 r. plan badawczy nad przestępczością dotyczącą świata wirtualnego oraz nowych technologii. Jest także jego podsumowaniem, gdyż ostatecznie dla sędziego i prokuratora najważniejsza jest treść sporządzonego wyroku czy postanowienia kończącego postępowanie dowodowe. Prezentowana monografia dotyczy właśnie analizy ponad dwustu decyzji finalnych.

Czy warto było podjąć taki wysiłek badawczy? Odpowiedź na tak postawione pytanie jest twierdząca, gdyż książka ma praktyczny walor dla pracy sędziów i prokuratorów, o czym będzie jeszcze mowa w dalszej części opracowania. Jednak warto także pokochać to, co się robi. Na pozór wydaje się, że trudno odnaleźć pasję w studiowaniu przestępczości komputerowej. To zagadnienie dotyczące w dużej mierze technologii, gdzie człowiek występuje niejako w tle, często wyeliminowane zostają wszelkie odniesienia do ludzkich uczuć, a na pierwszy plan wysuwają się systemy komputerowe, informatyczne i teleinformatyczne. To prawda, ale jednocześnie analiza przestępczości teleinformatycznej dokonywana jest na dużym poziomie abstrakcyjności, co wymaga zdolności pojęciowego ujmowania rzeczywistości, tworzenia wyobrażeń właściwych dla różnego rodzaju ataków hakerskich, narzędzi IT czy socjotechniki.

Badanie tego rodzaju przestępczości wymusza na sędziach i prokuratorach posiadanie umysłu analitycznego, wyobraźni i nowatorskości, ponieważ kreatywność cyberprzestępców nie zna granic. Parafrazując słowa wieszcza: studiując kwalifikację prawną i opis znamion przestępstw teleinformatycznych, sięgajmy tam, gdzie wzrok nie sięga. Bo chodzi przecież o wirtualną przestrzeń oraz cyfrowe artefakty i przełamywanie utartych schematów myślenia.

Dziękuję wszystkim osobom, które pomogły mi w przeprowadzeniu badań i wydaniu książki. Dziękuję za przychylność Radzie Programowej i Dyrekcji Krajowej Szkoły Sądownictwa i Prokuratury.

Paweł Opitek

Rozdział 1
Zagadnienia podstawowe

1.1. Uwagi wprowadzające

Tytuł książki brzmi: *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych*, a jej podtytuł doprecyzowuje, że chodzi o studium prawno-kryminalistyczne, a więc przedstawienie sposobu działania sprawców popełniających takie przestępstwa. Jeśli chodzi o przestępstwa nazywane teleinformatycznymi, to przywołana nazwa ma charakter umowny, gdyż nie sposób wskazać na ich zamknięty katalog. W większości przypadków dotyczą one czynów zabronionych stypizowanych w rozdziale XXXIII k.k.[1] i popełnianych „zdalnie" oraz ukierunkowanych na informacje, dane informatyczne, systemy informatyczne oraz sieci teleinformatyczne. Jednak wspomniany kodeks zawiera także inne przestępstwa, których przedmiotem zamachu są cyfrowe artefakty w postaci danych zapisanych na serwerach, w pamięci stacjonarnego komputera lub laptopa albo danych znajdujących się „w locie", tj. przesyłanych za pomocą łączy lub fal radiowych. Mowa przykładowo o art. 279 § 1 k.k., a więc sytuacjach związanych z włamaniami do mobilnych aplikacji bankowych i zaborem w celu przywłaszczenia środków zapisanych na rachunku, manipulacji danymi do zarządzania kryptowalutami czy „kradzieżą" awatarów w grach komputerowych (art. 287 § 1 k.k.). Przestępstwa takie zasługują na miano „teleinformatyczne".

Autor postawił sobie za cel, aby książka miała charakter eklektyczny, tj. nie dotyczyła wyłącznie wykładni przepisów prawa materialnego, ale także odwoływała się do kwestii proceduralnych, m.in. współpracy organu procesowego z biegłym o specjalności informatyka śledcza, czy realizacji zabezpieczania majątkowego na bitcoinie[2]. Wszystko w celu szerokiego naświetlenia metodyki prowadzenia postępowań karnych dotyczących nowych technologii w świetle formułowania opisu czynu. Nieprzypadkowo w tytule książki wskazano, że chodzi o studium prawno-kryminalistyczne podjętego tematu badawczego, gdyż wykładnia znamion przestępstwa nierzadko wymaga zrozumienia sposobu funkcjonowania nowoczesnych narzędzi i usług wykorzystywanych

[1] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138 z późn. zm.), dalej jako: k.k. lub Kodeks karny.

[2] W książce przyjęto, że „Bitcoin" pisany dużą literą oznacza program komputerowy w postaci księgi rozrachunkowej (blockchain), a „bitcoin" zaczynający się małą literą to jednostka obrachunkowa zarządzana przez protokół Bitcoina. Rozróżnienie takie jest konieczne, ponieważ dotyczy dwóch różnych, chociaż połączonych ze sobą, wartości binarnych i ma podstawowe znaczenie dla opisu czynu dotyczącego blockchaina i kryptowalut oraz jego kwalifikacji prawnej. Przykładowo, inaczej będzie brzmiała odpowiedź na pytanie, czy można ukraść „Bitcoina", a inaczej, czy „bitcoina". Uzasadnienie dla przyjęcia takiej pisowni akceptowane jest także na gruncie języka polskiego (zob.: https://dailyweb.pl/wielki-slownik-inwestora-bitcoin-wszystkie-pojecia-w-jednym-miejscu/ [dostęp: 12.07.2022], https://sjp.pl/bitcoin [dostęp: 12.07.2022]). Identyczne zasady pisowni autor przyjął w stosunku do pozostałych projektów i tokenów działających w oparciu o technologię blockchain, a obecnie ich liczba szacowana jest w tysiącach.

zarówno przez pokrzywdzonych, jak i przestępców. Dotyczy to realizacji transakcji kartą płatniczą, przetwarzania danych informatycznych przez komputer, czy funkcjonowania protokołu Bitcoina. Oczywiście, nie można wymagać, aby każdy prawnik znał wszystkie tajniki fintechu, jednak rozpatrując konkretną sprawę, powinien dysponować przynajmniej podstawową znajomością technologicznych aspektów czynu. W tym momencie dotyka się sfery właściwej dla kryminalistyki jako nauki praktycznej, zajmującej się technicznymi i taktycznymi aspektami śledztwa dotyczącymi m.in. zabezpieczenia i wykorzystania śladów cyfrowych, oględzin i przeszukania w wirtualnym świecie, czy metodyki przesłuchania hakera w taki sposób, aby uzyskać od niego wszystkie, niezbędne informacje. Bez takiej wiedzy organy ścigania oraz sąd nie są zdolne do efektywnego prowadzenia spraw z zakresu cyberprzestępczości.

Impuls do napisania książki stanowiła poczyniona przez autora obserwacja, wynikająca z doświadczenia związanego z wykonywaniem zawodu prokuratora, że kwalifikacja prawna i opis przestępstw teleinformatycznych stanowią problem dla sędziów i prokuratorów. Chodzi o to, że stosując prawo, zbyt często oceniają oni podobne, a niekiedy niemal identyczne, stany faktyczne w odmienny sposób, a więc niektóre z tych rozstrzygnięć są błędne. Część rozbieżności dotyczy skomplikowanego charakteru sprawy i dają się one w pewien sposób usprawiedliwić, ale zbyt wiele błędów jest tak oczywistych, że nigdy nie powinny się zdarzyć. Najgorzej, jeśli wynikają one z pewnego konformizmu organu procesowego polegającego na wyrywkowym stosowaniu poglądów doktryny lub orzecznictwa bez własnej, dogłębnej analizy rozpatrywanego zdarzenia. Szczególnie dotyczy to sytuacji, gdy śledztwo zostaje umorzone wobec niewykrycia sprawcy przestępstwa lub oskarżony przyznaje się do popełnienia zarzucanego mu czynu i wyrok skazujący ma charakter konsensualny. Wtedy żaden uczestnik postępowania nie jest zainteresowany „drążeniem" sprawy oraz wnikliwą analizą opisu i kwalifikacji prawnej czynu.

Zamiarem autora książki nie było wytyczanie ścisłych ram przeprowadzonej analizy, ale przekrojowe podejście do zagadnienia opisu i kwalifikacji prawnej czynów zabronionych popełnianych z wykorzystaniem nowoczesnych technologii oraz próba rozwiązania problemów, które pojawiły się w badanych aktach spraw karnych, a dyskutowanych także w orzecznictwie i doktrynie. Z tego względu nie podjęto rozważań nad niektórymi kwestiami ogólnymi, takimi jak chociażby definicja „cyberprzestępczości" czy komentowanie poszczególnych elementów składowych każdego przestępstwa tak, jak ma to miejsce w klasycznych komentarzach do Kodeksu karnego. Książka, oprócz naukowego, posiada również charakter praktyczny i stanowi w założeniu źródło wiedzy dla sędziów i prokuratorów w momencie, gdy będą rozstrzygać konkretne sprawy. Jej autor nie twierdzi, że prezentowane przez niego poglądy wyczerpują polemikę w zakresie spornych treści; przeciwnie, ma świadomość, że przeprowadzona analiza dotyczy nierzadko zagadnień skomplikowanych, które są i nadal będą żywo dyskutowane. Na większość problemów badawczych udało się odpowiedzieć w sposób jednoznaczny, ale

niektóre przeciwstawne poglądy co do kwalifikacji prawnej i opisu przestępstw teleinformatycznych opierały się na równorzędnych racjach i stanowcze poparcie jednego z nich było trudne. Dlatego autor nie rości sobie prawa do uznania, iż rozwiązał w sposób całościowy i ostateczny wszystkie poruszone w monografii kwestie, bo też wykładnia przepisów prawa nigdy nie jest definitywna i ostateczna. Na tym polega dyskretny urok zawodu prawnika. Jak metaforycznie ujął to wybitny francuski juryslingwista Jean-Claude Gémar: „prawo to kwestia słów", stąd też dyskurs prawny ma charakter polifoniczny.

1.2. Metodologia przeprowadzonych badań

Badanie przestępczości teleinformatycznej miało na celu rozwiązanie problemu naukowego, tj. udzielenie odpowiedzi na postawione pytania badawcze w celu sprawdzenia prawdziwości sformułowanej na wstępie hipotezy. Mając na uwadze, że problem naukowy to określona trudność, którą należy pokonać, wzbogacając obecny stan wiedzy o nowe elementy, autor pracy uznał, że uzyskane przez niego wyniki uzupełnią naukę o nowe spostrzeżenia i wnioski dotyczące omawianej przestępczości oraz zweryfikują (ewentualne) błędy i nieścisłości występujące w kwalifikacji prawnej i opisie konkretnych rodzajów przestępstw, pozwolą jeszcze lepiej poznać i zrozumieć, czym jest cyberprzestępczość, a ponadto udoskonalą metodykę prowadzenia czynności procesowo-kryminalistycznych na omawianym polu. W literaturze prawniczej brakuje bowiem kompleksowych i popartych aktualnymi badaniami opracowań na ten temat; spotkać można natomiast zawężone analizy bazujące na opisie jednej lub co najwyżej kilku spraw karnych.

Teza badawcza, która legła u podstaw napisania monografii, brzmiała: „Opis i kwalifikacja prawna przestępstw teleinformatycznych sprawia kłopoty sędziom i prokuratorom, co znajduje odzwierciedlenie w błędach dotyczących wydawanych przez nich rozstrzygnięć". W momencie przystąpienia do badań owo wstępne, prawdopodobnie prawidłowe twierdzenie o rzeczywistości, autor sformułował na podstawie własnego, kilkunastoletniego doświadczenia zawodowego nabytego przy realizacji spraw karnych oraz informacji uzyskanych w trakcie prowadzenia licznych szkoleń dla sędziów, prokuratorów oraz przedstawicieli służb ochrony prawa, gdzie dyskutowano na temat szeroko rozumianej cyberprzestępczości[3]. Analiza doktryny i orzecznictwa także dowodziła, że przestępczość teleinformatyczna rodzi trudności i kontrowersje co do charakterystyki znamion i kwalifikacji prawnej czynu. Zawarte w tezie logiczne przypuszczenie,

[3] W 2020 r. w jednym z opracowań autor pisał: „Wciąż aktualne pozostaje (...) twierdzenie, że zachodzą spore rozbieżności w kwalifikacji prawnej podobnych stanów faktycznych przestępstw teleinformatycznych; np. ataki typu ransomware opisywano jako przestępstwo z art. 267 k.k., 268 k.k., 268a k.k., 269 k.k. lub 287 k.k.", [w:] P. Opitek, *Aspekty kryminalistyczne, techniczne i prawne przestępczości kryptowalutowej*, [w:] *Kryptowaluty – szanse i zagrożenia. Funkcjonowanie niepieniężnych środków płatniczych, jako strategiczne wyzwanie dla bezpieczeństwa systemu finansowego państwa, publikacja pokonferencyjna*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego 2020, s. 159–160.

graniczące z pewnością, miało jednak charakter ogólny i nieuporządkowany. Jego weryfikacja stanowiła zatem kwestię niezwykle ważną wobec coraz liczniejszych spraw dotyczących przestępczości teleinformatycznej i konieczności prawidłowego ich osądzania, co znajduje bezpośrednie przełożenie na sytuację procesową nie tylko podejrzanego (oskarżonego), ale także pozostałych uczestników postępowania karnego.

Sposobem badawczym dotarcia do prawdy oraz jej pojęciowego przedstawienia było empiryczne poznanie aspektów procesowych i kryminalistycznych przestępczości teleinformatycznej. Charakter twórczy pracy dyktował konieczność rozwiązania problemów naukowych i udzielenia odpowiedzi na pytanie: Jak powinien wyglądać prawidłowy opis czynu i jego kwalifikacja prawna w zakresie wybranych przestępstw teleinformatycznych?

W celu udzielenia na nie odpowiedzi, opracowano problemy cząstkowe:

1. Jaki obraz przestępczości teleinformatycznej wynika z akt postępowań karnych?
   a. Czego dotyczą sprawy?
   b. Jaki jest profil przestępcy?
   c. Jak wygląda *modus operandi* sprawców?
   d. Czy ściganie przestępców jest efektywne?
2. Czy prokuratorzy i sędziowie popełniają błędy w kwalifikacji prawnej i opisie znamion przestępstw teleinformatycznych? W przypadku gdy takie błędy występują, to:
   a. Na czym polegają?
   b. Z czego wynikają?
   c. Jakie są skutki procesowe tych błędów?
   d. Co zrobić, aby wyeliminować pojawiające się nieprawidłowości?
3. Jak kształtował się obraz czynności kryminalistyczno-procesowych w sprawach dotyczących przestępczości teleinformatycznej?
   a. Jakie typowe czynności podejmowano?
   b. Jakie narzędzia i metody są wykorzystywane do popełniania przestępstw?
   c. Jaka była rola biegłego z zakresu informatyki śledczej w analizowanych sprawach?

Chodzi więc o pytania problemowe (robocze), z którymi autor pracy musiał się zmierzyć, przy czym podstawowe, wynikające z przedmiotu badań, znaczenie miało zagadnienie: Czy prokuratorzy i sędziowie popełniają błędy w kwalifikacji prawnej i opisie znamion przestępstw teleinformatycznych?

Pozostałe pytania numer 1 i 3 niejako dopełniały prawną „diagnozę" przestępczości teleinformatycznej, ale zastosowane narzędzia badawcze nie były ukierunkowane na ich szczegółową eksplorację.

W literaturze przedmiotu podejmowano już próby udzielenia odpowiedzi na niektóre z wyżej opisanych kwestii, lecz zawsze czyniono to w sposób ogólny, na podstawie wiedzy cząstkowej, niezweryfikowanej badaniami naukowymi lub bazującej na niewielkiej próbie badawczej (tzw. analizie przypadku). Prokuratorzy i sędziowie wiedzieli np.,

że w omawianych sprawach zachodzi konieczność powołania biegłego z zakresu informatyki śledczej, gdyż ustalenie sposobu przeprowadzenia „ataku" należy do sfery „wiadomości specjalnych", ale brak było krytycznego, naukowego opracowania dotyczącego ustalenia, czy tacy biegli zawsze są powoływani, czego dotyczą ekspertyzy kryminalistyczne oraz jak ostatecznie przedstawia się ich wartość dowodowa. Przeprowadzone badania miały uzupełnić ów niedostatek informacji.

Kolejny element metodologii badań stanowiła hipoteza badawcza, a więc przypuszczenie odnośnie do przyszłej odpowiedzi na sformułowane wcześniej pytania. Brzmiała ona:

> Błędy w opisie czynu i kwalifikacji prawnej przestępstw teleinformatycznych wynikają z kilku przyczyn: specyficznych, a niekiedy wręcz trudnych do zrozumienia, cech przestępczości teleinformatycznej, zaniechania lub niewłaściwego prowadzenia czynności procesowo-kryminalistycznych, a także konformizmu organu procesowego i braku dociekliwości w jego podejściu do sprawy. Wszystko to powodowało niewłaściwe przyporządkowanie stanu faktycznego, ustalonego w procesie stosowania prawa do sformułowanej w wyniku wykładni normy prawnej.

Autor zakładał intuicyjnie, że jeśli w konkretnych okolicznościach faktycznych zbadanych spraw karnych występują pewne cechy stałe, to można uznać z prawdopodobieństwem graniczącym z pewnością, że owe cechy nie są przypadkowe i nie ograniczają się tylko do badanego materiału, ale dają podstawę dokonywania uogólnień co do obrazu przestępstw teleinformatycznych. Na podstawie poczynionych ustaleń wysnuto logiczne wnioski w celu udzielenia odpowiedzi na pytanie główne i pytania cząstkowe, a następnie zweryfikowano hipotezę badawczą.

Wyniki badań miały odpowiedzieć na pytanie, jakie są konkretne omyłki popełniane na omawianym polu, co jest ich przyczyną i jak orzekać prawidłowo. Sąd, jako organ stosujący prawo i wydający wyroki w imieniu Rzeczpospolitej Polskiej, powinien odznaczać się bowiem najwyższymi kompetencjami i profesjonalizmem w stosowaniu prawa, gdyż jego rozstrzygnięcia mają niebagatelny i wielowymiarowy wpływ na sytuację życiową oskarżonego, a także osoby pokrzywdzonej przestępstwem. Podobne uwagi odnoszą się do pracy prokuratora. Autorowi chodziło zatem o uchwycenie związków i różnic pomiędzy własnymi poglądami a istniejącym stanem wiedzy, uporządkowanie tejże wiedzy, wykrycie luk i sprzeczności poznawczych występujących w badanym obszarze i udzielenie na nie odpowiedzi. Podsumowując: hermeneutyczne objaśnienie zastanych poglądów, krytyczne porównanie ze sobą odmiennych stanowisk doktryny, próba rozwiązania kontrowersji w wykładni przepisów prawa, wyjaśnienie rodzących się na tym tle sprzeczności lub niejasności – w taki sposób autor pisał monografię.

W pracy zastosowano kilka metod badawczych rozumianych jako zasady dochodzenia do prawdy. Wspomniana prawda to Arystotelesowska „zgodność rzeczy z intelektem" wynikająca z realizmu poznawczego. Być może założenie takie brzmi egzaltowanie, ale w gruncie rzeczy ów wymóg „dociekania prawdy" musi przyświecać każdemu

prawnikowi, jeśli chce, aby jego książka miała jakąkolwiek wartość poznawczą. Sposobem dotarcia autora do prawdy oraz jej pojęciowego przedstawienia było empiryczne poznanie aspektów prawnych i kryminalistycznych przestępczości teleinformatycznej poprzez kwerendę akt postępowań karnych i analizę wybranych spraw, wykładnię obowiązujących przepisów, posiłkowanie się w tym procesie poglądami doktryny prawniczej oraz własnym doświadczeniem zawodowym, a ponadto ocenę wyroków sądowych opublikowanych w ogólnodostępnych bazach danych.

W przypadku analizy akt spraw sądowych skupiono się pod względem terytorialnym na obszarze właściwości Sądu Okręgowego w Krakowie. Okręg krakowski obejmuje bowiem dużą przestrzeń, a działające tutaj sądy rozpatrują znaczną liczbę spraw dotyczących badanej przestępczości, co automatycznie zwiększyło reprezentatywność przeprowadzonych badań w skali całego kraju. Najpierw autor zwrócił się pisemnie do prezesów: Sądu Okręgowego w Krakowie, Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie, Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie, Sądu Rejonowego dla Krakowa-Podgórza w Krakowie oraz Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o udzielenie zgody na przeprowadzenie badań akt prawomocnie zakończonych spraw karnych, które procedowane były w latach 2010–2021 i przyjęto w nich kwalifikację prawną czynów z artykułów od 267 k.k. do 269c k.k. oraz art. 287 k.k. Na podstawie uzyskanych zgód wystąpiono do przewodniczących: III i VI Wydziału Karnego Sądu Okręgowego w Krakowie, II Wydziału Karnego Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie, II i VIII Wydziału Karnego Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie, II Wydziału Karnego Sądu Rejonowego dla Krakowa-Podgórza w Krakowie oraz II Wydziału Karnego Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o ustalenia, z wykorzystaniem bazy CURRENDA, spraw dotyczących przestępczości teleinformatycznej na podstawie odpowiednich kwalifikacji prawnych czynów, a następnie ich udostępnienie do badań. Od 19 do 23 kwietnia 2021 r. w siedzibach krakowskich sądów autor zapoznał się z aktami kilkuset spraw karnych. Uzyskany tym sposobem materiał badawczy poddano dalszej analizie na potrzeby niniejszego opracowania, a część zaczerpniętych z niego orzeczeń zacytowano w książce.

Do napisania monografii wykorzystano także orzecznictwo sądów powszechnych zamieszczone na Portalu Orzeczeń Sądów Powszechnych (https://orzeczenia.ms.gov.pl/) i w programie LEX firmy WoltersKluwer.

Kolejna ścieżka badawcza skupiła się na przestępczości dotyczącej tokenów cyfrowych. W tym celu zwrócono się do wszystkich powszechnych jednostek organizacyjnych prokuratury w Polsce (tj. prokuratur rejonowych, okręgowych i regionalnych) o nadesłanie informacji o postępowaniach karnych prowadzonych w okresie od 1 stycznia 2016 r. do 30 czerwca 2019 r., w których:

1. waluty wirtualne były związane z popełnieniem czynu zabronionego (tj. z *modus operandi* sprawcy) – wraz z nadesłaniem skanów decyzji końcowych;

2. dokonano zabezpieczenia majątkowego na kryptowalucie – wraz z nadesłaniem skanów postanowień o zabezpieczeniu majątkowym;
3. dokonano poręczenia majątkowego, którego przedmiotem była kryptowaluta.

Na tej podstawie uzyskano informacje i dokumenty dotyczące przestępczości z wykorzystaniem kryptoaktywów oraz zrealizowanych poręczeń majątkowych we wskazanym okresie; następnie decyzje procesowe poddano analizie, a jej wyniki zawarto w opracowaniu.

Autor zastosował ponadto dopuszczalną w nauce metodę obserwacji jako sposób prowadzenia badań, dotyczącą opisu zjawiska na podstawie własnej interpretacji miarodajnych i wiarygodnych źródeł. Polegało to na analizie i krytyce piśmiennictwa prawniczego, tj. poglądów wyrażonych w artykułach naukowych oraz książkach dotyczących przestępczości teleinformatycznej, w tym komentarzach do Kodeksu karnego.

Uzyskane i opisane w monografii wyniki badań uzupełnią naukę prawa karnego o nowatorskie spostrzeżenia i ciekawe wnioski dotyczące przestępczości teleinformatycznej oraz zweryfikują (ewentualne) błędy i nieścisłości występujące na tym polu. Książka ma także znaczenie praktyczne, gdyż w zamyśle autora analiza tematu badawczego i zaproponowane w monografii rozwiązania zastanych problemów w wykładni prawa przełożą się na prawidłowe stosowanie przepisów przez sędziów i prokuratorów, a co za tym idzie, zwiększy się chociaż w pewnym stopniu efektywność ścigania sprawców czynów zabronionych.

1.3. Opis znamion, kwalifikacja prawna czynu zabronionego i *modus operandi*

Zadanie, jakie autor postawił sobie za cel, przygotowując tę książkę, to analiza przestępstw teleinformatycznych pod kątem ich ustawowych znamion oraz kwalifikacji prawnej na podstawie decyzji procesowych wydanych przez sądy i prokuratorów. Znamiona te stanowią zespół charakterystycznych, wspólnych i powtarzalnych cech czynu zabronionego właściwych dla określonego rodzaju zdarzeń prawnych umożliwiających ich typizację. W procesie subsumpcji okoliczności faktycznych pod konkretną normę prawną w celu stwierdzenia, czy przestępstwo miało miejsce, konieczne jest ustalenie wszystkich opisanych w ustawie znamion przestępstwa[4]. Typizacja oznacza zatem sformułowanie abstrakcyjnych opisów ludzkiego postępowania, zabronionego przez prawo karne, i polega na podaniu przez ustawodawcę schematów takiego postępowania, jeżeli mają one odpowiadać warunkom określonych typów przestępstw (ustawowa określoność czynu). W takim legalnym opisie typu przestępstwa „przedstawia się" zespół jego znamion, eksponując te cechy, które najdokładniej oddają istotę zachowania sprawcy[5].

[4] A. Pietras, M. Kawecki, *Ustawowe znamiona czynów zabronionych w części wojskowej kodeksu karnego w tabelach*, Warszawa 2017, s. 47–48.

[5] T. Bojarski, *Odmiany podstawowych typów przestępstw w polskim prawie karnym*, Warszawa 1982, s. 11.

Ów „bilans znamion" zawsze musi wskazywać w sposób precyzyjny i kategoryczny na jego prawną jedność; *a contrario* nie może on stwarzać jakichkolwiek wątpliwości co do tożsamości zdarzenia. Znamiona przestępstwa określają zatem granicę między zachowaniem karalnym a niekaralnym, a poza tym wskazują na takie ważne kwestie, jak ewentualne przedawnienie karalności, działanie sprawcy w ramach recydywy, przyjęcie konstrukcji czynu ciągłego lub zbiegu przestępstw; są gwarantem przestrzegania zasad *ne bis in idem* oraz *rei iudicata*. Z powyższych względów opis czynu ma kardynalne znaczenie zarówno dla prawidłowego stosowania prawa materialnego, jak i procesowego, wyrażając ich wzajemne powiązanie[6].

Wynika z tego, że prawidłowe wskazanie oraz opisanie wszystkich znamion czynu zabronionego ma podstawowe znaczenie dla realizacji norm prawa karnego. Trafnie ujął to Sąd Apelacyjny w Katowicach:

> W opisie czynu należy zawrzeć te elementy, które należą do istoty czynu przestępnego, a więc dotyczące podmiotu czynu, rodzaju atakowanego dobra, czasu, miejsca i sposobu popełnienia czynu oraz jego skutków. Chodzi o objęcie opisem wszystkich elementów historycznego zdarzenia mających znaczenie dla prawidłowej kwalifikacji prawnej, gdyż nieprzystawanie opisu zachowania oskarżonego do znamion ustawowych przestępstwa, które wskazuje przyjęta kwalifikacja prawna, prowadzi wprost do stwierdzenia obrazy prawa materialnego. Z powyższego wynika zatem, iż warunkiem skazania jest udowodnienie, że zachowanie sprawcy wyczerpywało wszystkie znamiona czynu określone w danym przepisie prawa materialnego[7].

Stąd wymóg, by formułowany przez prokuratora i sąd opis ustawowych znamion przestępstwa był precyzyjny oraz kompletny, co w przypadku przestępczości teleinformatycznej nie zawsze jest łatwe z kilku powodów. Po pierwsze, ustawodawca stosuje w regulujących ją przepisach wyrażenia ze „świata techniki", które należy odszyfrować w odniesieniu do konkretnych stanów faktycznych; chodzi m.in. o takie zwroty, jak „system informatyczny", „system teleinformatyczny" lub „sieci teleinformatyczne", mające szczególne znaczenie dla bytu przestępstwa i nierzadko ujęte w definicjach legalnych zawartych w ustawach pozakodeksowych. Są też wyrażenia, które w języku potocznym używa się zamiennie, ale na gruncie Kodeksu karnego muszą posiadać odmienny zakres

[6] A. Zachuta, *Opis i kwalifikacja prawna czynu z uwzględnieniem sprawczych odmian przestępnego współdziałania*, „Prokuratura i Prawo" 2005, nr 1, s. 53–45.

[7] Wyrok Sądu Apelacyjnego w Katowicach z dnia 5 kwietnia 2018 r., II AKa 273/17, LEX nr 2490242. Podobnie stwierdził Sąd Apelacyjny w Lublinie, iż przedmiotem postępowania przed sądem nie jest przedstawiony w zarzucie aktu oskarżenia opis konkretnego zdarzenia czy jego kwalifikacja, lecz zdarzenie historyczne przedstawione przez uprawnionego oskarżyciela. Fakt oceny prawnej zachowania oskarżonego przez pryzmat różnych przepisów ustawy karnej nakłada na prokuratora obowiązek, by formułując akt oskarżenia, opis czynu zarzucanego uwzględniał wszystkie znamiona przepisów, których naruszenie zarzuca się oskarżonemu, z uwzględnieniem wymogów z art. 332 § 1 pkt 2 k.p.k., [w:] Wyrok Sądu Apelacyjnego w Lublinie z dnia 14 marca 2018 r., II AKa 40/18, LEX nr 2469980. Podobnie: wyrok Sądu Najwyższego z dnia 22 marca 2012 r., IV KK 375/11, OSNKW 2012, nr 7, poz. 78; wyrok Sądu Apelacyjnego w Gdańsku z dnia 28 października 2015 r., II AKa 138/15, LEX nr 2191591.

znaczeniowy; dotyczy to np. „informacji" oraz „danych". Podobne są do siebie niektóre znamiona czynności wykonawczej omawianych przestępstw, jak chociażby zwroty: „przetwarzanie, gromadzenie lub przekazywanie danych informatycznych", a w konkretnym przypadku nierzadko problematyczna okazuje się kwestia, z którą formą manipulowania danymi ma się do czynienia. Z drugiej strony działanie sprawcy może powodować przekształcenie zapisu binarnego na wielu poziomach i wówczas należy podać najistotniejsze znamię skutku tak, aby zarzut nie był irracjonalnie rozbudowany, a więc nieczytelny dla stron postępowania. Sytuacja taka dotyczy m.in. „kradzieży" bitcoina. W końcu samo *modus operandi* sprawców przestępstw teleinformatycznych ma skomplikowany charakter pod względem skutków ich działania oraz użytych narzędzi IT. Wszystko to sprawia, że opis znamion czynu oraz wynikająca z niego kwalifikacja prawna przestępstwa są niekiedy trudne do określenia.

Jednak wspomniane trudności nie zwalniają sądu i prokuratora z obowiązku wyjaśnienia wszystkich istotnych okoliczności sprawy, co wynika z art. 366 § 1 k.p.k.[8] i art. 413 § 2 pkt 1 k.p.k., a następnie dokładnego określenia w orzeczeniu przypisanego oskarżonemu (podejrzanemu) czynu. Kodeks postępowania karnego nie określa wprost, na czym to polega. Wskazówkę w tym zakresie zawiera art. 332 § 1 pkt 2 k.p.k. stanowiący, że akt oskarżenia powinien zawierać dokładne określenie zarzucanego oskarżonemu czynu ze wskazaniem czasu, miejsca, sposobu i okoliczności jego popełnienia oraz skutków, a zwłaszcza wysokości powstałej szkody. Precyzyjne określenie, o którym mowa w art. 332 § 1 pkt 2 k.p.k., to dokładny opis wszystkich jego elementów mających znaczenie dla prawidłowej kwalifikacji przestępstwa, niepomijający żadnego aspektu zachowania należącego do ustawowych znamion. Jednak nadmierna kazuistyka także nie jest wskazana. Jak zauważył Sąd Apelacyjny w Szczecinie, zwrot „dokładny opis" należy rozumieć jako wymóg objęcia nim wszystkich elementów istotnych, mających znaczenie dla indywidualizacji czynu, nie zaś konieczność szczegółowego opisywania każdej z czynności sprawczych lub każdego zachowania, jakie przestępca podjął. Generalnie stopień konkretności i szczegółowości opisu zależy od lingwistycznego ujęcia typu przestępstwa w przepisach prawa materialnego, od sposobu działania sprawcy, w pewnej mierze także od zgromadzonego w sprawie materiału dowodowego[9]. Podobnie zawyrokował Sąd Apelacyjny w Katowicach, że taki opis

> zamieszczony, czy to w akcie oskarżenia, czy to w wyroku, musi oczywiście odpowiadać pełnemu zespołowi znamion określonych w przepisie ustawy karnej. Nie oznacza to wszelako, że jedyną formą realizacji tego wymagania jest wierne przytoczenie słów

[8] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2022 r. poz. 1375 z późn. zm.), dalej jako: k.p.k. lub Kodeks postępowania karnego.

[9] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 28 września 2017 r., II AKa 192/16, LEX nr 2391897. W jednym z wyroków Sąd Apelacyjny we Wrocławiu stwierdził, że opis czynu może być dokonany na odpowiednim stopniu ogólności, istotne jest jednak to, aby odpowiadał on pełnemu zespołowi znamion przewidzianych w przepisie określającym dany typ czynu zabronionego, [w:] wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 września 2014 r., II AKa 242/14, LEX nr 1527320.

> ustawodawcy. Dopuszczalne jest natomiast zarówno posłużenie się sformułowaniami równoważnymi językowo, jak i takie zwerbalizowane przedstawienie działania oskarżonego, które w sposób nie pozostawiający wątpliwości odpowiada treści poszczególnych znamion przypisanego mu przestępstwa, albo w drodze nieodpartego logicznego wnioskowania świadczy o wyczerpaniu konkretnego elementu składającego się na ustawowy obraz określonego czynu zabronionego[10].

Autor nie zgadza się natomiast z twierdzeniem, jakoby opis czynu w przeważającej liczbie przypadków był „bogatszy od treści zastosowanej normy, gdyż poza niezbędnymi znamionami musi częstokroć obejmować dalsze elementy i okoliczności mające chociażby tylko znaczenie procesowe"[11]. Otóż, okoliczności modalne wykraczające poza zakres znamion przestępstwa, np. stan nietrzeźwości lub pozostawanie pod wpływem środka odurzającego, mogą wpływać na dyrektywy wymiaru kary i wcale nierzadko stanowią ważną część ustaleń faktycznych; jeśli nie należą jednak do samych ustawowych znamion, to nie powinny być zamieszczane w opisie przestępstwa, gdyż nie stanowią o jego bycie *per se*.

Postulat precyzyjnego określania znamion zarzucanego oskarżonemu czynu trudno byłoby zrealizować w praktyce, jeśli ustawodawca nie respektowałby zasad przyzwoitej legislacji, stanowiących element doktryny demokratycznego państwa prawnego. Trybunał Konstytucyjny stwierdził, że zasady te obejmują między innymi wymaganie określoności przepisów, które muszą być formułowane w sposób poprawny, precyzyjny i jasny, a standard ten wymagany jest, zwłaszcza gdy chodzi o ochronę praw i wolności[12]. Z reguły tej wynika, że każdy przepis winien być skonstruowany poprawnie z punktu widzenia językowego oraz logicznego i dopiero spełnienie tego podstawowego warunku pozwala na jego ocenę w aspekcie pozostałych kryteriów. Wymóg jasności oznacza nakaz tworzenia przepisów klarownych i zrozumiałych dla ich adresatów, którzy od racjonalnego ustawodawcy oczekiwać mogą stanowienia norm prawnych niebudzących wątpliwości co do treści nakładanych obowiązków i przyznawanych praw. Związana z jasnością precyzja przepisu winna przejawiać się w konkretności nakładanych obowiązków i przyznawanych praw tak, by ich treść była oczywista i pozwalała na wyegzekwowanie się[13]. Analiza wyroków sądowych oraz prokuratorskich postanowień pokazuje, że postulat dokładnego określenia *in concreto* wszystkich znamion czynu zabronionego, w sposób logiczny i jasny, nie zawsze był realizowany. Nieprzypadkowo zatem autor już ponad sześć lat temu napisał słowa, które nie straciły na swej aktualności:

> Spośród wielu wyzwań stojących przed ustawodawcą w związku ze wzrostem cyberprzestępczości, jedno z podstawowych stanowi określenie, co jest dozwoloną aktywnością w cyberprzestrzeni, a jakie zachowania prawo karne uważa za przestępstwo.

[10] Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 stycznia 2014 r., II AKa 397/13, LEX nr 1428051.
[11] A. Zachuta, *Opis i kwalifikacja prawna czynu*…, s. 53–45.
[12] Wyrok Trybunału Konstytucyjnego z dnia 11 stycznia 2000 r., K. 7/99, OTK ZU 2000, nr 1, poz. 2.
[13] Wyrok Trybunału Konstytucyjnego z dnia 21 marca 2001 r., K 24/00, OTK 2001, nr 3, poz. 51.

> Problem jest na tyle skomplikowany, że w tym kontekście coraz trudniejszy w realizacji staje się postulat, jakoby przepisy prawa zawsze mogły być jasne i w pełni zrozumiałe dla „przeciętnego" obywatela. Jeśli w przypadku zabójstwa każdy dorosły człowiek ma świadomość, na czym ono polega i jakie zachowanie jest zabronione, to wytyczenie ścisłych granic pomiędzy dozwolonym i niedozwolonym hakingiem nie jest już takie proste; m.in. sam termin „haking" ma wiele, często odbiegających od siebie znaczeń. Patrząc na problem z szerszej perspektywy, to praktycznie odchodzi w przeszłość dotychczasowe rozumienie dogmatu „racjonalnego ustawodawcy", jako posiadającego pełną wiedzę językową, prawniczą i naukową z zakresu przedmiotu regulacji aktu normatywnego oraz wiedzę o skuteczności działań. Na tej podstawie zakłada się (idealizuje), że każdy tekst prawny jest w pełni racjonalny, zbudowany na spójnej wiedzy i niesprzecznych ocenach. Rolą osoby stosującej prawo jest natomiast odnalezienie owej racjonalności, a następnie dokonanie właściwej wykładni. Pisząc „wykładnia" autor ma na myśli proces zrozumienia przepisów oraz rezultat tego zrozumienia, znajdujący odzwierciedlenie w decyzji procesowej. Świat staje się na tyle skomplikowany, że coraz trudniej tworzyć przejrzyste i łatwe do zrozumienia normy prawne, szczególnie, jeśli chodzi o prawo nowych technologii[14].

Wyniki przeprowadzonych badań potwierdziły ten pogląd i autor parokrotnie nawiązał do niego w dalszej części opracowania.

Skoro zostało wywołane słowo „wykładnia", to należy stwierdzić, że najważniejsza kwestia, będąca probierzem prawidłowego opisu czynu i jego kwalifikacji prawnej, dotyczy wykładni prawa.

Język, którym ludzie komunikują się między sobą, jest ze swej istoty wieloznaczny, a wykładnia prawa polega na redukcji owej wieloznaczności, tj. polisemiczności zwrotów językowych. Pojawia się ona każdorazowo, gdy prokurator lub sędzia styka się z tekstem prawnym i tylko stosując metody wykładni, można zrozumieć wytwór ducha ludzkiego, jakim jest prawo, a normy *in abstracto* przekuć w okoliczności konkretnego czynu. Celem wykładni jest zatem uzyskanie normy prawnej rozumianej jako wzorzec zachowania się nakazanego przez ustawę. Natomiast przepis prawny to najmniejsza jednostka redakcyjna aktu normatywnego, w której ujęta jest treść w formie zdania (artykułu, paragrafu, ustępu, punktu). W praktyce organy procesowe posługują się takimi zwrotami, jak: „dekodowanie normy", „rekonstrukcja przepisu", „przepis będący podstawą normy", „przepis znaczy", „z przepisu wynika, że", „tekst nie pozostawia wątpliwości", zrównując, nawet bezwiednie, pojęcie normy prawnej z przepisem prawa. Wypada jednak przypomnieć, że w 1992 r. Trybunał Konstytucyjny w pełnym składzie podjął uchwałę, w której stwierdzono, że „nie można utożsamiać przepisu z normą. Norma

[14] P. Opitek, *Legalny haking w Polsce – krytyczna ocena uregulowań Kodeksu karnego*, [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018, s. 115.

prawna może wynikać z kilku przepisów, a także jeden przepis może wyrażać więcej niż jedną normę prawną”[15].

Jeśli w przypadku przestępczości teleinformatycznej organ procesowy ma do czynienia z niełatwymi do oceny prawnej stanami faktycznymi, to zasadnicze wydaje się pytanie: Którą metodę lub metody wykładni zastosować, aby osiągnąć pożądany efekt, zawierający się w słowach „sprawiedliwy wyrok”?

Autor, chcąc rozstrzygnąć problem, jaką wykładnię zastosować do odkodowania znamion przestępczości teleinformatycznej, miał na uwadze dwie podstawowe teorie: klaryfikacyjną i derywacyjną. Pierwsza głosi, że normę postępowania zawiera sam tekst prawny, zatem musi on także – w wypadku prawa karnego – samoistnie wyrażać znamiona. W takim układzie norma prawa karnego materialnego jest inferencją (wnioskiem) zdekodowanych znamion ustawowych i ontycznie niczym więcej. W teorii klaryfikacyjnej wykładnia kończy się na etapie wykładni prowadzonej w granicach ogółu wyrazów wchodzących w skład danej regulacji, a metody celowościowa i systemowa mogą posiadać status co najwyżej subsydiarny. Teoria derywacyjna zakłada natomiast coś przeciwnego: najpierw deszyfruje się wzorzec powinnego zachowania i dopiero na tej podstawie wnioskuje się o znaczeniu poszczególnych znamion. W teorii derywacyjnej zrezygnowano z jawnego operowania dyrektywą językowej granicy wykładni, a uzyskane znaczenie można wydobyć także za pomocą metody funkcjonalnej i systemowej.

Bazując na metodzie klaryfikacyjnej i derywacyjnej, autor ostatecznie uznał, że najbardziej zbieżna z potrzebami prawa karnego, szczególnie w zakresie gwarancyjnym, jest konstrukcja teoretyczna, polegająca na uznaniu całego tekstu aktu normatywnego, jako definicji *sensu largo*, gdzie raz ustalone znaczenie znamienia jest konsekwentnie przyjmowane w procesie rekonstrukcji pozostałych norm prawnych[16]. Istotną rolę odgrywają zatem tzw. dyrektywy wykładni językowo-logicznej, nazywanej także literalną, które nie są bezpośrednio związane z żadną konkretną teorią wykładni, a stanowią powszechnie uznane reguły egzegezy, nie pozostające w sprzeczności z metodami wykładni klaryfikacyjną i derywacyjną. Dyrektywami wykładni językowo-logicznej są ogólne wskazania: zakaz wykładni homonimicznej i synonimicznej, dyrektywa stosowania języka prawnego i definicji legalnych, czy dyrektywa stosowania języków specjalistycznych. Taka konstrukcja teoretyczna skupia się przede wszystkim na znaczeniu językowym poddanego wykładni tekstu prawnego, ale też pozwala określać zakres penalizacji w pewien sposób niezależnie od znaczenia poszczególnych wyrazów (znamion). Wynika z tego, że organ dekodujący normę prawną winien ograniczyć luz interpretacyjny do alternatyw wynikających z tekstu prawnego, a nie kierować się determinantami pozatekstowymi. Jak podaje A. Kotowski, odgrywa to szczególną rolę dla sądu karnego, gdyż ta gałąź prawa wiąże się z precyzyjnym i wystandaryzowanym ustalaniem granic

[15] Uchwała Trybunału Konstytucyjnego z dnia 29 stycznia 1992 r., W 14/91, OTK 1992, poz. 20.

[16] Zob. A. Kotowski, *Z problematyki metody interpretacji językowo-logicznej – uwagi na gruncie dekodowania znaczenia prawno-karnego*, „Prokuratura i Prawo” 2015, nr 6, s. 132–133.

odpowiedzialności prawnej. Ta swoista linia demarkacyjna wyznaczona jest przez znaczenia językowe użytych w tekście prawnym zwrotów[17].

Chociaż dla autora determinującym stadium wykładni była metoda literalna, to jednak nie sposób było całkowicie uciec od koncepcji derywacyjnej. Nawet bowiem, jeśli Sąd Najwyższy wyraził w uchwale pogląd o pierwszeństwie wykładni językowej, gdyż w innym przypadku rola ustawodawcy byłaby pozorna[18], to w orzecznictwie tego samego sądu znajduje oparcie twierdzenie, że proces wykładni powinien polegać na zastosowaniu wszystkich metod: językowej, systemowej i funkcjonalnej. Jednak odstąpienie od rezultatów wykładni językowej może być uzasadnione jedynie ważnymi powodami[19], gdy:

1. sens językowy jest ewidentnie sprzeczny z fundamentalnymi wartościami konstytucyjnymi, a z istotnych powodów uchylenie przepisu byłoby w danym momencie niemożliwe lub niecelowe;
2. wykładnia językowa prowadzi do rozstrzygnięcia, które w świetle powszechnie akceptowanych wartości musi być uznane za rażąco niesłuszne, niesprawiedliwe, nieracjonalne lub niweczące *ratio legis* interpretowanego przepisu;
3. wykładnia językowa prowadzi *ad absurdum*;
4. zachodzi oczywisty błąd legislacyjny[20].

Sytuacje odstąpienia od ścisłej wykładni językowej znamion przestępstw teleinformatycznych autor monografii traktował jako wyjątkowe, kierując się założeniem, że rozumienie prawa nie może mieć charakteru prawotwórczego poprzez m.in. dodawanie określonych elementów normatywnych w przypadku istnienia luki konstrukcyjnej przepisu. Sąd Najwyższy podkreślił bowiem, że organ procesowy nie jest uprawniony do korygowania (w jego przekonaniu) niesłusznych unormowań[21]. Na gruncie prawa karnego dopuszczalny jest zatem tylko taki wynik dekodowania norm z zastosowaniem innych metod, aniżeli gramatyczna, który mieści się w zakresie tolerowanym przez rezultat wykładni językowej[22]. Nie zmienia to faktu, że prawna rzeczywistość, związana

[17] Tamże, s. 124.

[18] Uchwała Sądu Najwyższego z dnia 20 czerwca 2000 r., I KZP 16/00, OSNKW 2000, nr 7–8, poz. 60. Jak pisze L. Morawski: „W teorii prawa utrwaliło się przekonanie o pierwszeństwie wykładni językowej i pomocniczym charakterze wykładni systemowej i funkcjonalnej", [w:] L. Morawski, *Wstęp do prawoznawstwa*, Toruń 2014, s. 146, 154–155; subsydiarny charakter wykładni systemowej wyraźnie przyjmuje także M. Zieliński, [w:] M. Zieliński, *Wykładnia prawa. Zasady–reguły–wskazówki*, Warszawa 2012, s. 237.

[19] K. Kmąk, *Odstąpienie od rezultatów wykładni językowej w prawie karnym (na kanwie uchwały Sądu Najwyższego z dnia 26 marca 2009 r., sygn. I KZP 35/08)*, „Studenckie Zeszyty Naukowe" 2019, vol. XXII, nr 42, s. 78; zob. też uchwała Sądu Najwyższego z dnia 29 października 2004 r., I KZP 24/04, LEX nr 125547.

[20] Uchwała Sądu Najwyższego z dnia 26 marca 2009 r., I KZP 35/08, OSNKW 2009, nr 5 poz. 33.

[21] Uchwała pełnego składu Izby Karnej Sądu Najwyższego z dnia 11 stycznia 1999 r., I KZP 15/98, OSNKW 1999, nr 1–2, s. 3. W uzasadnieniu do uchwały stwierdzono, że żaden sąd, w tym i Sąd Najwyższy, nie może wkraczać w kompetencje władzy ustawodawczej i – pod pozorem dokonywania wykładni określonego przepisu prawa lub interpretacji wzajemnego stosunku przepisów prawa – tworzyć, w istocie, zupełnie nową treść analizowanych przepisów lub zaprzeczać wynikającej wyraźnie z treści ustawy ich wzajemnej relacji. Negatywna ocena zawartej w obowiązujących przepisach prawnych treści normy może jedynie stanowić przyczynę sformułowania postulatu *de lege ferenda* i wystąpienia przez uprawniony podmiot z inicjatywą legislacyjną.

[22] K. Kmąk, *Odstąpienie od rezultatów wykładni językowej*…, s. 78.

m.in. z nowymi technologiami, znacznie poszerza obszar zasad i reguł sędziowskiego i prokuratorskiego stosowania prawa. Wobec trudności wykładni norm sankcjonujących przestępstwa komputerowe, akcentuje się wymóg większej aktywności przedstawicieli wymiaru sprawiedliwości w takich sprawach. Ocenie sędziego podlegają bowiem nie tylko kwestie legalności oraz techniki prawodawczej, ale także zagadnienia merytoryczne z dziedziny informatyki i nowych technologii. W konsekwencji, ustalenie znaczenia przepisu następuje z wykorzystaniem obszerniejszej, aniżeli miało to miejsce jeszcze kilkanaście lat temu, wiedzy[23].

W pracy sędziego i prokuratora szczególnie ważna jest także kultura stosowanego języka prawniczego, czym zajmuje się juryslingwistyka, tj. dział nauki łączący wiedzę i metodologię językoznawstwa z naukami prawa. Ów język, za pomocą którego mówi się o prawie, stanowi narzędzie komunikacji pomiędzy organami stosującymi przepisy Kodeksu karnego a adresatami wydawanych przez nie orzeczeń. W interpretacji przepisów zwroty określające znamiona przestępstw mają swoistą wagę, odbiegającą często od ich znaczenia w języku ogólnym. Ustawodawca, ustalając własne zasady interpretacji, tworzy nowe terminy i nadaje im oficjalne znaczenie[24], co ma specyficzny sens odnośnie do przestępstw teleinformatycznych. W tym przypadku bowiem w stosowaniu prawa dochodzi do transpozycji językowej zachowania sprawcy na znamiona przestępstwa w środowisku wieloznacznym i skomplikowanym terminologicznie. Jest to tym trudniejsze, że cyberprzestępczość podlega ciągłej ewolucji, co oznacza, że proces dostosowania języka prawniczego do zmieniającej się rzeczywistości ma charakter dynamiczny.

Na koniec pozostał do omówienia jeszcze dodatkowy element znajdujący się w tytule książki, tj. *modus operandi*. W ujęciu wąskim „sposób działania" przestępcy dotyczy samego momentu popełnienia czynu zabronionego, ale jedno z siedmiu „złotych pytań" kryminalistyki – *Quo modo?* – należy jednak analizować we wszystkich etapach realizacji czynu zabronionego. Zdarza się, że cyberprzestępca już w stadium przygotowawczym posługuje się specyficznym dla niego sposobem rozpoznania użytkowników Internetu, którzy następnie staną się obiektami „ataku". W tym celu może tworzyć charakterystyczne strony internetowe, każdorazowo „legendować się" w podobny sposób np. podszywać pod zdjęcia atrakcyjnych fizycznie, wzbudzających zaufanie mężczyzn po to, aby metodą *romance scam* nawiązywać wirtualne znajomości z kobietami. W stadium dokonania przestępstwa, *modus operandi* bazuje np. na specjalnym oprogramowaniu wykorzystywanym przez hakera, którego działanie, na pierwszy rzut oka, może przypominać inne skrypty malware, jednak Indywidualny Wskaźnik Atakującego (ang. *Indicator of Attack* – IoA) pozwoli przypisać „atak" zawsze tej samej osobie lub organizacji. IoA ustala się na podstawie daty, typu i celu ataku, a także zidentyfikowanych

[23] Zob. A. Machnikowska, *Zasady niezawisłości sędziów a wykładnia prawa*, [w:] M. Herman, S. Sykuna, *Wykładnia prawa. Tradycja i perspektywy.* Monografie Prawnicze, Warszawa 2016, s. 238–239.

[24] Por.: M. Sobieszewska, *Juryslingwistyka: między językiem i prawem*, „Studia Iuridica Lublinensia" 2015, nr 4, s. 128.

technik MITRE ATT&CK[25], wykorzystanych podatności i słabości skompromitowanego systemu itp. Istotne dla działań wykrywczych mogą okazać się także szczególne wyznaczniki postępowania sprawcy na etapie ukrycia korzyści pochodzących z przestępstwa poprzez np. pranie pieniędzy z wykorzystaniem specyficznego rodzaju walut wirtualnych. Stąd niekiedy mówi się o konieczności specjalizacji przedstawicieli organów ścigania w zakresie cyberprzestępczości także po to, aby potrafili oni odpowiednio wykorzystać wiedzę związaną z *modus operandi* w prowadzonych śledztwach. Czym przestępstwo jest bardziej skomplikowane, tym sposób działania sprawcy przybiera na wyrazistości, ale też ma wiele elementów trudnych do określenia, szczególnie jeśli chodzi o przestępczość teleinformatyczną.

W gruncie rzeczy zdiagnozowanie *modus operandi* ustalonego lub anonimowego sprawcy wpływa nie tylko na technikę i taktykę realizacji działań kryminalistycznych, ale pozostaje również w nierozerwalnym związku ze stosowaniem norm prawa karnego. Wyrafinowany sposób działania będzie, co do zasady, miał znaczenie dla urealnienia dyrektyw wymiaru kary i wydania wyroku surowszego, aniżeli w sprawie przestępcy „przypadkowego". Poza tym charakterystyczny sposób działania nierzadko pokrywa się ze znamionami czynów zabronionych. Jeśli śledztwo jest na etapie poszukiwania przestępcy, to właściwe nakreślenie jego *modus operandi* może pomóc w odnajdywaniu związku między różnymi postępowaniami, łączeniu ich ze sobą i „wydobywaniu" w ten sposób nowych informacji i danych o tym samym człowieku: poznaniu jego tożsamości, zatrzymaniu i osądzeniu. Jednym słowem, wiedza o całej sferze działania przestępcy, w której należy upatrywać specyficznego *modus operandi*, pomaga w prawidłowej prawnokarnej ocenie czynu, ułatwia ustalenie winy, stopnia społecznej szkodliwości oraz przestępczego współdziałania. Warto bowiem przypomnieć treść art. 53 § 2 k.k. nakazującego uwzględnienie przy wymiarze kary szeregu elementów przedmiotowych i podmiotowych, właśnie odnajdywanych wśród nośników *modus operandi*[26].

[25] MITER ATT&CK to ogólnodostępna baza wiedzy na temat taktyki i techniki stosowanej przez cyberprzestępców, oparta na obserwacjach i analizach rzeczywistej ich działalności. Informacje i dane zawarte w bazie służą, jako podstawa do opracowywania konkretnych modeli zagrożeń i metodologii ich zwalczania oraz rekonstrukcji *modus operandi* działań hakerów. Baza ATT&CK dostępna jest pod adresem: https://attack.mitre.org/ [dostęp: 23.05.2023].

[26] M. Kulicki (red.), V. Kwiatkowska-Darul, L. Stępka, *Kryminalistyka: wybrane zagadnienia teorii i taktyki śledczo-sądowej*, Toruń 2005, s. 31.

Rozdział 2
Przedmiot czynności wykonawczej w przestępstwach teleinformatycznych

2.1. „Informacje", „dane" i „dane informatyczne"

Przedmiotem bezpośredniego działania sprawcy, o którym mowa w przepisach rozdziału XXXIII k.k., są „informacje" (art. 267 § 1 i 3 k.k., art. 268 § 1 k.k.) i „dane informatyczne" (art. 268a § 1 k.k., art. 269 § 1 k.k., art. 269a k.k.). Chociaż zakres znaczeniowy tych zwrotów jest różny, to w niektórych sytuacjach trudno jest rozgraniczyć oba pojęcia, co z kolei powoduje komplikacje w procesie subsumpcji prawa. Należy stawiać ścisłe rozgraniczenia między tym, co stanowi „informacje", a „danymi informatycznymi", chociaż analiza wyroków sądowych pokazała, że sądy zbyt często traktują oba pojęcia zamiennie. Jednak ich odmienne znaczenie jest zrozumiałe, jeśli wyjdzie się z założenia, że znamiona przestępstwa, sformułowane przy użyciu różnych słów, muszą posiadać odrębne znaczenie. Dlatego już na samym wstępie należy odrzucić pogląd A. Behana twierdzącego, że:

> biorąc pod uwagę założenia typologiczne związane z racjonalną kryminalizacją określonej grupy zachowań jako typowo społecznie mniej lub bardziej szkodliwych, na gruncie niniejszego rozdziału Kodeksu karnego (rozdziału XXXIII – przypis autora) spostrzeżenia te prowadzić powinny do jak najszerszego w sensie funkcjonalnym oraz gwarantującego szeroką ochronę rozmaitych dóbr prawnych traktowania informacji jako znamienia typu czynu zabronionego pod groźbą kary, zbliżając ją w istocie do pojęcia danych informatycznych"[27].

Przeciwko takiemu stanowisku przemawia idea „racjonalnego ustawodawcy", który wprowadził do ustawy karnej dwa różne pojęcia po to, aby nadać im odmienne znaczenie. W tym aspekcie nie może ujść uwadze zasada *nullum crime sine lege certa*, na którą powołuje się zresztą A. Behan w innym miejscu swojej monografii, nakazująca zachowanie pełnej określoności znamion czynu zabronionego, a nie ich wzajemne „przenikanie".

Gdy podda się analizie prawnej pogląd zaprezentowany przez wspomnianego autora, na myśl przychodzi wyrażona przez R. Kmiecika[28] krytyka „ery postmodernizmu" prawnego. Objawia się ona z jednej strony zbyt swobodnym podejściem do tradycyjnych zasad wykładni przepisów prawa, czemu towarzyszy ich nadinterpretacja, a nawet niczym nieuprawniona pokusa działalności „prawotwórczej" dokonywanej przez sędziów, prokuratorów czy komentatorów prawa.

---

[27] A. Behan, *Waluty wirtualne jako przedmiot przestępstwa*, Kraków 2022, s. 607.

[28] R. Kmiecik, *Osobliwości postmodernizmu a funkcja skargi „kontrkasatoryjnej" w procesie karnym (Rozdział 55a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 3, s. 6–7.

W mowie polskiej terminy „dane" i „informacja" należą do trudno definiowalnych z uwagi na swój pierwotny charakter, a w języku potocznym używa się ich zamiennie. W sposób szczególny zajmują się nimi dwie dziedziny nauki: zarządzanie wiedzą i teoria informacji, ale one także nie wypracowały jednoznacznych, zadowalających i powszechnie akceptowanych definicji „danych" oraz „informacji"[29]. Stąd prosty wniosek, że podejmowane w orzecznictwie i doktrynie prawa karnego próby wytyczenia ścisłej granicy pomiędzy wspomnianymi pojęciami mają charakter praktyczny i dotyczą stosowania przepisów penalizujących określone zachowania w okolicznościach konkretnej sprawy. Nie powinno się traktować ich jako powszechnego dogmatu rozstrzygającego, co jest „informacją", a co „danymi" w każdej dziedzinie nauki, szczególnie że nazwy te zostały zaadaptowane na potrzeby prawa karnego z innych obszarów wiedzy.

Słownik języka polskiego stanowi, że „dane" to fakty, liczby, na których można się oprzeć w wywodach, oraz informacje przetwarzane przez komputer[30]. W komputerowych systemach zarządzania dane są kodowane za pomocą odpowiednich symboli po to, aby można je było rejestrować, przetwarzać oraz przesyłać do świadomości odbiorcy w postaci komunikatu. Zatem każdy komunikat zawiera dane. Choć same dane nie mają znaczenia ani celu, to dobór odpowiednich symboli może narzucać lub sugerować ich określoną interpretację[31]. Wynika z tego, że dane mogą mieć postać tradycyjną (tj. zostać zapisane w postaci cyfr, liczb lub też innych znaków) oraz cyfrową. Ostatnia z wymienionych form danych stanowi przedmiot czynności wykonawczej z art. 268a § 1 k.k., art. 269 § 1 k.k., art. 269a k.k., gdyż w przepisach tych jest mowa o „danych informatycznych".

Legalna definicja danych informatycznych zawarta jest w art. 1 pkt b Konwencji Rady Europy o cyberprzestępczości[32], której Rzeczpospolita Polska jest stroną; oznaczają one dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny. Podobnie brzmi definicja „danych komputerowych" zawarta w art. 2 pkt b Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r., dotyczącej ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW[33]; „dane komputerowe" oznaczają przedstawienie faktów, informacji lub pojęć w formie nadającej się do

[29] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie" 2009, nr 798, s. 102–103.

[30] https://sjp.pwn.pl/szukaj/dane.html [dostęp: 23.06.2023].

[31] M. Grabowski, A. Zając, *Dane, informacja, wiedza*..., s. 16.

[32] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728), dalej jako: Konwencja Rady Europy o cyberprzestępczości.

[33] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dziennik Urzędowy Unii Europejskiej, https://european – union.europa.eu/select – language?destination=/node/1 [dostęp: 23.06.2023].

przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny. F. Radoniewicz[34] stwierdził, że:

> dane komputerowe są nośnikiem (medium) informacji, faktów i koncepcji, które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu informatycznego. W tym celu muszą zostać „zakodowane" w języku binarnym – zamienione w ciąg „0" i „1", a następnie mogą zostać zapisane na nośniku (np. płycie CD, DVD lub na dysku twardym komputera) czy przesłane za pośrednictwem sieci jako impulsy energetyczne. W świetle definicji danymi komputerowymi są też programy odpowiadające za wykonywanie funkcji przez system informatyczny.

Wynika z tego, że „dane informatyczne" stanowią język zrozumiały wyłącznie dla urządzeń komputerowych i dopiero ich odpowiednie przetworzenie przez program komputerowy może dostarczyć „informacji".

Grafika nr 1. Wizualizacja systemu kodu binarnego, tj. systemu liczbowego opartego na zerach i jedynkach, którego sposób zapisu używany jest we wszystkich systemach komputerowych, procesorach, pamięciach RAM i ROM oraz twardych dyskach

Jeśli mowa o „informacjach", to obejmują one to, co powiedziano lub napisano o kimś lub o czymś, zakomunikowanie czegoś, także dane przetwarzane przez komputer – tak definiuje je Słownik języka polskiego[35]. Informacje pochodzą z wyselekcjonowania danych tak, aby były użyteczne dla odbiorcy, niosą ze sobą jakiś sens i mają znaczenie dla człowieka. Informacje są tym, co powstaje w wyniku pewnych działań myślowych (obserwacji, analiz) z sukcesem zastosowanych do danych, by odkryć ich istotę lub znaczenie. Z kolei „dane" reprezentują nieustrukturyzowane, surowe fakty dotyczące zjawisk i obiektów, które dopiero po odpowiednim przekształceniu mogą, ale nie muszą, stać się informacją[36]. W informatyce znaki i symbole transmitowane są w sieciach informatycznych i teleinformatycznych i za pomocą specjalnych algorytmów przetwarzania danych mogą zostać odebrane przez człowieka (w formie dźwięku lub

[34] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13, s. 123.
[35] https://sjp.pwn.pl/szukaj/informacje.html [dostęp: 23.06.2023].
[36] P. Opitek, *Kontrola operacyjna urządzenia końcowego*, „Prokuratura i Prawo" 2023, nr 4, s. 40.

obrazu) jako informacje. Wynika z tego, że „informacje" powstają z wyselekcjonowania danych, ich podsumowania i prezentacji w taki sposób, by stały się użyteczne dla odbiorcy. Informacje są produktem istotnego przetwarzania danych i niekiedy mówi się o „postaci pozainformatycznej" danych.

Grafika nr 2. Dane po przetworzeniu przez algorytm komputerowy stały się informacją w postaci obrazu (kielicha kwiatu)

„Oczyszczając" w ten sposób przedpole do dalszej dyskusji, można przystąpić do omówienia znaczeniowego zakresu przepisów rozdziału XXXIII k.k. Na temat tego, co stanowi „informację" w rozumieniu art. 267 § 1 k.k., obszernie wypowiedział się Sąd Najwyższy w postanowieniu z dnia 5 marca 2019 r.[37] Sprawa dotyczyła „kluczy parujących" (ang. *boxkey*), służących do zapewnienia łączności pomiędzy składnikami systemu i odbierania zakodowanego sygnału telewizyjnej platformy cyfrowej poza usługami oferowanymi przez stację telewizyjną w otwartym, publicznie dostępnym paśmie transmisyjnym (tzn. nie płacąc abonamentu). Mężczyzna został oskarżony o to, że:

> w okresie od dnia 13 stycznia 2010 r. do dnia 27 stycznia 2011 r. we W., w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru oraz w celu osiągnięcia korzyści majątkowej, po uprzednim podłączeniu się i przełamaniu fizycznych oraz elektronicznych zabezpieczeń systemu szyfrowania pamięci flash dekoderów, świadczył usługi niedozwolone poprzez wydobywanie kluczy parujących i RSA z dekoderów korzystających z systemu dostępu warunkowego dostarczanego przez firmę /…/, które następnie udostępniał klientom swojej firmy w postaci plików skompresowanych na stronie internetowej www./.../.pl, czym działał na szkodę /…/, tj. o czyn z art. 6 ust. 1 i 2 ustawy z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym w zb. z art. 267 § 1 i 4 k.k. z zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.

[37] Postanowienie Sądu Najwyższego z dnia 5 marca 2019 r., II KK 208/18, LEX nr 2639897.

Oskarżony został uniewinniony od popełnienia zarzucanego mu czynu przez sądy I i II instancji, a na skutek kasacji wniesionej przez pełnomocnika oskarżyciela subsydiarnego w sprawie wypowiedział się Sąd Najwyższy. Stwierdził on, że na gruncie przepisu art. 267 § 1 k.k. za informację należy uznać tylko taki zestaw znaków, któremu można przypisać określone znaczenie, rozumiane jako wskazywany przez nie sens. Cechy takiej nie posiada „klucz parujący", który zapewnia łączność pomiędzy określonymi segmentami systemu informatycznego w postaci fizycznej (np. karta dostępu – urządzenie) albo abstrakcyjnej (np. algorytmy, składniki oprogramowania). Nie sposób uznać, aby *boxkey* posiadał atrybut sensu, znaczenia dla człowieka; przeciwnie, jest to zespół znaków, który pełni tylko pewną funkcję w systemie informatycznym. W analizowanym przypadku sprawca miał zamiar bezprawnie uzyskać dostęp do zakodowanego programu telewizyjnego lub udzielić innym osobom pomocy w uzyskaniu takiego dostępu. Kody *boxkey* stanowiły tylko narzędzie do ominięcia lub przełamania zabezpieczenia, gdyż celem sprawcy była informacja. Można porównać to z sytuacją, gdy ktoś „kradnie" hasło i login („dane") do aplikacji bankowości elektronicznej po to, aby otworzyć ją i sprawdzić stan konta („informacje"). Jednak program emitowany w sieci kablowej z natury rzeczy jest przeznaczony dla każdego, kto uiści abonament, a prawo logowania się do aplikacji posiada tylko jej użytkownik. Wynika z tego, że w przypadku kazusu *boxkey* sprawca nie zrealizował także znamion usiłowania dokonania czynu opisanego w art. 267 k.k. – orzekł Sąd Najwyższy.

Zgodnie z tym stanowiskiem, informację, o której mowa we wszystkich przestępstwach określonych w rozdziale XXXIII k.k., stanowi wiadomość lub określona suma wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach. Można je przedstawić w formie pisemnej, fonicznej, wizualnej oraz każdej innej postaci możliwej do odbioru za pomocą zmysłów. Wiadomość musi być kierowana „od człowieka do człowieka"; nie jest wiadomością, w rozumieniu potocznym, zestaw danych przesyłanych między urządzeniami. Od terminu „informacja", a więc obiektu wyposażonego w pewną treść, odróżnić należy pojęcia w rodzaju: „dane", „kod", „ciąg znaków" itp.[38] Te ostatnie wskazują na obiekty, które nie mają jakiegokolwiek sensu, nie są bowiem nośnikami znaczenia, np. kody dostępu chroniące informację[39]. Ma to istotne reperkusje dla tzw. przestępstw komputerowych, bowiem nie każdy ciąg znaków (kod, szyfr, układ graficzny) można uznać za informację. „Informacją" w rozumieniu dobra chronionego z rozdziału XXXIII k.k. ujmuje się jako pewną treść, czyli znaczenie, sensowny komunikat,

[38] W orzeczeniu z dnia 27 listopada 2019 r. Sąd Najwyższy także przyjął, że kodem dostępu jest indywidualne hasło dostępu użytkownika do komputera, ale także sieci Wi-Fi czy dekodera TV (postanowienie Sądu Najwyższego z dnia 27 listopada 2019 r., V KK 505/18, LEX nr 2966120). W podobnym duchu wypowiedział się F. Radoniewicz, wskazując, że charakter danych posiadają kody dostępu w postaci danych biometrycznych, haseł komputerowych, haseł Wi-Fi itp. (F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 332).

[39] „Kluczy" nie można zobaczyć „gołym okiem", co pokazuje prosty „eksperyment": po wpisaniu w wyszukiwarkę Google frazy „boxkey Polsat" i funkcji „Grafika" pojawiają się tylko nośniki takich kluczy w postaci kart pamięci i dekoderów.

a nie tylko funkcję w określonym układzie faktycznym. „Odkodowując" znaczenie słowa „informacja" na gruncie art. 267 k.k., Sąd Najwyższy odwołał się do pojęcia przeciwstawnego, tj. „danych". Jednak termin „dane" nie występuje w rozdziale XXXIII k.k., ale opis przestępstw zawiera zwrot „dane informatyczne" i temu znaczeniu, zdaniem sądu, odpowiadała natura *boxkey*. „Klucze" stanowią zatem szczególny rodzaj danych – to „dane informatyczne", o których mowa w art. 268 § 1 k.k., art. 268a § 1 k.k., art. 269 § 1 k.k., art. 269 § 2 k.k. i art. 269a k.k.

W praktyce organów ścigania zachodzi wiele nieścisłości, a nawet błędów, w zakresie rozumienia terminów „informacje" i „dane informatyczne", co przekłada się na niewłaściwy opis czynu zabronionego i jego kwalifikację prawną. W jednej ze spraw mężczyzna został oskarżony o to, że:

> w dniu 5 lutego 2015 r. w Krakowie bez uprawnienia uzyskał dostęp do systemu informatycznego /…/ S. A. oraz informacji dla niego nieprzeznaczonej, poprzez to, że ominął zabezpieczenie systemu komputerowego /…/ z bazami klientów wykorzystując przy tym uzyskane w nieustalony sposób login i hasło pracownika salonu /…/ następnie bezprawnie dokonał zmian w bazach danych informatycznych dotyczących wysokości abonamentu, a to zmniejszeniu kwoty zobowiązania miesięcznego klientów, na skutek czego powstały straty w wysokości 34.693 zł na szkodę /…/ S. A., tj. o przest. z art. 267 § 1 k.k. i art. 267 § 2 k.k. i art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k.[40]

Prokurator uznał, że system informatyczny operatora sieci komórkowej, do którego sprawca w sposób nieuprawniony uzyskał dostęp za pośrednictwem aplikacji, stanowi zarówno „informacje", jak i „dane informatyczne", a więc przyjął realny zbieg przestępstw z art. 267 § 1 k.k. i art. 267 § 2 k.k. W istocie tak jest, bowiem pod względem technicznym uzyskanie dostępu do danych zawartych w systemie za pośrednictwem konsoli komputera powoduje najczęściej, że ma się także dostęp do informacji, które powstają z przetworzenia artefaktów cyfrowych i wyświetlają się na monitorze ekranu komputera w formie słów, obrazu itd. Jednak po wygaszeniu monitora owa sensowna treść „ulatnia się" i „zalega na dysku" w postaci zapisu danych. W rozpatrywanej sprawie sprawca przestępstwa, po zalogowaniu się do systemu, oprócz czytania informacji teoretycznie miał również możliwość operowania na kodzie źródłowym programu komputerowego, ale tego nie uczynił, gdyż inny był zamiar jego działania, a zapewne nie posiadał także umiejętności umożliwiających mu bezpośredni dostęp do kodu cyfrowego. Dokonując zatem ustaleń faktycznych, organ procesowy powinien odpowiedzieć

[40] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 1706/15/S. Jeżeli w przypisie i bibliografii nie przywołano miejsca publikacji akt spraw karnych, oznacza to, że nie były one publikowane, a autor zapoznał się z nimi w czasie badań własnych.

na pytanie, jaki był zamiar sprawcy, tj. czy działał w celu uzyskania nieuprawnionego dostępu do „danych informatycznych" lub „informacji", i od tego uzależnić kwalifikację prawną czynu z art. 267 § 1 lub 2 k.k. Co prawda łączne przyjęcie tych dwóch przepisów jest możliwe, ale chodzi o sytuacje wyjątkowe, o których będzie jeszcze mowa w dalszej części opracowania. W tym miejscu należy natomiast zastanowić się, jakie znaczenie dla bytu przestępstwa hakingu mają indywidualne cechy sprawcy dotyczące jego możliwości odczytania sensu komunikatu.

2.2. Subiektywna lub obiektywna ocena pojęć „informacje" i „dane informatyczne"

Trudności w ocenie znamion niektórych przestępstw, opisanych w rozdziale XXXIII k.k., wynikają z faktu, że zarówno dane, jak i informacje są przetwarzane przez komputer, znajdują się w systemach informatycznych oraz teleinformatycznych i de facto ma się do czynienia z taką samą materią, ale reprezentowaną w różny sposób. Niekiedy, w trakcie analizy konkretnego układu znaków mogą pojawić się wątpliwości, czy ma się wciąż do czynienia z danymi informatycznymi, a może wyświetlony obraz stanowi komunikat o merytorycznej treści. Jako przykład niech posłużą zaprezentowane poniżej dwie postacie tej samej strony internetowej Prokuratury Krajowej.

Grafika nr 3. Widok strony internetowej Prokuratury Krajowej w takiej postaci, jaka w zamiarze administratora została przygotowana do odczytu dla użytkowników sieci i pojawia się w Internecie

```
<!DOCTYPE html>
<html lang="pl-PL" class="no-js ">
<head>
<title>Prokuratura Krajowa - Prokuratura Krajowa - Portal Gov.pl</title>
<meta charset="utf-8"/>
<meta content="initial-scale=1.0, width=device-width" name="viewport">
<meta property="govpl:site_published" content="true"/>
<meta name="msvalidate.01" content="D55ECD200B1844DB56FBA4DA551CF8D"/>
<meta property="og:site_name" content="Prokuratura Krajowa"/>
<meta property="og:url" content="https://www.gov.pl/web/prokuratura-krajowa"/>
<meta property="og:title"
content="Prokuratura Krajowa - Prokuratura Krajowa - Portal Gov.pl"/>
<meta property="og:type" content="website"/>
<meta property="og:image" content="https://www.gov.pl/img/fb_share_ogp.jpg"/>
<meta property="og:description" content=""/>
<meta name="twitter:description" content=""/>
<meta name="twitter:image" content="https://www.gov.pl/img/fb_share_ogp.jpg"/>
<meta name="twitter:card" content="summary_large_image">
<meta name="twitter:title"
content="Prokuratura Krajowa - Prokuratura Krajowa - Portal Gov.pl"/>
<meta property="govpl:site_hash" content="33bab76c-1891-0d15-60d9-b50918994f7"/>
<meta property="govpl:site_path" content="/web/prokuratura-krajowa"/>
<meta property="govpl:active_menu_item" content=""/>
<link rel="icon" type="image/png" href="/img/icons/favicon-16x16.png"
sizes="16x16">
<link rel="icon" type="image/png" href="/img/icons/favicon-32x32.png"
sizes="32x32">
<link rel="icon" type="image/png" href="/img/icons/favicon-96x96.png"
sizes="96x96">
```

Grafika nr 4. „Metatagi" umieszczone w kodzie źródłowym strony internetowej Prokuratury Krajowej

Nie ulega wątpliwości, że grafika nr 3 przedstawia informacje i zamieszczona na niej treść komunikuje odbiorcy o działaniach prowadzonych przez Prokuraturę Krajową. Jaki charakter ma natomiast grafika nr 4? Przedstawia ona „metatagi" umieszczone w kodzie źródłowym strony internetowej, stanowiące rodzaj metadanych treści witryny, które wykorzystywane są przez wyszukiwarki oraz przeglądarki do zarządzania np. sposobem wyświetlania polskich znaków u zagranicznych użytkowników. „Dane o metadanych" to coś pośredniego między informacjami a metadanymi; z grafiki nr 4 można „coś" odczytać, m.in., że ich treść związana jest z prokuraturą. Ale czy jest to wystarczająco „esencjonalny" przekaz, aby można było mówić o informacji?

Jeżeli przyjąć, że informacja na gruncie rozdziału XXXIII k.k. to przekazywany w określony sposób zespół znaków wyposażony dodatkowo w atrybut posiadania znaczenia, to konieczne jest ustalenie, czym jest owo „znaczenie" samo w sobie. Pojęcie to jest wieloznaczne i funkcjonują różne koncepcje „znaczenia" formułowane na gruncie filozofii oraz logiki, w tym także wykorzystywane przez teorie wykładni prawa. Wskazuje się na aspekt tożsamości tego pojęcia z nazwami w rodzaju: „sens" czy „treść". Oznacza to, że chodzi o takie zespoły znaków, które wskazują na jakieś obiekty (abstrakcyjne albo konkretne), a więc można im przypisać denotację (zakres znaczenia), i które realizują funkcję oznaczania. W takim ujęciu wiadomości, które zawierają co prawda „jakieś" treści, ale mają one charakter bliżej nieokreślony, tj. nie można z nich wyczytać żadnego sensu, nie stanowią informacji. Powracając zatem do obrazu z metatagami, to zdaniem autora, chociaż większość odbiorców potrafi wywnioskować z niego minimalny zakres sensownego przekazu („Prokuratura Krajowa", „Portal Gov.pl", „www.gov.pl"), to nie wypełniają one znamienia „informacja", o którym mowa na gruncie art. 267 § 1 k.k. Można jednak podnieść argumenty, iż metatagi „coś znaczą",

gdyż istnieje niewielki odsetek ludzi, zapewne biegłych w językach komputerowego programowania, dla których ich lektura stanowi źródło sensownych treści. Powstaje zatem pytanie: Czy uznanie czegoś za „dane" lub „informacje" zależy od indywidualnych możliwości sprawcy przestępstwa; a może ocena powinna opierać się na wzorcu „obywatela o przeciętnych umiejętnościach"? Innymi słowy, skoro wiedza pełni aktywną rolę w procesie interpretacji danych (nadawania im sensu), to o jaki stopień wiedzy chodzi, aby sprawca był zdolny do poniesienia odpowiedzialności karnej z art. 267 § 1 k.k.?

Proces interpretacji danych wymaga niekiedy posiadania specjalistycznej wiedzy o opisywanym przez nie wycinku rzeczywistości; osoba, która posiada taką wiedzę i zapoznaje się z „surowymi" danymi, uzyskuje informacje. Do zobrazowania problemu niech posłużą klucze prywatne przeznaczone do rozporządzania kryptowalutami; w tabeli poniżej przedstawiono trzy postacie tego samego klucza prywatnego zapisanego w różnych formatach:

5JoBSup7GzCohqzfCdU3FQmuQM8KLCu3TTKiTAtbzmWywJfzTni
L1Yq7N6vhZV79HFVcKxLvbwCJ3qHumWhqmBbxWemTyVLJHfaUjTc
6PYLTEjqt2huN6zgG8Gc2Sdifh33tcDLoJMXXqdK52YrQWXa3fD8az9Za7[41]

Jest oczywiste, że w świadomości zdecydowanej większości odbiorców przedstawione ciągi znaków nie zawierają żadnego logicznego sensu, a zatem są danymi, nie informacjami. Jednak, gdyby okazać je informatykowi lub osobie dobrze obeznanej w walutach wirtualnych, to mogliby oni fachowo zinterpretować takie zapisy i „wydobyć" z nich określone treści. Autor książki przeprowadził „eksperyment" i zadał programiście technologii blockchain pytanie: „Czy potrafisz odczytać informacje z nazwy klucza prywatnego?". Jego pisemną odpowiedź zamieszczono w ramce:

W formie „czystej" klucz prywatny jest ciągiem losowych znaków i dopiero zapisanie go w formacie konkretnego portfela pozwala uzyskać informację, że jest to klucz prywatny. Do obliczeń „kryptovoodo" należy go „przekodować" z powrotem na czystą formę danych. Na stronie *https://en.bitcoin.it/wiki/Private_key* mamy format WIF, który koduje „gołe" dane do base58 z odpowiednim przedrostkiem, co powoduje, że posiadają one konkretną długość i pierwszy znak. Jeżeli zapisujemy klucze w ten sposób, to widząc ciąg znaków określonej długości zaczynający się na konkretny znak możemy podejrzewać, że jest to klucz prywatny.

[41] *Guidelines for Digital Forensics First Responders – Best practices for search and seizure of electronic and digital evidence*, INTERPOL, marzec 2021, tłumaczenie na język polski: *Poradnik Cyber Ratownika, IV Konferencja Naukowa Przestępczość Teleinformatyczna XXI wieku*, Gdynia 2022, s. 45.

Klucze publiczne zapisuje się zwykle jako „czyste", gdyż nie podlegają one importowaniu.

Z adresami sprawy mają się jeszcze inaczej, ponieważ są zazwyczaj pochodną (jakimś haszem) klucza publicznego z dodanym przedrostkiem i sumą kontrolną (Bitcoin i protokoły pochodne) lub po prostu częścią hasza (Ethereum i protokoły pochodne). Z adresu można odczytać, jaka to sieć (informacja w przedrostku) i typ adresu (również informacja w przedrostku) np.:

„1" z przodu – adres P2PKH BTC

„3" z przodu – adres P2SH w BTC

„bc1" z przodu i długość 39 znaków – adres P2WPKH w BTC

„bc1" z przodu i długość 59 znaków – adres P2WSH w BTC

Nie sposób natomiast wywnioskować tylko z adresu P2SH/P2WSH zawartości skryptu (co dany adres reprezentuje – multisig? timelock? otwarcie kanału LN?) do momentu wydania środków z danego adresu: wtedy dopiero należy skrypt wyjawić (adres jest pochodną hasza skryptu). Sprawa jeszcze bardziej skomplikuje się przy użyciu podpisów Shnorra i MAST, gdzie zawartość skryptu wydania może być okrojona lub ukryta[42].

Z przytoczonej odpowiedzi wynika, że dla specjalisty technologii blockchain układ cyfr i liczb, budujący klucze prywatne, zawierał sens. Rzecz wygląda podobnie z numerem karty płatniczej zapisanym na plastiku: standardowo są to 4 liczby, a każdą tworzą 4 cyfry, przy czym układ cyfr jest ściśle określony. Przeciętnemu użytkownikowi karty owe liczby nie mówią nic, ale osoby znające się na płatnościach bezgotówkowych potrafią „rozszyfrować" ich znaczenie, gdyż liczby zawsze kodują określone wiadomości. W numerze karty płatniczej zawarte są następujące informacje:

1. pierwsze 6 cyfr (ang. Bank Identification Number – BIN) identyfikuje bank będący wystawcą karty, a pierwsza cyfra wskazuje na organizację firmującą swoim logo kartę (np. 4xxx xxxx xxxx xxxx – VISA),
2. kolejne 4 cyfry informują o regionie i oddziale banku,
3. następne 5 cyfr dotyczy numeru rachunku posiadacza karty,
4. ostatnia cyfra stanowi bazę dodatkowych informacji dla banku[43].

[42] R. Kiełbus, programista i advisor w blockchainowych projektach; programista smartkontraktów, członek Zarządu Izby Gospodarczej Blockchain i Nowych Technologii, arbiter Sądu Polubownego przy Izbie. Informacja otrzymana w wiadomości mailowej z 25.07.2022 r., zbiory własne autora.

[43] P. Opitek, *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Monografie Prawnicze, C.H. Beck 2017, s. 20.

Przyjąć należy, że nadanie określonemu zapisowi miana „danych informatycznych" lub „informacji", na podstawie okoliczności faktycznych konkretnej sprawy, powinno być uzależnione od tego, czy sprawca czynu zabronionego, ukierunkowanego na uzyskanie bez uprawnienia dostępu do tego zapisu, potrafiłby sam lub przy użyciu „zwykłych" środków odczytać z niego sens. W nauce zarządzania wiedzą przyjmuje się, że status informacji zależy od zdolności interpretacyjnych odbiorcy, a więc sama informacja ma charakter subiektywny[44] i ów pogląd należy uwzględnić także przy wykładni znamion art. 267 § 1 i 2 k.k. Proces interpretacji danych wymaga posiadania określonej wiedzy o obszarze, do którego dane się odnoszą – wiedza stanowi swego rodzaju translator pomiędzy danymi a informacjami. Stanowisko takie jest zgodne z zasadą indywidualizacji odpowiedzialności karnej (art. 21 § 1 k.k.), zgodnie z którą „okoliczności osobiste, wyłączające lub łagodzące albo zaostrzające odpowiedzialność karną, uwzględnia się tylko co do osoby, której dotyczą". Przez okoliczności osobiste, o których mowa w art. 21 § 1 k.k., należy rozumieć cechy charakteryzujące każdą osobę będącą podmiotem odpowiedzialności karnej, odnoszące się także do jej wiedzy specjalistycznej. W tym aspekcie kategoryczne twierdzenie, że „klucze uprawniające do dysponowania jednostkami kryptowalut, które wykorzystywane są do dokonania transferów, należy określić jako 'dane' (zgodnie z terminologią kodeksową)"[45] nie zawsze musi polegać na prawdzie. Z drugiej strony myli się A. Behan, pisząc, że bez wątpienia „klucz prywatny, klucz publiczny czy adres są informacjami w rozumieniu art. 267 § 1 k.k." i „każda z tych informacji ma lub może mieć bardzo duże znaczenie dla konkretnej sytuacji faktycznej"[46]. Może się zdarzyć, że dostęp bez uprawnienia do wspomnianych kluczy, pozostających w dyspozycji innej osoby, uzyskał sprawca obeznany z technologią blockchain i w ten sposób wypełni on znamiona art. 267 § 1 k.k. Podobnie osoba uzyskująca nieuprawniony dostęp do wiadomości mailowej w języku angielskim, nawet jeśli nie włada tym językiem, to i tak popełnia przestępstwo z art. 267 § 1 k.k. Może przecież za pomocą ogólnodostępnych, internetowych translatorów bez problemu poznać sens wiadomości. Jeśli haker uzyska dostęp do metatagów, to jego czyn wyczerpie znamiona § 2 art. 267 k.k. Tym bardziej popełni takie przestępstwo, gdy uzyska dostęp do podstawowej warstwy języka programowania (np. Python, SQL, C++, Java, C#, C, Visual Basic,

[44] M. Grabowski, A. Zając, *Dane, informacja, wiedza*…, s. 16.

[45] M. Małecki, P.M. Dudek, *Uzyskanie cudzego bitcoina karane jak kradzież*, Karne24com, 3 października 2018, https://karne24.com/uzyskanie – cudzego – bitcoina – karane – kradziez/ [dostęp: 04.08.2022].

[46] A. Behan, *Waluty wirtualne jako*…, s. 603-604. W kontekście przytoczonej wypowiedzi tego autora warto zwrócić uwagę, że klucz publiczny i adres kryptowalutowy mają charakter publiczny, tj. są dostępne w eksplorerach bloków i zazwyczaj rozgłaszane w sieci przez posiadaczy klucza publicznego i adresu. Nie sposób zatem uznać je za przedmiot czynności wykonawczej, o której mowa w art. 267 § 1 k.k. Nie polega także na prawdzie twierdzenie A. Behana, jakoby rodzaj informacji, czyli „istotność informacji", „nie miała szczególnego znaczenia w przypadku przestępstwa stypizowanego w art. 267 § 1 k.k., w którym ustawodawca nie wprowadził znamienia kwantyfikującego wagę rzeczonej informacji", a tylko „w przypadku przestępstwa z art. 268 § 1 k.k. wymóg 'istotności' jest warunkiem *sine qua non* pociągnięcia sprawcy do odpowiedzialności karnej". Trzeba bowiem pamiętać, że rodzaj dobra prawnego („istotność informacji") wpływa na zastosowanie dyrektyw wymiaru kary, a niekiedy może nawet decydować o bycie samego przestępstwa (znikoma społeczna szkodliwość czynu).

Delphi) tworzącego program komputerowy, a więc systemu informatycznego. Chociaż nie zależy mu na samym zapisie metadanych, to uzyskując bez uprawnienia dostęp do kodu źródłowego systemu informatycznego (art. 267 § 2 k.k.), może spowodować np. zniszczenie lub uszkodzenie danych informatycznych (art. 268a § 1 lub 2 k.k., art. 269 § 1 k.k.) albo zakłócić system komputerowy (art. 269a k.k.).

```
import java.io.IOException;

public class TomcatEmbedded {

    private static final String EMPTY = "";

    public static void main(String... args)
        throws Exception {
        File baseFolder = new File(System.getProperty("user.dir"));
        File appsFolder = new File(baseFolder,  child: "apps");

        Tomcat tomcat = new Tomcat();
        tomcat.setBaseDir(baseFolder.getAbsolutePath());
        tomcat.setPort(8080);
        tomcat.getHost().setAppBase(appsFolder.getAbsolutePath());

        // Call the connector to create the default connector.
        tomcat.getConnector();

        tomcat.addWebapp(EMPTY,  docBase: ".");
        Wrapper wrapper = tomcat.addServlet(EMPTY,  servletName: "hello", new HelloServlet());
        wrapper.setLoadOnStartup(1);
        wrapper.addMapping( s: "/*");

        tomcat.start();
        tomcat.getServer().await();
    }
```

Grafika nr 5. Kawałek ścieżki języka programistycznego Java, do którego nieuprawniony dostęp może wyczerpać znamiona art. 267 § 2 k.k.

Podejście takie jest zgodne z teorią informacji, która głosi, że dane mogą stać się informacją tylko wtedy, jeśli mają swojego odbiorcę, który chce je zinterpretować, a ponadto są dla niego w wystarczającym stopniu zrozumiałe. Jeśli podejmie się wysiłek intelektualny i zinterpretuje dane, to wtedy stają się one wiadomością. Następnie odbiorca określa, czy wiadomość jest powtórzeniem czegoś, co już wie, czy też stanowi dla niego element nowości; tylko w tym ostatnim przypadku wiadomość staje się informacją, także na gruncie art. 267 § 1 k.k. Dlatego czymś absurdalnym byłoby karać sprawcę za to, że uzyskał dostęp do pustej skrzynki poczty elektronicznej lub do tych samych informacji, które można przeczytać w otwartym Internecie. W grę wchodziłoby natomiast usiłowanie nieudolne (art. 13 § 2 k.k. w zw. z art. 267 § 1 k.k.), gdyby działał on w błędnym przeświadczeniu, że w skrzynce są zapisane istotne dla niego, poufne wiadomości.

2.3. Hasła zabezpieczające dostęp do danych lub informacji

W doktrynie i orzecznictwie toczy się spór co do charakteru prawnego haseł zabezpieczających akces do zasobów danych lub informacji. Powszechna jest dziś wiedza każdego dorosłego użytkownika elektroniki, jak zauważył Sąd Najwyższy, że komputery i inne urządzenia umożliwiające komunikację na odległość mogą posiadać różnorakie zabezpieczenia: od prostych haseł do systemu operacyjnego, przez dodatkowe hasła do aplikacji pocztowej, po zabezpieczenia symbolem, rozbudowanym hasłem bądź odciskiem palca (głównie urządzenia mobilne, ale także niektóre modele laptopów), czy też tokenem albo innym dodatkowym fizycznym środkiem weryfikacyjnym, m.in. w postaci chipa[47]. Najczęściej jednak zabezpieczenie ma postać hasła stanowiącego ciąg znaków używanych podczas logowania do poczty elektronicznej, systemów operacyjnych, baz danych czy portali internetowych. Składa się ono z liter, liczb i znaków specjalnych.

Hasła stanowią „bramę wejściową" do ważnych repetytoriów, gdyż wiele aplikacji sieciowych wymaga od swych użytkowników uwierzytelnienia (ang. *authentication*). Zestaw wymaganych danych uwierzytelniających może być odmienny w różnych aplikacjach, od prostego „duetu" w postaci loginu i hasła do skomplikowanych obliczeń opartych na formułach znanych tylko danemu użytkownikowi. Wymóg uwierzytelnienia użytkowników ogranicza dostęp do zasobów aplikacji i redukuje jej podatność na ataki ze strony użytkowników nieuwierzytelnionych. Ominięcie uwierzytelnienia (ang. *authentication baypass*) to zmuszenie aplikacji do uznania użytkownika za uwierzytelnionego, pomimo niepodania przez niego danych uwierzytelniających lub podszycia się pod inną osobę i uwierzytelnienia prawidłowymi hasłami. Techniki obchodzenia uwierzytelnienia bywają rozmaite, od wykorzystania słabego haszowania haseł za pomocą banalnych sum kontrolnych, przełamywania go atakami brute force, po wstrzykiwanie kodu SQL[48].

Czym innym jest natomiast omijanie autoryzacji. Użytkownicy aplikacji mogą mieć bowiem zróżnicowane uprawnienia pod względem dostępu do jej funkcji lub zasobów, tj. wszyscy będą posiadać ten sam interfejs, ale już możliwości dostępnych na niej działań zupełnie różne: ważne pliki konfiguracyjne mogą być modyfikowane przez administratora, a oglądane (bez możliwości modyfikowania) przez zaufanego użytkownika i zupełnie niedostępne dla „gościa". Gdy zalogowany użytkownik żąda od aplikacji wykonania pewnych działań, to aplikacja sprawdza, czy ten konkretny użytkownik jest do wydawania takich poleceń uprawniony; nazywa się to autoryzacją żądań. Haker, będąc legalnym użytkownikiem, lecz nieposiadającym np. uprawnienia do przeglądania pliku z zaszyfrowanymi hasłami, może próbować zaingerować w proces autoryzacji poprzez wykorzystanie luki w implementacji odpowiedzialnego za tę autoryzację protokołu

[47] Wyroku Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15, LEX nr 1866883.

[48] J. Forshaw, *Atak na sieci okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci*, Warszawa 2019, s. 261.

i w ten sposób uzyskać uprawnienie. Działanie takie nosi nazwę ominięcia autoryzacji (ang. *authorization baypass*)[49]. Należy zatem odróżnić ominięcie uwierzytelnienia od ominięcia autoryzacji, ale oba czyny będą wypełniać znamiona art. 267 § 1 lub 2 k.k. Przykładowo, jeśli sprawca posłuży się bez uprawnienia hasłem podpatrzonym u innej osoby i zaloguje na jej skrzynkę mailową (fałszywe uwierzytelnienie), to wypełni znamiona § 1 ww. artykułu. Jeśli jednak użytkownik systemu komputerowego, który ma bierne prawo do zapoznawania się z informacjami zamieszczonymi na wewnętrznym portalu swojej firmy, rozszerzy swoją swobodę działania i bez uprawnienia uzyska uprawnienia administratora danych informatycznych „budujących" portal (fałszywa autoryzacja), to popełni przestępstwo z art. 267 § 2 k.k. Celem uwierzytelnienia jest zatem weryfikacja tożsamości użytkownika; autoryzacja zaś ma na celu zweryfikowanie uprawnień użytkownika, którego tożsamość nie budzi wątpliwości. W analogiczny sposób różnią się zatem intencje hakera dążącego do ominięcia tych mechanizmów: przełamanie uwierzytelnienia ma pozwolić hakerowi na podszycie się pod innego użytkownika, a ominięcie autoryzacji da mu dodatkowe uprawnienia.

Zdaniem F. Radoniewicza, hasła komputerowe i kody dostępu nie są informacją w znaczeniu nadanym temu pojęciu przez art. 267 § 1 k.k., bo stanowią dane przedstawione w postaci ciągu znaków umożliwiającego uzyskanie dostępu do informacji przechowywanych w systemach informatycznych i sieciach teleinformacyjnych[50]. Podobnie, odwołując się do dominującej w prawoznawstwie polskim teorii znaczenia (semantycznej), Sąd Najwyższy stwierdził, że zgodnie z pierwszeństwem wykładni językowej, zachodzi istotna różnica między nazwą „informacja" a pojęciami „kod dostępu", „hasło", „szyfr", „dane"[51]. Poglądy takie należy zaaprobować, ale z pewnym zastrzeżeniem. Hasła komputerowe, zapewniające dostęp do prywatnych informacji, zapisane są w pamięci komputera w formie danych informatycznych, które „wyświetlają się" na jego monitorze w postaci danych (np. nus65d%yu) lub informacji (np. Paweł.Opitek.1978); podobnie rzecz się ma z zapisem utrwalonym na kartce lub hasłem wyartykułowanym głosowo przez człowieka. „Dane" i „dane informatyczne" nie są informacją, o której mowa w art. 267 § 1 k.k., ale hasło „Paweł.Opitek.1978", pełniące funkcję logowania, stanowi już samo w sobie informację, tj. pozwala ustalić, jak nazywa się dana osoba oraz rok jej urodzenia. Zatem uzyskanie takiej poufnej informacji w sposób opisany w art. 267 § 1 k.k. mogłoby wypełnić znamiona tego przestępstwa, jeśli zamiarem sprawcy byłoby poznanie treści hasła. Podsumowując, tylko w sytuacji, gdy ktoś celowo działał w zamiarze bezpośrednim uzyskania dostępu do poufnego hasła, które już samo w sobie stanowiło dla niego informację, a nie chciał jedynie wykorzystać tego hasła do otwarcia innego zasobu wiadomości, to można mówić o odpowiedzialności z art. 267 § 1 k.k.

[49] Tamże, s. 261.
[50] Por. F. Radoniewicz, *Odpowiedzialność karna za hacking*…, s. 332.
[51] Postanowienie Sądu Najwyższego z dnia 5 marca 2019 r., II KK 208/18, LEX nr 2639897.

Jednak w praktyce uzyskanie kodu będzie stanowiło tylko jeden z etapów realizacji znamion hakingu, gdy priorytetem sprawcy jest uzyskanie bez uprawnienia dostępu do innego zasobu danych z wykorzystaniem owego kodu. Jeśli informacja zapisana w haśle nie posiadała żadnego znaczenia dla osoby, która bezprawnie weszła w jego posiadanie, ale dzięki temu sprawca uzyskał nieuprawniony dostęp do informacji i np. zalogował się do cudzej poczty, to wypełni on znamiona przestępstwa z art. 267 § 1 k.k. Uzyskanie danych autoryzacyjnych, bez faktycznej możliwości uzyskania dostępu do informacji, mogłoby stanowić formę usiłowania z art. 13 § 1 k.k. w zw. z art. 267 § 1 k.k. Jak słusznie zauważają bowiem W. Wróbel i D. Zając, wyłudzenie hasła w celu jego wykorzystania do uzyskania dostępu do zabezpieczonych danych stanowi ominięcie zabezpieczenia, a zatem realizuje znamiona opisane w art. 267 § 1 k.k. Uzyskanie dostępu do informacji należy traktować w sposób podobny jak przełamanie zabezpieczenia, o którym mowa w przypadku kradzieży z włamaniem (art. 279 § 1 k.k.). Każde uzyskanie takiego dostępu z wykorzystaniem bezprawnie zdobytego „klucza" (hasła, szyfru, klucza do sejfu) realizuje znamiona art. 267 § 1 k.k. Za przyjęciem powyższej interpretacji przemawiają te same względy, które nakazują traktować posłużenie się kradzionym kluczem jako włamanie. W tej perspektywie nie zachodzą bowiem żadne istotne różnice między kradzieżą mienia a „kradzieżą" informacji[52]. Brak zatem podstaw, aby podzielić stanowisko Sądu Apelacyjnego w Szczecinie, który stwierdził:

> Nie stanowi przestępstwa z art. 267 § 1 k.k. bezprawne posługiwanie się hasłami lub kodami umożliwiającymi dostęp do informacji. Nie do zaaprobowania pozostaje stanowisko jakoby nielegalne, tj. bez zgody posiadacza, czy też nawet przy użyciu podstępu, uzyskanie kodów i haseł dostępu do konta bankowego tożsame było pojęciu przełamania.

W sprawie tej oskarżony – jak ustalił sąd – miał „realny dostęp do kodów znajdujących się w firmie i choć nie posiadał do tego uprawnień, mógł je wykorzystać. Kody znajdowały się w biurze firmy, a ich forma i brak zabezpieczenia umożliwiały łatwe ich odczytanie". Nie do zaaprobowania, zdaniem sądu, było stanowisko prokuratora, jakoby w takiej sytuacji nielegalne, tj. bez zgody posiadacza, czy też nawet przy użyciu podstępu, uzyskanie kodów i haseł do konta bankowego pokrzywdzonej spółki tożsame było pojęciu przełamania. Niewątpliwie, podkreślił szczeciński sąd, charakter życzeniowy stanowiło twierdzenie, jakoby pozyskane informacje były zastrzeżone i należycie zabezpieczone, skoro oskarżony pozyskał nieprzeznaczone dla niego informacje bez żadnych szczególnych starań, a jedynie nadużywając zaufania swojego pracodawcy[53]. Sąd nie zauważył jednak, że sprawca działał w zamiarze kierunkowym uzyskania bezprawnego dostępu do nieprzeznaczonych dla niego informacji znajdujących się w aplikacji

[52] W. Wróbel, D. Zając, *Art. 267*, [w:] *Kodeks karny. Część szczególna*, t. 2. cz. 2, *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2017, LEX, teza 20b.

[53] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.

bankowej pokrzywdzonego, a nie informacji stanowiących kody autoryzacyjne do tej aplikacji. Dlatego rozpatrywanie przez sąd znamion art. 267 § 1 k.k. pod kątem sposobu „uzyskania [przez sprawcę – przyp. autora] kodów i haseł dostępu do konta bankowego", znajdujących się w biurze firmy, nie miało decydującego znaczenia dla bytu tego przestępstwa. Pokazuje to stan faktyczny sprawy w wyroku Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie, kiedy oskarżona w podobny sposób, jak w przypadku sprawy rozpatrywanej przez Sąd Apelacyjny w Szczecinie, uzyskała kod do skrzynki paczkomatu. Co prawda, jej działanie stanowiło kradzież z włamaniem, ale ważne jest to, że zdaniem krakowskiego sądu, uzyskanie haseł/kodów nie musi wiązać się z jakimiś szczególnymi działaniami. W rezultacie sąd uznał kobietę za winną tego, że:

> w dniu 23 grudnia 2015 roku w Krakowie, na os. Piastów /…/, dokonała zaboru w celu przywłaszczenia przesyłki o numerze /…/ o wartości 531 zł, zawierającej zegarek marki Casio z paczkomatu o oznaczeniu /…/, należącego do przedsiębiorstwa /…/, posługując się kodem do skrzynki w tym paczkomacie, który to kod uzyskała wykorzystując swoje stanowisko służbowe w firmie /…/, co pozwoliło jej rozliczyć fikcyjną opłatę za przesyłkę w systemie informatycznym tej spółki, czym działała na szkodę /…/ tj. o przestępstwo z art. 278 § 1 k.k. i art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k.[54]

W sporze o charakter prawny haseł komputerowych wybrzmiewa niekiedy odwołanie do ogólnego rozróżnienia pomiędzy „danymi informatycznymi" a „informacją". A. Behan bezzasadnie domaga się zrównania znaczenia tych dwóch pojęć. Przywołany autor pisze:

> Jeśli bowiem przyjąć, że hasło musi nieść ze sobą „sens", to w jaki sposób należałoby go określać? Konsekwentnie – czy liczba może posiadać ów sens? Wydaje się, że na tak postawione pytanie odpowiedź musi być twierdząca. Liczba „3,14" dla każdego ma określone, najpewniej to samo znaczenie, ale już „1999" może – w zależności od interpretatora – oznaczać cenę, rok urodzenia, czy liczbę znaczków w kolekcji. Dalej – jeśli liczba jest informacją, to i taką informacją musi być hasło, bo możemy je zapisać w formie liczbowej. Przytaczany już ciąg „ala ma kota" możemy zapisać nie tylko za pomocą liter, ale również heksadecymalnie jako 61 6c 61 20 6d 61 20 6b 6f 74 61 lub binarnie za pomocą 0|1. Oczywiście tylko ostatnia forma będzie jednocześnie danymi, gdyż tylko taki zapis będzie zrozumiały dla mikroprocesorów, przy czym nie oznacza to, że standard jego zapisu czy kodowania będzie równoznaczny z utratą statusu informacji, nawet jeśli „modelowy obywatel" nie zrozumie jego znaczenia[55].

[54] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 228/17/N.
[55] A. Behan, *Waluty wirtualne jako*…, s. 607–608.

Oczywiście, jak podano już w monografii, „dane informatyczne" i „informacje", pod względem technicznym, stanowią „jedno i to samo" w tym znaczeniu, że z przetworzenia danych wyświetla się na monitorze komputera informacja i na odwrót; po wyłączeniu komputera informacja powraca do pierwotnej formy binarnej. Jednak pod kątem oceny znamion przestępstw teleinformatycznych ważne jest to, co „tu i teraz" stanowi przedmiot czynności wykonawczej lub co jest przedmiotem zamachu i w grę wchodzą dwa wzajemnie wykluczające się znamiona: „dane informatyczne" lub „informacje".

Sam fakt, że poprzez działanie algorytmu komputerowego „dane informatyczne" mogą zostać przetworzone na sensowną dla człowieka treść, nie czyni ich automatycznie informacjami w rozumieniu m.in. art. 267 § 1 k.k. Akceptacja przeciwnego stanowiska czyniłaby bezsensową treść większości przepisów zawartych w rozdziale XXXIII k.k. i niweczyła logiczne uzasadnienie dla wprowadzenia dwóch odmiennie brzmiących znamion czynów zabronionych, a w konsekwencji uniemożliwiła racjonalne stosowanie norm prawnych statuujących przestępstwa teleinformatyczne. Nawiasem mówiąc, myli się także A. Behan, twierdząc, że nieuporządkowany zbiór cyfr lub liczb stanowi informację, nawet jeśli „'modelowy obywatel' nie zrozumie jego znaczenia", gdyż przykładowy ciąg znaków „82748349389" nie ma żadnego sensu. Ogólnie rzecz biorąc, to analiza tematu odpowiedzialności karnej za haking haseł pokazała, że chodzi o zagadnienie skomplikowane, a konkretne rozstrzygnięcia stanów faktycznych pod kątem ich kwalifikacji prawnej musi poprzedzać wnikliwa analiza materiału dowodowego zgromadzone w sprawie. Należy wystrzegać się przy tym prostych uogólnień i stereotypowych sądów[56] oraz pamiętać, że hasła umożliwiające dostęp do danych i/lub informacji mogą być narzędziem służącym do popełnienia innych przestępstw, aniżeli tylko stypizowanych w art. 267 § 1 k.k.

[56] A. Behan: „Niewytłumaczalnym jest powód, dla którego otwarcie listu zawierającego gazetkę reklamową z supermarketu realizować będzie znamiona typu czynu zabronionego z art. 267 § 1 k.k., a zdobycie przez atakującego hasła do konta w serwisie społecznościowym czy skrzynki pocztowej – z którymi zintegrowane są dziesiątki usług umożliwiających atakującemu nie tylko poznanie olbrzymiej ilości informacji o ofierze, ale też dokonywanie płatności czy zamawianie usług - realizować znamion tego przepisu już nie będzie". A. Behan zapomina, że ocenę, czy ma się do czynienia z przestępstwem, należy zacząć od analizy rzeczywistego zdarzenia pod kątem elementów struktury czynu zabronionego. Jest wątpliwe, aby „otwarcie listu zawierającego gazetkę reklamową z supermarketu" było społecznie szkodliwe w stopniu wyższym niż znikomy. Poza tym „zdobycie przez atakującego hasła do konta w serwisie społecznościowym czy skrzynki pocztowej" i uzyskanie w ten sposób bez uprawnienia dostępu do całości lub części systemu informatycznego, może wyczerpać znamiona przestępstwa z art. 267 § 2 k.k., [w:] A. Behan, *Waluty wirtualne jako*…, s. 603, 606.

Rozdział 3
Przestępstwa przeciwko ochronie danych i informacji

3.1. Analiza spraw karnych dotyczących czynów z art. 267 § 1 k.k.

W dyskursie dotyczącym cyberprzestępczości popularne są słowa haker i haking nasuwające na myśl obraz młodego człowieka w kapturze i zakrywającej twarz „masce protestu" spopularyzowanej przez grupę Anonymous. Owszem, zdarzają się spektakularne działania hakerskie i takie przestępstwa zostały opisane w monografii, ale częściej przestępstwa stypizowane w art. 267 k.k. mają „prozaiczną twarz" i dotyczą drobnych występków popełnianych przez osoby, które nie są ponadprzeciętnie obeznane z techniką komputerową i szerzej – nowymi technologiami, a stały się przestępcami niejako „z przypadku".

Art. 267. [Bezprawne uzyskanie informacji]
§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.
§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego[57].

Badanie akt spraw karnych kwalifikowanych z art. 267 k.k. pokazało, że duża część z nich dotyczyła „tradycyjnych" form przestępczości, tj. niezwiązanych z nowymi

[57] Obecnie obowiązujący kształt art. 267 k.k. zyskał na podstawie ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2008 Nr 214, poz. 1344), a w pierwotnej wersji Kodeksu karnego przepis art. 267 k.k. miał brzmienie:
§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

technologiami i cyberprzestrzenią. Chociaż postępowania takie znajdują się poza zakresem przedmiotowym podjętego planu badawczego, to warto, chociażby dla ogólnego rozeznania, przytoczyć kilka wyroków zapadłych w tego typu sprawach; kolejno zacytowano orzeczenia trzech sądów: Sądu Rejonowego dla Krakowa-Nowej Huty, Sądu Rejonowego dla Krakowa-Podgórza i Sądu Rejonowego dla Krakowa-Krowodrzy, w których uznano oskarżonych za winnych tego, że:

> w bliżej nieustalonym dniu nie wcześniej niż 2 kwietnia 2014 roku i nie później niż 29 kwietnia 2014 roku w Krakowie uzyskała dostęp do informacji dla niej nie przeznaczonej w postaci faktury VAT z dnia 02.04.2014 r. przez otwarcie zamkniętego pisma adresowanego do G. M., tj. za przestępstwo z art. 267 § 1 k.k.[58]

> w nieustalonym dniu 2019 roku, nie później niż 12 lutego 2019 roku w Krakowie uzyskała bez uprawnienia dostęp do informacji dla niej nie przeznaczonej, poprzez otwarcie zamkniętego pisma adresowanego do A. F. w postaci rocznego obliczenia podatku przez organ rentowy za rok podatkowy 2018, tj. za przestępstwo z art. 267 § 1 k.k.[59]

> w dniu 25 października 2011 roku w Krakowie, działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru, w celu użycia za autentyczne podrobił podpis Z. G. na zwrotnym potwierdzeniu odbioru przesyłki z Urzędu Miasta /…/ oraz na karcie doręczeń Urzędu Pocztowego nr /…/ w Krakowie, a następnie przez otwarcie wymienionej przesyłki skierowanej do Z. G., bez uprawnienia odzyskał informację dla siebie nie przeznaczoną, tj. o popełnienie przestępstwa z art. 270 § 1 k.k. i art. 267 § 1 k.k. w zw. z art. 12 k.k.[60]

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.
§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.
Wynika z tego, że w pierwotnej wersji przepis art. 267 § 1 k.k. sankcjonował sam fakt zapoznania się przez hakera z treścią przechowywanej w systemie komputerowym informacji, np. cudzej korespondencji elektronicznej, danych strategicznych rozwoju i planowania konkurencyjnej firmy, [w:] P. Siemkowicz, *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym – z uwzględnieniem aktualnych zmian nowelizacyjnych*, CBKE e – Biuletyn, s. 4, http://www.bibliotekacyfrowa.pl/Content/34363/PDF/Przestepstwa_skierowane.pdf [dostęp: 28.07.2022].

[58] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 679/14/N.

[59] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1369/19/P.

[60] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 992/11/N. W wyroku skazującym Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie prawidłowo zmienił kwalifikację prawną czynu, przyjmując, że sprawca dopuścił się przestępstwa z art. 270 § 1 k.k. i art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.

w bliżej nieustalonych dniach w okresie od 19 do 25 listopada 2012 r. działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru poprzez otwarcie zamkniętego pisma dla niego nie przeznaczonego, dokonał kradzieży przesyłki zawierającej kartę debetową /…/ o numerze /…/ oraz przesyłki zawierającej kod pin do tej karty na szkodę F. D. tj. o przestępstwo z art. 278 § 5 k.k. i art. 267 § 1 k.k. w zw. z art. 12 k.k.[61]

w okresie od stycznia 2016 roku do daty bliżej nieustalonej, lecz nie później niż do dnia 24 maja 2016 roku w miejscowości /…/ woj. małopolskiego bez uprawnienia uzyskał informacje dla niego nie przeznaczone przez odbieranie i otwieranie zamkniętej korespondencji pocztowej adresowanej do swojej żony K. K., tj. o przestępstwo z art. 267 § 1 k.k.[62]

Przechodząc do typowych spraw związanych z hakingiem i kwalifikowanych z art. 267 § 1 k.k., na wstępie konieczne jest omówienie występującego w tym przepisie zwrotu „sieć telekomunikacyjna". Zgodnie z art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[63] „sieć telekomunikacyjna" to „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju". Jeżeli odwołać się do zwrotów zawartych w tej definicji, to:

1. system transmisyjny[64] stanowi układ wielu funkcjonujących jako całość elementów (urządzeń, przewodów), mający określoną strukturę i wykorzystywany do przesyłania sygnałów (transferowania danych). Przykładowo, urządzeniami sieci Internet są: karta sieciowa, wzmacniaki, koncentratory, mosty, rutery i przełączniki;
2. urządzenia komutacyjne zapewniają odpowiednią jakość transmisji danych między węzłami sieci. Wyróżnia się sieci z komutacją kanałów, pakietów, wiadomości i sieci ATM (zaawansowane technicznie szerokopasmowe sieci cyfrowe). Podstawową funkcją węzła komutacyjnego w systemie telekomunikacyjnym jest odbiór sygnalizacji od abonentów i przekazywanie jej do innych węzłów. Przykładem węzła komutacyjnego jest centrala telefoniczna. Urządzeniami komutacyjnymi będą zatem różnego rodzaju odbiorniki, nadajniki, procesory itp.;
3. urządzenia przekierowujące stanowią np. specjalne aplikacje na smartfonie, które umożliwiają odbierane połączeń na jednym urządzeniu z kilku różnych kart SIM;

[61] Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 32/14/K.
[62] Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 822/16/K.
[63] T.j. Dz. U. z 2023 r. poz. 57 z późn. zm., dalej jako: ustawa Prawo telekomunikacyjne.
[64] W internetowej Encyklopedii PWN „system teletransmisyjny" określono jako „rodzaj systemu telekomunikacyjnego, złożonego z urządzeń służących do przesyłania sygnałów elektronicznych i mających określone cechy konstrukcyjne", www.encyklopedia.pwn.pl [dostęp: 27.07.2022].

4. nieaktywnymi elementami sieci będą organizatory kabli, koryta kablowe, ramy montażowe, gniazda abonenckie, szafy dystrybucyjne (zapewniające odpowiednią pracę urządzeń, np. serwera), panele krosownicze oraz światłowód[65].

„Sieć telekomunikacyjną" budują zatem urządzenia telekomunikacyjne i linie telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz pomiędzy określonymi zakończeniami sieci. Łączy ona w sobie przesyłanie różnego rodzaju sygnałów i usług telekomunikacyjnych. Chodzi o transmisję informacji w dowolnej formie na odległość, przy czym pojęcie odległości w telekomunikacji jest obszerne: przekaz może odbywać się na bardzo długi dystans, jak ma to miejsce w przypadku przekazywania wyników pomiarów z sond czy próbników kosmicznych na Ziemię z zakątków Układu Słonecznego, ale także na niewielkie odległości, np. pomiędzy dwoma komputerami stojącymi na tym samym biurku lub elementami umieszczonymi w jednym układzie scalonym[66]. W omawianym zakresie, mając na uwadze rozwój historyczny technik komunikowania się, można wyróżnić sieci: telegraficzne, telefoniczne, transmisji danych, Internet, zintegrowane oraz inne sieci. Kolejny podział dotyczy rodzaju przesyłanego sygnału sieci telekomunikacyjnej i wtedy ma się do czynienia z siecią analogową lub cyfrową. Obszar przesyłania informacji determinuje wyróżnienie sieci: wewnętrznych, lokalnych, krajowych i międzynarodowych.

W art. 267 § 1 k.k. chodzi zatem o bezpośrednie „podłączenie się" do urządzenia rozumianego jako przedmiot wchodzący w skład systemu telekomunikacyjnego, a nie „podłączenie się" do transmisji danych poprzez np. odbiór fal radiowych. Jak wskazał Sąd Apelacyjny w Gdańsku, przyjęte w tym przepisie znamię „podłączając się do sieci telekomunikacyjnej" wskazuje na sieć w znaczeniu materialnym jako zespół urządzeń i przewodów (kabli) służących do przekazywania informacji. Zachowania takie polegają na przyłączeniu urządzenia odbiorczego do sieci kablowej (np. telefonicznej, komputerowej) lub innej infrastruktury (np. urządzenia radiowego), służącej do przekazywania informacji. Innymi słowy, „podłączenie" oznacza wyłącznie połączenie fizyczne[67], a błąd w wykładni omawianego znamienia pojawił się w subsydiarnym akcie oskarżenia, gdzie kobieta została oskarżona o to, że:

> w bliżej nieustalonym dniu miesiąca listopada 2013 r. uzyskała, nie posiadając uprawnień dostępu do informacji dla niej nie przeznaczonych, przez podłączenie się do sieci telekomunikacyjnej, przełamując informatyczne zabezpieczenia konta na portalu społecznościowym „Facebook" należącego do M. D. w czym weszła w sposób nieuprawniony w prywatną korespondencję i ujawniła ją osobom trzecim

[65] W. Kabaciński, M. Żal, *Sieci telekomunikacyjne*, Warszawa 2008, 2019, s. 23.
[66] Tamże, s. 1.
[67] Wyrok Sądu Apelacyjnego w Gdańsku z dnia 28 września 2016 r., II AKa 111/16, LEX nr 2191573.

na szkodę M. D. – czym zrealizowała znamiona czynów zabronionych, a to art. 267 § 1 k.k. oraz art. 267 § 4 k.k.[68]

Stan faktyczny opisany w skardze subsydiarnej mówił o tym, że M. D. posiadał konto na portalu społecznościowym zabezpieczone hasłem dostępu, a M. G.-D.

> uzyskała w sposób bezprawny informacje dla niej nieprzeznaczone przez przełamanie zabezpieczeń internetowych konta internetowego należącego do pokrzywdzonego. Naruszyła tajemnicę korespondencji, gdyż przełamując w/w zabezpieczenia weszła w zakładkę 'wiadomości' i pobrała znajdującą się tam korespondencję /…/. Część z tej korespondencji wykorzystała załączając ją do jednego z pism procesowych i ujawniła na rozprawie w Sądzie /…/.

W sprawie powołano biegłego z zakresu informatyki śledczej, który stwierdził, że:

> na dysku komputera brak było śladów użycia oprogramowania do przechwytywania haseł ani żadnych innych śladów wskazujących na próby przełamania zabezpieczeń portalu Facebook. Natomiast stwierdzono, iż przeglądarka internetowa była skonfigurowana w ten sposób, aby zapamiętywać wprowadzone przez użytkownika dane dostępowe, co umożliwiło zalogowanie się do odwiedzanego wcześniej portalu m.in. Facebook bez znajomości hasła lub wykonania innych czynności. Nadto z uwagi na uszkodzenia na dysku komputera brak było możliwości m.in. odtworzenia historii działania użytkownika w dniu 13.11.2013 r.

Na posiedzeniu 22 października 2015 r. Sąd Rejonowy dla Krakowa-Krowodrzy w Krakowie umorzył postępowanie przeciwko oskarżonej M. G.-D. o to, że:

> w bliżej nieustalonym dniu miesiąca listopada 2013 r. uzyskała nie posiadając uprawnień dostępu do informacji dla niej nie przeznaczonych, przez podłączenie się do sieci telekomunikacyjnej, przełamując informatyczne zabezpieczenia konta na portalu społecznościowym „Facebook" należącego do M. D. w czym weszła w sposób nieuprawniony w prywatną korespondencję i ujawniła ja osobą trzecim na szkodę M. D., tj. o przestępstwa z art. 267 § 1 k.k. i z art. 267 § 4 k.k. na podstawie art. 17 § 1 pkt 2 k.p.k.

Zdaniem sądu, w działaniu oskarżonego nie było znamion czynu zabronionego, gdyż „Nieuprawnione podłączenie się do sieci telekomunikacyjnej nie może mieć w tym przypadku zastosowania, albowiem oskarżona musiałaby nielegalnie podłączyć się do całości czy części systemu informatycznego, tj. systemu służącemu gromadzeniu i przetwarzaniu danych za pomocą techniki komputerowej". Sąd stwierdził, że w ustalonym

[68] Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 723/15/K.

stanie faktycznym „nie ma śladu przełamana albo ominięcia zabezpieczenia hasła" przez oskarżoną, a więc wypełnienia znamion zapisanych w art. 267 § 1 k.k.

Decyzja podjęta przez sąd była nieprawidłowa, gdyż oskarżona swoim zachowaniem wypełniła znamiona dwóch czynów zabronionych, tj. art. 267 § 1 k.k. i art. 267 § 4 k.k. Jeśli chodzi o pierwszy z nich, to ominęła informatyczne zabezpieczenie w postaci logowania się do zamkniętego dla osób trzecich konta internetowego. Świadomie bowiem skorzystała z faktu, że hasło było zapisane w wyszukiwarce internetowej, i wykorzystując funkcję automatycznego odczytywania hasła, świadomie zalogowała się na konto męża w portalu Facebook wbrew jego woli. W dalszej części opracowania szczegółowo omówione zostanie znamię „ominięcia zabezpieczenia"; teraz należy stwierdzić, że jeśli nawet w treści zarzutu subsydiarnego aktu oskarżenia błędnie wskazano, iż M. G.-D. „podłączyła się do sieci telekomunikacyjnej", to sąd był zobowiązany, nie wychodząc poza ramy aktu oskarżenia, zmodyfikować opis czynu i uznać oskarżoną za winną tego, że:

> w bliżej nieustalonym dnia w miesiącu listopadzie 2013 r. w Krakowie bez uprawnienia uzyskała dostęp do informacji dla niej nieprzeznaczonej w postaci treści konta na portalu Facebook, którego posiadaczem był M. D., w ten sposób, że skorzystała z automatycznej funkcji wyszukiwarki internetowej i zapisanego w niej hasła oraz omijając informatyczne zabezpieczenie dostępu do informacji zalogowała się na konto, działając na szkodę M. D., tj. popełnienia przest. z art. 267 § 1 k.k.

Z ustalonego stanu faktycznego wynika ponadto, że oskarżona ujawniła innym osobom informacje uzyskane w sposób opisany w art. 267 § 1 k.k., jednak sformułowanie drugiego zarzutu, co do znamion § 4 ww. artykułu, było niemożliwe z uwagi na brak skargi podmiotu uprawnionego. Owo „ujawnienie" nastąpiło bowiem po dokonaniu włamania na konto i pod względem historycznym stanowiło odrębne zdarzenie, a więc w analizowanej sprawie art. 267 § 1 k.k. i art. 267 § 4 k.k. nie mogły pozostawać w zbiegu realnym.

Badania pokazały, że przestępstwa z art. 267 § 1 k.k. dotyczyły najczęściej stosunkowo drobnej przestępczości o charakterze obyczajowym lub finansowym. Największa liczba spraw odnosiła się do przełamania zabezpieczenia platformy cyfrowej (skrzynki poczty elektronicznej, Facebooka, aplikacji bankowości elektronicznej itp.) i uzyskania przez sprawcę dostępu do informacji dla niego nieprzeznaczonej w postaci treści umieszczonych na indywidualnym koncie lub w aplikacji bankowości elektronicznej osoby trzeciej. Jeszcze przed 2017 r. włamania na rachunki bankowe często kwalifikowano jako haking, ale po zmianie definicji legalnej „rzeczy ruchomej" stosuje się do nich art. 279 § 1 k.k. Najczęściej działanie sprawców miało postać ominięcia zabezpieczenia poprzez fałszywe uwierzytelnienie i podszycie się pod faktycznego posiadacza konta oraz wykorzystanie „przechwyconego" w jakiś sposób hasła; rzadziej dochodziło

do „przełamania" zabezpieczenia w cyberprzestrzeni, które wymaga zaawansowanej wiedzy informatycznej. W przypadku komputera podłączonego do domeny uwierzytelnienie użytkowników przeprowadzane jest na kontrolerze domeny (adresie strony www), tj. serwerze, który gromadzi informacje o zabezpieczeniach sieci. Rozwiązanie takie pozwala internautom na uzyskanie z każdego miejsca na świecie dostępu do ich skrzynek pocztowych niezależnie od tego, czy posiadają przy sobie własnego laptopa[69]. Przestępcom chodzi natomiast o to, aby „oszukać" administratora domeny i zalogować się na konto tak, jakby robił to jego prawowity posiadacz. Przykład opisanego działania stanowi sprawa Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie, gdy K. W. został oskarżony o to, że:

> w bliżej nieustalonym okresie czasu od marca 2011 roku do października 2011 roku w Krakowie, działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, uzyskał bez uprawnienia, dostęp do informacji dla niego nie przeznaczonej, a w szczególności treści wiadomości e-mail, treści rozmów z portali społecznościowych A. W., przełamując istniejące zabezpieczenia w postaci hasła poprzez odgadnięcie jego treści, tj. o przestępstwo z art. 267 § 1 k.k. w zw. z art. 12 k.k.[70]

Zastrzeżenia w zacytowanym opisie czynu budzi element „odgadnięcie treści hasła". Z tego opisu wynika tak, jakby samo „odgadywanie haseł" było zabronione przez prawo, a przecież każdy, posiłkując się posiadaną wiedzą i intelektem, może to robić (pomijając kwestię, na ile wyjaśnienia podejrzanego o „odgadnięciu" hasła są wiarygodne). Znamię czynu zabronionego stanowiło natomiast ominięcie zabezpieczenia informatycznego poprzez nieuprawnione użycie kodu dostępu. W wyroku skazującym sąd przyjął wskazaną przez prokuratora kwalifikację prawną, ale stylistycznie „wygładził" opis znamion:

> w bliżej nieustalonych dniach w okresie od marca 2011 roku do października 2011 roku w Krakowie, działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, przełamując elektroniczne zabezpieczenie informacji, poprzez posłużenie się odgadniętymi hasłami logowania do skrzynki poczty elektronicznej A. W. oraz do należących do pokrzywdzonej profili na portalach społecznościowych, bez uprawnienia uzyskiwał dostęp do informacji dla niego nieprzeznaczonej w postaci treści wiadomości email wysyłanych i odbieranych przez A. W. oraz treści rozmów prowadzonych przez nią za pośrednictwem komunikatorów internetowych na portalach społecznościowych, co stanowi występek z art. 267 § 1 k.k. w zw. z art. 12 k.k.

[69] P. Bensel, *Systemy i sieci komputerowe. Podręcznik do nauki zawodu technik informatyk*, Gliwice 2010, s. 190.
[70] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 641/12/N.

Ustalenia takie prokurator, a następnie sąd poczynili na podstawie wyjaśnień podejrzanego, który powiedział, że hasło odgadł metodą prób i błędów, gdyż było ono bardzo podobne do hasła, którego jego żona używała przed zmianą zabezpieczeń (dotyczyło nazwy zakładu pracy podejrzanego i jego roku urodzenia; nowe hasło zawierało nazwę zakładu pracy pokrzywdzonej i jej datę urodzenia). Odgadnięcie sekwencji znaków i wykorzystanie ich do nieuprawnionego uwierzytelnienia się na platformie cyfrowej stanowi jednak „ominięcie" zabezpieczenia, a nie jego „przełamanie". Sąd prawidłowo opisał okoliczność modalną „bez uprawnienia" i wskazał, co stanowiło „informacje" („treści wiadomości e-mail, treści rozmów z portali społecznościowych").

W przyjętym przez sądy opisie czynów z art. 267 § 1 k.k. zbyt często zabrakło literalnego powołania się na znamię „bez uprawnienia", a w skrajnych przypadkach zupełnie je pominięto; sytuacja taka dotyczyła wyroku Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie, który skazał podsądnego za to, że:

> w okresie od 9 do 25 lipca 2010 r. w W., działając w krótkich odstępach czasu, w celu realizacji z góry powziętego zamiaru, uzyskała dostęp do informacji dla siebie nie przeznaczonej przez przełamanie zabezpieczenia elektronicznego konta pocztowego /…/.pl na szkodę K. P., tj. o czyn z art. 267 § 1 k.k. w zw. z art. 12 k.k.[71]

Klauzula normatywna „bez uprawnienia" stanowi niezbędny komponent znamion przestępstwa hakingu i służy oddaniu pełnej bezprawności działania sprawcy. Zachowanie podejmowane bez upoważnienia to czynność dokonana bez wiedzy i świadomości podmiotu dysponującego informacją, a nawet wbrew jego woli[72]. Innym razem zwrot „bez uprawnienia" sądy zastępowały takimi określeniami, jak: „nie będąc osobą uprawnioną" oraz „nie będąc do tego uprawnionym"; oto przykład:

> w okresie od sierpnia 2012 r. do 20 sierpnia 2013 r. w O., w wykonaniu z góry powziętego zamiaru, w krótkich odstępach czasu, nie będąc osobą uprawnioną ominął elektroniczne zabezpieczenie poczty e-mail /…/ uzyskał i ujawnił informacje dla niego nieprzeznaczoną w postaci treści prywatnej korespondencji elektronicznej A. Z. oraz zmienił hasło dostępu do poczty elektronicznej uniemożliwiając A. Z. gromadzenie i przekazywanie danych w niej zawartych, tj. o czyn z art. 267 § 1 i 4 k.k. w zb. z art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[73]

[71] Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 6 czerwca 2016 r., VIII K 654/11, LEX nr 2096681.

[72] P. Opitek, *Kwalifikacja prawna i opis czynów zabronionych dotyczących przestępczości teleinformatycznej (zagadnienia wybrane)*, „Consilium Iuridicum. Kwartalnik Naukowy Krajowej Rady Sądownictwa" 2022, nr 1–2, s. 168.

[73] Wyrok Sądu Okręgowego w Olsztynie z dnia 4 lutego 2015 r., VII Ka 1181/14, LEX nr 1835967.

Czy rezygnacja z literalnego brzmienia znamion w opisie czynu na rzecz stosowania zwrotów o podobnym sensie znaczeniowym jest błędem? Na pewno nie stanowi to obrazy przepisów prawa materialnego i nie dyskwalifikuje wyroku; ważne jest natomiast, by opis odpowiadał pełnemu zespołowi znamion określonych w przepisie ustawy karnej. Nie oznacza to wszelako, że jedyną formą realizacji tego wymagania jest wierne przytoczenie słów ustawodawcy. Dopuszczalne jest zarówno posłużenie się sformułowaniami równoważnymi językowo, jak i takie zwerbalizowane przedstawienie działania oskarżonego, które w sposób niepozostawiający wątpliwości odpowiada treści poszczególnych znamion przypisanego mu przestępstwa, albo w drodze nieodpartego logicznego wnioskowania świadczy o wyczerpaniu konkretnego elementu składającego się na ustawowy obraz określonego czynu zabronionego"[74]. Tyle w temacie powiedział Sąd Apelacyjny w Katowicach. Z drugiej jednak strony, zdaniem autora, brak powodów, aby ustawowe zwroty zastępować słowami bliskoznacznymi: nie wpływa to przecież na efektywność lub ergonomię pracy sędziego lub prokuratora. Prowadzi natomiast do rozdźwięku między językiem prawnym a jego prawniczym odpowiednikiem, co w skrajnych przypadkach może skutkować nieporozumieniami, a nawet błędami w konstruowaniu treści zarzutu lub wyroku albo ich zrozumienie przez adresatów orzeczenia. W opisywanych sprawach nie było logicznych przesłanek, aby sądy zrezygnowały z posługiwania się ustawowym zwrotem „bez uprawnienia", zamiast go zniekształcać. Błędy w formułowaniu opisu czynu dotyczą także dodawania do niego treści („quasi-znamion"), które nie decydują o zaistnieniu przestępstwa, a stanowią „jedynie" okoliczności wpływające na dyrektywy wymiaru kary (art. 53 k.k.), i tak np. społeczna szkodliwość czynu jest, ogólnie rzecz biorąc, wyższa u sprawcy, który nie tylko uzyskuje bez uprawnienia dostęp do informacji dla niego nieprzeznaczonej, ale także zapoznaje się z jej treścią. Fakt ten powinien natomiast znaleźć odzwierciedlenie w wymiarze kary i uzasadnieniu wyroku, a nie w opisie znamion.

Na zakończenie niniejszego podrozdziału warto dodać, że skazanie sprawcy za przestępstwo hakingu może rodzić dalsze, bardzo poważne konsekwencje prawne na gruncie prawa cywilnego, administracyjnego czy innego rodzaju regulacji. Sytuacja taka miała miejsce w postępowaniu toczącym się przed Sądem Okręgowym w Bielsku-Białej, w którym powód S. A. domagał się zobowiązania pozwanej M. Z. do złożenia w formie pisemnej przeprosin „za naruszenie jego dóbr osobistych poprzez skasowanie z jego internetowej skrzynki pocztowej /…/ całej poczty mailowej, a także za skasowanie rozliczeń finansowych zawartych w skrzynce mailowej byłej partnerki powoda" oraz zasądzenia kwoty 60 000 zł z ustawowymi odsetkami od dnia doręczenia pozwu do dnia zapłaty, jak też kosztów postępowania. Sąd cywilny ustalił, że

> toczące się wobec pozwanej postępowanie karne w związku z przełamaniem zabezpieczeń konta poczty elektronicznej D. G., uzyskaniem dostępu do informacji dla

[74] Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 stycznia 2014 r., II AKa 397/13, LEX nr 1428051.

siebie nieprzeznaczonej i usunięciem korespondencji e-mail, tj. o czyn z art. 267 § 1 k.k. i art. 268 § 1 k.k. w zw. z art. 11 § 2 k.k. i art. 12 k.k. zostało warunkowo umorzone na okres próby 1 roku (wyrok Sądu Rejonowego w Bielsku-Białej z 27 marca 2013 r. sygn. IX 946/12 oraz wyrok Sądu Okręgowego w Bielsku-Białej z 10 września 2013 r. sygn. VII Ka 483/13). Z kolei dochodzenie dotyczące uzyskania dostępu bez uprawnień i usunięcia poczty elektronicznej dotyczącej firmy /…/ z konta /…/ zostało umorzone.

W wyroku z dnia 8 czerwca 2016 r. sąd:

1. zobowiązał pozwaną, w terminie 7 (siedmiu) dni od prawomocności wyroku, do wysłania powodowi, na adres /…/, pisma zawierającego oświadczenie o następującej treści: „Przepraszam Pana S. A. za naruszenie jego dóbr osobistych poprzez skasowanie z jego internetowej skrzynki pocztowej /…/ poczty e-mail, a także za skasowanie z internetowej skrzynki pocztowej Pani D. G. wiadomości e-mail zawierających moje rozliczenia finansowe ze S. A.";
2. zasądził od pozwanej na rzecz powoda kwotę 5.000 złotych wraz z ustawowymi odsetkami od 31 stycznia 2016 r. do dnia zapłaty;
3. w pozostałym zakresie oddalił powództwo[75].

W uzasadnieniu do wyroku sąd stwierdził, że w sprawie doszło do naruszenia dóbr osobistych powoda poprzez działania godzące w tajemnicę istotnej dla stron korespondencji, a więc sfery powiązanej z prawem do prywatności. To z kolei było źródłem krzywdy powoda, a wziąwszy pod uwagę zawinienie w działaniach pozwanej, spełnione zostały przesłanki roszczenia o zadośćuczynienie.

3.2. „Przełamanie" albo „ominięcie" zabezpieczenia informacji (art. 267 § 1 k.k.)

Podobieństwo pomiędzy przestępstwem hakingu a kradzieżą z włamaniem dotyczy znamion określających czynność sprawczą, tj. pokonywania określonych zabezpieczeń w celu uzyskania dostępu do dobra chronionego prawem. Jednak przedmiot ochrony w obu przepisach jest zgoła odmienny: w przypadku art. 267 § 1 k.k. chodzi o szeroko rozumiane prawo do dysponowania informacją, a art. 279 § 1 k.k. chroni rzeczy ruchome. Interesująca jest kwestia, jak traktować zbieg tych dwóch przepisów w sytuacji, gdy sprawca wyczerpuje znamiona czynu polegającego na bezprawnym uzyskaniu informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, a następnie dokonuje zaboru w celu przywłaszczenia rzeczy ruchomej w postaci środków pieniężnych zapisanych na rachunku (art. 115 § 9 k.k.). Podobną sprawę rozpoznawał Sąd Apelacyjny w Szczeci-

[75] Wyrok Sądu Okręgowego w Bielsku-Białej z dnia 8 czerwca 2016 r., I C 534/15, LEX nr 2302379.

nie, a jego namysł wzbudził przyjęty przez sąd I instancji realny zbiegiem przestępstwa z art. 267 § 1 k.k. i art. 279 § 1 k.k.; w sprawie tej P. G. i D. Z. zostali oskarżeni o to, że:

> w okresie od dnia 9 maja 2007 r. do dnia 10 maja 2007 r. w S., działając wspólnie i w porozumieniu w wykonaniu z góry powziętego zamiaru, w krótkich odstępach czasu, w celu osiągnięcia korzyści majątkowej, bez uprawnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez Bank /…/ rachunku bankowego Spółki /…/ o nr /…/ uzyskali nie przeznaczoną dla nich informację odnośnie stanu salda, a następnie zmienili zapis danych informatycznych w elektronicznym systemie bankowym w ten sposób, że z rachunku pokrzywdzonej spółki na rachunek D. Z. prowadzony w /…/ Banku nr /…/ dokonali niżej wymienionych transakcji-przelewów:
>
> 1. kwoty 100.000 zł w dniu 9 maja 2007 r. o godzinie 23.53.22,
> 2. kwoty 100.000 zł w dniu 10 maja 2007 r. godz. 00.03.02,
> 3. kwoty 60.000 zł w dniu 10 maja 2007 r. godz. 00.10.23,
> 4. kwoty 40.000 zł w dniu 10 maja 2007 r. godz. 00.21.32,
>
> tj. sumy 300.000 zł, którą to następnie kwotę przelali na dalsze rachunki bankowe, tj.:
> - w dniu 11 maja 2007 r. sumę 20.000 zł na konto o nr /…/ prowadzone przez /…/ Banku dla A. B.,
> - w dniu 11 maja 2007 r. sumę 100.000 zł na konto o nr /…/ prowadzone przez /…/ Banku dla P. G.,
> - w dniu 10 maja 2007 r. sumy 28.000 zł, 2.000 zł oraz 10.000 zł, zaś w dniu 11 maja 2007 r. sumy 15.000 zł i 25.000 zł, tj. łącznie kwotę 80.000 zł na konto nr /…/ prowadzone przez /…/ Banku dla K. S., czym działali na szkodę /…/ Spółki oraz /…/ Banku, tj. o czyn z art. 267 § 1 k.k. w zb. z art. 279 § 1 k.k. w zb. z art. 287 § 1 k.k. w zw. art. 294 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z 12 k.k.[76]

Sąd Okręgowy w Szczecinie wyrokiem z dnia 11 czerwca 2008 r. wyeliminował z opisu czynu fragment „bez uprawnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez /…/ bank rachunku bankowego /…/ spółki o nr /…/ uzyskali nieprzeznaczoną dla nich informację odnośnie stanu salda", a z jego kwalifikacji prawnej usunął art. 267 § 1 k.k. W tym zakresie prokurator zarzucił wyrokowi obrazę prawa materialnego, tj. przepisu art. 267 § 1 k.k., poprzez jego wyeliminowanie, chociaż w sprawie ustalono, że oskarżony uzyskał dostęp do listy haseł jednorazowych nielegalnie: w czasie nieobecności w firmie osób upoważnionych do dokonywania przelewów pobrał ją z szuflady jednego z biurek i zeskanował, a także poprzez oddziaływanie na osobę trzecią uzyskał hasło dostępu do rachunku spółki. W ten sposób – zdaniem oskarżyciela publicznego – oskarżony wypełnił znamię przełamania szczególnego

[76] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.

zabezpieczenia i bez uprawnienia uzyskał dostęp do konta, a zatem zrealizował przesłanki z art. 267 § 1 k.k.

Sąd odwoławczy nie podzielił argumentacji prokuratora i zaskarżony wyrok utrzymał w mocy, jednak z innych powodów, aniżeli należało się spodziewać. W okolicznościach sprawy ustalonych przez Sąd Okręgowy w Szczecinie zaszedł pomijalny zbieg przestępstw pomiędzy art. 267 § 1 k.k. i art. 279 § 1 k.k. i haking powinien zostać wyeliminowany z opisu czynu i jego kwalifikacji prawnej. Nie można bowiem dokonać tego samego włamania na podstawie dwóch różnych przepisów, a skoro zamiarem sprawcy był zabór środków zgromadzonych na rachunku bankowym, a nie zapoznanie się z informacjami zamieszczonymi w aplikacji bankowej, to należało przyjąć samą kradzież z włamaniem. Na marginesie należy wskazać, że oba sądy błędnie przywołały art. 287 § 1 k.k., tak jakby chciały ukarać jedną czynność sprawczą, tj. zabór mienia, na podstawie dwóch przepisów karnych, tj. art. 279 § 1 k.k. i art. 287 § 1 k.k. Zastanawia poza tym, dlaczego sąd nie uznał działań oskarżonych w dniach 10 i 11 maja 2007 r. jako pranie pieniędzy (art. 299 § 1 k.k.) uzyskanych z przestępstwa bazowego (art. 279 § 1 k.k.) dokonanego 9 maja 2007 r., skoro dwa dni po włamaniu środki takie sprawcy przetransferowali na kolejne rachunki bankowe po to, aby zatrzeć ślady. Należy bowiem opowiedzieć się za dominującą w orzecznictwie sądowym koncepcją, że przedmiotem „prania" może być mienie pochodzące bezpośrednio z czynu zabronionego pomijając już fakt, że trudno mówić o tożsamości rzeczy w przypadku artefaktów cyfrowych statuujących pieniądz zgromadzony na rachunku.

Powracając do wyroku Sądu Apelacyjnego w Szczecinie, to w jego uzasadnieniu organ orzekający wskazał, że nie stanowi przestępstwa z art. 267 § 1 k.k. bezprawne posługiwanie się hasłami lub kodami umożliwiającymi dostęp do informacji i nie nastąpiło uzyskanie przez podsądnego nieprzeznaczonej dla niego wiedzy na skutek przełamania specjalnych zabezpieczeń bankowych. Oskarżony, jak ustalił szczeciński sąd:

> miał realny dostęp do kodów znajdujących się w firmie i choć nie posiadał do tego uprawnień, mógł je wykorzystać. Kody /…/ znajdowały się w biurze firmy, a ich forma i brak zabezpieczenia umożliwiały łatwe ich odczytanie. Nie do zaaprobowania pozostaje przy tym także stanowisko prokuratora – napisał sąd – jakoby nielegalne, tj. bez zgody posiadacza, czy też nawet przy użyciu podstępu, uzyskanie kodów i haseł dostępu do konta bankowego spółki tożsame było pojęciu przełamania. Oskarżony pozyskał bowiem nie przeznaczone dla niego informacje nie podejmując żadnych szczególnych starań, a jedynie nadużywając zaufania swojego pracodawcy. Co prawda nie posiadał on dostępu do hasła, ale pracując w pomieszczeniu biurowym mógł je usłyszeć. Wykorzystanie lekkomyślności, czy też niedbalstwa posiadacza konta, jego dysponenta, nie mieści się natomiast w pojęciu przełamania.

Sąd i prokurator, na rozprawie apelacyjnej, wyrazili stanowisko, iż swoim działaniem oskarżeni, a zwłaszcza P. G., wyczerpali także znamiona przestępstwa z art. 269b

§ 1 k.k., który to przepis penalizuje m.in. bezprawne (nieuprawnione) pozyskiwanie haseł komputerowych, kodów dostępu lub innych danych umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej[77].

W sprawie rozpoznawanej przez Sąd Apelacyjny w Szczecinie pojawiło się zagadnienie prawne, jak interpretować znamię „przełamuje zabezpieczenie", które od samego początku obowiązywania art. 267 § 1 k.k. budziło kontrowersje. W pierwotnym kształcie omawiany przepis brzmiał:

> Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Treść art. 267 § 1 k.k. zmieniona została przez art. 1 pkt 4 ustawy z dnia 24 października 2008 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw[78]. Jak wynika z uzasadnienia do ustawy nowelizującej, głównym celem poczynionych zmian miało być poszerzenie kręgu czynów, które zostaną uznane za haking. W uzasadnieniu napisano:

> Nie wszystkie z tych zachowań (dotyczących przełamywania zabezpieczeń hasłami dostępu – przypis autora) są aktualnie penalizowane w polskim prawie karnym, co czyni konieczną modyfikację niektórych przepisów w sposób prowadzący do pełnej ich zgodności z wymaganiami wynikającymi z Decyzji ramowej [chodziło o Decyzję ramową Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne – przypis autora][79].

Projekt poszerzał opis znamienia czasownikowego czynności wykonawczej przestępstwa hakingu o sformułowanie „albo omijając" z uwagi na okoliczność, że „zgodnie ze stanowiskiem specjalistów zajmujących się prawem informatycznym jest możliwe uzyskanie dostępu do zabezpieczonej informacji bez przełamywania, lecz przez ominięcie jej zabezpieczeń"[80]. Stanowisku takiemu wtórował R. Koszut, pisząc, że posłużenie się przez polskiego ustawodawcę pojęciem „przełamania zabezpieczeń" poważnie

[77] W tym miejscu wypada tylko wskazać , że „poprawienie" przez Sąd Apelacyjny w Szczecinie kwalifikacji prawnej czynu przypisanego oskarżonym w trybie art. 445 § 1 k.p.k. przez przyjęcie w niej także art. 269b § 1 k.k. na etapie postępowania odwoławczego było niedopuszczalne, a ponadto oskarżeni swoim zachowaniem nie wyczerpali znamion art. 269b § 1 k.k., o czym będzie mowa w podrozdziale poświęconym temu artykułowi.

[78] Dz. U. z 2008 r. Nr 214, poz. 1344.

[79] Uzasadnienie projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, wersja: ustawa po rozpatrzeniu stanowiska Senatu, Sejm przyjął poprawki Senatu, LEX.

[80] Tamże.

ogranicza zakres praktycznego zastosowania art. 267 § 1 k.k.[81] Przed nowelizacją twierdzono bowiem, że wszelkie zachowania otwierające sprawcy drogę do informacji zgromadzonych w systemie komputerowym, które nie stanowią oddziaływania na zabezpieczenie, lecz sprowadzają się do wyszukania drogi dojścia do informacji niejako „obok" zabezpieczenia (obejście), nie stanowią realizacji znamion przestępstwa określonego w art. 267 § 1 k.k., nawet jeżeli sprawca uzyskuje bez uprawnienia dostęp do informacji[82]. W związku z tym Sąd Okręgowy w Szczecinie prawidłowo wyeliminował z opisu czynu i jego kwalifikacji prawnej ww. artykuł, gdyż przestępstwo zostało popełnione w 2007 r. (pomijając kwestię, że dzisiaj art. 267 § 1 k.k. i tak zostałby skonsumowany przez art. 279 § 1 k.k.).

Obecnie, aby odpowiedzieć na pytanie, czym różni się „ominięcie" zabezpieczenia od jego „przełamania", wpierw należy ustalić, czym jest owo „zabezpieczenie" informacji przetwarzanych w systemie informatycznym i zapisanych na nośnikach danych.

Najpopularniejsze zabezpieczenie, stosowane przez użytkownika końcowego sieci, stanowi procedura logowania się do systemu, określana w nauce o cyberbezpieczeństwie mianem uwierzytelnienia. Bezpieczeństwo logowania ma zapewnić, że tylko uprawnione osoby mogą uzyskać dostęp do swoich kont działających online, a „niewłaściwych aktorów" się odrzuca. Funkcjonują różne metody uwierzytelnienia się w systemie: kiedyś jedynym sposobem ochrony poufnych informacji zamieszczonych na specjalnie utworzonych do tego kontach była kombinacja nazwy użytkownika oraz hasła i nadal jest ona powszechnie stosowana. Ale najlepsze rozwiązania dotyczące bezpieczeństwa logowania rozwinęły się wraz ze schematami działań cyberprzestępców, którzy nieustannie szukają kolejnych sposobów na łamanie i omijanie haseł. Nowoczesne narzędzia zabezpieczające wykraczają poza kombinacje danych logowania i hasła, gdyż stosuje się np. uwierzytelnianie wieloskładnikowe, które pomaga z większą dozą pewności zweryfikować tożsamość rzeczywistych użytkowników, jednocześnie udaremniając próby „kradzieży" danych. W logowaniu wieloskładnikowym oprócz samego loginu i hasła należy podać kod autoryzacyjny, przesłany przez dostarczyciela usługi np. SMS-em lub mailem; kod może być też pobierany rzez aplikację lub inne dedykowane urządzenie[83]. Czyni to bezpieczniejszymi treści ulokowane w systemie informatycznym, jakie narażone są na „ataki" hakerów, wśród których można wyróżnić:

1. ataki siłowe: przestępcy używają metody prób i błędów, efektywniejszej dzięki automatyzacji procesów obliczeniowych w komputerach, aby uzyskać nieuprawniony dostęp do kont. To prosta metoda rozpoczęcia hakowania w celu kradzieży poświadczeń logowania, kluczy szyfrowania i haseł;

[81] R. Koszut, *Kwestie sporne na tle wykładni przestępstwa hackingu*, „Nowa Kodyfikacja Prawa Karnego" 2001, nr 8, s. 79.

[82] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1 (25), LEX.

[83] *Co to jest bezpieczeństwo logowania*?, https://www.microsoft.com/pl – pl/security/business/security – 101/what – is – login – security [dostęp: 09.07.2023].

2. ataki oparte na inżynierii społecznej: napastnicy stosują metody socjotechniczne „manipulowania" ludźmi i doprowadzają np. do dobrowolnego przekazania przez pokrzywdzonego haseł, wysyłają fałszywe maile do firm, zachęcające internautów do połączenia się z oszukańczą witryną i zalogowania do umieszczonej tam „bramki" itp.;
3. stosowanie przez hakerów złośliwego oprogramowania, takiego jak wirusy, robaki, ransomware. Złośliwe oprogramowanie może być zaprojektowane do pobierania z zainfekowanych komputerów danych lub informacji, a nawet niszczenia sieci oraz systemów;
4. funkcjonowanie programów szpiegujących, które w tajemnicy przed użytkownikiem komputera rejestrują poświadczenia logowania i aktywność przeglądarki oraz kopiują dane tak, aby wykorzystać je do kradzieży tożsamości lub włamań[84].

Przestępca może uzyskać akces do konta nie tylko przez wejście w posiadanie haseł dostępu indywidualnego klienta usługi, czy jeszcze innym sposobem „skompromitować" procedurę uwierzytelniania się po stronie użytkownika końcowego. „Atak" i uzyskanie dostępu do informacji następuje czasami poprzez przełamanie albo ominięcie zabezpieczenia po stronie dostarczyciela usługi lub innego profesjonalnego podmiotu internetowego rynku i dotyczy „inwigilacji" serwera, na którym zgromadzone są informacje lub podglądu pulpitu zhakowanego komputera administratora sieci. Inny *modus operandi* cyberprzestępców, czyli man in the middle, polega na niejawnym podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami. Podstawową cechą czynnego przechwytywania jest ingerencja w ruch sieciowy, realizowana najczęściej w formie tzw. ataku z człowiekiem pośrodku, przy czym „człowiek" to operator urządzenia przechwytującego. Urządzenie to, ulokowane na drodze przepływu danych między klientem a serwerem, pełni rolę pomostu, a konfiguracja taka daje przestępcy możliwość wyłączenia szyfrowania danych, czyniąc je wygodniejszymi do analizy lub eksploatacji „dziury" w zabezpieczeniach[85].

Wynika z tego, że działania polegające na kompromitacji zabezpieczeń tylko w aspekcie procedury logowania się klienta na konto nie wyczerpują przypadków zdarzeń penalizowanych przez art. 267 § 1 k.k. Należy przyjąć, że „ominięcie" dotyczy zniwelowania zabezpieczenia konta poprzez użycie rzeczywiście ustanowionych dla tego konta zabezpieczeń, najczęściej w postaci haseł; w przypadku „przełamania" uzyskuje się dostęp do identycznych zasobów, ale z pominięciem oficjalnej procedury logowania (np. przechwytując ruch sieciowy metodą man in the middle). „Szczególne zabezpieczenia" informacji to także różnego typu mechanizmy zabezpieczeń informatycznych i teleinformatycznych, umiejscowione na poszczególnych etapach przesyłania i przetwarzania danych cyfrowych: poczynając od serwera właściciela usługi, przez dostarczycieli przeglądarek, do wyszukiwania stron „podpiętych" do konta aplikacji płatności elektronicznych, usług poczty elektronicznej, a kończąc na użytkowniku ostatecznym.

[84] Tamże.

[85] J. Forshaw, *Atak na sieci okiem hakera*…, s. 43.

Każdy z podmiotów działających w cyberprzestrzeni narażony jest na obejście lub przełamanie przez przestępcę uwierzytelnienia lub kontroli bezpieczeństwa jego systemu, wielowektorowe ataki hakerskie i socjotechniczne, ataki DDoS, mail boombing i SPAM, ataki ukierunkowane na zainstalowanie wirusów (sniffing, phishing, spoofing), czego skutkiem może być nieuprawnione uzyskanie dostępu do poufnych informacji. W takich przypadkach należy rozważyć ponadto, czy sprawca swoim działaniem nie wypełnił oprócz znamion art. 267 § 1 k.k. również tych z art. 267 § 3 k.k. Chodzi bowiem o dwa różne zdarzenia prawne: przestępstwo z § 1 ma charakter materialny i dla realizacji jego znamion niezbędne jest przełamanie zabezpieczenia oraz uzyskanie dostępu do informacji bez konieczności zapoznania się z treścią. Przestępstwo z § 3 jest formalne w zakresie czynności posługiwania się urządzeniem, natomiast materialne w odniesieniu do posłużenia się oprogramowaniem. Chodzi zatem o sytuację, gdy oprogramowanie umożliwiające uzyskanie informacji zostało zainstalowane w systemie informatycznym lub teleinformatycznym. Wynika z tego, że dla realizacji znamion opisanych w art. 267 § 3 k.k. nie jest konieczne przełamanie zabezpieczenia i uzyskanie nieuprawnionego dostępu do informacji, a zarzut ogłoszony podejrzanemu mógłby brzmieć następująco:

> w dniu 1 stycznia 2023 r. w Krakowie działając w celu uzyskania informacji, do której nie był uprawniony, zainstalował zdalnie na komputerze J. K. oprogramowanie typu *keylogger* i monitorował proces logowania się przez pokrzywdzonego do poczty elektronicznej założonej w domenie /…/ o nazwie konta /…/, a następnie przejął hasła logowania i w ten sposób, omijając informatyczne zabezpieczenia, uzyskał dostęp do informacji dla niego nieprzeznaczonej w postaci treści korespondencji prowadzonej przez pokrzywdzonego, działając na szkodę J. K., tj. o przestępstwo z art. 267 § 1 i 3 k.k.

Powracając do sedna problemu, tj. rozróżnienia pomiędzy znamionami „przełamać" i „omijać" na gruncie art. 267 § 1 k.k., to w pierwszej kolejności należy odwołać się do znaczenia językowego tych słów. Zgodnie z internetowym Słownikiem języka polskiego PWN[86] „ominąć – omijać" znaczy tyle, co „okrążając, minąć coś, przejść, przejechać obok czegoś nie zatrzymując się", „nie dotknąć, nie dosięgnąć kogoś", „przejść obok siebie, nie dotykając się". Drugi wyraz, „przełamać – przełamywać" to „naciskając, uderzając, zginając, rozdzielić coś na dwa kawałki"; też: „łamiąc, rozdzielić przez środek", „przezwyciężyć coś, co stanowiło przeszkodę w czymś". Synonimami słowa „przełamać", w znaczeniu „rozłamania czegoś na części", są takie wyrazy, jak „poprzełamywać, przepołowić, rozłupać, złamać"[87]. Zatem określenie „przełamując zabezpieczenie informatyczne" będzie dotyczyło czynności uzyskania dostępu w sposób „brutalny",

[86] Słownik języka polskiego PWN, https://sjp.pwn.pl/slowniki/ [dostęp: 10.07.2023].
[87] https://synonim.net/synonim/kod [dostęp: 23.06.2023].

z pominięciem oficjalnej procedury uwierzytelniania się posiadacza konta, gdy sprawca stosuje specjalistyczne oprogramowanie hakerskie, ukierunkowane na łamanie szyfrów, kodów, haseł. Inaczej sprawa wygląda w przypadku „ominięcia zabezpieczenia", kiedy dostęp do informacji uzyskuje się za pomocą przeznaczonych do tego procedur, gdyż przestępca podszywa się pod posiadacza konta, np. wpisuje prawidłowe hasło, które podpatrzył, przypadkowo usłyszał lub odnalazł, przeszukując notatnik pokrzywdzonego. Uzyskanie dostępu poprzez automatyczne zalogowanie się do zasobów z komputera „ofiary" będzie stanowiło „ominięcie" zabezpieczenia, podobnie jak odgadnięcie hasła i zalogowanie się do systemu. Ponadto, jak słusznie zauważa W. Wróbel, ominięcie zabezpieczeń informatycznych może polegać na skorzystaniu z błędów (bugów) w programie komputerowym, czyli błędów w jego kodzie źródłowym albo wynikłych na etapie kompilacji, skutkujących nieprawidłowym jego działaniem, co umożliwia napastnikowi ominięcie zabezpieczeń bez konieczności ich pokonywania i dostęp do informacji znajdujących się w programie bez posiadania stosownych uprawnień. Ominięcie polega również na wykorzystaniu backdoora, czyli celowo stworzonej „luki" w kodzie oprogramowania, umożliwiającej jego modyfikację[88]. Twierdzenie, że znamiona przestępstwa z art. 267 § 1 k.k. realizuje wykorzystanie „słabości" systemu i uzyskanie nieuprawnionego dostępu do informacji, nawet jeśli nie wymaga to korzystania ze specjalistycznego oprogramowania, potwierdza fakt ustanowienia kontratypu działania w celu wykrycia błędów w zabezpieczeniach (art. 269c k.k.). Systemy informatyczne i teleinformatyczne posiadają jakieś niedociągnięcia, a media regularnie informują o włamaniach do baz danych największych korporacji, pomimo że firmy te przeznaczają olbrzymie środki finansowe na cyberbezpieczeństwo. Przyjęcie odmiennego poglądu, tj. że wykorzystanie podatności systemu na manipulację nie wypełnia znamion art. 267 § 1 k.k., legitymizowałoby ich hakowanie.

Jeśli mowa o znamieniu „przełamania" zabezpieczenia informatycznego, to czynem wypełniającym znamiona art. 267 § 1 k.k. będzie atak typu brute force. Polega on na zautomatyzowanym wypróbowaniu za pomocą specjalnego oprogramowania każdej możliwej kombinacji danych uwierzytelniających, zwykle nazw użytkownika i haseł, w celu znalezienia właściwej, a następnie nieautoryzowanego dostępu do konta lub systemu. Ataki typu brute force mogą być skierowane na każdy system wymagający uwierzytelnienia, np. konta internetowe, konta mailowe, serwery i urządzenia mobilne. Jego algorytm oddziałuje online na dane stanowiące informatyczne zabezpieczenie dostępu do informacji po to, aby testować owe zabezpieczenie różnymi kombinacjami znaków. Do „przełamania zabezpieczenia", o którym mowa w art. 267 § 1 k.k., dojdzie także w wyniku zastosowania złośliwego oprogramowania niwelującego działanie programów antywirusowych, dzięki czemu sprawca uzyskuje zdalny dostęp do dokumentów zapisanych w pamięci „zaatakowanego" komputera, a także w sytuacji, gdy „trojan"

[88] W. Wróbel, *Art. 267*, *teza 20a,* [w:] *Kodeks karny. Część szczególna*, t. 2, *Komentarz do art. 117–277 k.k.*, red. A. Zoll, Wolters Kluwer Polska 2017, LEX.

będzie znajdował się na urządzeniu podłączonym do laptopa (np. pendrivie), i stamtąd „zainfekuje" komputer pokrzywdzonego, co umożliwi hakerowi utworzenie zdalnego pulpitu i śledzenie obrazu wyświetlanego na ekranie przejętej maszyny.

Należy się zgodzić z F. Radoniewiczem, który twierdzi, że pojęcie zabezpieczenia obejmuje wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalistycznej lub posiadania szczególnego urządzenia lub kodu. Zabezpieczeniem takim może być hasło dostępu do informacji zgromadzonych na nośniku komputerowym, szczególny program umożliwiający odszyfrowanie zapisu informacji, zapis magnetyczny uruchamiający urządzenie, a wraz z nim dostęp do informacji, specjalne urządzenie do przechwytywania informacji nadawanych na falach radiowych (dekoder). Z perspektywy realizacji znamion nie jest ważny charakter zabezpieczenia, ale istotna jest przede wszystkim manifestacja dysponenta informacji[89]. Nie sposób natomiast mówić o wypełnieniu znamion przestępstwa z art. 267 § 1 k.k. przez sprawcę, który podejdzie do niezabezpieczonego komputera innej osoby i pod jej nieobecność przeglądnie zapisane w komputerze informacje, łącznie z otwartym kontem na portalu społecznościowym. Brak tutaj przełamania albo ominięcia elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia informacji. Takie samo stanowisko przyjął Sąd Okręgowy w Siedlcach i uniewinnił oskarżonego od zarzucanego mu czynu z art. 267 § 1 k.k. Sąd stwierdził bowiem, że nie doszło do ominięcia elektronicznego zabezpieczenia w postaci hasła do konta należącego do W. S., skoro pokrzywdzona nie wylogowała się z portalu Facebook w telefonie oskarżonego. W takiej sytuacji nie musiał on podjąć jakiejkolwiek aktywności w celu ominięcia hasła do tegoż konta. Nie popełnia bowiem przestępstwa z art. 267 § 1 k.k. osoba uzyskująca nieuprawniony dostęp do informacji bez przełamania lub ominięcia zabezpieczenia, nawet jeśli zrobi to podstępem[90].

Funkcjonują jednak mylące orzeczenia sądowe, które niesłusznie wymagają od sprawcy specjalistycznej wiedzy i wyrafinowanego działania po to, aby przypisać mu znamię „przełamania" lub „ominięcia" szczególnego zabezpieczenia. Napisał tak w uzasadnieniu do wyroku Sąd Okręgowy w Świdnicy, twierdząc, że:

> istotą przestępstwa z art. 267 § 1 k.k. jest to, że sprawca nie znając sposobu zabezpieczenia (np. kodów dostępu do określonych informacji, czy też treści haseł) po zastosowaniu, podjęciu pewnych działań (w tym np. rozszyfrowanie kodu lub hasła dostępu do informacji) bądź dokonuje przełamania takiego szczególnego zabezpieczenia bądź takie szczególne zabezpieczenie omija[91].

Aby ponieść odpowiedzialność karną za haking, zdaniem sądu, oskarżony musiałby dysponować „specjalistyczną wiedzą lub specjalistycznymi narzędziami", gdyż

[89] F. Radoniewicz, *Odpowiedzialność karna za hacking*…, s. 292.
[90] Wyrok Sądu Okręgowego w Siedlcach z dnia 30 listopada 2021 r., II Ka 561/21, LEX nr 3290107.
[91] Wyrok Sądu Okręgowego w Świdnicy z dnia 10 kwietnia 2019 r., IV Ka 112/19, LEX nr 2728262.

przełamanie, o którym mowa w z art. 267 § 1 k.k., musi sprawcy „sprawić jakąś trudność". Dlatego uzyskanie dostępu, bez uprawnienia, do informacji, o jakich mowa w treści art. 267 § 1 k.k., poprzez np. posłużenie się hasłem przekazanym czy udostępnionym wcześniej przez pokrzywdzonego lub też np. hasłem zapamiętanym przez przeglądarkę internetową czy też pozostawienie komputera z wpisanym hasłem do danego konta i po zalogowaniu się do systemu nie sposób uznać za przełamania hasła, a zatem powyższe nie wyczerpuje znamion występku z art. 267 § 1 k.k.

Sąd powołał się przy tym na podobny pogląd wyrażony przez Sąd Apelacyjny w Szczecinie[92] tak samo, jak zrobił to A. Lach, twierdząc, iż poza zakresem art. 267 § 1 k.k. pozostaje np. posłużenie się hasłem podglądniętym u autoryzowanego użytkownika lub wyłudzonym przez podanie się za inną osobę[93].

Pomijając już kwestię, dlaczego Sąd Okręgowy w Świdnicy, rozpatrując ww. sprawę, skupił się tylko na ocenie znamienia „przełamując", zapominając, że na kanwie art. 267 § 1 k.k. sprawca może także „ominąć" szczególne zabezpieczenie, wypada powtórzyć, iż wykorzystanie haseł dostępu do ominięcia zabezpieczenia spełnia znamiona hakingu. Na takim stanowisku stanął Sąd Rejonowy w Wałbrzychu, twierdząc, że:

> Co do czynu z art. 267 k.k. wskazać należy, że dla realizacji jego ustawowych znamion nie jest konieczne by uzyskanie dostępu do całości lub części systemu informatycznego połączone było z przełamaniem jakiegokolwiek szczególnego zabezpieczenia i wystarczające jest by sprawca działał wbrew woli uprawnionego podmiotu, który jest dysponentem sieci. Przenosząc powyższe rozważania teoretyczne na grunt przedmiotowej sprawy nie ulega wątpliwości, że oskarżona swoim zachowaniem wyczerpała znamiona czynu z art. 267 § 1 i 2 k.k.

Sąd uznał kobietę za winną tego, że:

> w dniu 20 stycznia 2015 r. w W. /…/ korzystając z /…/ po uprzednim przełamaniu zabezpieczeń informatycznych w postaci loginu i hasła bez uprawnienia uzyskała dostęp do systemu informatycznego Biura /…/ z siedzibą w W. i informacji dla niej nie przeznaczonych stanowiących tajemnicę ww. przedsiębiorstwa dokonując w imieniu Biura /…/ rezerwacji turystycznej o nr /…/, czym dział na szkodę Biura /…/, z siedzibą w W., to jest występku z art. 267 § 1 i 2 k.k.[94]

Sąd przyjął jednak nieprawidłową kwalifikację prawną czynu, tj. zbieg idealny § 1 i 2 art. 267 k.k.; za to czynność czasownikową: „dokonanie w imieniu Biura /…/ rezerwacji turystycznej" w systemie informatycznym tegoż biura, można było uznać, za wypełnienie znamion z art. 287 § 1 k.k. Najważniejszą rzecz, na kanwie omawianego problemu,

[92] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 2728262.
[93] A. Lach, *Art. 267*, *teza 4*, [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Wolters Kluwer Polska 2020.
[94] Wyrok Sądu Rejonowego w Wałbrzychu z dnia 23 września 2016 r., III K 865/15, LEX nr 2146034.

stanowi jednak stwierdzenie sądu, że przełamanie zabezpieczenia informacji polega na posłużeniu się oryginalnymi hasłami dostępu do tejże informacji. Zatem prawidłowy opis i kwalifikacja prawna ustalonych w sprawie okoliczności faktycznych mogłyby wyglądać następująco:

> w dniu 20 stycznia 2015 r. w W. /…/, poprzez wykorzystanie hasła dostępu i ominięcie informatycznego zabezpieczenia zalogowała się na stronę administracyjną Biura /…/ uzyskując bez uprawnienia dostęp do informacji dla niej nieprzeznaczonej i działając w celu osiągnięcia korzyści majątkowej bez upoważnienia wprowadziła nowy zapis danych informatycznych w systemie Biura w postaci rezerwacji turystycznej o nr /…/ doprowadzając do automatycznego przetwarzania i przekazania innym podmiotom danych informatycznych związanych z rezerwacją i jej akceptacją, działając na szkodę Biura /…/ reprezentowanego przez /…/ w wysokości 3000 zł, tj. o przestępstwo z art. 267 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

Zbieg realny pomiędzy art. 267 § 1 k.k. i art. 287 § 1 k.k. może budzić kontrowersje i są argumenty przemawiające przeciwko jego dopuszczalności; pomimo tego autor opowiada się za przyjęciem takiego rozwiązania w pewnych okolicznościach, o czym będzie jeszcze mowa w rozdziale poświęconym kwalifikacji czynów z art. 287 § 1 k.k.

Powracając jednak do kwestii znamion hakingu, to doświadczenie autora wyniesione z sali sądowej i poparte treścią analizowanych wyroków pokazuje, że podstępne uzyskanie hasła i wykorzystanie go do ominięcia zabezpieczenia informatycznego wypełnia znamiona art. 267 § 1 k.k. Otóż, zdecydowanie największa liczba spraw penalizowana z ww. przepisu dotyczy zdobycia hasła w prosty sposób, a nie przy użyciu specjalistycznych programów lub wyrafinowanych technik hakerskich. Sprawcy przestępstwa z art. 267 § 1 k.k. posiadają w zdecydowanej większości przypadków jedynie podstawową wiedzę o technologiach informatycznych i nie są w stanie przeprowadzać jakichkolwiek ataków hakerskich lub przełamywać skomplikowanych zabezpieczeń komputerowych. Analiza orzeczeń dotyczących art. 267 § 1 k.k. pokazała ponadto, że sądy mają dużo trudności z ustaleniem i oceną znamienia „przełamuje" lub „omija" i niekiedy poprzestają na ogólnych stwierdzeniach typu: „W świetle poczynionych przez sąd ustaleń faktycznych, nie budzi żadnych wątpliwości, że oskarżony K. O. przełamał zabezpieczenie w postaci hasła do prywatnego konta pocztowego A. B.", chociaż w uzasadnieniu do wyroku Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie nie sposób odnaleźć jakichkolwiek ustaleń, jak doszło do „przełamania zabezpieczenia w postaci hasła"; tym bardziej owe kategoryczne stwierdzenie sądu co do sposobu działania sprawcy jest niezrozumiałe, gdyż oskarżony wyjaśnił, że hasło

ustalał razem z żoną (pokrzywdzoną), a sąd w tym zakresie nie dał wiary jego wersji zdarzeń i skazał mężczyznę za to, że:

> w bliżej nieustalonym dniu pomiędzy 14 a 27 marca 2012 r. bez uprawnienia uzyskał dostęp do informacji dla niego nie przeznaczonych w postaci widomości e-mail w ten sposób, że przełamał zabezpieczenie informatyczne poprzez uzyskanie hasła do konta internetowego /…/ należącego do A. B., bez jej zgody oraz wiedzy, tj. o przest. z art. 267 § 1 k.k.[95]

W innej sprawie Sąd Rejonowy w Wałbrzychu wymierzył oskarżonemu karę za to, że:

> w dniu 31 maja 2016 r. w W. /…/ poprzez przełamanie hasła zabezpieczającego dostęp do komputera oraz hasła profilu na portalu społecznościowym F. bez uprawnień uzyskał dostęp do informacji dla niego nie przeznaczonych czym działał na szkodę J. A., tj. występek z art. 267 § 1 k.k.[96]

Sąd ustalił, iż bez wątpienia informacje zawarte na portalu społecznościowym F. należącym do J. A. nie były przeznaczone dla oskarżonego i nie miał on uprawnienia do dostępu do tych informacji. Ewidentnym wyrazem woli pokrzywdzonej, dotyczącej zabezpieczenia tychże informacji przed dostępem osób trzecich, było ustanowienie hasła dostępu do portalu, a także do komputera, który użytkowała. Wygenerowanie tego rodzaju haseł bez wątpienia stanowiło zabezpieczenie, o jakim mowa w art. 267 § 1 k.k. W tym przypadku niepodważalne przekonanie sądu o tym, że doszło do przełamania zabezpieczenia, wynikało z faktu, że oskarżony „jako wykształcony informatyk posiada wiedzę specjalistyczną w zakresie funkcjonowania zabezpieczeń informatycznych, która nie jest dostępna dla przeciętnego użytkownika", pomimo że sam oskarżony zaprzeczył, jakoby „potrafił złamać hasła dostępu". W sprawie tej razi dowolność, jeśli nie frywolność, samodzielnie dokonanych przez sąd ustaleń faktycznych, zważywszy na to, że stwierdzenie sposobu przełamania lub ominięcia zabezpieczenia wymaga zazwyczaj powołania stosownego biegłego.

W postępowaniach karnych dotyczących przestępczości informatycznej często niezbędne okazuje się zasięgnięcie opinii biegłego (instytucji specjalistycznej lub naukowej) w celu stwierdzenia okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymagających wiadomości specjalnych (art. 193 § 1 k.p.k.). Dotyczy to takich kwestii, jak: mechanizmu działania przestępcy, możliwości uzyskania z zabezpieczonego urządzenia śladów pozwalających na spersonalizowanie hakera i indywidualizację

[95] Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 26 kwietnia 2017 r., XIV K 1204/12, LEX nr 2392142.

[96] Wyrok Sądu Rejonowego w Wałbrzychu z dnia 11 października 2017 r., II K 1036/16, LEX nr 2421166.

jego adresu IP wykorzystanego do ataku, odpowiedzi, gdzie przetransferowano cyfrowe mienie stanowiące przedmiot zamachu, czy w pamięci telefonu lub laptopa znajdują się ślady niezgodnej z prawem działalności, np. przełamania szczególnego zabezpieczenia informacji itd. Teoretycznie, zgodnie z najwyższymi standardami metodyki prowadzenia śledztwa, niemalże każda sprawa kwalifikowana z art. 267 k.k. – 269a k.k. wymaga sporządzenia opinii biegłego, ale niekiedy, z różnych względów, organ procesowy rezygnuje z jego powołania. Może to skutkować poważnymi błędami w gromadzeniu i ocenie materiału dowodowego, a więc traci się możliwość wnikliwego i szczegółowego ustalenia okoliczności faktycznych sprawy. Takie „niedociągnięcia" w procesie dowodzenia w skrajnych przypadkach prowadzą nawet do uniknięcia odpowiedzialności karnej przez osobę, która swoim zachowaniem, ocenionym *lege artis*, wypełniłaby znamiona czynu zabronionego. Częściej jednak oportunizm po stronie prokuratorów w powoływaniu biegłych i uzyskiwaniu sporządzonych przez nich opinii wynika z kwestii praktycznych, takich jak chociażby wysokie koszty, ponoszone przez Skarb Państwa, wynagrodzenia biegłych. W sytuacji zatem, gdy wina podejrzanego jest oczywista, przyznaje się on do popełnienia zarzucanego mu czynu, a badanie „zaatakowanego" przez hakera komputera stanowiłoby tylko „sztukę dla sztuki", pragmatycznym rozwiązaniem okazuje się rezygnacja z badania tego urządzenia przez wykwalifikowaną osobę. Podobnie jest, gdy od samego początku wiadomo, że ustalenie sprawcy ataku typu ransomware będzie niemożliwe, a badanie zainfekowanego malware'em sprzętu nie wniesie nic nowego do sprawy. Wydaje się wtedy postanowienia o umorzeniu śledztwa lub dochodzenia na podstawie art. 322 § 1 k.p.k. bez uzyskania opinii z dziedziny informatyki śledczej.

Powiedziano już, że ustalenie wykorzystanej przez sprawcę metody ataku, szczegółów jego przeprowadzenia oraz skutku popełnionego przestępstwa ma duże znaczenie w sprawie o haking. Pozwala to m.in. na wskazanie konkretnej czynności wykonawczej zrealizowanej przez sprawcę szczególnie wtedy, gdy przepis ustawy dopuszcza alternatywne znamiona czynności wykonawczej. W art. 267 § 1 k.k. można przełamać lub ominąć zabezpieczenie; w art. 268a § 1 k.k. działanie przestępcy polega na: niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych, a ponadto na ich zakłócaniu lub uniemożliwieniu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Wymienionego problemu, tj. dokładnego określenia znamion czynności czasownikowej, dotyczył wyrok Sądu Najwyższego z dnia 30 września 2015 r.[97] Sądy I oraz II instancji uznały skazanego za winnego tego, że trzykrotnie włamał się na skrzynkę mailową innej osoby, spreparował z poziomu tejże skrzynki wiadomości mailowej i wysłał je na swój adres. Opis jednego z czynów brzmiał następująco:

[97] Wyrok Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15, LEX nr 1866883.

w dniu 22 marca 2009 r. w W., będąc zatrudnionym w /…/ sp. z o.o. z siedzibą w W. na stanowisku kierownika ds. kluczowych klientów, dokonał włamania na konto internetowe M. L. /…/ poprzez pokonanie zabezpieczeń, a następnie w celu użycia za autentyczny podrobił dokument elektroniczny w postaci e-mail w ten sposób, że podrobił treść wiadomości e-mail M. L. /…/, następnie posłużył się tym dokumentem jako autentycznym i przesłał korzystając z prywatnego adresu IP na swoją pocztę /…/, tj. o czyn z art. 268a § 1 k.k.

Pomijając już, że sprawca swoim zachowaniem wypełnił także znamiona art. 267 § 1 k.k. („dokonał włamania"), to z opisu sprawy wynikało, co wskazał Sąd Najwyższy, że w przypadku charakterystycznej dla przestępstw teleinformatycznych mnogości alternatywnych znamion czynności wykonawczych, zadanie organu procesowego polega na wskazaniu, o które konkretne znamię chodzi w działaniu sprawcy. Wiązało się to z koniecznością wykorzystania wiadomości specjalnych do ustaleń faktycznych, tj. uzyskania opinii biegłego z zakresu informatyki śledczej lub innej dziedziny wiedzy dotyczącej nowych technologii, a czynności takich – zdaniem sądu – zabrakło w rozpatrywanej prawie. Nie ustalono zatem, na podstawie wiedzy specjalnej dotyczącej szczegółów techniczno-informatycznych, jak doszło do zarzucanego skazanemu przełamania zabezpieczeń i wysyłania wiadomości przez nieuprawnioną osobę. Jako dalece uproszczony należało uznać wniosek sądu I instancji, płynący z ustalenia, że zakwestionowane maile wysłano z komputerów o różnych adresach IP, skoro jest wiedzą powszechną, że wiadomości takie można wysłać z każdego miejsca na Ziemi posiadającego dostęp do Internetu i aplikacji pocztowej. W żadnej mierze nie przesądzono o tym, że musiała je wysłać inna osoba niż skazany. Pozwoliło to jedynie na uznanie, że wysłano je z komputerów podłączonych do różnych sieci. Do porządku dziennego, wskazywał dalej Sąd Najwyższy, sądy przeszły także nad kluczową kwestią – przełamaniem zabezpieczeń poczty elektronicznej pokrzywdzonego. Przełamanie takiego zabezpieczenia jest trudne, a w przypadkach zaawansowanych zabezpieczeń wręcz niemożliwe. Tymczasem w materiale dowodowym zgromadzonym przez sądy I i II instancji zabrakło jakichkolwiek analiz (zwłaszcza z udziałem biegłego) na temat stosowanych przez pokrzywdzonego zabezpieczeń skrzynki pocztowej, kręgu osób mających do niej dostęp (znających hasło lub weryfikowanych jako uprawnione w inny sposób). Nie poczyniono także jakichkolwiek ustaleń, by skazany znał hasło do komputera lub aplikacji pocztowej oskarżyciela posiłkowego. Brak powyższych ustaleń, zdaniem Sądu Najwyższego, dyskwalifikował rozumowanie sądów niższych instancji jako spekulatywne, a więc dowolne, co stanowiło rażące naruszenie normy art. 7 k.p.k.

Skutkiem tego, z powodu kasacji wywiedzionej przez obrońcę, było uchylenie sprawy i przekazanie jej do ponownego rozpoznania. Następnie Sąd Apelacyjny w Warszawie

w dniu 21 grudnia 2015 r. uchylił zaskarżony wyrok w zakresie rozstrzygnięcia czynów kwalifikowanych z art. 268a § 1 k.k. aktu oskarżenia i w tej części przekazał sprawę Sądowi Okręgowemu w Warszawie do ponownego rozpoznania, twierdząc, że konieczne było zasięgnięcie uzupełniającej opinii biegłego z zakresu informatyki. Poprzedzone winno to zostać uzyskaniem od M. L. wiedzy na temat zabezpieczeń stosowanych przez niego w używanym koncie pocztowym, do którego uzyskano nieautoryzowany dostęp. Biegły winien dokonać oceny siły i skuteczności takich zabezpieczeń oraz tego, jak szeroką i dogłębną wiedzą, a także jakimi środkami technicznymi należałoby dysponować, aby „włamać się" na konto[98]. Z perspektywy opisanej sprawy należy zapytać: Jaką wartość dowodową ma badanie sprzętu komputerowego, który stał się przedmiotem hakingu, kilka lat po popełnienia przestępstwa? Jest to bezcelowe, jeśli w tym czasie komputer zwrócono jego użytkownikowi i M. L. mógł wykonywać na nim różne operacje.

Sprawy z zakresu przestępczości teleinformatycznej są źródłem jaskrawych przykładów, jak ważną rolę źródeł dowodowych pełnią w nich zabezpieczone nośniki danych. Przykładu na to dostarcza lektura akt sprawy prowadzonej przez Prokuraturę Rejonową dla Wrocławia-Stare Miasto we Wrocławiu, zakończonej wydaniem postanowienia o umorzeniu śledztwa na podstawie art. 322 § 1 k.p.k.:

> w sprawie włamania w dniu 25 września 2018 roku w nieustalony miejscu, do systemu spółki /…/ poprzez uzyskanie nieuprawnionego dostępu do infrastruktury informatycznej i utworzenie zlecenia wypłat kryptowalut należących do firm /…/ w ilości 36.000 jednostek waluty LISK, co stanowi kwotę ok. 300.000 zł, waluty Fururcoin w ilości 80.000 jednostek, co stanowi kwotę ok. 2.400.000 zł oraz waluty Bitcoin w ilości 108 jednostek, co stanowi kwotę ok. 2.265.000 zł działając na szkodę w/w tj. o czyn z art. 279 § 1 k.k. w zw. z art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[99]

W uzasadnieniu postanowienia napisano, że „w tego typu sprawach niezbędne jest pilne zabezpieczenie urządzeń i dokonanie ich ekspertyzy, natomiast zawiadomienie o podejrzeniu popełnienia przestępstwa wpłynęło ze strony zgłaszającego z dużym opóźnieniem", co, zdaniem referenta sprawy, czyniło zbędnym zabezpieczenie i badanie „zaatakowanego" nośnika danych informatycznych. Napisał on:

> Nadto ustalono, że zlecenie ekspertyzy sprzętu należącego do pokrzywdzonych po upływie 6 miesięcy od zdarzenia jest bezzasadne, albowiem dane, które sprawca może po sobie pozostawić, są danymi ulotnymi lub o niskiej trwałości i ich odzyskanie jest z reguły niemożliwe ze względu na technologię i techniki zacierania śladów.

[98] Wyrok Sądu Apelacyjnego w Warszawie z dnia 21 grudnia 2015 r., II AKa 409/15, LEX nr 2031083.
[99] Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 818.2019.

> Analizując materiał dowody zgromadzony w sprawie stwierdzić należy, iż w sprawie nie zdołano ustalić sprawcy przestępstwa, a wszelkie możliwości dowodowe zostały wyczerpane.

Inaczej, bo prawidłowo, procedowano w sprawie Sądu Rejonowego dla Krakowa-Podgórza w Krakowie, gdzie prokurator już na etapie postępowania przygotowawczego powołał biegłego z zakresu informatyki śledczej i wyjaśnił okoliczności, których stwierdzenie wymagało wiadomości specjalnych. W śledztwie ustalono, że sprawca przestępstwa po rozwiązaniu umowy o pracę nadal posiadał aktualny login i hasło dostępu do kilku serwerów spółki znajdujących się w Wielkiej Brytanii i bez uprawnienia zapoznawał się z informacjami przeznaczonymi dla ścisłego kierownictwa przedsiębiorstwa, dotyczącymi m.in. kontraktów negocjowanych z przyszłymi klientami spółki, obowiązujących umów biznesowych, wysokości wynagrodzeń pracowników, strategii firmy oraz jej planów inwestycyjnych.

Podstawę działań w śledztwie stanowił dołączony do złożonego przez spółkę zawiadomienia o podejrzeniu popełnienia przestępstwa tzw. raport powłamaniowy[100]. W formie śladów cyfrowych udokumentowano w nim pozostawione przez „atakującego" logi systemowe, pozwalające zrekonstruować jego akces do serwera i manipulowanie zapisanymi tam informacjami. Sprawcę udało się ustalić, wiążąc fakt zwolnienia jednego z informatyków spółki w okresie, gdy zaczęły się nieuprawnione logowania do systemu. Podejrzany przyznał się do popełnienia zarzucanego mu czynu i wyjaśnił, że inwigilując serwer, chciał sprawdzić, czy były pracodawca podjął wobec niego niekorzystne czynności faktyczne lub prawne. Wyrok skazujący brzmiał:

> w okresie od dnia 8 września 2012 r. do dnia 20 lipca 2013r. w Krakowie, działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru, po uprzednim pozyskaniu haseł komputerowych umożliwiających dostęp do informacji przechowywanych na serwerach /…/ LTD z siedzibą w Londynie, a także dodając nieautoryzowany klucz dostępu i omijając w ten sposób ich zabezpieczenie, uzyskał bezprawnie dostęp do systemu informatycznego w/wym. Spółki, a tym samym do informacji dla niego nieprzeznaczonych, tj. o przestępstwo z art. 267 § 1 k.k., art. 267 § 2 k.k. i art. 269b § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[101]

[100] W perspektywie prowadzenia śledztwa korzystna jest sytuacja, kiedy administrator „zaatakowanego" systemu doręczy prokuratorowi wraz z zawiadomieniem o podejrzeniu popełnienia przestępstwa tzw. raport powłamaniowy zawierający opis incydentu z załączonymi śladami cyfrowymi mającymi znaczenie dla ustalenia stanu faktycznego sprawy. Podstawą reagowania na incydent jest bowiem prawidłowe zabezpieczenie materiału dowodowego, na podstawie którego następnie wykonuje się analizę incydentu przez administratora systemu lub sieci. Jeśli doszło do hakerskiego włamania, najistotniejszy jest czas oraz prawidłowe zabezpieczenie materiału dowodowego, nie tylko dla celów sądowych ale również, aby odpowiedzieć na pytanie, jak doszło do włamania oraz jakie operacje zostały wykonane przez przestępcę.

[101] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie Wydział II Karny o sygn. II K 875/16/P.

Powracając do wykonanych w śledztwie czynności procesowych, to niedługo po złożeniu zawiadomienia o podejrzeniu popełnienia przestępstwa prokurator, działając na podstawie art. 219 §1 k.p.k., postanowił

> zarządzić przeszukanie pomieszczeń mieszczących się pod adresem /…/ w celu zabezpieczenia centralnej jednostki komputera, nośników danych, wszelkiej dokumentacji związanej z działalnością prowadzoną pod wskazanym adresem, a mogącej wskazywać na wykorzystanie danych bezprawnie uzyskanych ze spółki /…/ oraz ewentualnie innych przedmiotów mogących stanowić dowód w sprawie.

Realizacja czynności została powierzona właściwej jednostce policji. Zachodziło bowiem prawdopodobieństwo, że osoba podejrzewana „wykradła" istotne informacje o spółce w celu wykorzystania ich w działalności konkurencyjnej. W trakcie przeszukania lokali zabezpieczono: 4 dyski twarde komputera, 3 karty pamięci SD, 2 notebooki oraz iPad; urządzenia następnie przekazano do badań biegłemu z zakresu informatyki śledczej w celu stwierdzenia:

1. czy na zabezpieczonych nośnikach (urządzeniach przekazanych do badań – zabezpieczonych w toku przeszukania) znajdują się pliki tożsame z plikami zabezpieczonymi na kopii dysków serwerów pokrzywdzonej spółki tj. /…/
2. czy w wyniku badania nośników (urządzeniach przekazanych do badań – zabezpieczonych w toku przeszukania) można stwierdzić, że następowały połączenia z serwerami spółki /…/
3. czy na nośniki (urządzeniach przekazanych do badań – zabezpieczonych w toku przeszukania) pobrano pliki oraz pocztę elektroniczną należącą do spółki /…/

Wnioski sformułowane przez biegłego, na podstawie przeprowadzonej ekspertyzy, brzmiały następująco:

1. W trakcie analizy materiału dowodowego w postaci dysków twardych i kart pamięci stwierdzono, iż na dyskach dow. 4, 5, 6, 7, 9.1, 10.1 zapisane są pliki tożsame z plikami zabezpieczonych na kopii dysków serwerów spółki /…/, dostarczonej w postaci dysku oznaczonego jako dow. 11.
2. Analizując systemy operacyjne i oprogramowanie służące do łączenia się oraz przeglądania zasobów w sieci Internet stwierdzono, że z wykorzystaniem programu ssh oraz przeglądarek internetowych nawiązywano połączenia ze stronami i serwerami związanymi ze spółką /…/.
3. Zebrane w trakcie badań informacje nie pozwoliły stwierdzić, czy pobierano pliki z serwerów spółki /…/. Stwierdzono natomiast, że z wykorzystaniem przeglądarki internetowej Google Chrome łączono się z serwerem wyżej wymienionej spółki, tj. /…/.com po dacie 8 września 2012 roku.

Dzięki opinii sporządzonej przez biegłego ustalono, że w pamięci komputera użytkowanego przez podejrzanego znajdowały się ślady świadczące, że urządzenie łączyło się zdalnie z serwerem spółki, pamięć dowodowego komputera zawierała takie same dane, jakie znajdowały się na serwerze, ale biegły nie był wstanie ustalić, czy pobierano na badany komputer pliki z serwerów pokrzywdzonego przestępstwem podmiotu.

3.3. Różnica pomiędzy art. 267 § 1 k.k. a art. 267 § 2 k.k.

Gdy przystępuje się do charakterystyki art. 267 § 2 k.k., na samym wstępie nasuwa się uwaga, że w praktyce stosowania prawa przez sędziów i prokuratorów występuje duża rozbieżność pomiędzy wykładnią znamion tego przepisu na gruncie podobnych okoliczności faktycznych. Analiza orzeczeń sądowych pokazuje, że nieuprawniony dostęp do informacji w postaci rozmów, zdjęć czy filmów umieszczonych na zamkniętym forum w Internecie (koncie) kwalifikowany jest przez organy procesowe w różny sposób, tj. z art. 267 § 1 k.k. lub art. 267 § 2 k.k. albo z art. 267 § 1 i 2 k.k. Jeśli chodzi o pierwszą możliwość, to w jednej ze spraw mężczyzna został oskarżony o to, że:

> w okresie od 28 maja 2010 r. do września 2011 r. w nieustalonym miejscu na terenie Rzeczypospolitej Polskiej wykorzystując posiadany login i hasło bez zgody A. A. uzyskał dostęp do konta pokrzywdzonego /…/ na platformie U., tj. o przestępstwo z art. 267 § 2 k.k.[102]

Oskarżony został uniewinniony od popełnienia zarzucanego mu czynu, ale nie ma to znaczenia w aspekcie problemu badawczego. Istotne jest natomiast to, że Sąd Rejonowy w Nowym Sączu[103], a potem Sąd Okręgowy Nowym Sączu[104] uznał, że dostęp do „konta pokrzywdzonego /…/ na platformie U.", gdzie znajdowała się m.in. korespondencja i informacje handlowe, typizowany jest w art. 267 § 2 k.k., a w opisie czynu zabrakło znamienia „uzyskania bez uprawnień dostępu do części systemu informatycznego". W akcie oskarżenia posłużono się jedynie sformułowaniem akcesu „do konta pokrzywdzonego na platformie U.".

Podobne stanowisko zajął Sąd Rejonowy dla Wrocławia-Śródmieścia we Wrocławiu[105], gdzie dwóch sprawców zostało oskarżonych o to, że posługując się łączem internetowym bez uprawnienia uzyskało dostęp do konta o nazwie /…/ w systemie informatycznym firmy /…/. Konto zawierało informacje o rodzaju produktów, którymi handlowała spółka, stanach magazynowych, cenach detalicznych i hurtowych jej

[102] Wyrok Sądu Okręgowego w Nowym Sączu z dnia 17 czerwca 2014 r., II Ka 188/14, LEX nr 1859693.
[103] Wyrok Sądu Rejonowego w Nowym Sączu z dnia 28 stycznia 2014 r., II K 322/13, LEX nr 1859693.
[104] Wyrok Sądu Okręgowego w Nowym Sączu z dnia 17 czerwca 2014 r., II Ka 188/14, LEX nr 1859693.
[105] Wyrok Sądu Rejonowego dla Wrocławia-Śródmieścia we Wrocławiu z dnia 14 sierpnia 2013 r., II K 87/12, LEX nr 1903395.

produktów. Dzięki temu przestępcy mogli na bieżąco analizować poziom sprzedaży, dostawy, zestawienie wyników rocznych firmy w rozbiciu na miesiące, wartości zamówień itp. Sąd ustalił, że jeden z mężczyzn znał lub zapamiętał login oraz hasło i zalogował się do systemu informatycznego spółki, nie będąc już jej pracownikiem, co miało charakter nielegalny, a zatem naruszający prawo innego podmiotu do dysponowania informacją. Sąd stwierdził: „Nie ma w tej sprawie wątpliwości, że system G. był systemem informatycznym" zgodnie z art. 1 pkt a konwencji Rady Europy z 2001 r. o cyberprzestępczości. Wyrok ten został utrzymany w mocy przez Sąd Okręgowy we Wrocławiu[106], który stwierdził, że naruszeniem prawa będzie zarówno „wejście" do sieci informatycznej przez sprawcę, który uzyskał odpowiednie, niezbędne dane drogą ataku, jak też korzystanie z zastrzeżonych źródeł informatycznych przez osobę, która, nie łamiąc prawa, poznała login i hasło, ale nie miała uprawnienia do wykorzystania tych danych i zalogowania się na konto.

Druga grupa spraw dotyczy sytuacji, kiedy sądy podobne czyny, jak wcześniej opisane, kwalifikowały z art. 267 § 1 k.k. Uczynił tak Sąd Rejonowy w Giżycku, uznając oskarżonego za winnego tego, że:

> w bliżej nieustalonym czasie w okresie od 11 listopada 2009 r. do dnia 16 sierpnia 2012 r. w miejscowości R. gmina M. w krótkich odstępach czasu w wykonaniu z góry powziętym zamiarem, bez uprawnienia uzyskał dostęp do informacji dla niego nie przeznaczonej w postaci prywatnej korespondencji A. A. znajdującej się na jej internetowej skrzynce pocztowej /…/, przełamując jej informatyczne zabezpieczenie w postaci hasła przeglądając ww. skrzynkę pocztową, ujawniając uzyskane w ten sposób informacje poprzez przesłanie ich na konta internetowe: /…/ tj. o czyn z art. 267 § 1 k.k. w zb. z art. 267 § 4 k.k. w zw. z art. 12 k.k.[107]

Ustalono, że sprawca, korzystając z oprogramowania szpiegowskiego, rozszyfrował hasło do skrzynki mailowej swojej żony i przełamując zabezpieczenie, uzyskał dostęp do zapisanych w niej informacji. Następnie skopiował korespondencję (m.in. wiadomości przesyłane między kobietą i jej partnerem) oraz pliki z dokumentami (m.in. pisma z prokuratury adresowane do pokrzywdzonej) i rozesłał część z nich do osób trzecich. Identycznej kwalifikacji prawnej czynu, w podobnych okolicznościach faktycznych sprawy, dokonał Sąd Rejonowy dla Krakowa-Podgórza w Krakowie, skazując sprawcę przestępstwa za to, że:

> w dniu 1 stycznia 2022 roku w Krakowie działając w celu uzyskania bez uprawnienia dostępu do informacji dla niego nieprzeznaczonej w postaci treści rozmów

[106] Wyrok Sądu Okręgowego we Wrocławiu z dnia 5 lutego 2014 r., IV Ka 1233/13, LEX nr 1882446.
[107] Wyrok Sądu Rejonowego w Giżycku z dnia 3 sierpnia 2015 r., II K 84/14, LEX nr 2070430.

prowadzonych przez J. K. na wewnętrznym komunikatorze internetowym o nazwie /…/ poprzez przełamanie informatycznego zabezpieczenia konta pokrzywdzonej hasłem dostępu, wszedł w posiadanie tego hasła i usiłował za jego pomocą zalogować się do czatu, co jednak nie nastąpiło z uwagi na interwencję J. K. i zamknięcie przez pokrzywdzoną matrycy laptopa, tj. o przest. z art. 13 § 1 k.k. w zw. z art. 267 § 1 k.k.[108]

W trzecim rozwiązaniu przyjmuje się kwalifikację prawną czynu łącznie z art. 267 § 1 i 2 k.k.; Sąd Rejonowy w Dzierżoniowie uznał oskarżoną za winną tego, że:

uzyskała bez uprawnienia w okresie luty – marzec 2012 r. w D. będąc zatrudnioną w firmie /…/ Sp. z o.o.z/s przy ul. /…/ dostęp do informacji dla niej nieprzeznaczonej w postaci wyroku wydanego w dniu 20 grudnia 2010 r. przez Sąd Rejonowy w D. w sprawie /…/, poprzez przełamanie albo ominięcie informatycznego zabezpieczenia oraz uzyskanie dostępu do całości lub części systemu informatycznego w ww. firmie, to jest o czyn z art. 267 § 1 i 2 k.k.[109]

W uzasadnieniu do wyroku sąd napisał, że:

> normy prawne wynikające z art. 267 § 1 i 2 k.k. pozwalają pociągnąć sprawcę do odpowiedzialności karnej dopiero wówczas, gdy na skutek przełamania zabezpieczeń uzyska on zastrzeżoną dla niego informację przechowywaną w systemie. Uzyskanie nieuprawnionego dostępu do systemu komputerowego jest wedle tego przepisu wyłącznie środkiem prowadzącym do celu, a nie samoistnym przestępstwem. Nie chroni też ów przepis informacji znajdujących się na serwerze pracodawcy (m.in. informacje prywatne) i pozostawia poza penalizacją działanie związane z poufnością danych i systemów komputerowych, które nie polegają na przełamywaniu zabezpieczeń. Jak skarżący sam wskazał w swoim zawiadomieniu o popełnieniu przestępstwa, nie są dla niego jasne okoliczności w jakich M. S. weszła w posiadanie ww. wyroku, w związku z czym w tym zakresie zasadnym jest uwzględnienie jej twierdzeń opisujących okoliczności pozyskania przez nią ww. informacji[110].

W tym miejscu należy zasygnalizować, że wywody sądu są *contra legem*, bowiem przestępstwo hakingu polega na uzyskaniu dostępu do informacji lub systemu informatycznego bez konieczności uzyskania tejże informacji/tych danych. Przywołane przez sąd przepisy chronią także zawartość serwerów, a o tym, czy nieuprawnione uzyskanie dostępu do serwera będzie kwalifikowane z § 1 lub § 2 art. 267 k.k., decyduje to, do

[108] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie, II K 130/22/P.
[109] Postanowienie Sądu Rejonowego w Dzierżoniowie z dnia 16 kwietnia 2014 r., II Kp 44/14, LEX nr 1906875.
[110] Tamże.

czego uzyskano akces: do informacji czy danych informatycznych. Podobną kwalifikację prawną z realnym zbiegiem przestępstw przyjął Sąd Rejonowy w Wałbrzychu:

> w dniu 20 stycznia 2015 r. w W. /…/ korzystając z /…/ po uprzednim przełamaniu zabezpieczeń informatycznych w postaci loginu i hasła uzyskała dostęp do informacji dla niej nie przeznaczonej dokonując w imieniu Biura /…/ rezerwacji turystycznej o nr /…/ oraz uzyskując tym samym dostęp do systemu informatycznego Biura /…/, czym działał na szkodę Biura /…/, to jest o czyn z art. 267 § 1 i 2 k.k.[111]

Odkodowując znaczenie znamion opisanych w art. 267 § 1 k.k. oraz art. 267 § 2 k.k., należy przyjąć na wstępie ogólną zasadę, że w kategoriach błędu ustawodawcy rozpatrywać należałoby przypadek, gdyby dwa typy czynów zabronionych miały identyczny zakres normatywny. Jest przeciwnie: skoro prawodawca decyduje się na wprowadzenie do systemu odrębnych typów przestępstw, to domniemywać należy, że regulują one różne zachowania (dotyczy to także typów zmodyfikowanych, które do opisu typu podstawowego dodają kolejne znamiona bądź te znamiona doprecyzowują)[112]. Czy zatem ustawodawca wprowadził faktycznie odrębne typy czynów zabronionych? A może popełnił błąd legislacyjny i art. 267 § 1 k.k. oraz art. 267 § 2 k.k. mają identyczny zakres normowania? A może jest tak, że dane informatyczne tworzą informacje, a informacje przechowywane są w postaci danych informatycznych i na gruncie art. 267 k.k. § 1 i 2 ma się de facto do czynienia z identycznym przedmiotem czynności wykonawczej?

Przyjąć należy, że logując się do całości lub części systemu informatycznego, o którym mowa w art. 267 § 2 k.k., otrzymuje się akces do danych informatycznych. Wynika to z definicji tego systemu, który „wykonuje automatyczne przetwarzanie danych" (art. 1 pkt a. konwencji budapesztańskiej). Ale uprawniony jest także pogląd, że logując się do systemu, uzyskuje się równocześnie dostęp do informacji, bo dane informatyczne można przetworzyć na sensowne treści w postaci zdjęć, tekstów czy filmów. Jednak zdecydowanej większości sprawców przestępstwa hakingu nie zależy na uzyskaniu dostępu do „surowych" artefaktów cyfrowych, które nic dla „przeciętnego" człowieka nie znaczą, ale do treści będących wynikiem przetworzenia tych artefaktów na informacje. Rzadko bowiem osoby skazywane na podstawie art. 267 k.k. posiadają wiedzę informatyczną, która pozwalałaby im zrobić użytek z dostępu do samych danych. Jak zatem praktycznie rozgraniczyć występek z § 2 od tego, stypizowanego w § 1 art. 267 k.k.?

Zdaniem W. Wróbla i D. Zająca, zachowanie opisane w art. 267 § 2 k.k. może realizować znamiona przestępstwa, „o ile informacja, do której uzyskuje się dostęp, ma postać danych informatycznych (komputerowych), co do których sprawca nie jest

[111] Wyrok Sądu Rejonowego w Wałbrzychu z dnia 23 września 2016 r., III K 865/15, LEX nr 2146034.
[112] Zob. Wyrok Sądu Najwyższego z dnia 4 października 2017 r., II KK 162/17, LEX nr 2397594.

uprawniony”[113]. Należy zgodzić się z przywołanym stanowiskiem, zastrzegając, że przedmiotem oddziaływania na gruncie przepisów z art. 267–269a k.k. jest albo „informacja”, albo są „dane informatyczne”; *a contrario*, w procesie wykładni znamion czynów zabronionych stypizowanych w rozdziale XXXIII k.k. trzeba ściśle respektować ten dychotomiczny podział. Nie zmienia tego fakt, że pod względem technicznym „informacja” przybiera formę zarówno danych informatycznych zapisanych w pamięci komputera, jeśli analizuje się jej kod źródłowy, jak i „zwykłej” informacji, gdy na monitorze komputera wyświetla się komunikat. Znamiona czynów zabronionych opisanych w art. 267 k.k. § 1 lub § 2 stanowią jednak dwa odrębne typy przestępstw, polegające na uzyskaniu nieuprawnionego dostępu do „informacji” (§ 1) lub do „całości lub części systemu informatycznego” (§ 2), a sprawca, działający w zamiarze bezpośrednim, obejmuje swoją świadomością do jakiej postaci „materii” chce taki dostęp uzyskać. Pojęcie „dostępu”, to nie tylko stworzenie sobie możliwości zapoznania się z informacją lub danymi informatycznymi, ale także przejęcie we władanie nośnika, na którym się znajdują, oraz ich skopiowanie[114]. W języku polskim czasownik „uzyskać” oznacza „otrzymać coś, co było przedmiotem starań”, a „dostęp” to „możność dostania się do jakiegoś miejsca”, „możność przyjścia do kogoś, zetknięcia się z kimś, korzystania z czegoś”[115]. Zatem „uzyskać dostęp” to sytuacja, kiedy sprawca dzięki poczynionym staraniom ma faktyczną możność pozyskania wiedzy (§ 1) lub zalogowania się do całości lub części systemu informatycznego (§ 2). Dostęp taki uzyskuje „bez uprawnienia”, a więc bez „prawa do czegoś przysługującego lub nadanego komuś innemu”[116].

Przepis art. 267 § 2 k.k., funkcjonujący w obecnym brzmieniu, został wprowadzony do Kodeksu karnego ustawą z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw i pomimo upływu 15 lat od nowelizacji ustawy, nadal sprawia on wiele problemów w procesie „odkodowywania” znamion. Gdyby oprzeć się tylko na wykładni językowej, to penalizowałby uzyskanie nieuprawnionego dostępu do „tego wszystkiego”, co znajduje się w komputerze, niezależnie, w jakiej formie byłoby reprezentowane. Jednak dużo w temacie jego wykładni wyjaśnia treść uzasadnienia do projektu ustawy wprowadzającej art. 267 § 2 k.k.; napisano w nim, że projektowany przepis

> penalizuje czyn skutkujący uzyskaniem, bez uprawnienia, dostępu do systemu informatycznego lub jego części, nawet bez złamania jakiegokolwiek zabezpieczenia zainstalowanego w komputerze użytkownika lub zabezpieczenia systemowego. Czyn taki może polegać np. na wprowadzeniu do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe.

[113] W. Wróbel, D. Zając, *Art. 267…*, *teza 15*.
[114] Tamże, *teza 6*.
[115] Słownik języka polskiego PWN, https://sjp.pwn.pl/slowniki/ [dostęp: 10.08.2022].
[116] Tamże.

> Sprawca w takim przypadku nie działa w celu uzyskania informacji znajdującej się w zasobach przejętego systemu lub dostępu do niej, lecz w celu przejęcia kontroli nad systemem jako narzędziem do bezprawnego wykorzystywania. Przewidując omawiany nowy typ przestępstwa, projekt usuwa i niweluje istotną lukę w obowiązującym prawie, gdyż tego rodzaju szkodliwe działania pozostają obecnie poza zakresem penalizacji[117].

Potwierdza się zatem, że na gruncie art. 267 § 2 k.k. ustawodawca chce karać bezprawne uzyskanie dostępu do danych, a nie informacji, oraz bez znaczenia dla bytu tego przestępstwa jest to, co konkretnie utożsamiają przetwarzane przez ten system dane informatyczne (może to być natomiast istotna okoliczność w aspekcie dyrektyw wymiaru kary). Podobnie twierdzi P. Siemkowicz, wskazując, że komplementarność przepisu art. 267 § 2 k.k. w odniesieniu do § 1 art. 267 k.k. ogranicza praktycznie zakres jego stosowania do takich sytuacji, gdy uzyskanie nieuprawnionego dostępu do systemu komputerowego nie wiąże się równocześnie z uzyskaniem dostępu do zawartych w tym systemie informacji[118]. Podobnie uważa F. Radoniewicz: „Wydaje się w związku z tym, że najbardziej racjonalnym rozwiązaniem jest przyjęcie, iż przepis art. 267 § 2 k.k. będzie znajdował zastosowanie w przypadkach, gdy głównym elementem czynu sprawcy było samo uzyskanie dostępu do całości lub części systemu informatycznego, a nie uzyskanie dostępu do informacji"[119]. Z przytoczonymi poglądami współgra stanowisko N. Kłączyńskiej, która słusznie podnosi, iż „Wprowadzenie art. 267 § 2 k.k. uzupełniło w dużym zakresie lukę obejmującą wszystkie te działania, w których hackerzy nie działają w celu uzyskania konkretnej informacji, lecz ze zgoła innych pobudek (np. wykazanie braku skutecznych zabezpieczeń w systemie informatycznym, pozostawienie śladu swojej bytności, sprawdzenie własnych umiejętności informatycznych)"[120]. W sprawie prowadzonej przed Sądem Rejonowym w Kaliszu celem działania sprawcy było uzyskanie dostępu do systemu zakładu opieki zdrowotnej po to, aby przetransferować znajdujące się w systemie dane. Wyrokiem Sądu Rejonowego w Kaliszu W. B. został uznany za winnego tego, że:

> w dniu 12 kwietnia 2018 r., w K., pozostając zatrudniony w firmie /…/ z/s w K. na stanowisku lekarz stomatolog, nie posiadając uprawnień, nadużywając udzielonego mu zaufania, uzyskał dostęp do całości systemu informatycznego firmy w sposób nieuprawniony na serwerze firmowym uruchomił program /…/ zdalnie udostępnił

[117] Uzasadnienie projektu ustawy wprowadzającej karalność za przest. z art. 267 § 2 k.k., druk sejmowy nr 458 Sejmu VI kadencji, LEX.
[118] P. Siemkowicz, *Przestępstwa skierowane przeciwko poufności…*, s. 4.
[119] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu,* s. 310.
[120] N. Kłączyńska, *Art. 267*, *teza 11*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, LEX 2014.

> całość systemu informatycznego oraz bazę klientów firmy /…/ przekazując dane na inny zewnętrzny komputer, jednocześnie uzyskując dostęp do danych zastrzeżonych wyłącznie dla właściciela części systemu informatycznego, czym działał na szkodę firmy /…/ tj. o czyn z art. 267 § 2 k.k.[121]

Kwalifikacja prawna czynu z art. 267 § 2 k.k. znalazła także zastosowanie do sprawcy, który wielokrotnie, na szkodę różnych podmiotów, uzyskiwał lub usiłował uzyskać dostęp do ich systemu informatycznego i wysyłał na serwery pokrzywdzonych firm wiadomości mailowe imitujące pochodzenie od podmiotów, pod które się podszywał (m.in. GIODO lub operator komórkowy P4) wraz załącznikiem zawierającym złośliwe oprogramowanie po to, aby wykorzystać infrastrukturę firm w celu rozsyłania malware'a do kolejnych osób; T. T. został oskarżony o to, że:

> w nieustalonym okresie jednak nie później niż do dnia 23 czerwca 2017 r. w nieustalonym miejscu a ujawnionego w Krakowie bez uprawnienia uzyskał dostęp do części systemu informatycznego podmiotu /…/.pl prowadzonego przez /…/ w postaci konta poczty elektronicznej biuro@/.../.pl znajdującego się na serwerach podmiotu nazwa.pl, poprzez przełamanie lub ominięcie informatycznych zabezpieczeń i wysłanie 15 593 maili imitujących pochodzenie od Generalnego Inspektora Ochrony Danych Osobowych wraz załącznikiem o treści Powiadomienie o planowanej kontroli GIODO.vbs z zawartością złośliwego oprogramowania ransomware w postaci wirusa określanego jako Polski Ransomware, Vortex lub Flotera szyfrującego dane działając tym na szkodę /…/ – tj. o czyn z art. 267 § 2 k.k.[122]

Nieprawidłowa natomiast jest kumulatywna kwalifikacja prawna przestępstw z § 1 i § 2 art. 267 k.k. w taki sposób, jak zrobił to prokurator w sprawie zawisłej przed Sądem Rejonowym dla Krakowa-Podgórza w Krakowie. Sprawca został oskarżony o to, że:

> działając w krótkich odstępach czasu w ramach z góry powziętego zamiaru po uprzednim pozyskaniu w nieustalonym dniu, nie później niż 25 października 2012 r. w Krakowie hasła dostępu do internetowego konta bankowego K. B. uzyskała po jego wykorzystaniu w dniu 25 października 2012 r. bez uprawnienia dostęp do wyżej wymienionego konta bankowego, zawierającego informacje dla niej nie

[121] Wyrok Sądu Rejonowego w Kaliszu z dnia 15 marca 2022 r., II K 882/19, LEX nr 3500689.
[122] Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.

> przeznaczone, tj. o przest. z art. 269b § 1 k.k. i art. 267 § 1 i 2 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[123]

W niniejszej sprawie oskarżona uzyskała dostęp do „konta bankowego, zawierającego informacje", a więc działała w ramach znamion z art. 267 k.k. § 1, a nie § 2; chodzi bowiem o dwa różne typy przestępstw, które zasadniczo się wykluczają. Jedynie w sytuacji, gdyby sprawca w ramach tego samego czynu uzyskał nieuprawniony dostęp do nietożsamych repozytoriów: jednego, zawierającego informacje, i drugiego, stanowiącego całość lub część systemu informatycznego, można by przyjąć realny zbieg przestępstw. Skoro jednak w niniejszej sprawie ustalono, że przestępca uzyskał akces do informacji, a nie danych informatycznych, to w stanie prawnym obowiązującym w dacie orzekania przyjąć należało, iż wypełnił znamiona art. 267 § 1 k.k. (błędnie natomiast przypisano oskarżonej popełnienie przestępstwa z art. 269b § 1 k.k., o czym będzie mowa w dalszej części monografii). Data czynu to rok 2012, według obecnie obowiązujących przepisów taki sposób działania sprawcy wypełniłby znamiona przestępstwa kradzieży z włamaniem (art. 279 § 1 k.k.). Podobnie w wyroku Sądu Rejonowego dla Krakowa-Podgórza w Krakowie z dnia 20 kwietnia 2016 r. należało skazać podsądnego z art. 267 § 1 k.k., a nie § 2:

> w dniu 25 października 2012 r. w Krakowie, wykorzystując bez zgody pokrzywdzonej K. B. hasło i login, uzyskała bez uprawnienia dostęp do jej panelu klienta systemu bankowości internetowej /…/ Bank S.A. w część służącej do obsługi rachunku bankowego nr /…/ co stanowi występek z art. 267 § 2 k.k.[124]

Z poczynionych przez sąd ustaleń wynikało, że czyn oskarżonej powinien zostać zakwalifikowany z § 1 analizowanego artykułu, gdyż uzyskała ona dostęp do informacji, a nie danych informatycznych. Sąd wskazał, że „panel klienta systemu bankowości internetowej /…/ Bank S.A., służący do obsługi rachunku bankowego nr /…/ stanowi część systemu informatycznego, zawierającego szereg istotnych informacji o rachunku bankowym nr /…/, takie jak dane posiadacza, saldo czy szczegółowa historia operacji"[125]. Dla kwalifikacji czynu nie miało znaczenia, że panel klienta „stanowi część systemu informatycznego", gdyż oskarżony nie chciał poznać danych cyfrowych, ale informacje wyświetlane na monitorze komputera po otwarciu aplikacji bankowej, wygenerowane przez algorytm komputerowy po przetworzeniu wspomnianych danych.

[123] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.
[124] Tamże.
[125] Tamże.

Uzasadnienie do wyroku jest istotne pod kątem rozumienia przez sąd wykładni znamion art. 267 § 2 k.k. dotyczących sposobu uzyskania przez sprawcę dostępu do informacji. Sąd wskazał, że oskarżona znała login i hasło do bankowości internetowej pokrzywdzonej, gdyż K. B. sama jej udostępniła ww. dane w ramach prowadzonej współpracy. Nawet po tym, jak obie kobiety założyły odrębne firmy, nie przestały współpracować, a login oraz hasło do nowego rachunku bankowego K. B. pozostały niezmienione. Pokrzywdzona nie wyraziła natomiast zgody, aby oskarżona dalej z nich korzystała. Finalnie pomiędzy kobietami doszło do kłótni na tle finansowym, a 25 października 2012 r. system bankowy odnotował dziewięć nieautoryzowanych logowań na konto pokrzywdzonej i każda ze współoskarżonych, jak napisał sąd, dokonała przynajmniej jednego z nich („Brak jest możliwości ustalenia ilu dokładnie logowań dopuścili się poszczególni oskarżeni"). Ustalono ponadto, że oskarżeni chcieli sprawdzić, ile środków pieniężnych pokrzywdzona zgromadziła na rachunku, i po zalogowaniu się do aplikacji bankowości elektronicznej uzyskali m.in. informację, że zapłaciła ona całość opłaty leasingowej za samochód. Dalej sąd stwierdził:

> Dostęp do powyższego systemu jest zabezpieczony elektronicznie, w ten sposób, że jest możliwy tylko po podaniu właściwego loginu i hasła, nadawanych wyłącznie osobom do tego uprawnionym. Do posiadania powyższych informacji była uprawniona pokrzywdzona, czyli posiadaczka rachunku, użytkowniczka tego indywidualnego systemu, natomiast nie byli do tego uprawnienie oskarżeni. /…/ Niezależnie od tego, czy dane do logowania oskarżeni znali z kartki na tablicy korkowej, czy też wcześniej podała im je sama pokrzywdzona, to istotne jest to, że nie mieli uprawnienia dysponowania nimi. Nie została wyrażona na to zgoda, ani wprost, ani konkludentnie[126].

Na podstawie prawidłowo ustalonych okoliczności faktycznych krakowski sąd doszedł do fundamentalnego wniosku, który należy brać pod uwagę przy wykładni znamion art. 267 § 1 i 2 k.k., ale i tak błędnie przypisał sprawcy popełnienie przestępstwa z art. 267 § 2 k.k.:

> Czyn z art. 267 § 2 k.k., w przeciwieństwie do art. 267 § 1 k.k., nie zawiera znamienia przełamania lub ominięcia zabezpieczenia. Tak więc już sam nieuprawniony dostęp do części systemu informatycznego stanowi występek penalizowany w tym przepisie, niezależnie od faktu posiadania loginu i hasła[127].

W tym kontekście P. Siemkowicz podniósł, że zachowanie opisane w art. 267 § 2 k.k. mające postać „czystego dostępu do systemu informatycznego" wzbudza zastrzeżenia i wątpliwości interpretacyjne. W szczególności w opisie tego czynu nie występuje

[126] Tamże.
[127] Tamże.

w odróżnieniu do dyspozycji art. 267 § 1 k.k. element „przełamania" lub „omijania" zabezpieczeń. Przepis ten w zasadzie w ogóle nie charakteryzuje sposobu działania sprawcy i ma bardzo ogólny charakter, co oznacza, że kryminalizuje on wszelkie możliwe przypadki uzyskania nieuprawnionego dostępu do systemu informatycznego oraz przy użyciu jakiejkolwiek metody, a także bez względu na to, czy system ten posiada jakieś zabezpieczenia, czy też zabezpieczeń takich wcale nie ma. Pociąga to za sobą niebezpieczeństwo objęcia kryminalizacją wszelkich zachowań, które wiążą się z uzyskaniem dostępu do takiego systemu. W tym kontekście uznać należy art. 267 § 2 k.k. za nieprecyzyjny oraz stwarzający praktyczne problemy interpretacyjne, co może prowadzić do serii postępowań karnych dotyczących sytuacji przypadkowego uzyskania dostępu przez użytkowników sieci Internet do systemu informatycznego, który nawet nie musi być zabezpieczony. Łatwo można wyobrazić sobie niezamierzone podłączenie się do otwartej sieci bezprzewodowej Wi-Fi np. sąsiada z bloku, co prowadzi do uzyskania nieuprawnionego dostępu do cudzego systemu komputerowego, i jeśli osoba podłączająca się przewidywała taką możliwość i godziła się z nią, to poniesie każdorazowo odpowiedzialność karną z art. 267 § 2 k.k. Zatem na gruncie art. 267 k.k. ma się do czynienia z faktyczną przewagą przepisu uzupełniającego (art. 267 § 2 k.k.) nad przepisem zasadniczym (art. 267 § 1 k.k.), ponieważ § 2 ma w odniesieniu do § 1 znacznie szersze granice stosowania, a ponadto nie przewiduje on w odniesieniu do sprawcy uzyskującego nieuprawniony dostęp do całości lub części systemu informatycznego żadnych dodatkowych warunków ograniczających zakres jego odpowiedzialności karnej. Sytuacja taka stwarza niebezpieczeństwo zbyt dużej swobody interpretacyjnej w stosowaniu prawa przez organy ścigania. R. Koszut dodaje, iż faktycznie przepis art. 267 § 2 k.k. w jego aktualnym brzmieniu, będąc przykładem kryminalizacji tzw. czystego dostępu do systemu komputerowego (naruszenia miru komputerowego), jest zbliżony do przestępstwa naruszenia miru domowego z art. 193 k.k.[128]

Odnosząc się do stanowiska P. Siemkowicza, trudno zaprzeczyć, że potencjalne granice stanów faktycznych, w których stosuje się art. 267 § 2 k.k., zakreślono szeroko. Jednak obawy ww. autora dotyczące „przypadkowego" uzyskania dostępu do części lub całości systemu informatycznego są o tyle nieuzasadnione, że przestępstwo hakingu ma charakter umyślny, może zostać popełnione w formie zamiaru zarówno bezpośredniego, jak i ewentualnego, a więc sprawca, wykonując określone czynności, musi co najmniej przewidywać, że poskutkują one uzyskaniem bez uprawnienia dostępu do całości lub części systemu informatycznego osoby trzeciej i na to się godzić.

Zatem uzyskanie dostępu, o którym mowa w art. 267 § 2 k.k., może polegać na takich samych czynnościach, jak opisane w § 1, czyli na przełamaniu albo ominięciu elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń całości lub części systemu informatycznego. Jednak istotna różnica między § 1 i § 2 art. 267 k.k. sprowadza się do tego, że realizacja przestępstwa opisanego w § 2 nie

[128] P. Siemkowicz, *Przestępstwa skierowane przeciwko poufności*…, s. 9–10.

wymaga przełamania lub ominięcia zabezpieczenia. Tak więc już sam nieuprawniony dostęp do części systemu informatycznego stanowi występek, niezależnie od faktu posiadania przez sprawcę loginu i hasła[129]. W zdecydowanej większości przypadków czyn karalny wyczerpie znamiona art. 267 § 1 k.k. lub art. 267 § 2 k.k., a wyjątkowo tylko dojdzie do realnego zbiegu tych przepisów. Kwalifikację taką przyjął prokurator, oskarżając mężczyznę o to, że:

> w dniu 5 lutego 2015 r. w Krakowie bez uprawnienia uzyskał dostęp do systemu informatycznego /…/ S. A. oraz informacji dla niego nieprzeznaczonej, poprzez to, że ominął zabezpieczenie systemu komputerowego /…/ z bazami klientów wykorzystując przy tym uzyskane w nieustalony sposób login i hasło pracownika salonu /…/ następnie bezprawnie dokonał zmian w bazach danych informatycznych dotyczących wysokości abonamentu, a to zmniejszeniu kwoty zobowiązania miesięcznego klientów, na skutek czego powstały straty w wysokości 34.693 zł na szkodę /…/ S. A., tj. o przest. z art. 267 § 1 k.k. i art. 267 § 2 k.k. i art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k.[130]

Po rozpoznaniu sprawy Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie wyrokiem z dnia 12 września 2016 r. uznał mężczyznę za winnego tego, że:

> działając w celu osiągnięcia korzyści majątkowej przez inne osoby i wyrządzenia szkody /…/ S. A. w dniu 5 lutego 2015 r. w Krakowie bez uprawnienia uzyskał dostęp do części systemu informatycznego /…/ S. A. oraz bez uprawnienia uzyskał dostęp do informacji dla niego nieprzeznaczonej w postaci bazy danych o klientach /…/ S. A. poprzez to, że ominął informatyczne zabezpieczenie systemu komputerowego /…/ z bazami klientów wykorzystując uzyskane w nieustalony sposób indywidualny login i hasło przynależne do pracownika /…/, a następnie wyrządził /…/ szkodę w kwocie 34.693 zł dokonując bez upoważnienia zmian w bazach danych informatycznych klientów /…/ dotyczących wysokości abonamentu oraz w zakresie wysokości opłaty za usługę multipak, polegających na zmniejszeniu kwot zobowiązania miesięcznego klientów w zakresie abonamentu i opłaty za usługę multipak, tj. za występek z art. 267 § 1 k.k. i art. 267 § 2 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[131]

[129] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.
[130] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 1706/15/S.
[131] Tamże.

W uzasadnieniu do wyroku sąd stwierdził, że:

> oskarżony bez uprawnienia uzyskał dostęp do informacji dla niego nieprzeznaczonej w postaci bazy danych o klientach /…/ S. A. poprzez to, że ominął informatyczne zabezpieczenie systemu komputerowego /…/. Jednocześnie oskarżony bez uprawnienia uzyskał dostęp do części systemu informatycznego w postaci systemu informatycznego CRM za pomocą którego można dokonywać wobec klientów /…/ S. A. zmian w zakresie m.in. opłat za usługi na ich rzecz. To działanie realizowało znamiona art. 267 § 2 k.k. Stąd to zachowanie oskarżonego realizowało znamiona art. 267 § 1 k.k. i art. 267 § 2 k.k. Dla oddania pełnej zawartości kryminalnej jego zachowania niezbędne jest przywołanie obu przepisów w kwalifikacji prawnej czynu, gdyż ona wskazują na nieco inne zachowania – art. 267 § 1 k.k. dotyczy ochrony informacji, a art. 267 § 2 k.k. dotyczy ochrony systemu informatycznego.

Sąd przyjął jednocześnie, że „znamiona art. 267 § 1 k.k. i art. 267 § 2 k.k. nie zawierają się w znamionach art. 287 § 1 k.k., stąd dla oddania całej zawartości kryminalno-prawnej działania oskarżonego niezbędne było powołanie wszystkich tych przepisów, tj. art. 267 § 1 k.k. i art. 267 § 2 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[132]". Jednak analiza akt spraw karnych, ale także doświadczenie życiowe, pokazują, że przestępstwa popełniane przez podsądnych wyczerpują najczęściej znamiona tylko § 1 komentowanego przepisu, bowiem dla „przeciętnego człowieka" wartość mają informacje dostarczające określonej wiedzy, a nie dane informatyczne. Zatem umyślne uzyskanie bez uprawnienia dostępu do całości lub części systemu informatycznego dotyczy działań profesjonalnych hakerów potrafiących zrobić użytek z dostępu do cyfrowych artefaktów.

3.4. Analiza spraw karnych dotyczących czynów z art. 267 § 3 k.k.

Na skutek nieograniczonego wręcz dostępu na rynku do urządzeń służących prowadzeniu różnych form „podsłuchów" przestępstwo stypizowane w art. 267 § 3 k.k. stosunkowo często pojawiało się w badanym okresie na wokandzie. Urządzenie, o którym mowa w tym przepisie, to mechanizm lub zespół mechanizmów, służący do wykonania określonych czynności[133]; może ono stanowić monolit lub składać się z połączonych ze sobą elementów stanowiących spójną, funkcjonalną całość. W przypadku programów komputerowych chodzi np. o różne wersje oprogramowania sniffer (np. DSniff), których zastosowanie pozwala „atakującemu" na uwierzytelnienie się w komputerze osoby trzeciej i poznanie interesujących go treści. Będą to informacje związane z uwierzytelnianiem danego użytkownika (loginy i hasła do poczty, bankowości elektronicznej, serwisów społecznościowych), dające przestępcy możliwość dostępu do zasobów repetytoriów systemu komputerowego oraz informacji przesyłanych z monitorowanego

[132] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie, II K 1706/15/S.
[133] https://sjp.pwn.pl/slowniki/urządzenie.html [dostęp: 19.11.2023].

komputera do innej maszyny, np. treści wiadomości mailowych, danych transmitowanych w ramach sieci www, rozmów prowadzonych za pomocą komunikatorów internetowych[134]. Inny rodzaj oprogramowania szpiegującego typu SpyPhone ujawnił biegły z zakresu informatyki i telekomunikacji w sprawie prowadzonej przez Sąd Okręgowy we Wrocławiu. W opinii wskazał on, że oskarżony dzięki ww. oprogramowaniu miał dostęp do wiadomości wychodzących i przychodzących na dowodowy numer telefonu. Na podstawie przeprowadzonych badań telefonu komórkowego użytkowanego przez P. S. biegły jednoznacznie stwierdził, że:

> SMS-y znajdujące się w skrzynce odbiorczej telefonu przedłożonego do badań, tj. aparatu marki /…/ o numerze /…/ świadczą o tym, że aparat był wykorzystywany jako telefon sterujący podsłuchem typu SpyPhone i odbierał on wszystkie wiadomości SMS od telefonu podsłuchiwanego o numerze /…/. Biegły wskazał ponadto, że w pamięci telefonu marki /…/ znajdowały się SMS-y służące do sterowania podsłuchem i lokalizacji telefonu podsłuchiwanego[135].

W przypadku art. 267 § 3 k.k. chodzi nie tyle o uzyskanie dostępu do informacji za pomocą specjalnego urządzenia lub oprogramowania, ale wystarczy samo jego założenie lub posługiwanie się nim w celu uzyskania informacji, do której sprawca nie jest uprawniony, aby wypełnić znamiona przestępstwa.

Kwerenda spraw zakończonych prawomocnymi wyrokami skazującymi pokazała, że kilkanaście z nich dotyczyło lokalizatorów GPS zainstalowanych na karoserii samochodu lub w środku pojazdu. Zgodnie z orzecznictwem Sądu Najwyższego, bezprawne zainstalowanie w cudzym pojeździe urządzenia służącego do pozyskiwania informacji o trasie jazdy oraz miejscu przebywania danej osoby jest niedozwolone i stanowi czyn zabroniony, o którym mowa w art. 267 § 3 k.k.[136] W postanowieniu z dnia 27 listopada 2019 r. Sąd Najwyższy podkreślił, że „informacja" obejmuje m.in. skonkretyzowaną wiedzę o miejscu przebywania osoby pokrzywdzonej w określonym czasie i bezprawne jest zainstalowanie w cudzym pojeździe urządzenia służącego do pozyskiwania informacji o trasie jazdy i tym samym o miejscu przebywania danej osoby[137]. Lokalizator z wbudowanym modułem GPS (ang. *Global Positioning System*) korzysta ze specjalnego sygnału wysyłanego najpierw z naziemnego nadajnika do satelity, a stamtąd trafia do odbiornika, który przekazuje do urządzenia administrowanego przez sprawcę współrzędne śledzonego obiektu. W podobnej sprawie toczącej się przed Sądem Rejonowym dla Krakowa-Nowej Huty w Krakowie oskarżony został uznany za winnego tego, że:

[134] M. Domagała, *Prawnokarna ochrona prywatności użytkowników Internetu*, „Państwo i Prawo" 2010, nr 3, s. 80.
[135] Wyrok Sądu Okręgowego we Wrocławiu z dnia 20 lutego 2015 r., III K 137/11, LEX nr 1841717.
[136] Zob. postanowienie Sądu Najwyższego z dnia 27 listopada 2019 r., VKK 505/2018, LEX nr 2966120.
[137] Postanowienie Sądu Najwyższego z dnia 27 listopada 2019 r., V KK 505/18, LEX nr 2966120.

> w okresie od nieustalonego dnia lipca 2013 roku do dnia 21 sierpnia 2013 roku w miejscowości D. woj. małopolskie, w celu uzyskania nieuprawnionej informacji o trasie poruszania się samochodu /…/ nr rej. /…/ własności A. W. użytkowanym przez P. W. w tylnej okolicy podwozia założył elektroniczne urządzenie namierzające w postaci lokalizatora GPS oraz codziennie sprawdzał lokalizację tego urządzenia na stronie internetowej www.gps.guardian.pl, tj. o przest. z art. 267 § 3 k.k.[138]

P. C. wyjaśnił, że był przekonany, iż kierowca samochodu śledził go i dlatego, chcąc się dowiedzieć, o co mu chodzi, przyczepił magnesem do podwozia pojazdu nadajnik GPS (prosty moduł telefonu komórkowego z kartą SIM) i wykorzystując specjalistyczne oprogramowanie zainstalowane w jego laptopie, śledził na stronie internetowej trasę przejazdu. Na kanwie analizowanej sprawy należy zadać pytanie: Co stanowiło „informację", do której uzyskania oskarżony nie był uprawniony?

Sąd w sentencji wyroku napisał, że chodziło o „informację o trasie poruszania się samochodu". Jednak bezpośredni przedmiot ochrony art. 267 § 3 k.k. stanowi szeroko rozumiane prawo do dysponowania informacją o charakterze podmiotowym, umocowane w przepisach Konstytucji RP dotyczących ochrony życia prywatnego i rodzinnego. Z analizy stanu faktycznego niniejszej sprawy wynika, że sprawca działał w zamiarze kierunkowym śledzenia miejsca pobytu (trasy przemieszczania się) osoby użytkującej samochód, a nie trasy przemieszczania się pojazdu. Sprawcy dopuszczający się podobnych przestępstw nie obejmują, co do zasady, swoim zamiarem chęci lokalizacji środka transportu w oderwaniu od ustalenia, co robi i gdzie znajduje się jego kierowca lub pasażer; przeciwnie, to miejsce pobytu konkretnego człowieka ma dla nich wartość. Treść wyroku skazującego mogła zatem brzmieć następująco:

> w okresie od nieustalonego dnia lipca 2013 roku do dnia 21 sierpnia 2013 roku w miejscowości D. woj. małopolskie w celu uzyskania informacji, do której nie był uprawnionych, o trasie przemieszczania się P. W. samochodem marki /…/ nr rej. /…/ założył na karoserii samochodu urządzenie umożliwiające lokalizowanie położenia pojazdu przy użyciu sygnału GPS i jej odczytywanie w systemie GpsGuardian, tj. o przest. z art. 267 § 3 k.k.

W sprawie Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie nieprecyzyjne wskazano, jakoby sprawca śledził samochód, a nie kierowcę, niemniej wykonano więcej czynności dowodowych, aniżeli w większości przypadków dotyczących podobnych czynów, tj. prokurator poddał badaniom specjalistycznym urządzenie podsłuchowe. Zazwyczaj bowiem ujawnienie takiego urządzenia i przyznanie się sprawcy do

[138] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 911/13/N.

popełnienia przestępstwa stanowi wystarczającą podstawę dla oskarżyciela publicznego do sporządzenia aktu oskarżenia, a sądu do skazania sprawcy.

W celu ustalenia wszystkich okoliczności faktycznych popełnionego przestępstwa, prokurator prokuratury Rejonowej Kraków-Nowa Huta w Krakowie wydał postanowienie o powołaniu biegłego z zakresu informatyki śledczej, przekazał mu do badań zabezpieczone urządzenie podsłuchowe i urządzenie służące do odbioru informacji (nadajnik GPS, laptop, elementy GPS-u) oraz zlecił:

1. odczytanie zapisu pamięci telefonu komórkowego oraz karty SIM w zakresie danych użytkownika;
2. ustalenie, czy na dysku twardym dowodowego laptopa istnieją zapisy mogące świadczyć o nabywaniu, korzystaniu z urządzeń służących do lokalizacji obiektów/osób z użyciem protokołu GPS;
3. wskazanie, jakiego typu urządzenie stanowią zabezpieczone w wyniku neutralizacji szczątki, jakie było jego przeznaczenie oraz sposób działania;
4. odczyt zawartości pamięci karty SIM tego urządzenia;
5. inne wnioski biegłego.

W opinii biegły stwierdził, że zgodnie ze specyfikacją pobraną z sieci Internet badane urządzenie umożliwiało m.in. lokalizowanie położenia osób/obiektów przy użyciu sygnału GPS, monitorowanie aktualnej pozycji w czasie rzeczywistym, podsłuch lub rozmowę z użytkownikiem. Ustalono, na podstawie wyselekcjonowanych plików z dysku twardego komputera, że jego użytkownik otwierał witrynę o adresie http://www.gps.guardian.pl, logował się do systemu GpsGuardian i otwierał stronę www umożliwiającą tworzenie raportu z przebiegu-zapisu trasy przemieszczania się nadajnika. Sprawca uzyskał szczegółowy raport z przebiegu trasy w systemie GpsGuardian za okres od 1 sierpnia 2013 r. do 1 września 2013 r. dla obiektu. Wobec takich ustaleń problematyczny jest przyjęty przez sąd i prokuratora czasookres czynu, tj. „od nieustalonego dnia lipca 2013 roku do dnia 21 sierpnia 2013 roku" skoro, jak wynikało z opinii, urządzenie podsłuchowe pozycjonowało samochód od 1 sierpnia do 1 września 2013 r., a oskarżony posiadał informacje („szczegółowy raport") o przemieszczaniu się pojazdu w tym okresie. W trakcie badań ustalono numer identyfikacyjny lokalizatora IMEI oraz numer abonencki karty SIM. W wyniku analizy zawartości dysku twardego, zainstalowanego w dowodowym laptopie, ujawniono zapisy wskazujące na logowanie się użytkownika do „szpiegującej" strony internetowej przy użyciu ww. numerów identyfikacyjnych. Przekazane do badań urządzenia wskazywały na wykorzystanie lokalizatora GPS przez użytkownika dowodowego komputera. Opinia potwierdziła zatem, jak duże znaczenie dowodowe mają ślady cyfrowe ujawnione w wyszukiwarce zabezpieczonego urządzenia: „Stwierdzono, że użytkownik dowodowego komputera przenośnego otwierał stronę WWW z informacjami na temat: 'Gdzie zamontować lokalizator GPS? Doradza P. M. z firmy rikaline, twórca platformy GpsGuardian'".

Często zdarza się, że podłożem przestępstwa z art. 267 § 3 k.k. jest konflikt emocjonalny (zdrada małżeńska, rozwód, zazdrość, chęć rozstania itp.) pomiędzy dwiema

osobami i jedna z nich zakłada „podsłuch" byłemu partnerowi. W sprawie Sądu Rejonowego dla Krakowa-Podgórza w Krakowie dwie osoby zostały skazane za to, że:

> w dniu 8 stycznia 2019 roku w K., woj. łódzkiego działając wspólnie i w porozumieniu wdarli się do cudzej części domu jednorodzinnego, wynajmowanego przez A. F., w którym to pomieszczeniu pokoju bez uprawnienia założyli urządzenie podsłuchowe i wizualne w celu uzyskania informacji co do której nie byli uprawnieni, tj. o czyn z art. 193 k.k. i art. 267 § 3 k.k. w zw. z art. 11 § 2 k.k."[139].

W sprawie tej sąd ustalił, że „urządzenie", o którym mowa w art. 267 § 3 k.k., stanowiły kamera i mikrofon umieszczone na półce i rejestrujące obraz i dźwięk z pomieszczenia. Były one schowane w pudełku, a sprawcy wywiercili w nim niewielki otwór, dzięki któremu obiektyw kamery rejestrował to, co działo się w pomieszczeniu. Skazanych przez sąd mężczyzn zatrudniła firma detektywistyczna, której mąż pokrzywdzonej zlecił zebranie obciążającego ją materiału dowodowego. Na kanwie omawianego przypadku warto przypomnieć, że zgodnie z art. 7 ustawy z dnia 6 lipca 2001 r. o usługach detektywistycznych[140], wykonując usługi detektywistyczne, detektyw nie może stosować środków technicznych oraz metod i czynności operacyjno-rozpoznawczych zastrzeżonych dla upoważnionych organów na mocy odrębnych przepisów. Tymczasem niejawny podsłuch miejsc niepublicznych jest formą kontroli operacyjnej, o której mowa w art. 19 ust. 6 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji[141].

W dochodzeniu prowadzonym przez autora, mąż posądzał żonę o zdradę i – pod swoją nieobecność – rejestrował dźwięk w domu, gdzie mieszkali razem z kilkuletnim dzieckiem. Przed dłuższymi wyjazdami poza Kraków podejrzany załączał dwa dyktafony i pozostawiał urządzenia pod łóżkiem w sypialni. Na urządzeniach zostały utrwalone, a następnie przegrane do pamięci laptopa, dowody zdrady małżeńskiej i wykorzystane przez mężczyznę w sprawie rozwodowej. Jednocześnie nagrane osoby złożyły do prokuratury zawiadomienie o podejrzeniu popełnienia przestępstwa z art. 267 § 3 k.k. W toku dochodzenia należało odpowiedzieć na pytanie: Czy mąż, rejestrując rozmowy innych osób bez ich zgody, wypełnił swoim działaniem znamiona niedozwolonego hakingu?

Po przeprowadzeniu postępowania dowodowego prokurator wydał postanowienie o umorzeniu dochodzenia na podstawie art. 17 § 1 pkt 3 k.p.k., tj. znikomej społecznej szkodliwości czynu. W uzasadnieniu decyzji stwierdzono, że co prawda mężczyzna rejestrował w formie zapisu cyfrowego poufne rozmowy dwóch osób w miejscu niepublicznym, jednak tak samo jak kobieta i jej partner mieli prawo do poufności prowadzonych rozmów, to nagrywający miał prawo do uszanowania przez obcego dla niego mężczyznę

[139] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1534/19/P.
[140] T.j. Dz. U. z 2020 r. poz. 129.
[141] T.j. Dz. U. z 2023 r. poz. 171.

swojego miejsca zamieszkania. Rodzinny dom dla każdego człowieka stanowi azyl, miejsce poniekąd intymne, wolne od ingerencji osób trzecich, miejsce przechowywania najcenniejszych rzeczy w sensie duchowym i materialnym. Nie dziwi zatem fakt, argumentował prokurator, że mężczyzna, mając podejrzenia, że ktoś narusza mir domowy, chciał to sprawdzić. Chęć zweryfikowania podejrzeń była tym bardziej uzasadniona, że wierność należy do obowiązków prawnych małżonków względem siebie zgodnie z art. 23 Kodeksu rodzinnego i opiekuńczego. Dochodzi do tego ustalenie, że w mieszkaniu, w trakcie spotkań osób nagrywanych, przebywało małoletnie dziecko, a więc działania nagrywającego motywowane były troską o syna. Zamiarem sprawcy było zatem ustalenie, co tak naprawdę dzieje się z jego rodziną. Na decyzję prokuratora o umorzeniu dochodzenia pokrzywdzeni złożyli zażalenie, a rozpoznający środek odwoławczy Sąd Rejonowy dla Krakowa-Podgórza w Krakowie utrzymał zaskarżoną decyzję w mocy.

W podobnej sprawie Sąd Rejonowy w Toruniu ustalił, że oskarżona kobieta zleciła M. C. zainstalowanie w altanie, z której korzystała również jej córka i partner, urządzenia podsłuchowego w postaci mikrofonu podłączonego do rejestratora, które nagrywało rozmowy osób będących w altanie, i uznał kobietę za winną tego, że:

> w dniu 25 sierpnia 2020 r. w miejscowości B. przy ul. /.../ w celu uzyskania informacji, do której nie była uprawniona, założyła w altanie przy domu urządzenie podsłuchowe i wizualne, przyjmując, iż czyn oskarżonej J. S. wyczerpał znamiona występku z art. 267 § 3 k.k.[142]

Sąd Rejonowy w Lesku Zamiejscowy Wydział VI Karny z siedzibą w Ustrzykach Dolnych po rozpoznaniu sprawy W. J. uznał go za winnego tego, że:

> w okresie od 20 do 23 listopada 2016 r. posługiwał się urządzeniem podsłuchowym model W-11, które to zamontował w zabawce dziecięcej, a następnie podarował go synowi F. celem uzyskania informacji w postaci prywatnych rozmów jego byłej konkubiny D. R., do których nie był uprawniony, czym działał na szkodę ww., tj. o czyn z art. 267 § 3 k.k.[143]

Wyrokiem z dnia 15 lutego 2016 r. oskarżony został uznany przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie za winnego popełnienia następującego przestępstwa:

> w okresie od dnia 15 lutego 2014 r. do dnia 30 listopada 2015 r. w Krakowie założył kilkukrotnie urządzenie podsłuchowe w mieszkaniu pokrzywdzonej oraz w torebce damskiej należącej do pokrzywdzonej, tj. o czyn z art. 267 § 3 k.k. w zw. z art. 91 § 1 k.k.[144].

[142] Wyrok Sądu Rejonowego w Toruniu z dnia 19 kwietnia 2022 r., II K 1517/21, LEX nr 3355925.
[143] Wyrok Sądu Rejonowego w Lesku z dnia 31 sierpnia 2017 r., VI K 46/17, LEX nr 2445511.
[144] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 628/15/S.

Pokrzywdzona wyjaśniła, że w podszewce torebki ujawniła „podsłuch, który posiadał napis VINUS oraz kartę SIM w sieci Orange o nr /…/"; gdy zaczęła podejrzewać, że urządzenia podsłuchowe mogą być założone także w jej mieszkaniu, to „za szafą w dużym pokoju w kontakcie zauważyła wpięte urządzenie plastikowe w którym znajdowała się karta SIM w sieci Orange o nr /…/. Następnie wypięła to urządzenie oraz wyjęła z niego kartę", a sprawę zgłosiła na policję. W opisie czynu brak jednego ze znamion przestępstwa, o którym mowa w art. 267 § 3 k.k., gdyż sprawca musi działać „w celu uzyskania informacji, do której nie był uprawniony".

W przywołanych sprawach działanie przestępcze zakończyło się na etapie „założenia urządzenia", gdyż do realizacji znamion art. 267 § 3 k.k. nie jest konieczne, aby uzyskać dostęp do informacji, co do których nie jest się uprawnionym. M. Kalitowski podkreśla, że takie określenie zachowania sprawcy, szczególnie w zakresie objętym słowem „zakłada", typizuje stadium poprzedzające uzyskanie informacji[145]. Może się wszakże zdarzyć, że sprawca założy lub posłuży się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem, a następnie uzyska dostęp do informacji, a nawet zapozna się z jej treścią. Tak było w postępowaniu prowadzonym przez Sąd Rejonowy w Wałbrzychu, gdzie kobieta została oskarżona o to, że:

> w okresie od 20 sierpnia 2014 r. do 3 września 2014 r. w W. województwa /…/ w celu uzyskania informacji do których nie była uprawniona w postaci treści rozmów, a w tym rozmów telefonicznych prowadzonych przez K. K. założyła urządzenie podsłuchowe /…/ w domu przy ul. /…/, uzyskując dostęp do takich informacji, działając na szkodę K. K., tj. o czyn z art. 267 § 1 i 3 k.k. w zw. z art. 12 k.k.[146]

W uzasadnieniu do wyroku sąd wskazał:

> Zachowanie oskarżonej odpowiadało znamionom występku stypizowanego w art. 267 § 1 k.k. i art. 267 § 3 k.k. jako że skutek polegający na uzyskaniu dostępu do danych dla niej nieprzeznaczonych, wzmiankowany w art. 267 § 1 k.k., osiągnęła zakładając urządzenie podsłuchowe, o którym mowa w art. 267 § 3 k.k. Działając w ten sposób oskarżona uzyskiwała dostęp do treści poufnych rozmów oskarżyciela posiłkowego w okresie od 20 sierpnia 2015 r. do czasu ujawnienia urządzenia podsłuchowego w dniu 3 września 2015 r., dlatego jej zachowanie, które było przedmiotem umorzonego postępowania zostało zakwalifikowane jako czyn ciągły opisany w art. 12 k.k.[147]

Sąd nie uwzględnił jednak faktu, że jednym ze znamion art. 267 § 1 k.k. jest „przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego" zabezpieczenia informacji, czego nie sposób stwierdzić w zachowaniu

[145] M. Kalitowski, *Art. 267*, *teza 10*, [w:] *Kodeks karny. Komentarz*, red. M. Filar, Wolters Kluwer 2016, LEX.
[146] Wyrok Sądu Rejonowego w Wałbrzychu z dnia 6 października 2015 r., III K 242/15, LEX nr 1931358.
[147] Tamże.

skazanej kobiety. Podobnego błędu jak Sąd Rejonowy w Wałbrzychu nie popełnił Sąd Rejonowy dla Warszawy Pragi-Południe w Warszawie, który rozpoznawał sprawę podsądnego oskarżonego o to, że:

> w miesiącu wrześniu 2012 r. w W., bez uprawnień uzyskała informacje dla niej nieprzeznaczone, dotyczące lokalizacji samochodu marki M. nr rej. /…/ poprzez zamontowanie w ww. samochodzie modułu GPS, a informację tak uzyskaną przekazywała innym osobom, czym działała na szkodę męża G. K., tj. o czyn z art. 267 § 1 i § 3 k.k.

Jednak Sąd Rejonowy dla Warszawy-Pragi Północ w Warszawie wyrokiem z dnia 17 maja 2016 r.[148] wyeliminował z kwalifikacji prawnej czynu art. 267 § 1 k.k. i ustalił, że A. K. w bliżej nieustalonym dniu września 2012 r. w celu uzyskania informacji o lokalizacji samochodu M. nr rej /…/, do której nie była uprawniona, posłużyła się urządzeniem GPS zamontowanym w ww. pojeździe użytkowanym przez G. K., tj. za winną popełnienia przestępstwa z art. 267 § 3 k.k. i postępowanie karne wobec A. K. warunkowo umorzył. Sąd Okręgowy Warszawa-Praga w Warszawie, rozpatrując apelację od ww. wyroku, wskazał na słuszny wywód sądu I instancji mówiący o tym, że dla bytu przestępstwa opisanego w art. 267 § 3 k.k. nie ma znaczenia, czy osoba finalnie informację uzyskała, czy też nie. Dlatego sąd I instancji nie był obowiązany do ustalenia, kto łączył się z lokalizatorem GPS i kto w rzeczywistości odczytywał dane z rejestratora. Dla bytu tego przestępstwa wystarczy samo posłużenie się urządzeniem w celu zdobycia informacji[149]. O ile dla samego bytu przestępstwa nie ma znaczenia, w jaki sposób zostało wykorzystane urządzenie podsłuchowe po jego zainstalowaniu na samochodzie, to zdaniem autora, ważne są jednak pozostałe ustalenia faktyczne, poczynione w tym zakresie w celu określenia wszystkich istotnych okoliczności spraw. Fakt, czy oskarżony uzyskał ostatecznie dostęp do informacji, a być może zapoznał się z nią, ma bowiem znaczenie dla społecznej szkodliwości czynu i dyrektyw wymiaru kary.

Napisano już, że dla realizacji znamion czynności wykonawczej z art. 267 § 3 k.k. wystarczające jest założenie urządzenia podsłuchowego w celu uzyskania informacji, co do których sprawca nie posiadał uprawnienia, chociażby nie doszło do jego wykorzystania ani też do uzyskania za jego pomocą określonych treści. Karalne jest samo posługiwanie się urządzeniem podsłuchowym, nawet jeśli osoba posługująca się takim urządzeniem wcześniej go nie instalowała[150]. Można zatem powiedzieć, że w konstrukcji art. 267 § 3 k.k. jest pewna „luka legislacyjna", tj. jeśli skutek działania sprawcy wypełnia znamiona tego przepisu, a ponadto przestępca uzyskuje bez uprawnienia dostęp do informacji, ale bez przełamania lub ominięcia zabezpieczenia informacji, to materialny skutek czynu nie

[148] Wyrok Sądu Rejonowego dla Warszawy-Pragi Północ z dnia 17 maja 2016 r., III K 1013/13.
[149] Wyrok Sądu Okręgowego Warszawa-Praga w Warszawie z dnia 21 marca 2017 r., VI Ka 1343/16, LEX nr 2278402.
[150] W. Wróbel, D. Zając, *Art. 267…*, *teza 28*.

zostaje ujęty w kwalifikacji prawnej przestępstwa. Można go natomiast zawrzeć w opisie czynu i sądy postąpiły w ten sposób, uznając sprawców za winnych tego, że:

> w nieustalonym dniu w okresie od kwietnia do 13 października 2013 r. w W., działając wspólnie i w porozumieniu, w celu uzyskania informacji, do której nie byli uprawnieni w postaci treści rozmowy gości restauracji /…/ w W., posłużyli się urządzeniem podsłuchowym, w ten sposób, że M. F. zaoferował Ł. N. wynagrodzenie w postaci pieniędzy i udziału w przyszłych zyskach z transakcji biznesowych w zamian za założenie w Sali /…/ urządzenia podsłuchowego umożliwiającego rejestrację dźwięku i posłużenie się tym urządzeniem do zarejestrowania rozmów gości, w wyniku czego Ł. N. utrwalił przebieg rozmowy P. G. i dwiema innymi ustalonymi osobami, a następnie Ł. N. przekazał M. F. nośnik informatyczny zawierający zapis nagrania tej rozmowy, tj. o czyn z art. 267 § 3 k.k.[151]

> w okresie od 1 kwietnia 2019 r. do 2 sierpnia 2020 r. w W. gm. W. woj. /…/ posługując się urządzeniem podsłuchowym zamontowanym w listwie zasilającej a które to urządzenie łącząc się poprzez sieć telefonii komórkowej przekazywało sygnał głosowy do jego telefonu, uzyskiwał informacje do których nie był uprawniony działając tym na szkodę M. M. i J. M. – to jest o przestępstwo z art. 267 § 3 k.k.[152]

Co jednak, gdy sprawca przestępstwa wypełni swoim zachowaniem znamiona art. 267 § 3 k.k., a następnie, dzięki urządzeniu lub oprogramowaniu, którymi się posłużył, przełamie/ominie zabezpieczenie i uzyska bez uprawnienia dostęp do informacji dla niego nieprzeznaczonej (art. 267 § 1 k.k.)? W takiej sytuacji założenie lub posłużenie się przez sprawcę urządzaniem lub oprogramowaniem będzie czynem współukaranym uprzednio w stosunku do czynu z art. 267 § 1 k.k. Zakwalifikowanie działania sprawcy z tego ostatniego przepisu odda całą zawartość kryminalną jego zachowania, a oba przestępstwa mogą być popełnione tylko z zamiarem bezpośrednim, gdyż trudno sobie wyobrazić, by sprawca nie miał świadomości faktu, że uzyskuje dostęp do informacji dla niego nieprzeznaczonych[153]. W takim kierunku deliberował prokurator Prokuratury Rejonowej Katowice-Północ w Katowicach, który umorzył na podstawie art. 322 § 1 k.p.k., śledztwo w sprawie o to, że nieustalona osoba:

> w dniu 9 maja 2019 roku w nieustalonym miejscu ze skutkiem w Katowicach za pośrednictwem sieci internet celu osiągnięcia korzyści majątkowej w kwocie 969 dolarów amerykańskich w wirtualnej walucie Bitcoin bez upoważnienia wpłynął na

[151] Wyrok Sądu Okręgowego w Warszawie z dnia 29 grudnia 2016 r., XVIII K 5/16, LEX nr 2188993.
[152] Wyrok Sądu Rejonowego w Łukowie z dnia 5 maja 2022 r., II K 793/20, LEX nr 3369999.
[153] Zob. wyrok Sądu Najwyższego z dnia 2 czerwca 2003 r., II KK 232/02, LEX nr 78373.

> automatyczne przetwarzanie i przekazywanie danych informatycznych w postaci utrwalenia, przechowywania i udostępniania hasła do portfeli społecznościowych oraz poczty e-mail pokrzywdzonej /…/, do którego uzyskał dostęp bez uprawnienia poprzez ominięcie informatycznego jego zabezpieczenia, a także nie będąc do tego uprawnionym, poprzez transmisję na tableta pokrzywdzonej marki Apple iPade oprogramowania, który zapewnił mu dostęp do ekranu i kamery internetowej tego urządzenia, czym w istotny sposób zakłócił pracę systemu komputerowego pokrzywdzonej, tj. o czyn z art. 267 § 1 k.k. i art. 269a k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[154]

Pomijając w tym miejscu kwestie manipulowania danymi informatycznymi dla okupu, o czym będzie jeszcze mowa, warto zauważyć, że sprawca posłużył się oprogramowaniem, które „zapewniło mu dostęp do ekranu i kamery internetowej tego urządzenia", tj. przejętego zdalnie komputera, i śledzenie zapisu kamery. Formalnie doszło zatem do wypełnienia znamion art. 267 § 3 k.k., ale czyn ten został pochłonięty przez art. 267 § 1 k.k. Natomiast w sprawie rozpoznanej przez Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie pokrzywdzony zgłosił, że nieustalony sprawca trzykrotnie włamał się na konto uczestnika i administratora niewielkiego portalu społecznościowego, a następnie „wprowadził wirusa do portalu, do kodu gry i pobrał dane, które nie były ogólnodostępne". P. K. przyznał się do popełnienia zarzucanego mu czynu i został przez sąd uznany winnym tego, że:

> w dniu 18 grudnia 2011 roku w Krakowie uzyskał bez uprawnienia dostęp do informacji dla niego nieprzeznaczonej w postaci adresów e-mail, haseł dostępu, numerów telefonów uczestników portalu internetowego /…/ przełamując zabezpieczenie informatyczne w postaci hasła dostępu założyciela strony internetowej M. C. – tj. o przestępstwo z art. 267 § 3 k.k.[155]

Podejrzany wyjaśnił, że przełamał zabezpieczenie w postaci hasła dostępu jednego z założycieli portalu i zalogował się na stronie internetowej z ciekawości, aby sprawdzić, jakie są jej zabezpieczenia i o czym dyskutuje się na forum. Mężczyzna powiedział, że na prywatne konto logował się za pomocą hasła odnalezionego przypadkowo w Internecie. Problem jednak w tym, że opis czynu w żadnej mierze nie odzwierciedla, jakoby oskarżony miał „wprowadzić wirusa do portalu, do kodu gry", a nawet gdyby tak się stało, to złośliwe oprogramowanie nie posłużyło mu do przełamania zabezpieczenia, ale zostało wykorzystane już po zalogowaniu się na platformę. Opisane działanie mogło ewentualnie wyczerpać znamiona art. 268a § 1 k.k. lub art. 287 § 1 k.k. Treść wyroku obrazuje

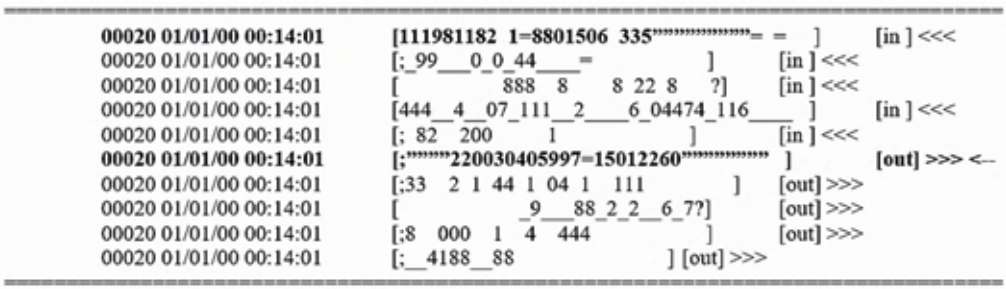
[154] Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 2 Ds. 1843.2019.
[155] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 406/12/N.

jeszcze inną, niepokojącą prawidłowość w sprawach hakerskich: sądy i prokuratorzy, bezkrytycznie przyjmują wyjaśnienia podejrzanych/oskarżonych dotyczące sposobu przełamania zabezpieczenia elektronicznego, które są bardzo ogólnikowe, a niekiedy wręcz logicznie niewiarygodne.

Nielegalne działania związane z uzyskiwaniem dostępu do wrażliwych informacji lub danych, kwalifikowane art. 267 § 3 k.k., dotyczyły także spraw poważniejszych, o skomplikowanym stanie faktycznym, przestępstw realizowanych przez zorganizowane grupy, których *modus operandi* charakteryzował się zaawansowaniem technologicznym i wyrafinowaniem. Skimming bankomatowy składał się z następujących po sobie etapów działania:

1. bezprawne skopiowanie danych z paska magnetycznego i rejestracja numeru PIN,
2. produkcja fałszywej karty i identyfikacja przypisanego jej PIN-u,
3. realizacja transakcji płatniczych przy użyciu fałszywych kart.

Działanie skimmera oparte jest na układzie czytnika i dekodera zapisu magnetycznego umożliwiającego odczyt i składowanie w jego pamięci danych umieszczonych na drugiej ścieżce paska magnetycznego karty płatniczej. W momencie włożenia instrumentu płatniczego do bankomatu plastik, zanim dotrze do oryginalnego czytnika, przechodzi przez fałszywą nakładkę umieszczoną na podajniku i głowica skimmera odczytuje informacje zapisane na pasku. Skopiowane informacje modyfikowane są następnie przez moduł do przetwarzania danych z czytnika pola magnetycznego i magazynowane w pamięci wewnętrznej urządzenia (mikrokontrolera). Ponieważ „skradzione" dane są zmagazynowane w pamięci nakładki, to w celu dalszego ich wykorzystania należy „wydobyć" je ze skimmera. Pobieranie danych z układów pamięci odbywa się po ściągnięciu urządzenia z bankomatu za pośrednictwem przewodu łączącego gniazdo komunikacyjne nakładki i port jednostki stałej komputera. Aplikacja, działająca przeważnie w środowisku systemu operacyjnego Windows, odczytuje dane i przenosi je do pamięci stałej laptopa. Przestępcy stosują do tego specjalne oprogramowanie, dedykowane nierzadko konkretnemu skimmerowi, którego algorytmy dekodują cyfrowe artefakty, i otrzymuje się gotowy „produkt" w postaci ciągu znaków skopiowanych z drugiej ścieżki karty[156].



Grafika nr 6. Dane kart płatniczych odczytane z pamięci skimmera. Tylko fragmenty zaznaczone wytłuszczonym drukiem zawierają pełne dane paska magnetycznego (usunięto cyfry pełnego numeru karty)

[156] P. Opitek, *Skimming – aspekty kryminalistyczne*…, s. 104–107.

W art. 267 § 3 k.k. mowa jest o celu działania sprawcy w postaci „uzyskania informacji", ale przykład skimmingu pokazuje, jak płynna jest granica pomiędzy tym, co przepisy rozdziału XXXIII k.k. traktują jako „dane informatyczne", a treściami uznawanymi za „informacje". Grafika nr 6 poświadcza bowiem, że skimmer rejestrował na początku dane, a w toku dalszej „obróbki" komputerowej przekształcane one były na informacje. Informacje niosące konkretny sens były zrozumiałe tylko dla osób obeznanych w systemie kart. Sądy traktowały takie czyny jako wyczerpujące znamiona art. 267 § 3 k.k. Oto przykład orzeczenia wydanego przez Sąd Okręgowy w Olsztynie, który skazał sprawcę za to, że:

> w okresie od /…/ r. w G., w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru, działając wspólnie i w porozumieniu z obywatelami /…/ V. J., w celu uzyskania korzyści majątkowej oraz uzyskania informacji, do których nie był uprawniony, zamontował na bankomacie Banku /…/ S.A., znajdującym się na ul. /…/ w G. oraz bankomacie Banku /…/ S.A. znajdującym się na ul. /…/ w G., urządzenia kopiujące zapis paska magnetycznego oryginalnych kart płatniczych oraz nagrywającego kombinację klawiszy wybieranych na klawiaturze bankomatu podczas wpisywania kodu PIN, uzyskując w ten sposób dostęp do sekwencji kodów PIN, a także danych identyfikujących poszczególne karty dotyczące kart bankomatowych i tak: w bankomacie 369 kart płatniczych wydanych przez /…/ S.A. o numerach: /…/, oraz 103 karty płatnicze w bankomacie Banku /…/ S.A. przy ul. /…/ o numerach: /…/, które to dane przekazane zostały elektronicznie innym osobom, czym czynił przygotowania do podrobienia innych środków płatniczych w postaci kart magnetycznych oraz po przełamaniu zabezpieczeń bankomatów i przy użyciu skopiowanych danych kart usiłował wpłynąć na automatyczne przetwarzanie i przekazywanie danych informatycznych zgromadzonych na serwerach bankowych, poprzez wypłatę bez upoważnienia pieniędzy, zamiaru swego jednak bankowych, poprzez wypłatę bez upoważnienia pieniędzy, zamiaru swego jednak nie osiągnął z uwagi na zatrzymanie go przez funkcjonariuszy Policji z Komendy Powiatowej w G. oraz zablokowanie skopiowanych kart bankomatowych - tj. o czyn z art. 267 § 3 k.k. w zb. z art. 310 § 4 k.k. w zb. z art. 13 § 1 k.k. w zw. z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. i art. 12 k.k.[157]

Oprócz art. 267 § 3 k.k. w przypadku skimmingu w grę wchodzą jeszcze inne przepisy Kodeksu karnego, przede wszystkim ukierunkowane na podrobienie karty płatniczej. W rozumieniu art. 310 k.k. „karta płatnicza" to „inny środek płatniczy", który stanowi przedmiot czynności wykonawczej. Zachowanie sprawcy opisane w § 1 cytowanego przepisu polega na podrobieniu lub przerobieniu środka płatniczego. Przy

[157] Wyrok Sądu Okręgowego w Olsztynie z dnia 28 kwietnia 2015 r., II K 181/14, LEX nr 1835835.

podrobieniu środka płatniczego przedmiotem przestępstwa jest rzecz naśladująca oryginalną kartę. Z kolei przestępstwo z art. 310 § 2 k.k. polega na puszczeniu w obieg sfałszowanej karty, przy czym sprawca popełnia czyn karalny już w momencie „puszczenia", bez konieczności wystąpienia skutku w postaci wykorzystania „białego plastiku" do transakcji bankomatowych. Skutku w postaci przyjęcia, przechowywania, przewożenia, przenoszenia i przesyłania fałszywych kart płatniczych będzie natomiast wymagało przestępstwo z art. 310 § 2 k.k. popełnione w kilku odmianach sprawczych. Przepis art. 310 § 4 k.k. penalizuje czynności przygotowawcze do popełnienia przestępstwa określonego w art. 310 § 1 i 2 k.k., np. poprzez nabycie urządzeń skimmujących do kopiowania kart w bankomacie. Nieuprawnione gromadzenie, posiadanie czy przekazywanie zeskimmowanych numerów i przyporządkowanych im PIN-ów zalicza się także do czynów karalnych z art. 310 § 4 k.k. w przypadku udowodnienia, że miały one posłużyć do wyprodukowania „białego plastiku". Karalnym przygotowaniem, a nie przestępstwem z art. 269b § 1 k.k., będzie zaopatrzenie się w program komputerowy umożliwiający modyfikację i szyfrowanie danych na ścieżce magnetycznej karty w celu jej sfałszowania.

Warto jeszcze wspomnieć o zagadnieniu wzbudzającym kontrowersje, tj. podsłuchiwaniu policji. W doktrynie i orzecznictwie przez lata pojawiały się rozbieżne stanowiska dotyczące kwestii nasłuchiwania radiowego kanału policyjnego; w wyroku Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie mężczyzna został uznany za winnego tego, że:

> w dniu 13 września 2014 roku w Krakowie w celu uzyskania informacji, do której nie był uprawniony, posługiwał się urządzeniem podsłuchowym Baofeng, pozwalającym na nasłuchiwanie korespondencji na częstotliwości policyjnej, to jest za czyn z art. 267 § 3 k.k.[158]

Rozstrzygnięcie takie mogłoby wydawać się słuszne, bowiem w doktrynie twierdzi się, że dla wystąpienia bezprawnego podsłuchu transmisji nie jest istotne, czy przesyłane w sieci dane zostały uprzednio zabezpieczone w szczególny sposób, np. zaszyfrowane, bowiem podsłuch narusza powszechne w demokratycznych systemach prawnych prawo tajemnicy komunikacyjnej, zwanej też tajemnicą korespondencji[159]. Jednak w apelacji od wyroku sądu I instancji obrońca oskarżonego zarzucił wyrokowi błąd w ustaleniach faktycznych poprzez przyjęcie przez sąd, że urządzenie Baofeng jest urządzeniem podsłuchowym, o którym mowa w art. 267 § 3 k.k., gdyż „nie posiada ono jakiejkolwiek funkcji rejestracji czy też zapisu dźwięku na nośniku aby było urządzeniem

[158] Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 28/15/K.

[159] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Wydział Prawa Uniwersytetu w Białymstoku, praca doktorska napisana w Katedrze Prawa Karnego pod kierunkiem dr hab. Ewy M. Guzik-Makaruk, prof. UwB, Białystok 2017, s. 167.

podsłuchowym". W apelacji podniesiono ponadto zarzut braku ustalenia przez sąd rejonowy „modelu oraz cech zabezpieczonego urządzenia", a nawet faktu użytkowania go przez oskarżonego w celu nasłuchiwania częstotliwości fal radiowych kanału policyjnego. W trakcie postępowania odwoławczego uzyskano informację od Prezesa Urzędu Komunikacji Elektronicznej wskazującą, że „urządzenie Baofeng A52 jest urządzeniem radiowym nadawczo-odbiorczym" i jego używanie „wymaga posiadania pozwolenia radiowego". Mając to na uwadze, Sąd Okręgowy w Krakowie w wyroku z dnia 9 marca 2017 r.[160] zmienił treść orzeczenia pierwszoinstancyjnego i przyjął, że oskarżony:

> w dniu 13 września 2014 roku w Krakowie bez wymaganego pozwolenia używał urządzenie nadawczo odbiorcze Baofeng to jest, że czyn stanowi wykroczenie z artykułu 208 pkt 1 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne.

W uzasadnieniu do wyroku sąd powołał się na orzeczenie Sądu Najwyższego z dnia 19 października 2006 r.[161], w którym stwierdzono, iż urządzenie nadawczo-odbiorcze Baofeng A52 nie jest urządzeniem w specjalnym w rozumieniu art. 267 § 3 k.k. Osoba, która posiada pozwolenie używania urządzenia nadawczo-odbiorczego, a więc także uprawnienie do wykorzystywania określonych w tym pozwoleniu częstotliwości, może używać tego urządzenia wyłącznie w warunkach określonych tym pozwoleniem, a jeżeli robi to niezgodnie z przyznanymi w pozwoleniu uprawnieniami, to naraża się na odpowiedzialność w trybie postępowania administracyjnego, o której mowa w art. 209 ust. 1 pkt 9 ustawy Prawo telekomunikacyjne. Poza sporem pozostaje okoliczność, że Andrzej R. tego dnia prowadził nasłuch kanałów oficera dyżurnego policji za pomocą urządzenia nadawczo-odbiorczego Baofeng A52. Zdaniem Sądu Najwyższego, ustawa Prawo telekomunikacyjne, obok występku polegającego na używaniu bez wymaganego pozwolenia urządzenia radiowego nadawczego lub nadawczo-odbiorczego (art. 208 ust. 1 cyt. ustawy), przewidziała możliwość nałożenia administracyjnej kary pieniężnej za wykorzystywanie częstotliwości bez posiadania do tego uprawnień lub niezgodnie z tym uprawnieniami (art. 209 ust. 1 pkt 9 cyt. ustawy). Mamy zatem do czynienia z sytuacją, w której ustawodawca określił dwa, różne przecież w swej treści, typy zachowań, przewidując dla każdego z nich inną sankcję. Pierwsze polega na używaniu określonego urządzenia bez wymaganego pozwolenia, za co grozi odpowiedzialność karna, natomiast w drugim przypadku osoba, która wprawdzie posiada uprawnienia do wykorzystywania częstotliwości, ale czyni to niezgodnie z tymi uprawnieniami, podlega odpowiedzialności w trybie postępowania administracyjnego. Takie ujęcie przez ustawodawcę omawianej kwestii oznacza, że osoba, która posiada pozwolenie używania

[160] Akta Sądu Okręgowego w Krakowie o sygn. IV Ka 1131/16.
[161] Wyrok Sądu Najwyższego z dnia 19 października 2006 r., V KK 221/06, LEX nr 198105.

urządzenia nadawczo-odbiorczego, a więc także uprawnienie do wykorzystywania określonych w tym pozwoleniu częstotliwości, może używać tego urządzenia wyłącznie w warunkach określonych tym pozwoleniem, bo inaczej naraża się na odpowiedzialność z art. 209 ust. 1 pkt 9 ustawy Prawo telekomunikacyjne. Sąd Najwyższy uznał, że w rozpoznawanej sprawie miał do czynienia właśnie z taką sytuacją: Andrzej R. posiadał pozwolenie na używanie urządzenia nadawczo-odbiorczego na określonych częstotliwościach, jednak 5 kwietnia 2001 r. prowadził nasłuch za pomocą urządzenia nadawczo-odbiorczego na innych, niż przewidywało.

Wspomniany wyrok Sądu Najwyższego może budzić pewne kontrowersje, bowiem urządzenia do przechwytywania informacji nie muszą mieć żadnego szczególnego charakteru, a nade wszystko nie muszą odkodowywać zaszyfrowanej treści. W tym kontekście przepis art. 267 § 3 k.k. penalizuje np. nagrania poufnej rozmowy dwóch osób wykonane „zwykłym" dyktafonem. W analizowanej sprawie łączność pomiędzy funkcjonariuszami policji była zabezpieczona, co wynika chociażby z faktu, że skazany musiał kupić urządzenie specjalistyczne do podsłuchu, znać parametry pasma wykorzystywanego przez policję i dostrajać do niego owo urządzenie, aby „podsłuchiwać". Podobnego zaangażowania wymaga zainstalowanie odbiornika GPS na samochodzie, a ów czyn wypełnia znamiona art. 267 § 3 k.k. Przemieszczanie się osoby (samochodu) także nie jest w sposób szczególny zabezpieczone przed „podrzutką" GPS-a, ale dorozumiana wola potencjalnego pokrzywdzonego wystarczy, aby jego śledzenie było zabronione. Powszechnie wiadomą rzeczą jest, że komunikaty przekazywane drogą radiową pomiędzy funkcjonariuszami policji mają charakter poufny, o czym przesądza treść przekazu (dane wrażliwe o działaniach służby, dane osobowe ludzi pozostających w jej zainteresowaniu) i wola policjantów realizujących przekaz (transmisja na paśmie „prywatnym", zasadniczo nieodbieranym przez urządzenia znajdujące się w powszechnym użytku). Niemniej, stanowisko Sądu Najwyższego przesądza o tym, że nasłuchiwanie częstotliwości fal radiowych kanału policyjnego w taki sposób, jak czynił to oskarżony, nie stanowi przestępstwa. Każda sprawa musi być rozpatrywana indywidualnie, szczególnie że analizowane wyroki zapadły już wiele lat temu (2006 i 2014) i od tego czasu wiele się zmieniło w organizacji zdalnej łączności policji oraz pozostałych służb ochrony prawa. Trwająca od 2010 r. modernizacja policyjnego systemu łączności (m.in. prace nad wdrożeniem TETR-y) polega na coraz lepszym zabezpieczeniu przekazywanych informacji poprzez zastępowanie transmisji radiowej kodowaną łącznością cyfrową. Uzyskanie dostępu do takich informacji, tj. wszelkie próby podsłuchiwania kodowanej łączności cyfrowej, wypełniłoby znamiona przestępstwa hakingu.

3.5. Utrudnianie zapoznania się z informacją i niszczenie danych informatycznych (art. 268 k.k. i art. 268a k.k.)

Jeśli w dużym uproszczeniu haking można porównać do przestępstwa kradzieży z włamaniem, to przestępstwa stypizowane w art. 268 k.k. i art. 268a k.k. bardziej przypominają uszkodzenie lub zniszczenie mienia. Ich znamiona są pojemne i stanowi to jedną z przyczyn, dlaczego wymienione przepisy stosuje się w sposób zbyt dowolny. Gdy mowa o „dowolnym" stosowaniu, autorowi chodzi o rozbieżności w kwalifikacji prawnej podobnych stanów faktycznych, na podstawie odmiennych przepisów dotyczących utrudnienia zapoznania się z informacją lub niszczenia danych informatycznych.

Art. 268. [Utrudnianie zapoznania się z informacją]
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a. [Niszczenie danych informatycznych]
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,
podlega karze pozbawienia wolności do lat 3.
§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Sposób podejścia ustawodawcy do penalizacji niszczenia informacji i danych informatycznych, uwidoczniony w treści art. 268 k.k. i art. 268a k.k., przypomina regulacje dotyczące ochrony dostępu do informacji (art. 267 § 1 k.k.) i systemu informatycznego (art. 267 § 2 k.k.) – w obu przypadkach przedmiotem czynności wykonawczej jest swego

rodzaju „esencja", która stanowi jedną materię, ale dla człowieka objawia się w dwóch formach: informacji lub danych informatycznych. Zatem odkodowując znaczenie znamion art. 268 k.k. i art. 268a k.k., ponownie należy przeprowadzić rozgraniczenie pomiędzy ww. pojęciami. Dane informatyczne, o których mowa w art. 268a § 1 k.k., oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, a więc stanowią język zrozumiały wyłącznie dla urządzeń komputerowych i dopiero ich odpowiednie przetworzenie przez algorytm może dostarczyć „informacji"[162]. Informacje (art. 268 § 2 k.k.) pochodzą bowiem z wyselekcjonowania danych i niosą sens dla ich odbiorcy, tj. posiadają znaczenie dla człowieka. Uzyskane z przetworzenia danych „informacje" w formie tekstu, wyświetlane na monitorze laptopa, są „wizualizowane" przez program komputerowy w taki sposób, aby można je było odczytać i zrozumieć. Do 2008 r. była luka w prawie i brakowało takiego przepisu jak art. 268a k.k., chroniącego dane informatyczne przed zniszczeniem. A. Adamski zauważył wtedy, że „ustawodawca traktuje komputer jako zaawansowaną maszynę do pisania, ograniczając ochronę zapewnioną przez przepis art. 268 § 2 k.k. jedynie do informacji zrozumiałych dla człowieka, podczas gdy procesy składające się na funkcjonowanie systemu polegają na wymianie danych między jego elementami (programowymi i sprzętowymi) i wykonywaniu instrukcji, odbywającymi się w pełni automatycznie, bez udziału i kontroli człowieka, w języku binarnym, bezpośrednio niezrozumiałym dla niego"[163].

W literaturze przedmiotu panuje niezrozumienie co do charakteru dobra chronionego na gruncie art. 268 k.k. i dwóch różniących się od siebie przedmiotów zamachu z § 1 i § 2 tego przepisu. Prawdą jest, że bezpośrednim przedmiotem ochrony w tym przepisie jest prawo do dysponowania informacją w aspekcie zachowania jej integralności oraz prawo dostępu do informacji[164]. Ów dostęp należy interpretować inaczej, aniżeli ma to miejsce na gruncie art. 267 § 1 k.k. W tym ostatnim przypadku bowiem przestępca nie zna treści informacji i bez uprawnienia uzyskuje do niej dostęp. W przypadku art. 268 k.k. sprawca ma wiedzę o treści informacji, a nawet posiada prawo dostępu do niej, a wypełnia znamiona przestępstwa w ten sposób, że nie będąc do tego uprawniony, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią. Błędne są przeto twierdzenia, że art. 268 § 2 k.k. „obecnie można uznać za zbędny, gdyż jego rolę pełnić mógłby z powodzeniem

[162] Jak stwierdził Sąd Najwyższy: „Dane informatyczne, o których mowa w przepisie art. 268a k.k. to zapis określonej informacji przechowywanej na dysku komputera lub na innym komputerowym nośniku informacji", [w:] wyrok Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15, LEX nr 1866883.

[163] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 767. Jednak powoływanie się na stanowisko A. Adamskiego jako rzekomo świadczące o „niedoskonałości" prawa, po nowelizacji Kodeksu karnego w 2008 r. i wprowadzeniu przepisu penalizującego niszczenie danych informatycznych, jest nieporozumieniem; F. Radoniewicz przywołał pogląd A. Adamskiego w monografii wydanej w 2016 r., a więc w momencie obowiązywania już regulacji, której wprowadzenia domagał się A. Adamski, [w:] F. Radoniewicz, *Odpowiedzialność karna za hacking*…, s. 315–316.

[164] W. Wróbel, D. Zając, *Art. 268, teza 1*, [w:] *Kodeks karny. Część szczególna*, t. 2. cz. 2, *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2017, LEX.

art. 268a § 1 k.k."[165]. Ostatni z wymienionych przepisów chroni bowiem przed zniszczeniem dane informatyczne, a nie informacje; obrazują to dwie sytuacje:

1. sprawca pod nieuwagę posiadacza konta na Facebooku zasiada do klawiatury komputera, zapoznaje się z treścią zamieszczoną na otwartym przez pokrzywdzonego koncie i zmienia część zapisów, a część usuwa z tego konta, a więc zmienia i usuwa informacje na serwerze, na którym firma (właściciel Facebooka) przechowuje treść (art. 268 § 2 k.k.);
2. sprawca pod nieuwagę posiadacza laptopa zasiada do klawiatury komputera i zmienia część zapisów danych informatycznych na jego dysku, a część danych kasuje bez zapoznana się z jakimikolwiek informacjami (art. 268a § 1 k.k.).

Widać zatem, że przedmiotem czynności wykonawczej na gruncie art. 268a k.k. są ważne artefakty cyfrowe nazwane przez ustawodawcę danymi informatycznymi, zapisanymi na informatycznym nośniku danych. Dlatego, odmiennie niż twierdzi F. Radoniewicz, wyodrębnienie dwóch typów czynów zabronionych, opisanych w § 1 i § 2 art. 268 k.k. nie nastąpiło „ze względu na wyższy stopień szkodliwości społecznej" typu kwalifikowanego z § 2, ale z konieczności ochrony innej, aniżeli tradycyjna, formy informacji powstałej po przetworzeniu danych cyfrowych i prezentowanej z wykorzystaniem komputera[166]. Nie polega na prawdzie twierdzenie S. Hoca, że „jeśli sprawca spełnił znamiona czynu zabronionego określonego w art. 268a k.k. i zarazem art. 268 k.k. wtedy art. 268a k.k. na zasadzie *lex consumens* wyłączy stosowanie art. 268 k.k., nie będzie więc kumulatywnego zbiegu przepisów"[167], gdyż przepisy te mają odmienny przedmiot czynności wykonawczej, tj. informacje i dane informatyczne. Zatem w przypadku ich zbiegu nie znajdzie zastosowania reguła konsumpcji, ale kumulatywnej kwalifikacji. S. Hoc myli się, pisząc, iż „w przypadku gdy zachowania sprawcy odnosić się będą do danych informatycznych będących nośnikiem określonych informacji w rozumieniu art. 268 k.k., przepis ten stanowić będzie *lex specialis* w stosunku do art. 268a k.k."[168]. Powtórzyć wypada, że treść znamion art. 268 § 2 k.k. i art. 268a § 1 k.k. powoduje, że nie konkurują one między sobą. Jedna z fundamentalnych reguł prawa karnego, zasada *nullum crimen sine lege*, zakłada wewnętrzną określoność typu czynu zabronionego, czyli nakazuje konstruowanie takiego opisu poszczególnych zachowań karalnych, aby dało się je odróżnić. W sprawie R. J. z 2008 r., oskarżonego o przest. z art. 268 § 1 k.k. w zw. z art. 12 k.k. i uniewinnionego przez Wojskowy Sąd Okręgowy w Poznaniu[169], czyn oskarżonego miał polegać na tym, że

[165] F. Radoniewicz, *Odpowiedzialność karna za hacking*…, s. 316.

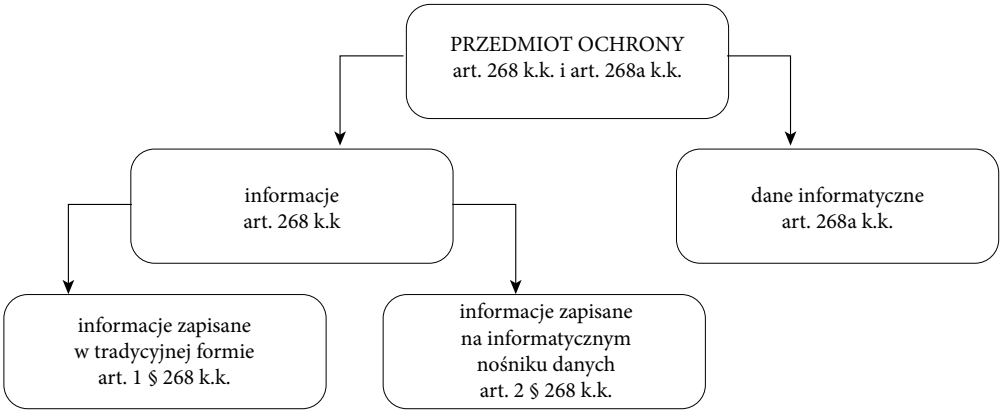
[166] Tamże, s. 311.

[167] S. Hoc, *Komentarz do art. 268a kk, teza G*, [w:] *Kodeks karny. Komentarz*, red. R. Stefański, Legalis 2021. Autor powołuje się na: B. Kunicką-Michalską, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Komentarz*, Komentarze Karne Becka, s. 725, [w:] L. Gardocki, *Komentarz do art. 268a*, SPK t. 8, red. Gardocki 2018, Legalis; autor powołuje się na: J. Piórkowskaą-Flieger, [w:] *Kodeks karny. Komentarz*, red T. Bojarski, Wolters Kluwer 2009, s. 597; B. Kunicka-Michalska, *Komentarz do art. 268a k.k.*, [w:] *Kodeks karny. Część szczególna, Komentarz do artykułów 222–316*, t. 2, red. A. Wąsek, R. Zawłocki, Duże Komentarze Becka 2010.

[168] S. Hoc, *Komentarz do art. 268a kk*…

[169] Wyrok Wojskowego Sądu Okręgowego w Poznaniu z dnia 6 listopada 2008 r., So 30/07, LEX.

od listopada 2001 r. do marca 2002 r. jako dowódca jednostki wojskowej bezpodstawnie zatrzymywał korespondencję st. chor. sztab. W. T. w postaci skarg kierowanych do zwierzchników. Skargi te zostały zarejestrowane w kancelarii tajnej, a następnie przekazane oskarżonemu, który poczynił na nich stosowne adnotacje wiarygodnie odzwierciedlające jego stosunek do istoty pism i podjęte działania służbowe. Czynności takie, wskazał sąd w uzasadnieniu do wyroku, nie spowodowały zniekształcenia treści skarg; pisma nie zostały też w wyniku działania oskarżonego zdekompletowane, nie zniszczono zapisu informacji zawartych w tych skargach. Oskarżony po zapoznaniu się ze skargami i uznaniu, że zostały złożone z naruszeniem drogi służbowej, zainicjował wszczęcie postępowań dyscyplinarnych, czyniąc tym samym wskazane skargi relewantnym elementem tych postępowań, mając jednocześnie świadomość, że w przypadku niekorzystnego dla niego rozstrzygnięcia dyscyplinarnego skarżący nie zawaha się wykorzystać dostępnych środków prawnych w celu wykazania nietrafności decyzji przełożonego, co spowoduje, że z pismami zapozna się organ dyscyplinarny – zawyrokował sąd. Widać zatem, że przedmiotem czynności wykonawczej z art. 268 § 1 k.k. był tradycyjny zapis informacji, tj. kartki, których treść stanowiła „skargi" podwładnego żołnierza na zachowanie jego dowódcy.



Grafika nr 7. Przedmiot ochrony w poszczególnych przepisach art. 268 k.k. i art. 268a k.k.

Czynność sprawcza oraz postać zamiaru podmiotu realizującego przestępstwo z art. 268 k.k. nie są ukierunkowane na uzyskanie dostępu do informacji lub zapoznanie się z nią, ale na bezprawną ingerencję w treść informacji, poczynając od jej zmiany, a kończąc na anihilacji informacji. Obrazowo można powiedzieć, że art. 268 § 1 k.k. ma zastosowanie do „świata realnego" w tym znaczeniu, że chodzi w nim o informację zapisaną w tradycyjnej formie, a czyn może polegać na fizycznym zniszczeniu nośnika danej treści, np. papieru lub kliszy fotograficznej[170]. W. Wróbel i D. Zając, w kontekście znamion art. 268 k.k., mówią także o zniszczeniu nośnika cyfrowego. Jednak w momencie

[170] W. Wróbel, D. Zając, *Art. 268…*, *tezy 7 i 10.*

fizycznego niszczenia np. dysku twardego, kryptowalutowego portfela sprzętowego czy pendrive'a, sprawca nie widzi zapisanych na nośniku informacji, a więc swoim działaniem wypełnia znamiona art. 268a § 2 k.k., a nie § 1 art. 268 k.k. Oczywiście, można sobie wyobrazić sytuację, że niszczenie fizyczne dysku następuje w momencie, gdy pokrzywdzony zapoznaje się z informacją, np. czyta na monitorze treść odtworzoną z dysku, i wtedy można mówić o popełnieniu przestępstwa z art. 268a § 1 k.k., ale w praktyce będą to sytuacje zupełnie wyjątkowe. Działanie sprawcy, w kontekście znamion art. 268 § 1 k.k., nie musi się odnosić do samego zapisu informacji bądź nośnika, na którym został on sporządzony, ale przestępstwo zostanie popełnione także wówczas, gdy sprawca ukryje nośnik informacji (schowa list adresowany do innej osoby) lub zastosuje szczególne utrudnienia w dostępie do nośnika lub do samej informacji, m.in. przez zmianę kodu w sejfie.

Przechodząc do przestępstw teleinformatycznych, to rozpatrywane są one w kontekście art. 268 § 2 k.k., a nie § 1, gdyż dopiero w drugiej części redakcyjnej przepisu pojawia się „informatyczny nośnik danych". W pierwotnym brzmieniu tego przepisu była mowa o „komputerowym nośniku danych", ale pojęcie takie ma zbyt wąski zakres znaczeniowy i dlatego w 2008 r. zapis „komputerowy" zastąpiono określeniem „informatyczny"[171]. Definicja legalna „informatycznego nośnika danych" znajduje się w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[172]. W art. 3 pkt 1 wskazano: „informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej", a więc chodzi o pendrive'a, kartę pamięci SD, kartę płatniczą z mikroprocesorem, płytę CD, serwer itd. Badania aktowe wykazały szereg błędów w kwalifikacji prawnej i opisie czynów z art. 268 k.k. oraz art. 268a k.k.; dotyczy to chociażby wyroku wydanego przez Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie, gdzie kobieta została uznana za winną tego, że:

> w dniu 15 lutego 2010 r. w Krakowie nie będąc do tego uprawnioną zmieniła zapis istotnej informacji na komputerowym nośniku informacji i usunęła konto Nasza Klasa czym znacznie utrudniła osobie uprawnionej D. Ś zapoznanie się z przedmiotową informacją, tj. o przestępstwo z art. 268 § 2 k.k.[173]

Oskarżona wyjaśniła, że najpierw dokonała nieuprawnionych wpisów na koncie pokrzywdzonego w portalu Nasza Klasa, a potem usunęła to konto, chcąc zemścić się na byłym partnerze. Ustalono, iż kobieta posiadała dane uwierzytelniające do konta,

[171] Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. z 2008 r. Nr 171, poz. 1056).

[172] Dz. U. z 2020 r. poz. 346, 568, 695, dalej jako: ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.

[173] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 787/10/N.

ponieważ gdy była w związku z pokrzywdzonym, razem logowali się do Naszej Klasy z jej komputera i przeglądarka zapamiętała hasło. Przechodząc do oceny wyroku, to razi niefrasobliwość sądu, który użył znamienia „komputerowy nośnik informacji", a więc odbiegającego od brzmienia przepisu („informatyczny nośnik danych"). Nie ma tutaj mowy o dopuszczalnej modyfikacji językowego brzmienia treści przepisu, bowiem na gruncie rozdziału XXXIII k.k. „informacje" to coś zupełnie innego, aniżeli „dane"[174]. Rodzi się ponadto wątpliwość, czy usunięcie konta, o czym zeznał sprawca, nie spowodowało bezpowrotnej utraty informacji, a nie tylko, jak przyjął sąd, „znacznego utrudnienia" zapoznania się z nimi.

W kolejnej sprawie ustalono, że oskarżona bez uprawnienia uzyskała dostęp do konta innej kobiety założonego na Naszej Klasie i wysyłała wiadomości do jej znajomych oraz usuwała komentarze przychodzące; zmieniła także hasła dostępu i dlatego A. G. nie mogła zapoznać się z rozsyłanymi w jej imieniu wiadomościami, których treść poznała od znajomych. Oskarżona włamała się do portalu w akcie zemsty, gdyż wcześniej romansowała z mężem pokrzywdzonej. W trakcie przesłuchania w charakterze podejrzanego kobieta wyjaśniła, że „Pierwszy raz wchodząc [na konto pokrzywdzonej – przyp. autora] i wpisując login i hasło nie sądziłam, że wejdę na jej hasło że to się uda. A kiedy się udało pchała mnie do tego ludzka ciekawość"; „Ja login i hasło odgadłam sama, ja wcześniej miałam dostęp do komputera jej męża A., ja nie pamiętam czy tam gdzieś widziałam to hasło. Ja zalogowałam się na konto Naszej Klasy metodą prób i błędów i udało mi się to po kilku próbach". Wyrok skazujący, wydany w niniejszej sprawie przez Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie, brzmiał następująco:

> w bliżej nieokreślonych dnach i miesiącach w okresie czasu od stycznia 2010 roku do 8 czerwca 2010 roku w Krakowie nie będąc osobą uprawnioną uzyskała dostęp do informacji dla niej nieprzeznaczonej poprzez przełamanie elektroniczne zabezpieczenia portalu Nasza Klasa oraz w dniu 8 czerwca 2010 roku wysyłała wiadomości do innych użytkowników portalu i kasowała korespondencję osoby uprawnionej, czym znacznie utrudniła osobie uprawnionej A. G. zapoznanie się z nią, tj. o przestępstwo z art. 267 § 1 k.k. i art. 268 § 2 k.k. w zw. z art. 11 § 2 k.k.[175]

[174] Brak ścisłego rozróżnienia pomiędzy tymi znamionami czynów zabronionych, które określane są przez ustawodawcę jako „informacje" i „dane informatyczne", stanowi powód wielu błędów popełnianych w wykładni prawa przez organy procesowe i przedstawicieli doktryny. W jednej z książek, nomen omen cennej i jedynej tak szczegółowej pozycji na rynku, autor, analizując art. 268 § 2 k.k., opisuje przedmiot czynności wykonawczej jako „niszczenie nośnika" danych informatycznych czy godzenie w integralność danych poprzez „działanie o charakterze logicznym, polegające np. na ich kasowaniu, usuwaniu, często za pomocą specjalnych programów, takich jak wirusy, robaki, trojany. Dane na informatycznym nośniku danych można unicestwić również poprzez działania fizyczne, np. niszcząc nośnik czy uszkadzając go (np. poprzez umieszczenie w polu elektromagnetycznym)". Odwołuje się zatem do czynów wypełniających znamiona art. 268a § 1 k.k., gdyż przedmiotem zamachu w art. 268 § 2 k.k. jest informacja, a więc treść nosząca sens dla człowieka, a nie dane informatyczne; zob. F. Radoniewicz, *Odpowiedzialność karna za hacking*…, s. 312.

[175] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 1094/10/N.

Nieprawidłowa była kwalifikacja prawna czynu przyjęta w wyrokach Sądu Rejonowego w Bydgoszczy oraz Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu. Mężczyźni zostali uznani za winnych tego, że:

> w okresie od 30 sierpnia 2012 r. do 12 października 2012 r. pomimo ustania stosunku pracy nie udostępnił dyrekcji Zespołu Szkół Ogólnokształcących nr /…/ haseł dostępowych do konta /…/ serwera szkoły, do których miał dostęp jako administrator sieci informacyjnej, czym utrudniał dostęp do systemów informatycznych i działał na szkodę Zespołu Szkół Ogólnokształcących nr /…/, tj. o czyn z art. 268a § 1 k.k.[176]

> w dniu 22 grudnia 2015 r. w nieustalonym dotąd miejscu, nie będąc do tego uprawnionym poprzez zmianę haseł do konta o nazwie /…/ użytkowanego przez N. W., utrudnił jej dostęp do danych informatycznych powiązanych z tym kontem tj. czynu z art. 268a § 1 k.k.[177]

Z art. 268a § 1 k.k. zakwalifikowano czyn polegający na znacznym utrudnieniu dostępu osobie uprawnionej (dyrektorowi szkoły) do zapisanych na informatycznym nośniku danych (serwerze) informacji w postaci (zapewne) danych osobowych uczniów szkoły, ich ocen z poszczególnych przedmiotów, obecności na lekcjach itp. Opis czynu wskazuje na popełnienie przez sprawcę przestępstwa z art. 268 § 2 k.k., a organ wyrokujący powinien posługiwać się legalnym zwrotem „informatyczny nośnik danych", zamiast pojęciem „system informatyczny" (zwrotu „system informatyczny" użyto w art. 269a k.k.). Gdyby w przedmiotowej sprawie serwer szkoły był częścią większego systemu informatycznego lub teleinformatycznego i brak dostępu do niego zakłócałby w istotnym stopniu pracę ww. systemu, to należałoby rozważyć przyjęcie kwalifikacji prawnej z art. 268 § 2 k.k. i art. 269a § 1 k.k. w zw. z art. 11 § 2 k.k. Jeśli chodzi o sprawę rozpoznaną przez Sąd Rejonowy Poznań-Nowe Miasto i Wilda w Poznaniu, to zamiar sprawcy włamania na konto indywidualnego użytkownika, założone na platformie społecznościowej czy handlowej, prawie zawsze ukierunkowany jest na uzyskanie dostępu do informacji, a nie danych. Nikt przecież, oprócz wysoko kwalifikowanych hakerów, nie „atakowałby" tych repetytoriów, gdyby po ich otwarciu wyświetlały się metadane kodu programu komputerowego służącego do budowania stron internetowych i ich zawartości, a nie tekst lub zdjęcia. A taki irracjonalny wniosek można by wysnuć z opisu czynu zamieszczonego w wyroku ww. sądu. Podobną sytuację rozpoznawał Sąd Rejonowy w Lipnie z tą różnicą, że sprawca wcześniej uzyskał bez uprawnienia dostęp do

[176] Wyrok Sądu Rejonowego w Bydgoszczy z dnia 1 grudnia 2014 r., IX K 126/14, LEX nr 1829043.
[177] Wyrok Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu z dnia 8 grudnia 2017 r., VI K 358/17, LEX nr 2415381.

„dwóch kont A. C. na portalu społecznościowym F.", a więc do informacji dla niego nieprzeznaczonych; mężczyzna został skazany za to, że:

> w okresie od 23 listopada 2013 r. do dnia 20 grudnia 2013 r. w /…/ bezprawnie uzyskał dostęp do informacji dla niego nie przeznaczonych znajdujących się na dwóch kontach A. C. na portalu społecznościowym F. poprzez wykorzystanie znanego mu hasła dostępu a następnie nie będąc do tego uprawnionym dokonał zmiany haseł dostępu do danych informatycznych tj. o czyn z art. 267 § 1 k.k. i 268a § 1 k.k. w zw. z art. 11 § 2 k.k.[178]

Uniemożliwienie właścicielce zalogowania się do konta było równoznaczne z tym, że nie mogła ona zapoznać się z informacjami, a nie danymi informatycznymi, jak napisał sąd. Brak zatem w opisie czynu znamienia skutku, o którym mowa w art. 268 § 2 k.k. („udaremnienie osobie uprawnionej zapoznania się z informacją"). Prawidłowa kwalifikacja prawna czynu powinna zatem być następująca: art. 267 § 1 k.k. i art. 268 § 2 k.k. w zw. z art. 11 § 2 k.k. Przyjmowanie przez sądy, jeśli czyn dotyczy informacji znajdujących się na internetowym koncie, kwalifikacji z 268a § 1 k.k., zamiast art. 268 § 2 k.k., wynika z braku rozróżnienia pomiędzy informacją a danymi informatycznymi, o czym już parokrotnie przypomniano. Prawidłowo procedował natomiast Sąd Rejonowy Gdańsk-Południe w Gdańsku, chociaż w treści wyroku brak znamienia przestępstwa „nie będąc do tego uprawnionym", gdy skazał mężczyznę za to, że:

> w dniu 6 października 2014 r. w nieustalonym miejscu dokonał usunięcia danych informatycznych zgromadzonych na dysku twardym komputera przenośnego marki T. model /…/ o nr ser 881 /…/, stanowiącego własność /…/ sp. z o.o. czym działano na szkodę ww. spółki, tj. o czyn z 268a § 1 k.k.[179]

W trzech kolejnych wyrokach sądy stwierdziły, że zanim sprawca przestępstwa wypełnił znamiona z art. 268a § 1 k.k., to bez uprawnienia uzyskał dostęp do całości lub części systemu informatycznego. Skoro bowiem przedmiotem czynności wykonawczej były dane informatyczne, gdyż art. 268a § 1 k.k. mówi o takich danych, to w orzeczeniach wskazywano na „bezprawne uzyskanie dostępu do danych informatycznych", „zmianę danych", „modyfikację zawartości bazy danych" oraz „usunięcie danych informatycznych". Warto jednak zbadać, czy podsądni rzeczywiście operowali na danych informatycznych, czy jednak na informacjach. Zostali oni skazani za to, że:

[178] Wyrok Sąd Rejonowy w Lipnie z dnia 15 lutego 2016 r., II K 313/14, LEX nr 2243448.
[179] Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 14 grudnia 2017 r., X K 806/16, LEX nr 2785661.

w dniu 30 listopada 2014 r. bezprawnego uzyskania dostępu do danych informatycznych znajdujących się na skrzynce pocztowej e-mail w.gaudyn@gmail.com przez osobę nieupoważnioną poprzez przełamanie zabezpieczenia w postaci hasła, a następnie usunięcie wybranych danych informatycznych przez sprawcę działającego w ten sposób na szkodę W. G., tj. o czyn z art. 268a § 1 k.k.[180]

w dniu 16 czerwca 2013 r. w G. /…/, nie będąc osobą uprawnioną, poprzez przełamanie hasła na portalu allegro.pl dokonał wejścia na konto o N. /…/, należącego do J. J. po czym zmienił dane i umieścił ogłoszenie o sprzedaży telefonu komórkowego S. /…/, modyfikując zawartość baz danych, działając w ten sposób na szkodę ww., tj. o czyn z art. 268a § 1 k.k.[181]

w dniu 15 września 2012 r. w B., nie będąc do tego uprawnionym, za pomocą haseł administratora zalogował się do serwera /…/ sp. z o.o. w R., a następnie z dysków usunął dane informatyczne w postaci plików i katalogów: baza klientów, księgowość, kadry, płace, system obsługujący cykl produkcyjny i inne pochodne dane, wyrządzając tym samym wyżej wymienionemu pokrzywdzonemu szkodę nie mniejszą niż 22.020 zł, tj. przestępstwa z art. 268a § 1 k.k.[182]

Jedynie z treści wyroku Sądu Okręgowego w Gliwicach można domniemywać, iż w rzeczywiści przedmiot czynności wykonawczej osądzonego czynu stanowiły dane informatyczne, gdyż sprawca manipulował zapisem bezpośrednio na poziomie serwera. Jeśli jednak uzyskał bez uprawnienia dostęp do części lub całości systemu informatycznego, a serwer niewątpliwie jest głównym elementem takiego systemu, to jego czyn powinien zostać zakwalifikowany z art. 267 § 2 k.k. i art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k. Czym innym jest bowiem usuwanie bez uprawnienia danych informatycznych, którego dokonuje osoba mająca prawo dostępu do tych danych (np. administrator systemu), a czym innym uzyskanie bez uprawnienia dostępu do systemu przez sprawcę, a następnie usunięcie danych. W jednym z wyroków sąd stwierdził, że oskarżony „uzyskał dostęp do zawierających dane informatyczne serwerów /…/ Sp. z o.o.", a więc kwalifikacja prawna hakingu, w zbiegu z art. 268a § 1 k.k., powinna przyjąć postać art. 267 § 2 k.k. Przepisu tego zabrakło w kwalifikacji prawnej poniższego wyroku, gdzie sprawca został uznany za winnego tego, że:

[180] Postanowienie Sądu Rejonowego w Siedlcach z dnia 23 września 2015 r., VII Kp 203/15, LEX nr 1922632.

[181] Wyrok Sądu Rejonowego w Jaworznie z dnia 7 grudnia 2015 r., II K 621/14, LEX nr 2155219. Na gruncie orzeczenia Sądu Rejonowego w Jaworznie pojawia się problem, jak zakwalifikować „wprowadzenie nowych informacji", skoro takiej czynności czasownikowej nie przewiduje art. 268 § 1 k.k. W tym temacie wypowiedział się Sąd Najwyższy, o czym będzie jeszcze mowa przy analizie uzasadnienia do wyroku Sądu Apelacyjnego w Warszawie z dnia 21 grudnia 2015 r., II AKa 409/15, LEX nr 2031083

[182] Wyrok Sądu Okręgowego w Gliwicach z dnia 17 kwietnia 2015 r., VI Ka 51/15, LEX nr 1831810.

> w dniu 25 sierpnia 2011 w J. nie będąc do tego uprawnionym uzyskał dostęp do zawierających dane informatyczne serwerów /…/ Sp. z o.o. i zmieniając zapis w plikach konfiguracyjnych systemu operacyjnego poprzez zmianę hasła i odebranie uprawnień administratora utrudnił osobom uprawnionym dostęp do tych danych, tj. czynu z art. 268a § 1 k.k.[183]

Zdarzają się sytuacje odwrotne, gdy sąd ustalił, że oprócz wypełnienia znamion art. 267 § 1 k.k. przestępca modyfikuje także informacje na koncie, które zapisane są na informatycznym nośniku danych, a mimo tego nie przywołuje się w kwalifikacji prawnej art. 268 § 2 k.k. W wyroku Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie mężczyzna został uznany za winnego tego, że:

> w dniu 16 marca 2012 r. o godz. 23:33:04 w W. /…/ w miejscu swojego zamieszkania korzystając z adresu IP /…/ przydzielonego przez dostawcę usługi dostępu do sieci Internet /…/ Sp. z o.o. w W. działając bez uprawnienia w bliżej nieustalony sposób przełamał hasło stanowiące zabezpieczenie skrzynki pocztowej o nazwie /.../@op.pl należącej do J. A. uzyskując w ten sposób dostęp do informacji dla siebie nieprzeznaczonej a następnie zmienił hasło dostępu uniemożliwiając J. A. dostęp do wyżej wymienionej skrzynki pocztowej, tj. o czyn z art. 267 § 1 k.k.[184]

Powracając do orzeczenia Sądu Rejonowego w Siedlcach, to sąd ustalił, że oskarżony uzyskał dostęp do „skrzynki pocztowej e-mail /.../@gmail.com", a Sąd Rejonowy w Jaworznie stwierdził, że sprawca „dokonał wejścia na konto o N." na portalu Allegro.pl. Nie budzi zatem wątpliwości, że sprawcy ci działali z zamiarem uzyskania dostępu do informacji, a nie danych informatycznych, i poprzez przełamanie zabezpieczenia rzeczywiście zapoznali się z wiadomościami umieszczonymi w skrzynce poczty elektronicznej oraz na koncie portalu aukcyjnego. Zatem treść zapadłych wyroków powinna brzmieć następująco:

> w dniu 30 listopada 2014 r. bez uprawnienia, poprzez ominięcie procedury uwierzytelnienia i użycie hasła dostępu należącego do W. G., uzyskał dostęp do informacji dla niego nieprzeznaczonych zapisanych na informatycznym nośniku danych dostarczyciela usługi pocztowej w postaci zawartości skrzynki poczty elektronicznej o adresie /.../@gmail.com i usunął zapis istotnych informacji stanowiących

[183] Wyrok Sądu Okręgowego w Gliwicach z dnia 29 grudnia 2016 r., V Ka 135/16, LEX nr 2206759.
[184] Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 29 stycznia 2016 r., VIII K 232/15, LEX nr 2148091.

części korespondencji znajdującej się w skrzynce, działając na szkodę W. G., tj. o czyn z art. 267 § 1 k.k. i art. 268 § 2 k.k. w zw. z art. 11 § 2 k.k.

w dniu 16 czerwca 2013 r. w G. /…/ bez uprawnienia, poprzez ominięcie procedury uwierzytelnienia i użycie hasła dostępu należącego do J. J., uzyskał dostęp do informacji dla niego nieprzeznaczonych zapisanych na informatycznym nośniku danych dostarczyciela usługi pocztowej w postaci zawartości konta na portalu Allegro należącego do pokrzywdzonej i zmienił zapis istotnych informacji poprzez umieszczenie na koncie ogłoszenia o sprzedaży telefonu komórkowego S. /…/, działając na szkodę J. J., tj. o czyn z art. 267 § 1 k.k. i art. 268 § 2 k.k. w zw. z art. 11 § 2 k.k.

Kolejna sprawa, gdy sąd pomylił „dane informatyczne" z „informacjami", dotyczy oskarżonej, która otrzymała hasła dostępu do strony internetowej firmy cateringowej przygotowującej posiłki i za zgodą właściciela restauracji uaktualniała menu. W momencie gdy pracodawca zwolnił z pracy jej matkę, oskarżona w akcie zemsty wprowadziła nowe zapisy w elektronicznym jadłospisie, które nie znajdowały pokrycia w rzeczywistości. Spowodowało to kłopoty ze sprzedażą posiłków; pokrzywdzony zeznał, że nie mógł przywrócić odpowiedniego zapisu i poniósł straty finansowe w wysokości co najmniej 1000 zł, gdyż klienci byli zdezorientowani informacjami, jakie oskarżona zamieszczała na witrynie internetowej, dotyczącymi m.in. ceny produktów i godzin otwarcia lokalu. Strona została „zablokowana" przez oskarżoną w taki sposób, że nawet informatyk nie mógł odzyskać praw administratora. Wyrok skazujący brzmiał następująco:

w dniu 18 i 19 grudnia 2012 r. w Krakowie korzystając z urządzenia o zmiennym numerze IP działając w sieci Play dokonała nieuprawnionej zmiany na stronie internetowej /…/ danych informatycznych w postaci cen potraw dań oferowanych do sprzedaży oraz wprowadziła na tej stronie błędne informacje na temat godzin otwarcia formy na szkodę K. i. A. z d. /…/, tj. o przestępstwo z art. 268a § 1 k.k.[185]

W sprawie należało rozważyć, czy czynność sprawcza oskarżonej była przestępstwem trwałym, czy została zrealizowana w ramach czynu ciągłego (kobieta wyjaśniła, że dwa razy zalogowała się na stronę internetową i dokonywała zmian jej treści, tj. 18 i 19 grudnia). Dodatkowo pokrzywdzony zeznał, że „poniósł straty w wysokości co najmniej 1000 zł z powodu umieszczenia na stronie restauracji błędnych informacji dla klientów oraz braku możliwości zalogowania się na konto". W opisie czynu należało uwzględnić wysokość szkody materialnej i orzec środek karny w postaci obowiązku jej

[185] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1168/13/P.

naprawienia, czego sąd nie uczynił. Dochodzą do tego ewidentne błędy językowe: sąd napisał „formy" zamiast „firmy" i „ceny potraw dań", a przecież „potrawy" i „dania" to synonimy. Mając powyższe na uwadze, a przede wszystkim fakt, że strona zawierała informacje dla klientów, a właściciel firmy cateringowej w wyniku przestępstwa został pozbawiony dostępu do danych informatycznych tworzących stronę, to opis czynu mógłby mieć następującą postać:

> w dniu 18 i 19 grudnia 2012 r. w Krakowie działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru i nie będąc do tego uprawnioną zmieniła zapisy istotnych informacji dla funkcjonowania firmy cateringowej /…/ o zestawie oferowanych dań i godzinach otwarcia lokalu zamieszczone na stronie internetowej ww. firmy oraz uniemożliwiła właścicielowi firmy dostęp do danych informatycznych tworzących ww. stronę internetową działając na szkodę /…/ w wysokości nie mniejszej, niż 1000 zł, tj. o przestępstwo z art. 268 § 2 k.k. i art. 268a § 1 k.k. w zw. z art. 12 k.k.

Gdy bazuje się na opisie czynów, dane informatyczne rzeczywiście mogły być przedmiotem zamachu w sytuacjach opisanych w postanowieniu Sądu Rejonowego w Dzierżoniowie, wyroku Sądu Rejonowego dla Krakowa-Podgórza w Krakowie oraz Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie. W sprawie dzierżoniowskiej zarzut dotyczył:

> zaistniałego w nieokreślonym czasie, w okresie do dnia 15 marca 2016 r., w D., utrudniania dostępu do danych informatycznych oraz w istotny sposób uniemożliwianie przetwarzania takich danych J. P., poprzez przejęcie identyfikatora sieciowego, a także poprzez przejęcie dotychczas używanych systemów w sieci /…/, to jest o czyn z art. 268a § 1 k.k.[186]

Z kolei sądy krakowskie skazały sprawczynię przestępstw teleinformatycznych za to, że:

> w dniu 22 grudnia 2011 roku w Krakowie, nie będąc do tego uprawnioną, usunęła wszelkie dane ze służbowego laptopa marki /…/ na szkodę /…/ spółki jawnej z siedzibą w Krakowie (obecnie /…/ z siedzibą w Krakowie), tj. o przestępstwo z art. 268a § 1 k.k.[187]

[186] Postanowienie Sądu Rejonowego w Dzierżoniowie z dnia 27 czerwca 2016 r., II Kp 171/16, LEX nr 2080684.
[187] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 559/15/P.

> w dniu 16 czerwca 2009 r. w Krakowie bez uprawnienia uzyskała dostęp do internetowego konta pocztowego „/…/@vp.pl" znajdującego się na portalu internetowym Onet.pl, a następnie zmieniła hasło dostępu do tego konta i kopiowała dane informatyczne w nim znajdujące się, uniemożliwiając tym samym G. K. korzystanie z zapisanych tam danych informatycznych, a w szczególności przetwarzanie, dalsze gromadzenie i przekazywanie takich danych, tj. za winną przestępstwa z art. 267 § 1 k.k. w zw. z art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k.[188]

Z treści ww. orzeczeń wynika, że sprawca nie działał w zamiarze usunięcia lub zmodyfikowania konkretnej informacji, nie zapoznawał się z komunikatami mającymi sens dla człowieka, tylko utrudnił automatyczne przetwarzanie cyfrowych artefaktów, chociaż w przypadku postanowienia Sądu Rejonowego w Dzierżoniowie należałoby rozważyć, czy nie doszło do wypełnienia znamiona art. 296a k.k. (w opisie czynu mowa jest o „uniemożliwieniu przetwarzania danych w istotny sposób"). W drugiej sprawie przestępca anihilował całość danych informatycznych zapisanych na laptopie po to, aby jego pracodawca nie mógł z nich skorzystać. W innej sprawie Sąd Rejonowy dla Krakowa-Podgórza w Krakowie uniewinnił mężczyznę oskarżonego o to, że:

> nie będąc do tego uprawnionym – usunął z pamięci komputera przenośnego marki Lenovo ThinkPad R400 o nr seryjnym /…/ zapisy stanowiące istotne informacje dla Spółki /…/ w postaci m.in. korespondencji prowadzonej z kontrahentami Spółki w zakresie współpracy handlowej, realizacji umów i treści składanych ofert, tj. o przest. z art. 268 § 2 k.k.[189]

Zdaniem sądu, co prawda oskarżony, nie będąc do tego uprawniony, usunął z pamięci komputera dane stanowiące istotne informacje dla pokrzywdzonego, jednakże czyn taki nie stanowił przestępstwa, bowiem działanie oskarżonego nie udaremniło ani też nie utrudniło w sposób znaczny osobie uprawnionej zapoznania się z usuniętymi danymi. Przywrócenie takich danych nie było, zdaniem sądu, możliwe co prawda w trybie standardowej pracy z komputerem i wymagało skorzystania ze specjalistycznego oprogramowania, ale skoro zdaniem biegłego dało się to wykonać przez osobę dysponującą przeciętną wiedzą informatyczną, to tym bardziej mógł to zrobić administrator spółki. W uzasadnieniu wyroku sąd napisał także, że skala trudności w odzyskaniu danych ograniczała się w zasadzie wyłącznie do kwestii finansowych, tj. do zaopatrzenia się w stosowne oprogramowanie i dysponowania umiejętnościami posługiwania się nim w odpowiedni sposób.

[188] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 44/10/S.
[189] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. XI K 971/13/P.

Stanowisko sądu jest błędne. Przepis art. 268 § 2 k.k. mówi o tym, że odzyskanie usuniętego/zmienionego zapisu danych na informatycznym nośniku informacji musi być „udaremnione lub znacznie utrudnione". Słowo „udaremnić" oznacza „sprawić, że coś nie zostanie zrealizowane, nie dojdzie do skutku". „Utrudnić", z kolei, to „stanowić lub stworzyć przeszkodę, uczynić trudnym". Sąd Najwyższy[190] orzekł, że znamię „znacznego utrudnienia osobie uprawnionej zapoznania się z informacją" sprowadza się do tego, iż odczytanie informacji wymaga znacznego nakładu czasu lub wysiłku, bądź też do tego, że informacja, z którą zapoznaje się uprawniony, ma charakter niekompletny lub zniekształcony. W omawianej sprawie zasady doświadczenia życiowego i logicznego rozumowania każą wątpić w stwierdzenie sądu rejonowego jakoby odzyskanie danych uwarunkowane „zakupem specjalistycznego oprogramowania" i posiadaniem „przeciętnej wiedzy informatycznej" gwarantującej jego obsługę nie stanowiło „znacznego utrudnienia" w rozumieniu art. 268 § 2 k.k. Stanowisko zaprezentowane przez sąd oznaczałoby w praktyce, że każda osoba, zanim zgłosi podejrzenie popełnienia przestępstwa z art. 268 § 2 k.k., powinna zakupić specjalistyczne oprogramowanie i sama sprawdzić, czy za jego pomocą odzyska utracone dane. Znamię „znacznego utrudnienia" należy rozpatrywać w kontekście możliwości technicznych i umiejętności informatycznych konkretnego pokrzywdzonego, czy bez dodatkowych, szczególnych nakładów ma możliwość odtworzenia zniszczonych/zmienionych zapisów. Szczególnie że w omawianej sprawie nawet pracownicy pokrzywdzonej spółki z branży IT sami nie potrafili odtworzyć danych skasowanych z dysku twardego laptopa. Z kolei biegły do ich odzyskania użył, jak wynikało z opinii, specjalistycznego stanowiska badawczego składającego się m.in. z wysokiej klasy komputerów, kilku dysków twardych i oprogramowania X-Ways Forensics. Dlatego błędny był wywód sądu, że dla odzyskania danych wystarczyła przeciętna wiedza informatyczna, a „skala trudności czynności pozwalających odzyskać przedmiotowe dane – ograniczona w zasadzie wyłącznie do kwestii finansowych tj. faktu zaopatrzenia się w stosowne oprogramowanie oraz do dysponowania umiejętnościami posłużenia się nim w odpowiedni sposób". Sąd nie sprecyzował, co oznacza „wyłącznie kwestie finansowe", o zakup jakiego oprogramowania chodzi i ile ono kosztuje. Logiczne jest natomiast, że jeśli ma się korzystać ze „specjalistycznego oprogramowania", to trzeba posiadać ku temu „specjalistyczną wiedzę".

Badania akt spraw karnych dotyczących przestępstw teleinformatycznych pokazały, że zastrzeżenia w niektórych przypadkach budził zbyt ogólnikowy opis sposobu działania sprawcy, jeśli chodzi o znamię czasownikowe czynu. Może to powodować niejasność, za co sprawca został skazany i co w konkretnych okolicznościach faktycznych stanowiło działanie naruszające prawo. Sytuacja taka zaistniała w postępowaniu Sądu Apelacyjnego w Warszawie, rozpatrującego sprawę osoby skazanej za to, że:

[190] Postanowienie Sądu Najwyższego z dnia 29 września 2009 r., OSNwSK 9009, nr 1, poz. 1903.

w dniu 9 kwietnia 2009 r. w W., będąc zatrudnionym w /…/ sp. z o.o. z siedzibą w W. na stanowisku kierownika ds. kluczowych klientów, dokonał włamania na konto internetowe M. L. /…/ poprzez pokonanie zabezpieczeń, a następnie w celu użycia za autentyczny podrobił dokument elektroniczny w postaci e-mail w ten sposób, że podrobił treść wiadomości e-mail /…/, następnie posłużył się tym dokumentem jako autentycznym i przesłał korzystając z prywatnego adresu IP na swoją pocztę /…/, tj. o czyn z art. 268a § 1 k.k.[191]

Pomijając już fakt, że w kwalifikacji prawnej brak art. 267 § 1 k.k., to podrobienie dokumentu, którego definicja legalna znajduje się w art. 115 § 14 k.k., penalizuje art. 270 § 1 k.k., a nie art. 268a § 1 k.k., zastrzeżenia co do prawidłowości opisu czynu i jego kwalifikacji prawnej we wskazanym wyroku zgłosił Sąd Najwyższy. Stwierdził on, że przestępstwo przypisane skazanemu budzi poważne wątpliwości, zwłaszcza że sąd nie poświęcił praktycznie w ogóle miejsca na rozważania natury prawnej o znamionach typu czynu z art. 268a k.k. Wobec powyższego nie było jasne, które znamię tego typu czynu zabronionego – zdaniem sądów I i II instancji – skazany zrealizował. Treść zapadłych wyroków nie wskazywała bowiem, czy w przypadku napisania wiadomości mailowych z poziomu cudzej skrzynki pocztowej chodzi o niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo w istotny sposób zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (art. 268a § 1 k.k.). Sąd Najwyższy stwierdził natomiast, że w takim przypadku chodzi niewątpliwie o stworzenie zupełnie nowych danych informatycznych. Zatem nie można mówić o niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu, gdyż czynności te zakładają uprzednie istnienie danych informatycznych w systemie: niszczy się wszakże coś już istniejącego. Trudno także uznać takie zachowanie jako zakłócające w istotnym stopniu lub uniemożliwiające automatyczne przetwarzanie, gromadzenie lub przekazywanie danych. Wszakże nie zarzucono skazanemu ingerowanie w już sporządzone maile lub wprowadzenie takich zmian, że automatyczne procesy na serwerach dostawcy usługi pocztowej zostały zakłócone. Wobec powyższego, stwierdził Sąd Najwyższy, przyjęta kwalifikacja prawna budziła daleko idące wątpliwości. Co istotne, Sąd Najwyższy sformułował dwie podstawowe kwestie dla wykładni znamion art. 268a § 1 k.k.: po pierwsze, w każdym przypadku opisu czynu należy wskazać, którą czynność czasownikową zrealizował sprawca. Kolejna rzecz: nie każdy zapis w systemie informatycznym powoduje zakłócenie lub uniemożliwienie w istotnym stopniu automatycznego przetwarzania, gromadzenia lub przekazywania danych[192].

[191] Wyrok Sądu Apelacyjnego w Warszawie z dnia 21 grudnia 2015 r., II AKa 409/15, LEX nr 2031083.
[192] Tamże.

Oprócz najczęstszych spraw związanych z włamaniami do skrzynek mailowych i kont na platformach społecznościowych, niektóre przestępstwa mają bardziej nietypowy charakter. Dowodzi tego przypadek zakłócenia przesyłania danych informatycznych w celu kradzieży paliwa. Firma, która zajmowała się przewozem oleju napędowego na rynku dystrybucji paliw, zamontowała elektroniczne zabezpieczenia w naczepach ciągników, gdyż podczas przewozów paliwa cysternami dochodziło do nieuzasadnionych ubytków płynu z komór cysterny. Okazało się, że oskarżony zamontował na czujniku otwarcia klapy skrzyni załadunkowej naczepy urządzenie zagłuszające sygnał GPS i w ten sposób zakłócił pracę systemu przesyłającego dane z cysterny do serwera firmy w taki sposób, że otwarcie klapy nie powodowało przesłania informacji o tym zdarzeniu. Sprawca przestępstwa został skazany za czyn polegający na tym, że:

> w dniu 22 lipca 2014 roku w miejscowości P. woj. łódzkie, nie będąc do tego uprawnionym w istotnym stopniu zakłócił automatyczne przekazywanie danych informatycznych pomiędzy systemem komputera zainstalowanym w skrzyni załadunkowej cysterny składającej się z naczepy m-ki LAG nr rej. /…/ i ciągnika siodłowego m-ki Scania nr rej. /…/ a systemem komputerowym kontrolowanym przez /…/ Sp. z o.o. z siedzibą w Sandomierzu, co stanowi występek z art. 268a § 1 k.k.[193]

Pojęcie zakłócenia automatycznego przetwarzania, przekazywania lub gromadzenia danych informatycznych obejmuje bowiem wszelkie czynności oddziałujące na te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych treści. Uniemożliwienie natomiast oznacza zatrzymanie tych procesów lub niemożność ich podjęcia[194]. W niniejszej sprawie oskarżony, wykorzystując specjalne urządzenie, uniemożliwił automatyczne przekazywanie danych informatycznych pomiędzy systemem komputera zainstalowanym w skrzyni załadunkowej cysterny a odbiornikiem danych znajdującym się w siedzibie firmy.

3.6. Zakłócenie pracy systemu komputerowego (art. 269a k.k.)

Przedmiotem czynności wykonawczej z art. 296a k.k. są dane informatyczne, a sprawca swoim działaniem, które może polegać na „transmisji, zniszczeniu, usunięciu, uszkodzeniu, utrudnieniu dostępu lub zmianie" takich danych, powoduje skutek w postaci istotnego zakłócenia pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, chociaż w praktyce funkcjonowania „Internetu rzeczy" najczęściej dojdzie równocześnie do zakłócenia pracy systemu (systemów) oraz bezprawnej

[193] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 104/15/N.
[194] Wyrok Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15, LEX nr 1866883.

ingerencji w przesyłanie generowanych przez system danych. Jeśli o danych informatycznych była już mowa, to komentowany przepis zawiera nowe określenia: „system informatyczny", „system teleinformatyczny" i „sieć teleinformatyczna", a zatem wymagają one scharakteryzowania.

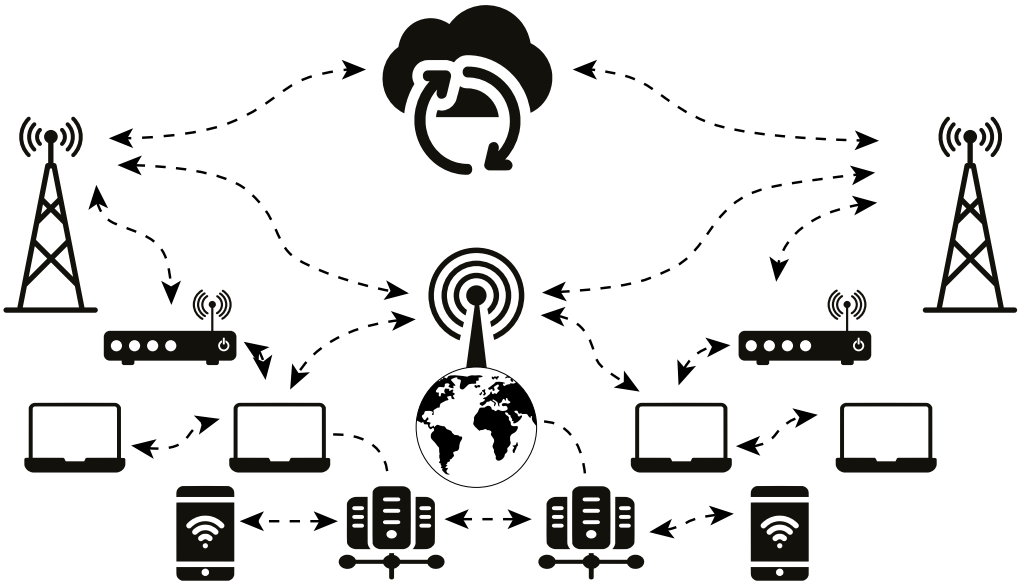
> Art. 269a. [Zakłócenie systemu komputerowego]
> Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej,
> podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

W Słowniku języka polskiego PWN system informatyczny określono jako zespół systemów komputerowych, sieci i oprogramowania, służący do przetwarzania informacji; w skład systemu informatycznego wchodzi z reguły komputer lub komputery (połączone w sieć lub pracujące osobno) wraz z oprogramowaniem, a także urządzenia pomocnicze („peryferyjne"), np. drukarki, skanery itp. System informatyczny może być uniwersalny lub przeznaczony do realizacji wąskiej klasy zadań, np. rezerwacji biletów lotniczych albo prowadzenia dokumentacji finansowo-księgowej przedsiębiorstwa[195]. Słownikowemu znaczeniu „systemu teleinformatycznego" odpowiada jego definicja legalna zawarta w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; chodzi o „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne"[196]. Termin „telekomunikacyjne urządzenie końcowe" został zdefiniowany w art. 2 pkt 43 ustawy Prawo telekomunikacyjne[197] jako „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci". Są to telefony (stacjonarne i komórkowe), tablety, komputery, faksy, drukarki, kryptowalutowy portfel sprzętowy – jednym słowem wszystkie urządzenia, dzięki którym można przesłać i odczytać dane informatyczne, po ich przetworzeniu przez algorytm, w formie rozmów telefonicznych, krótkich wiadomości SMS lub MMS, wiadomości mailowych oraz tych, dostarczonych komunikatorami typu Signal lub WhatsApp. Ostatecznie chodzi więc o zarządzanie danymi informatycznymi przetwarzanymi na „komunikat", tj. informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie

[195] https://encyklopedia.pwn.pl/haslo/system – informatyczny;3982203.html [dostęp: 23.06.2023].
[196] Zob. przypis 172.
[197] Zob. przypis 63.

dostępnych usług telekomunikacyjnych (art. 2 pkt 17 ustawy Prawo telekomunikacyjne). Wynika z tego, że rozgraniczenie pomiędzy „informatycznym nośnikiem danych" a „telekomunikacyjnym urządzeniem końcowym" sprowadza się do funkcji nawiązywania przez przedmiot komunikacji z urządzeniami zewnętrznym[198], gdyż to ostatnie stanowi końcowy element przetwarzania danych i uzyskania informacji przez człowieka.

System teleinformatyczny to, zgodnie z art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[199], zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy Prawo telekomunikacyjne. Z kolei mianem sieci teleinformatycznych określa się sieci telekomunikacyjne specjalizowane w celu zapewnienia usług wymiany informacji dla systemów informatycznych[200].



Grafika nr 8. Współdziałające urządzenia, systemy i sieci, które wspólnie tworzą systemy informatyczne, systemy teleinformatyczne i sieci teleinformatyczne

Trudno jest z kilku powodów wytyczyć ścisłe ramy pojęciowego znaczenia każdej z trzech opisanych wyżej kategorii, a tym bardziej fizycznie oddzielić od siebie w praktyce wszystkie trzy systemy. Widać chociażby, że definicje legalne „systemu

[198] P. Opitek, *Kontrola operacyjna urządzenia końcowego*…, s. 40.
[199] Dz. U. z 2020 r. poz. 344.
[200] J. Jarmakiewicz, *Sieci teleinformatyczne*, http://mml.pl/TT/wp – content/uploads/2016/05/Skrypt – TELEINFORMATYKA – 2002.pdf, s. 3–4 [dostęp: 23.06.2023].

teleinformatycznego" i „systemu teleinformatycznego", zawarte w dwóch różnych ustawach, w gruncie rzeczy brzmią identycznie. Poza tym odróżnienie ich od informatycznego nośnika danych ma umowny charakter, gdyż komputer w momencie pracy offline można uznać za informatyczny nośnik danych, a jeśli podłączy się go do Internetu, to staje się on częścią systemu informatycznego. Ponadto czynności wykonawcze z art. 269a k.k. mogą obejmować obszerny zakres tego, co nazywa się „sieciami teleinformatycznymi", stosowanymi niemalże w każdym obszarze aktywności ludzkiej; służą one do przetwarzania danych, transferu plików, automatyzacji prac biurowych, edycji tekstów, obsługi poczty elektronicznej, realizacji usług telefonicznych, telekonferencji, przesyłania sygnału radiowego i telewizyjnego itd.[201]

Odkodowując dalej znamiona tworzące art. 269a k.k., warto zacząć od odróżnienia ich od treści art. 268a § 1 k.k., szczególnie że oba przepisy mają podobne brzmienie. Czy jednak ustalenie między nimi precyzyjnej granicy jest w ogóle możliwe? Nie pomagają w tej kwestii orzeczenia sądów, które stosują zamiennie art. 268a § 1 k.k. i art. 269a k.k. w niemalże identycznych stanach faktycznych; za dowód tego posłuży kazus usunięcia konta w serwisie internetowym. Sąd Okręgowy w Bydgoszczy przyjął, że działanie takie wyczerpuje znamiona art. 269a k.k., i uznał oskarżonego za winnego tego, że:

> w dniu 10 października 2012 r. o godz. 18:17 nie będąc do tego uprawnionym, po uprzednim zalogowaniu się w serwisie internetowym /…/, do którego podłączony jest Zespół Szkół Ogólnokształcących Nr /…/ w B., dokonał w nim zmian poprzez usunięcie konta użytkownika przypisanego do jednego z nauczycieli, tj. P. D., tj. o czyn z art. 269a k.k.[202]

Jednak w orzeczeniach zacytowanych w podrozdziale pt. *Utrudnianie zapoznania się z informacją i niszczenie danych informatycznych (art. 268 k.k. i art. 268a k.k.)* podobne stany faktyczne sądy kwalifikowały z art. 268 § 2 k.k.[203], art. 268a § 1 k.k.[204] lub art. 268a § 2 k.k. Kolejna rzecz: zgodnie z dominującym w piśmiennictwie poglądem, nie zachodzi zbieg realny art. 269a k.k. z art. 268 k.k. i art. 268a k.k.[205], gdyż przepis art. 269a k.k. wyłącza na zasadzie konsumpcji stosowanie art. 268 k.k. i art. 268a k.k.[206] Jak zatem uporządkować przywołane kwestie w sytuacji, gdy nie wszystkie zaprezentowane twierdzenia są słuszne? Przykładowo, mylące jest stanowisko, że przepis art. 269a k.k.

[201] Tamże.
[202] Wyrok Sądu Okręgowego w Bydgoszczy z dnia 13 maja 2015 r., IV Ka 141/15, LEX nr 1829043.
[203] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 1094/10/N.
[204] Zob. Wyrok Sądu Rejonowego w Bydgoszczy z dnia 1 grudnia 2014 r., IX K 126/14, LEX nr 1829043 i postanowienie Sądu Rejonowego w Siedlcach z dnia 23 września 2015 r., VII Kp 203/15, LEX nr 1922632.
[205] J. Giezek, *Art. 269(a). Zakłócenie systemu komputerowego*, *teza 12*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, LEX. Większość autorów powołuje się na pogląd B. Kunickiej-Michalskiej, [w:] *Kodeks karny – część szczególna*, t. 2, *Komentarz do artykułów 222–316*, red. A. Wąsek, Warszawa 2006, s. 739.
[206] B. Kunicka-Michalska, *Komentarz do art. 268a k.k.*..., s. 739.

„wyłącza na zasadzie konsumpcji przepis art. 268 k.k.", skoro przedmiotem czynności wykonawczej w pierwszym z nich są „dane informatyczne", a w drugim „informacje". Nie może zatem czyn ukierunkowany na nieuprawnione manipulowanie danymi informatycznymi pochłaniać czynu, którego przedmiotem działania sprawcy są informacje.

Na wstępie odrzucić należy kategoryczne stanowisko M. Kalitowskiego, zgodnie z którym: „Podmiot, część znamion strony przedmiotowej (zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu, zmiana jako postacie zachowania sprawcy) oraz strona podmiotowa art. 269a k.k. są takie same jak w art. 268a k.k. Jednak w wypadku art. 269a k.k. zachowanie sprawcy może polegać także na transmitowaniu danych informatycznych[207]". Otóż, także przestępstwa stypizowane w art. 268a § 1 k.k. realizowane są w związku z transmitowaniem danych informatycznych na odległość, gdyż np. przekazywanie takich danych następuje w wyniku ich przesłania z jednego komputera na drugi (np. z komputera, na którym loguje się sprawca, na serwer firmy będący przedmiotem „ataku"). Zresztą „skasowanie" bez uprawnienia samej skrzynki poczty elektronicznej jako danych informatycznych jest kwalifikowane z art. 268a § 1 k.k., a w takiej sytuacji komputer użytkowany przez sprawcę łączy się zdalnie (następuje transmisja danych na odległość) z serwerem poczty elektronicznej, który może być usytuowany w dowolnym miejscu na świecie (sporadycznie tylko historia poczty przechowywana jest w pamięci domowego komputera).

Pewne wskazówki, co do rozgraniczenia *in abstracto* sytuacji, w których stosuje się art. 268a § 1 i 2 k.k. lub art. 269a k.k., podaje W. Wróbel, twierdząc:

> Z uwagi na znamiona określone w art. 268a k.k. uzasadnione wydawałoby się przeprowadzenie rozróżnienia pomiędzy zakłóceniem pracy samego systemu informatycznego (teleinformatycznego) oraz zakłóceniem automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych w tym systemie, zwłaszcza z uwagi na fakt, że istota pracy takiego systemu polega właśnie na przetwarzaniu, gromadzeniu i przekazywaniu owych danych. Rozróżnienie to wszakże nie wydaje się możliwe. Z uwagi na wyższe zagrożenie sankcją karną, należy uznać, iż do realizacji znamion z art. 269a k.k. dochodzi wówczas, gdy następuje kwalifikowane zakłócenie automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych, odnoszące się do całości funkcjonalnie wyodrębnionego systemu lub sieci[208].

Za taką wykładnią komentowanych przepisów przemawiają zawarte w nich znamiona skutku: uniemożliwienie lub w istotnym stopniu zakłócenie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych (art. 268a k.k.), pomimo że niesie ze sobą realną szkodę, to stanowi jednak mniej uciążliwe działanie, aniżeli zakłócenie w istotnym stopniu pracy całego systemu lub sieci; z tego wynika

[207] M. Kalitowski, *Art. 269(a). Zakłócenie systemu komputerowego*, *Kodeks karny. Komentarz*, red. M. Filar, WK 2016, LEX.

[208] W. Wróbel, *Art. 269(a), teza 8*, [w:] *Kodeks karny. Część szczególna*, t. 2, *Komentarz do art. 117–277 k.k.*, red. A. Zoll, LEX 2013.

surowsze zagrożenie karą w art. 269a k.k. Według słownika języka polskiego PWN „istotny" znaczy tyle, co „duży, znaczny", „rzeczywisty, prawdziwy"[209]. Przykładowo, czyn stypizowany w art. 268a § 1 k.k. spowoduje niemożność korzystania przez personel medyczny z komputerowej rejestracji pacjentów lub systemu wypisywania recept stanowiącego część szpitalnego systemu informatycznego. Jednak zakłócenie systemu informatycznego i teleinformatycznego placówki ochrony zdrowia, które podtrzymują funkcjonowanie całego szpitala, skutkować będzie jego znacznym lub całkowitym unieruchomieniem, a w konsekwencji wywoła bezpośrednie niebezpieczeństwo dla zdrowia i życia chorych pacjentów. Podobne wydarzenia, które należałoby zakwalifikować z art. 269a k.k., miały miejsce w Wielkiej Brytanii, kiedy w 2017 r. kampania cyberataków ransomware'a o nazwie WannaCry, przeprowadzona przez grupę hakerską Lazarus, unieruchomiła pracę wielu brytyjskich placówek służby zdrowia (United Kingdom's National Health Service, NHS).

Powracając na grunt krajowy, Sąd Rejonowy w Kłodzku, rekonstruując zachowanie sprawcy przestępstwa z art. 269a k.k., napisał w uzasadnieniu do wydanego wyroku, że jego czyn spowodował „istotny stopnień zakłócenia pracy systemu informatycznego" polegający na „utrudnieniu dostępu do sytemu komputerowego obsługującego pracę sklepu internetowego". W dacie popełnienia przestępstwa art. 269a k.k. miał brzmienie: „Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5", a obecny kształt zyskał dzięki ustawie z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[210]. Sąd wskazał, że w subsumpcji normy prawnej należało wziąć pod uwagę liczbę złożonych przez sprawcę fikcyjnych zamówień na cyfrowej platformie sprzedażowej, liczbę zamawianego w ten sposób towaru lub konieczność „tłumaczenia" przez system informatyczny firmy wprowadzonych przez sprawcę do systemu znaków, a także długi czasookres nielegalnego działania oskarżonego. Wyrok skazujący brzmiał następująco:

> w okresie od października 2013 r. do kwietnia 2014 r. w J. i w K., województwa /…/, nie będąc do tego uprawnionym, poprzez składanie fałszywych zamówień oraz transmisję danych informatycznych utrudnił dostęp do sytemu komputerowego obsługującego pracę sklepu internetowego na stronie /…/ w istotnym stopniu

[209] https://sjp.pwn.pl/szukaj/istotny.html [dostęp: 23.06.2023].
[210] Dz. U. z 2017 r. poz. 768.

> zakłócając jego pracę, działając na szkodę A. L. K., to jest czynu z art. 269a k.k. w zw. z art. 12 k.k.[211]

W postępowaniu, które toczyło się przed Sądem Rejonowym w Iławie, sprawca wykorzystał *SYN flood attack* i został uznany za winnego tego, że:

> w dniu 31 maja 2013 r. w miejscowości Z. nie będąc do tego uprawnionym przy pomocy karty /…/ oraz oprogramowania znajdującego się na dysku laptopa /…/ wysyłał pakiety SYN blokując pracę systemu komputerowego oraz strony internetowej /…/ w istotnym stopniu zakłócając pracę systemu komputerowego, czym działał na szkodę M. Ż., tj. o czyn z art. 269a k.k.[212]

SYN flood attack to popularny wśród cyberprzestępców rodzaj ataku dotyczący „odmowy usługi" (DDoS) i polega na wielokrotnym wysyłaniu, z anonimowych adresów IP, do wszystkich portów zaatakowanego serwera dużej ilości pakietów danych z ustawioną w nagłówku flagą synchronizacji (SYN). W rezultacie dochodzi do anomalii w pracy systemu, gdyż serwer poszkodowanej instytucji zostaje przeciążony zbyt wieloma próbami nawiązania z nim kontaktu i przestaje działać lub jego praca jest znacznie spowolniona. Niekiedy atak DDoS może być poprzedzony żądaniem okupu za odstąpienie od ataku. Dochodzenie w takiej sprawie prowadziła Prokuratura Rejonowa w Rybniku, a postanowienie o jego umorzeniu z powodu niewykrycia sprawcy przestępstwa brzmiało:

> w sprawie groźby bezprawnej, kierowanej drogą mailową, dnia 19 września 2017 r. o godz. 20:16 do właścicieli firmy /…/ S.A., poprzez przesłanie informacji o planowanym cyberataku Ddos na serwer firmy /…/, który zagrozić miał ich głównej działalności, w celu zmuszenia firmy do wpłaty kryptowaluty BitCoin na podany przez sprawcę portfel, tj. o czyn z art. 191 k.k.[213]

W zaleceniach dla prokuratorów wskazano, że złożoność ataku DDoS i odmienne, stosowane przez przestępców scenariusze, determinują przyjęcie właściwej kwalifikacji prawnej w stosunku do ustalonych okoliczności i sposobu działania sprawcy, celu i skutku ataku, charakteru danych, do których utrudniono dostęp lub których przetwarzanie

[211] Wyrok Sądu Rejonowego w Kłodzku z dnia 21 sierpnia 2017 r., VI K 527/16 utrzymany w mocy wyrokiem Sądu Okręgowego w Świdnicy z dnia 9 stycznia 2018 r., IV Ka 720/17, LEX nr 2474562.

[212] Wyrok Sądu Rejonowego w Iławie z dnia 30 września 2014 r., II K 59/14 zamieszczony w uzasadnieniu do wyroku Sądu Okręgowego w Elblągu z dnia 12 lutego 2015 r., VI Ka 11/15, LEX nr 1830133.

[213] Akta Prokuratury Rejonowej w Rybniku o sygn. PR 1 Ds. 1825.2017.

zakłócono. Implikuje to odpowiedzialność karną z art. 268a § 1 k.k., którego bezpośredni przedmiot ochrony stanowi dostępność i integralność danych informatycznych. Jeśli czyn powoduje zakłócenie w istotnym stopniu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, winno się zastosować art. 269a k.k. Gdy skutkiem ataku DDoS jest zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca on lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, to w grę wchodzi art. 269 § 1 k.k. Ustalając odpowiedzialność karną za „atak odmowy", należy ponadto baczyć na art. 267 § 1–3 k.k. („infekowanie" szkodliwym oprogramowaniem komputerów w celu podłączenia ich do botnetu), art. 269b § 1 k.k. (wytworzenie lub udostępnienie specjalistycznego oprogramowania służącego do budowania sieci „komputerów-zoombi") i art. 299 § 1 k.k. (pranie pieniędzy stanowiących okup za odszyfrowanie treści)[214].

Zalecenia mówią także, że jeśli sprawca działał w celu osiągnięcia korzyści majątkowej lub wyrządzenia szkody zaatakowanemu podmiotowi, to rozważyć należy realny zbieg art. 268a § 1 k.k., art. 269a k.k., art. 269 § 1 k.k. z art. 287 § 1 k.k. To słuszne stanowisko z tym zastrzeżeniem, że kumulatywna kwalifikacja prawna czynu może dotyczyć art. 269a k.k. i art. 287 § 1 k.k., ale nie art. 268a § 1 k.k. i art. 269a k.k. Przemawiają za tym następujące argumenty: znamiona art. 268a § 1 k.k. zawierają się w opisie „oszustwa komputerowego", a ponadto, realizując dyspozycję art. 287 § 1 k.k., przestępca działa „w celu osiągnięcia korzyści majątkowej", co znajduje pokrycie w żądaniu okupu za zaprzestanie ataku DDoS. Inaczej przedstawia się kwestia relacji pomiędzy art. 269a k.k. i art. 287 § 1 k.k., które się uzupełniają, tj. skutkiem popełnienia przestępstwa z art. 269a k.k. jest istotne zakłócenie pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej; art. 287 § 1 k.k. zapewnia „tylko" prawidłowe funkcjonowanie „danych informatycznych". Zasadniczym przedmiotem ochrony art. 287 § 1 k.k. pozostaje mienie, a pojęcie to należy rozumieć jako zbiorczą nazwę dla wszelkich praw majątkowych, których dowodem istnienia jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym związany jest taki zapis. Omawiany przepis chroni zatem przed działaniami oszukańczymi ukierunkowanymi przeciwko prawu własności lub innemu prawu rzeczowemu albo obligacyjnemu przysługującemu do mienia, wyrażonemu w postaci cyfrowej. Tylko jako dobro poboczne przepis art. 287 § 1 k.k. chroni dane informatyczne oraz ich przetwarzanie, gromadzenie lub przesyłanie[215]. W przypadku art. 269a k.k. bezpośredni przedmiot

[214] Zalecenia Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 10 sierpnia 2021 r. w sprawie ataków DDoS, znak: 1001 – 7.025.1.2021 (zbiory własne autora), dalej jako: Zalecenia z 10 sierpnia 2021 r.

[215] M. Dąbrowska-Kardas, P. Kardas, *Art. 287*, *tezy 13 i 15,* [w:], *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. A. Zoll, W. Wróbel, LEX 2022.

ochrony stanowi natomiast bezpieczeństwo funkcjonowania systemów informatycznych i teleinformatycznych oraz sieci teleinformatycznych. Dlatego w treści zarzutu aktu oskarżenia skierowanego przeciwko T. T., który organizował ataki DDoS, zabrakło kwalifikacji prawnej z art. 269a k.k., tym bardziej że w opisie czynu wskazano skutek w postaci „czasowej niedostępności systemu informatycznego podmiotu" oraz „spowodowania znacznej szkody majątkowej w wysokości 344 727 zł".

> w dniu 15-16 września 2013 r. w nieustalonym miejscu, a ujawnionym w Szczecinie w celu osiągnięcia korzyści majątkowej oraz wyrządzenia szkody majątkowej przeprowadził atak Ddos na spółkę /…/ w ten sposób, że bez upoważnienia, nie będąc do tego uprawnionym, wpłynął przy pomocy złośliwego oprogramowania na automatyczne przetwarzanie danych teleinformatycznych na serwerze użytkowanym przez /…/, co skutkowało czasową niedostępnością systemu informatycznego podmiotu w postaci strony www./.../.pl oraz poczta./…/.pl stanowiących infrastrukturę do logowania do usług klientów spółki, a następnie zażądał kwoty 8 000 zł oraz 3 000 zł za każdy dzień zwłoki w płatności w zamian za zaniechanie dalszego ataku Ddos co spowodowało znaczną szkodę majątkową w wysokości 344 727 zł na rzecz spółki /…/ reprezentowanego przez /…/, przy czym z popełnienia przestępstwa uczynił sobie stałe źródło dochodu – tj. o czyn z art. 287 §1 k.k. w zw. z art. 294 §1 k.k. w zb. z art. 191 §1 k.k. w zw. z art. 11 §2 k.k. w zw. z art. 65 §1 k.k.[216]

Nie sposób zgodzić się jednak z zakwalifikowaniem w akcie oskarżenia czynu sprawcy z art. 191 § 1 k.k. Przepis ten brzmi: „Kto stosuje przemoc wobec osoby lub groźbę bezprawną w celu zmuszenia innej osoby do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3". Zgodnie z art. 115 § 12 k.k. „Groźbą bezprawną jest zarówno groźba, o której mowa w art. 190, jak i groźba spowodowania postępowania karnego lub innego postępowania, w którym może zostać nałożona administracyjna kara pieniężna, jak również rozgłoszenia wiadomości uwłaczającej czci zagrożonego lub jego osoby najbliższej". Z treści zarzutu wynika, że prokurator przypisał podejrzanemu groźbę, o której mowa w art. 190 § 1 k.k.; zgodnie z tym przepisem: „Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". W art. 190 § 1 k.k. chodzi zatem o sytuację, kiedy przestępstwo, opisane w groźbie, nie zostało jeszcze popełnione, a w przypadku żądania okupu jako części składowej *modus operandi* ataku DDoS, sprawca wypełnił już znamiona art. 268a § 1 k.k. lub art. 269a § 1 k.k. Nie sposób grozić popełnieniem czegoś, co już zaistniało. Przede wszystkim jednak groźba bezprawna, w brzmieniu art. 191 § 1 k.k.

[216] Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.

przed dniem 1 października 2023 r.[217], musiała przełamać wolność decyzyjną u innej osoby, aniżeli ten pokrzywdzony, wobec którego stosowano taką groźbę. Komunikat o żądaniu okupu kierowany jest natomiast bezpośrednio do użytkownika atakowanego komputera. W innym przypadku żądanie zapłaty kryptowaluty może być kierowane do osoby prawnej, instytucji lub innego podmiotu zbiorowego, będącego właścicielem infrastruktury teleinformatycznej, a kierowanie wobec takich podmiotów gróźb nie wyczerpuje znamion przestępstwa z art. 191 § 1 k.k. Podsumowując, w treści omawianego zarzutu zachowanie sprawcy w postaci żądania okupu zawierało się w znamionach art. 287 § 1 k.k., gdyż działał on w celu uzyskania korzyści majątkowej. Jeśli powodem manipulacji danymi byłaby chęć zemsty, to należało przyjąć działanie w celu wyrządzenia innej osobie szkody.

W postępowaniu toczącym się przed Sądem Rejonowym dla Wrocławia-Fabrycznej we Wrocławiu znamiona przestępstwa z art. 269a k.k. zostały tak opisane w wyroku skazującym:

> w okresie od 16 maja 2005 r. do listopada 2006 r., działając w warunkach czynu ciągłego, będąc administratorem polskich stron internetowych o nazwach /…/ umieszczał na nich skryptu zawierające różne zagraniczne adresy, mające w końcowej części charakterystyczne zapisy /…/ oraz trzycyfrowe numery /…/ który to skrypt miał za zadanie automatyczne przekierowywanie /…/ internetowych wielu użytkowników sieci Internet, logujących się na podane wyżej polskie strony, do innych zagranicznych stron internetowych, zawierających złośliwe oprogramowanie, pochodzące od nieustalonych administratorów stron /…/, a później /…/, które to następnie automatycznie oraz bez wiedzy i zgody użytkowników Internetu instalowało się i zmieniało dane /…/ systemów operacyjnych ich komputerów, co w konsekwencji w istotny sposób zakłócało działanie tych systemów, czym działał na szkodę wielu użytkowników sieci Internet, w tym ustalonych osób: M. D., J. K., R. W., R. H. i M. R., przy czym z popełniania powyższego przestępstwa uczynił sobie stałe źródło dochodu, w łącznej wysokości około 20 tysięcy złotych, tj. o czyn z 269a k.k. w zw. z art. 12 k.k. w zw. z art. 65 §1 k.k.[218]

W sprawie tej oskarżony, przesłuchiwany w toku śledztwa, wyjaśnił, że miał świadomość, iż umieszczenie skryptu na stronach internetowych spowoduje przekierowanie innych osób do witryny, która samoczynnie, tj. bez ich wiedzy i zgody, instalowała złośliwe oprogramowanie na komputerach pokrzywdzonych, jednocześnie dokonując

[217] Zob. art. 1 pkt 74 lit a ustawy z dnia 7 lipca 2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2022 r. poz. 2600).

[218] Wyrok Sądu Okręgowego we Wrocławiu z dnia 23 września 2014 r., IV Ka 1222/13 utrzymujący w mocy wyrok Sądu Rejonowego dla Wrocławia-Fabrycznej we Wrocławiu z dnia 29 sierpnia 2013 r., II K 1227/10, LEX nr 1882442.

zmian w danych informatycznych i zakłócając pracę całego systemu. Zainfekowanie maszyn spowalniało proces przetwarzania danych informatycznych.

Kontrowersyjna pod kątem wyczerpania przez sprawcę znamion przestępstwa z art. 269a k.k. była sprawa prowadzona przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie. Mężczyzna został oskarżony o to, że:

> w dniu 21 listopada 2010 r. w Krakowie nie będąc do tego uprawnionym poprzez zainstalowanie w nieustalony do chwili obecnej sposób programu typu „bot" na forum internetowym www./.../.pl założył kilkadziesiąt tematów dyskusji znieważających w sieci Internet M. B. oraz P. B. słowami powszechnie uznanymi za obelżywe, czym w istotny sposób zakłócił prace systemu komputerowego, tj. o przest. z art. 269a k.k. i art. 216 § 2 k.k. w zw. z art. 11 § 2 k.k.[219]

Z treści zarzutu nie wynikało wprost, co zakłóciło pracę systemu komputerowego: treść postów zamieszczonych na forum internetowym przez oskarżonego czy przeciążenie systemu komputerowego ruchem sieciowym generowanym przez bota. W sprawie ustalono, że mężczyzna przesłał na forum prowadzone hobbystycznie przez przyjaciół M. B. obraźliwe informacje o jego matce. Pokrzywdzony zeznał, że sprawca „założył domenę gayonly.pl i dokonał ingerencji w domenę www./.../.pl w ten sposób, że automatycznie przekierowywał ruch z domeny gayonly.pl na stronę domeny www./.../.pl, tzn. jeśli ktoś wchodził na stronę gayonly.pl, to trafiał na stronę www./.../.pl. Ponadto 21 listopada 2010 r. M. P. zaatakował stronę www./.../.pl za pomocą tzw. bota, który założył na forum kilkadziesiąt tematów o tytule 'Matka P. B. daje dupy żulom'". Oskarżony nie przyznał się do popełnienia zarzucanego mu czynu, a ustalenie kluczowych okoliczności faktycznych wymagało powołania biegłego z zakresu informatyki śledczej. Prokurator zadał biegłemu następujące pytania:

> 1. Czy z dostarczonych do badań komputerów dokonywano połączeń z forum o adresie „gameonly.pl/forum" i czy publikowano tam wiadomości? Jeśli tak to o jakiej treści?
> 2. Udzielenie informacji o rodzaju plików i danych rozpowszechnianych za pośrednictwem zabezpieczonych komputerów, przy użyciu jakiego rodzaju programów były one rozpowszechniane, w jakim czasie?

Po zbadaniu zabezpieczonego od podejrzanego komputera biegły stwierdził w opinii, że nie udało mu się uzyskać dostępu do zawartości dysku, gdyż komputer został zaszyfrowany za pomocą programu TrueCrypt na tyle skutecznie, że przełamanie tego

[219] Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 578/11/S.

zabezpieczenia bez znajomości hasła jest niemożliwe. TrueCrypt to darmowy program służący do szyfrowania danych „w locie". Pozwala zarówno na szyfrowanie całych dysków, ich partycji i przenośnych dysków USB (pendrive'ów) oraz tworzenie wirtualnych, zaszyfrowanych dysków o określonej pojemności zabezpieczonych hasłem przed nieautoryzowanym uwierzytelnieniem. Ochrona dostępu do danych odbywa się za pomocą bardzo silnych algorytmów szyfrujących AES-256, Serpent i Twofish; możliwe jest także szyfrowanie kaskadowe, tzn. szyfrowanie danych równocześnie kilkoma algorytmami[220].

W sprawie rozpoznawanej przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie pytania do biegłego, chociaż prawidłowo sformułowane, to dotyczyły jednak ograniczonego zakresu opiniowania. Generalna reguła głosi natomiast, że czym bardziej skomplikowany *modus operandi* sprawcy, tym większa trudność w opiniowaniu. Przykładowo, ataki DDoS stanowią specyficzny przedmiot pracy biegłego, gdy określa on natężenie ruchu sieciowego na osi czasu, dąży do wyselekcjonowania i zidentyfikowania adresów IP występujących w logach, z których mógł być prowadzony atak, określa przedziały czasowe, kiedy odnotowano największe natężenie ruchu sieciowego, bada, w jakich przedziałach czasowych i przy jakim natężeniu ruchu nastąpił brak dostępności usługi, stwierdza, czy natężenie przepływu danych wskazuje na atak DDoS, identyfikuje adresy IP biorące udział w ataku, oraz identyfikuje, czy istnieje korelacja parametrów aktualnego zdarzenia z ewentualnym wcześniejszym, podobnym przestępstwem. Dopiero uzyskanie opinii w podanym zakresie pozwala na podjęcie dalszych, kluczowych czynności dowodowych, m.in. zażądania od podmiotów dostarczających usługi sieciowe wydania danych retencyjnych dotyczących abonentów, którym przydzielono adresy IP zidentyfikowane przez biegłego jako generujące podwyższony ruch sieciowy. Na podstawie zgromadzonego materiału dowodowego sporządza się analizy kryminalne i ustala m.in. osoby, które posiadają urządzenia podpięte do botnetu, a więc mające procesowy status pokrzywdzonych przestępstwem hakingu[221].

Problem dotyczący zaszyfrowania danych informatycznych dowodowego dysku pojawił się także w sprawie rozpoznanej przez Sąd Okręgowy w Krakowie, który uznał oskarżonego za winnego tego, że:

> w okresie od 8 stycznia 2013 r. do 20 stycznia 2013 r. w Krakowie działając w krótkich odstępach czasu w ramach z góry powziętego zamiaru w celu osiągnięcia korzyści majątkowej w stosunku do mienia znacznej wartości w wysokości 300 000 zł bez upoważnienia wprowadziła nowy zapis danych informatycznych w postaci hasła do serwera /…/ Sp. z o.o., w ten sposób bezprawnie utrudniając dostęp do zgromadzonych tam danych informatycznych, czym w istotny sposób zakłócił pracę

[220] https://www.dobreprogramy.pl/ [dostęp: 26.07.2023].
[221] Zalecenia z 10 sierpnia 2021 r.

> systemu komputerowego na szkodę /…/ Sp. z o.o., tj. o przest. z art. 287 § 1 k.k. w zw. z art. 294 § 1 k.k. i art. 269a § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[222]

Mężczyzna przyznał się do popełnienia zarzucanego mu czynu i wyjaśnił, że motyw jego działania stanowiła chęć zdobycia pieniędzy, a ponadto był rozżalony, że pracodawca zwolnił go z pracy i dlatego zablokował serwer, a potem zażądał okupu. System serwera zaszyfrował programem TrueCrypt i po wyłączeniu urządzenia wygenerował hasło Linux/…/. W celu jego ponownego uruchomienia należało podać hasło dostępowe, którego nie znał administrator systemu informatycznego spółki. Następnie oskarżony założył anonimowe konto i wysłał z tego konta do prezesa spółki informację o zaszyfrowaniu serwera oraz żądanie równowartości kwoty 300 000 zł płatnych w bitcoinach za odszyfrowanie danych. W tej sprawie badaniu poddano „dyski macierzy RAID typu Mirror znajdującej się na serwerze zabezpieczonym w /…/ sp. z o.o. poprzez sporządzenie kopii binarnych przedmiotowych dysków". Biegły stwierdził, że

> zaszyfrowanie obejmuje całą powierzchnię dysku wraz z sektorem startowym MBR. Przy użyciu posiadanego oprogramowania oraz mocy obliczeniowej stanowiska badawczego nie posiadam możliwości odszyfrowania dysku. Na podstawie doświadczenia zawodowego mogę stwierdzić, że na stanowisku o bardzo dużej mocy obliczeniowej, odszyfrowanie hasła programu metodą „brute force" w zależności od długości i skomplikowania hasła oraz zastosowanego algorytmu szyfrowania, może trwać od kilkunastu dni do kilku lat nieprzerwanej pracy[223].

Zagadnienie, które ma istotne znaczenie w aspekcie kwalifikacji prawnej i opisu czynu z art. 269a k.k., to ocena znamienia „istotnego stopnia zakłócenia pracy systemu". Problem ten pojawił się w postępowaniu toczącym się przed Sądem Rejonowym dla Krakowa-Podgórza w Krakowie, gdzie mężczyzna został skazany za to, że:

> w okresie od dnia 24 lipca 2015 do dnia 29 lipca w Krakowie, nie będąc uprawnionym, poprzez usunięcie danych informatycznych /…/ Sp. z o.o. w postaci partycji jednego z serwerów oraz informacji o drukarkach z serwera wydruku, w istotnym stopniu zakłócił pracę sieci informatycznej Spółki, tj. o przestępstwo z art. 269a k.k.[224]

Sama lektura wyroku nie przekonuje co do słuszności przyjętej przez sąd kwalifikacji prawnej czynu, a bardziej trafne wydawałoby się skazanie oskarżonego z art. 268a § 1 k.k. Jak zatem sąd uzasadnił swoją decyzję? Jednym z kluczowych dowodów

[222] Akta Sądu Okręgowego w Krakowie Wydział III Karny o sygn. III K 272/13.
[223] Akta Prokuratury Rejonowej Kraków-Podgórze w Krakowie o sygn. 2 Ds. 180/13.
[224] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 469/16/P.

obciążających sprawcę był dostarczony przez pokrzywdzoną spółkę tzw. raport powłamaniowy; napisano w nim, że:

> Po analizie logów oraz metodyki działania (zarówno nieudanych jak i skutecznych prób logowania) można przypuszczać, iż osoba, która wykorzystała domowego użytkownika /…/ dobrze znała infrastrukturę sieci lokalnej. Osoba ta próbowała logować się na nazwiska pracowników nie tylko firmy /…/, ale również osoby z innych oddziałów co może oznaczać, iż je znała. Należy zauważyć, iż osoba ta dobrze wiedziała jaki jest adres VPN firmy. Dodatkowo znała hasło użytkownika /…/ do połączenia zdalnego. Osoba ta również wiedziała, że na serwerze /…/ domenowy użytkownik /…/ (a więc ten, który został użyty), posiada uprawnienia lokalnego administratora, dzięki czemu może prowadzić działania administracyjne (jak np. usuwanie partycji). Osoba znała również hasło administratora, ponieważ te zostało przywrócone po zmianie na inne około dzień wcześniej /…/.

Z ustaleń faktycznych sprawy wynikało, że „atakujący" w systemie informatycznym spółki otworzył sesję i włączył funkcję zarządzania dyskami oraz usunął jedną z partycji, a ponadto skasował dwa foldery z dysku systemowego będące składową aplikacji odpowiedzialnej za drukowanie. Ponadto usiłował usunąć z systemu zainstalowane i udostępnione drukarki; wykonał taki zabieg na 70 urządzeniach. Została także zmieniona nazwa sieci bezprzewodowych, a administrator nie mógł dostać się do przełącznika zarządzającego tą siecią (hasła dostępu zostały zmienione).

W sprawie tej oskarżony przyznał się do popełnienia zarzucanego mu przestępstwa, tj. ingerencji w system i usunięcia danych, a sąd warunkowo umorzył postępowanie karne na okres próby, chociaż w swoich wyjaśnieniach złożonych w toku dochodzenia P. D. zaprzeczył, aby usunięte dane były istotne i zakłóciły pracę systemu spółki. Mężczyzna powiedział, że „zarówno usunięcie tej kolejki czyli sterownika drukarek oraz usunięcie partycji, czyli logicznej części dysku zakłóca pracę pewnego wąskiego obszaru systemu jedynie czasowo, do momentu przywrócenia tych danych z backupa, snapshota lub kopii zapasowej". Wyjaśnił także, że usunięcie sterowników drukarki spowodowało tylko chwilową niemożność drukowania, zatem nie było istotnego zakłócenia sieci informatycznej firmy. Jednak informatyk zatrudniony w pokrzywdzonej spółce wskazał na wiele negatywnych skutków ataku, m.in. usunięcie kilkudziesięciu zainstalowanych w serwerze drukarek, zmianę nazwy sieci bezprzewodowej, zmianę haseł dostępowych. Firma musiała podjąć wiele czynności naprawczych, aby przywrócić prawidłową pracę sieci informatycznej.

Analiza akt postępowania Sądu Rejonowego dla Krakowa-Podgórza w Krakowie pokazała, że opis i kwalifikacja prawna czynu powinna zawierać także art. 267 § 2 k.k., bowiem P. D. zalogował się do serwera firmy za pomocą przydzielonego mu hasła, gdy pracował w spółce, a hasła tego nie zmieniono po jego odejściu z firmy. Wynika z tego, że w momencie popełnienia czynu uzyskał zdalnie bez uprawnienia dostęp do

systemu informatycznego spółki. W akcie oskarżenia wskazano na zakłócenie pracy „sieci informatycznej", a w art. 269a k.k. mowa jest o „systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej". Lektura akt sprawy każe wątpić, że rzeczywiście doszło do nieuprawnionej ingerencji w system informatyczny lub teleinformatyczny w rozumieniu art. 269a k.k., gdyż działanie sprawcy zakłóciło „tylko" automatyczne przetwarzanie i przekazywanie danych związanych z pracą drukarek, stanowiących niewielką część systemu firmy.

Typowe sytuacje, gdy znajduje zastosowanie art. 269a k.k., dotyczą rozległych „ataków sieciowych", a więc rozproszonych działań obejmujących dużą liczbę komputerów podłączonych do sieci teleinformatycznej, nad którymi kontrola zostaje przejęta poprzez użycie, zdobytego bezprawnie, identyfikatora i hasła użytkownika. Po otwarciu „bramy" do systemu lub sieci działania takie przyjmują różne postacie, szeroko opisane w nauce o cyberbezpieczeństwie. Ich pasywna metoda bazuje na danych zdobytych przez monitorowanie transmisji informacji, co odpowiada pod względem technicznym realizacji legalnej, zarządzonej przez sąd, kontroli operacyjnej. Ataki „czynne" to np. snoofing i sniffing. Pierwsza metoda to podszywanie się pod inną stację w sieci i może dotyczyć każdej warstwy protokołu TCP/IP. Scenariusz ataku polega na przesłaniu przez sprawcę do komputera docelowego fałszywej informacji o komputerze obsługiwanym jako bezpiecznym, i uzyskaniu dostępu do systemu. Metody oparte na sniffingu wymagają bardziej zaawansowanej wiedzy i stanowią duże zagrożenie przede wszystkim dla danych przesyłanych siecią Internet. Przestępca za pomocą specjalnego urządzenia lub oprogramowania może śledzić na interfejsie swojego komputera pakiety danych, w tym wiadomości przesyłane pocztą elektroniczną przez osoby trzecie oraz dane logowania się do kont bankowych lub platform społecznościowych. To tylko niektóre z wielu *modus operandi* cyberprzestępców, które często łączą się z zastosowaniem odpowiedniej socjotechniki.

Działaniem wyczerpującym znamiona art. 269a k.k. jest atak ransomware. Chodzi o rodzaj złośliwego oprogramowania wykorzystywanego przez cyberprzestępców do szyfrowania dostępu do informacji i danych informatycznych. Schemat ataku przedstawia się następująco:

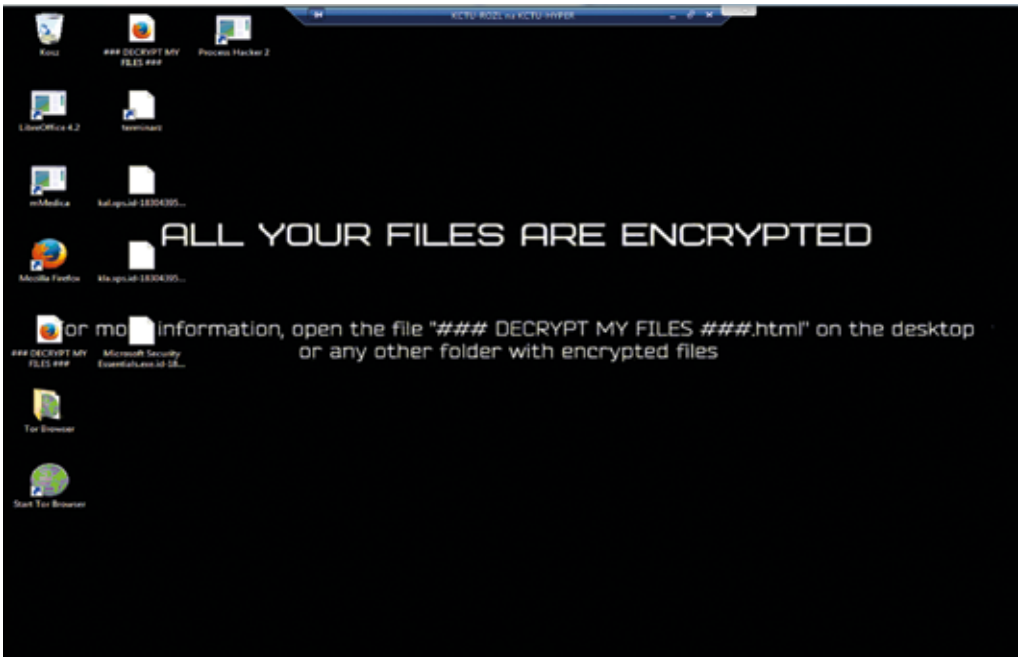
1. następuje dystrybucja malware'a za pomocą działań socjotechnicznych, fałszywych stron internetowych lub infekcji z wykorzystaniem wyszukiwarek sieciowych;
2. jeśli potencjalna ofiara pobierze kod wykonywalny złośliwego oprogramowania, to rozpocznie się infekcja jej komputera, tj. kopiowanie „podrzuconego" pliku wykonalnego do lokalnego katalogu laptopa czy maszyny stacjonarnej;
3. malware skanuje pamięć zaatakowanego komputera i szyfruje wskazane przez atakującego pliki (dokumenty, filmy, pliki dźwiękowe itd.);
4. równocześnie złośliwe oprogramowanie blokuje pracę urządzenia i wyświetla własny interfejs z komunikatem, co się stało i jak postępować, aby odzyskać zaszyfrowane treści; najczęściej szantażysta żąda okupu w kryptowalucie;

5. po zapłacie bitcoinów na wskazany adres otrzymuje się klucze deszyfrujące dane informatyczne lub wciąż pozostają one niedostępne[225].

Pod nazwą ransomware kryją się różnego rodzaju programy mniej lub bardziej niebezpieczne dla użytkowników sieci: szyfrujące (np. WannaCry, CryptoWall, CryptoLocker i Locky), nieszyfrujące (np. Winlocker i Reveton), oparte na blokadzie dostępu do maszyny lub wyłącznie na socjotechnice. Najbardziej znany, wspomniany już, malware o nazwie WannaCry 12 maja 2017 r. „zaraził" w ciągu kilku godzin tysiące komputerów na całym świecie. Jego cechą charakterystyczną była duża zdolność samodzielnego propagowania się i rozprzestrzeniania w Internecie z wykorzystaniem luk w systemie Windows. Cały proceder ataków ransomware wpisuje się w zjawisko crime as a service: poszczególni uczestnicy nielegalnych kampanii odpowiedzialni są za budowę i dostarczenie oprogramowania, jego hostowanie, zarządzanie kanałami dystrybucji, a ostatecznie gromadzą kryptowaluty pochodzące z okupu i przetransferowują je w bezpieczne dla przestępców miejsce[226]. Dlatego ściganie sprawców ataków ransomware jest niezwykle trudne.

W innym postępowaniu prokurator Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu, podejmując decyzję o umorzeniu śledztwa na podstawie art. 322 § 1 k.p.k., wskazał, jak ważne jest niezwłoczne zatrzymanie po zdarzeniu i poddanie ekspertyzie przez biegłego sprzętu elektronicznego, który stał się przedmiotem ataku ransomware: „zlecenie ekspertyzy sprzętu należącego do pokrzywdzonych po upływie 6 miesięcy od zdarzenia jest bezzasadne, albowiem dane, które sprawca może po sobie pozostawić są danymi ulotnymi lub o niskiej trwałości i ich odzyskanie jest z reguły niemożliwe ze względu na technologię i techniki zacierania śladów"[227]. W innym postępowaniu prokurator zwrócił się do biegłego z zakresu informatyki w celu wydania opinii i odszyfrowania danych informatycznych. Biegły stwierdził, że „metoda szyfrowania w takich sytuacjach następuje przez kilkudziesięcioznakowe hasło, co w praktyce przy próbie przełamania tego zabezpieczenia może oznaczać kilkaset lat działania komputera"; biegły dodał, że „z jego doświadczenia wynika, że w takich sprawach jedyną możliwością odzyskania danych jest zapłacenie bitcoinów". W uzasadnieniu do postanowienia napisano ponadto, że w przypadku infekcji serwera złośliwym oprogramowaniem typu ransomware bardzo wątpliwe jest uzyskanie jakichkolwiek danych o sprawcach zdarzenia, albowiem przestępcy działają profesjonalnie i z dużym prawdopodobieństwem można powiedzieć, że pozostaną niewykryci. Sprawy związane z szyfrowaniem serwera są bardzo skomplikowane i czasochłonne, a wykrycie sprawców jest praktycznie niemożliwe[228].

[225] P. Opitek, *Cyberprzestępczość w pracy prokuratora*, Prokuratura Krajowa 2018, s. 71.
[226] Tamże, s. 8.
[227] Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 818.2019.
[228] Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 2354.2018.



Grafika nr 9. Informacja, która wyświetliła się na komputerach zainfekowanych złośliwym oprogramowaniem typu ransomware, a należących do pracowników niewielkiej przychodni zdrowia w Krakowie

To decrypt your files you need to buy the special software – «Nemesis decryptor»
To recover data, follow the instructions!

You can find out the details/ask questions in the chat:
https://7yyqbue3umcwumiz.onion.to, https://7yyqbue3umcwumiz.onion.cab (not need Tor)

If the resources is not available for a long time, install and use the Tor-browser:
1. Run your Internet-browser
2. Enter or copy the address https://www.torproject.org/download/download-easy.html in the address bar of your browser and press key ENTER
3. On the site will be offered to download the Tor-browser, download and install it. Run.
4. Connect with the button "Connect" (if you use the English version)
5. After connection, the usual Tor-browser window will open
6. Enter or copy the address http://7yyqbue3umcwumiz.onion in the address bar of Tor-browser and press key ENTER
7. Wait for the site to load

// If you have any problems installing or using, please visit the video tutorial https://www.youtube.com/watch?v=gOgh3ABju6Q

OR contact by email

mk.shapkahn@aol.com

Grafika nr 10. Sprawca „ataku" na komputery przychodni zdrowia w Krakowie przesłał żądanie zapłaty okupu za odszyfrowanie danych informatycznych oraz instrukcję, jak zapłacić okup w kryptowalucie

Modus operandi przestępców w sprawach dotyczących ransomware można podzielić na cztery zasadnicze etapy realizacji czynu zabronionego, które rzutują na metodykę prowadzenia postępowania przygotowawczego:

1. kampanie adresowane do nieokreślonego albo ograniczonego kręgu potencjalnych pokrzywdzonych (np. kancelarie prawne, zakłady opieki zdrowotnej, klienci instytucjonalni);
2. ataki ukierunkowane na zindywidualizowanego pokrzywdzonego i poprzedzone rozpoznaniem jego sytuacji zawodowej, rodzinnej, materialnej itd.;
3. ataki poprzedzone niejawnym, trwającym przez dłuższy okres czasu, zdalnym inwigilowaniem zasobów informatycznych i teleinformatycznych potencjalnej ofiary ataku, wpływaniem na przetwarzane przez system dane informatyczne łącznie z ich przejęciem, a ostatecznie uzyskaniem treści dotyczących np. tajemnicy handlowej przedsiębiorstwa, czy jego *know-how*, bazy klientów, warunków sprzedaży produktów lub świadczenia usług. Następnym krokiem przestępcy jest zaszyfrowanie danych na urządzeniach użytkowanych przez instytucję i żądanie okupu w zamian za udostępnienie „dekryptora" (narzędzia służącego do odszyfrowania danych). Niekiedy szantaż może opierać się na groźbie upublicznienia przejętych informacji, jeśli stanowią one materiał o charakterze obyczajowym (np. zdjęcie intymne) lub sprzedaży danych wrażliwych w darknecie (ang. *double extortion ransomware*);
4. ataki niezwiązane z żądaniem okupu, mające na celu wyrządzenie szkody w postaci zaszyfrowania danych i uniemożliwienia funkcjonowania systemów informatycznych i teleinformatycznych zaatakowanego podmiotu[229].

Aby przejąć kontrolę nad danymi informatycznymi, sprawcy wykorzystują trzy zasadnicze sposoby, określane jako wektory ataku. Ustalenie takiego „wektora" to pierwsze zadanie stojące przed osobą prowadzącą śledztwo, które determinuje dalsze czynności procesowe. Sprawcy działają na trzy różne sposoby:

1. stosując socjotechnikę, przesyłają na adres poczty elektronicznej pokrzywdzonego wiadomość z załącznikiem lub odnośnikiem, którego otwarcie powoduje zainfekowanie komputera złośliwym oprogramowaniem;
2. przełamują zabezpieczenia narzędzi informatycznych, wykorzystywanych przez pokrzywdzonego, w celu uzyskania zdalnego dostępu do jego systemu (usługi zdalnego pulpitu);
3. korzystają z wcześniej wykrytej podatności (luki) w systemie informatycznym ofiary; podatność taka może być znana firmie tworzącej oprogramowanie, która w celu zniwelowania błędu w kodzie źródłowym wydała aktualizacje, ale pokrzywdzony ich nie zainstalował; w innym przypadku haker wykorzystuje do włamania podatności na atak, które są jeszcze nieznane osobom odpowiedzialnym za utrzymanie prawidłowej pracy systemu (tzw. podatność dnia zerowego, ang. *zero-day exploit*) [230].

[229] Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 6 grudnia 2021 r. dotyczące ataków ransomware, sygn. 1001 – 7.024.5.2021 (zbiory własne autora), dalej jako: Pismo z 6 grudnia 2021 r.

[230] Tamże.

Badane sprawy aktowe, odnośnie do ransomware, dowiodły dwóch rzeczy: większość z nich kończyła się umorzeniem dochodzenia lub śledztwa z powodu niewykrycia sprawcy przestępstwa, a w opisie i kwalifikacji prawnej czynów występowały błędy. W postępowaniu nadzorowanym przez Prokuraturę Rejonową Warszawa-Wola w Warszawie prokurator postanowił:

> umorzyć dochodzenie w sprawie zainfekowania laptopa i bazy danych firmy /…/ Sp. z o.o. dotyczącego zainfekowania w okresie od 21 do 22 kwietnia 2019 r. i skierowanie żądania przelania kryptowaluty Bitcoins przez użytkownika posługującego się adresem e-mail sprt@kwwmail.me, suport@cock.li tj. o czyn z art. 267 § 1 k.k. wobec nie wykrycia sprawcy czynu na zasadzie art. 322 § 1 k.p.k.[231]

Styl wypowiedzi funkcjonariusza policji w decyzji, którą zatwierdził prokurator, znacznie odbiega od języka prawniczego, a przecież posługiwanie się nim jest ważne szczególnie w postanowieniu kończącym postępowanie i doręczanym stronom, a ponadto opis czynu zawiera błędy merytoryczne. W oficjalnym języku urzędowym nie powinno stosować się takich zwrotów mowy potocznej, jak „zainfekować", „przelewać" (kryptowalutę). W sprawie doszło do ataku ransomware i zaszyfrowania danych informatycznych na dysku laptopa, a więc unieruchomienia pracy komputera; zatem sprawca wypełnił znamiona przestępstwa z art. 268a § 1 k.k. (ewentualnie art. 269a k.k.) w zbiegu realnym z art. 267 § 1 lub § 2 k.k. w zależności od tego, czy przełamano zabezpieczenie w dostępie do informacji, a może atak polegał na nieuprawnionym dostępie do systemu informatycznego. W niniejszej sprawie prawidłowa treść postanowienia mogła brzmieć następująco:

> umorzyć dochodzenie w sprawie uzyskania w nieustalonym czasie pomiędzy 21 i 22 kwietnia 2019 roku w Krakowie bez uprawnienia przez sprawcę działającego w celu uzyskania korzyści majątkowej, zdalnego dostępu do systemu informatycznego laptopa marki /…/ o nr seryjnym /…/ stanowiącego własność /…/ Sp. z o.o. i wprowadzenia nowych zapisów w pamięci laptopa uniemożliwiających dostęp do zapisanych w komputerze danych informatycznych oraz żądania okupu w kryptowalucie bitcoin za ich odszyfrowanie działając na szkodę /…/ Sp. z o.o., tj. o czyn z art. 267 § 2 k.k. i art. 268a § 1 k.k. w zw. z art. 11 § 2 k.k. wobec nie wykrycia sprawcy czynu na zasadzie art. 322 § 1 k.p.k.

W analizie kwalifikacji prawnej przestępstw ransomware, podobnie jak miało to miejsce w przypadku ataków DDoS, pojawia się problem kumulatywnej kwalifikacji

[231] Akta Prokuratury Rejonowej Warszawa-Wola o sygn. PR 4 Ds. 1848.2019.

prawnej art. 287 § 1 k.k. i art. 269a k.k. I chociaż w doktrynie wyrażany jest pogląd, że czyn nazywany w języku prawniczym „oszustwem komputerowym" (art. 287 § 1 k.k.) nie pozostaje w realnym zbiegu z art. 269a k.k., gdyż pierwszy stanowi *lex specjalis* w stosunku do art. 269a k.k.[232], to trudno zgodzić się z tak kategorycznym twierdzeniem odnośnie do wszystkich możliwych stanów faktycznych. W przypadku poważnych ataków, jak ransomware, dochodzi do czegoś więcej, aniżeli tylko do skutku opisanego w art. 287 § 1 k.k.; dobitnie pokazuje to treść zatwierdzonego przez prokuratora Prokuratury Rejonowej w Tarnobrzegu postanowienia o umorzeniu dochodzenia na podstawie art. 322 § 1 k.p.k.:

> w sprawie oszustwa internetowego dokonanego przez n/n osobę, która działając w celu osiągnięcia korzyści majątkowej w okresie pomiędzy 16 a 19 lutego 2018 roku w T. woj. podkarpackiego bez uprzedniej zgody uzyskała dostęp do informacji dla niego nieprzeznaczonej poprzez przełamanie informatycznego zabezpieczenia w postaci hasła a następnie w celu osiągnięcia korzyści majątkowej zmieniła zapis istotnych informacji zawartych w komputerach firmowych /…/ Sp. z o.o. z siedzibą w /…/ poprzez zaszyfrowanie danych zawartych w tych komputerach czym działała na szkodę prezesa zarządu /…/ Sp. z o.o. /…/, który za rozszyfrowanie danych miał zapłacić Bitcoinami osobie posługującej się adresem poczty email decrypthelp2@qq.com tj. o czyn z art. 287 § 1 kodeksu karnego[233]

Sprawca ww. przestępstwa zaszyfrował dane w komputerach obsługujących pracę spółki i unieruchomił w taki sposób, że nie można było komunikować się ze światem zewnętrznym, wysyłać i odbierać wiadomości, transferować danych z zasobów chmurowych itd. Z kwalifikacji prawnej przestępstwa wynika natomiast, jakby skutkiem ataku ransomware były jedynie zakłócenia w automatycznym przetwarzaniu danych (art. 287 § 1 k.k.), chociaż sprawca w istotnym stopniu utrudnił, a nawet uniemożliwił pracę systemu informatycznego i teleinformatycznego całej firmy. Na skutek ataku zaszyfrowane zostały dyski komputerów, nie działało oprogramowanie i sieci przesyłające dane, a w konsekwencji unieruchomione zostały urządzenia „peryferyjne", np. drukarki, skanery. Całość wymienionego oprogramowania i skorelowanych z nim urządzeń spełniała ustawową definicję „system informatyczny", a więc należało przyjąć kwalifikację prawną czynu w postaci: art. 269a k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. Postąpił tak prokurator z Prokuratury Rejonowej Katowice-Północ w Katowicach, oceniając, że

[232] M. Dąbrowska-Kardas i P. Kardas piszą: „Przepis art. 287 stanowi lex specialis w stosunku do przepisu art. 269a, co wyklucza kumulatywny zbieg tych przepisów"; zob. M. Dąbrowska-Kardas, P. Kardas, *Art. 287..., teza 8;* G. Łabuda podnosi, że: „Wydaje się, że art. 287 stanowi *lex specialis* wobec art. 268, 268a §1 oraz 269a"; zob. G. Łabuda, *Art. 287, Oszustwo komputerowe*, *teza 23*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, WKP 2021, LEX.

[233] Akta Prokuratury Rejonowej w Tarnobrzegu o sygn. PR 1 Ds. 610.2018.D.

usunięcie przez sprawcę zapisów na serwerze spółki spowodowało w istotnym stopniu zakłócenie pracy jej systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej. Jednak autor decyzji nie wskazał, który z trzech alternatywnych skutków nastąpił; ponadto zastrzeżenie budzi przyjęcie art. 267 § 1 k.k., skoro sprawca bez uprawnienia uzyskał dostęp do systemu informatycznego, zatem danych, a nie informacji. Poniżej wpierw zacytowano postanowienie o umorzeniu dochodzenia, a następnie zaproponowano inną treść tej decyzji.

> Umorzyć dochodzenie w sprawie wpływania na automatyczne przetwarzania danych gdzie nieznany sprawca w dniu 14 kwietnia 2019 roku w nieustalonym miejscu co ujawniono w Katowicach, działając w celu osiągnięcia korzyści majątkowej, po uprzednim przełamaniu elektronicznych zabezpieczeń bez upoważnienia wpłynął na automatyczne przetwarzanie i przekazywanie danych informatycznych usuwając zapisy na serwerze a za ich przywrócenie zażądał kwoty 0,5 Bitcoina – 250 dolarów amerykańskich co stanowi równowartość 942,50 złotych z zawiadomienia /…/, tj. o czyn z art. 267 § 1 k.k. w zw. z art. 269a k.k. w zw. z art. 287 § 1 k.k. przy art. 11 § 2 k.k.[234]

> Umorzyć dochodzenie w sprawie uzyskania w dniu 14 kwietnia 2019 roku w nieustalonym miejscu, ze skutkiem w Katowicach, przez osobę nieuprawnioną działającą w celu osiągnięcia korzyści majątkowej dostępu do systemu informatycznego /…/ Sp. z o.o. i wpłynięcia na automatyczne przetwarzanie danych informatycznych na serwerze Spółki poprzez ich zaszyfrowanie i żądanie okupu w wysokości 0,5 bitcoina za odszyfrowanie danych, co w istotnym stopniu zakłóciło pracę systemu informatycznego i systemu teleinformatycznego /…/ Sp. z o.o. i przerwało ciągłość pracy komputerów obsługujących bazy danych, aplikacje i strony www, działając na szkodę /…/ Sp. z o.o., tj. o czyn z art. 267 § 2 k.k. i art. 269a k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

W Prokuraturze Rejonowej Gliwice-Zachód w Gliwicach w podobnym stanie faktycznym przyjęto kwalifikację prawną czynu „z art. 268a § 1 k.k., art. 267 § 1 k.k. i inne", a prokurator zatwierdził postanowienie o umorzeniu dochodzenia w sprawie:

> dokonania przez nieustalonego sprawcę w dniu 15 maja 2018 r. w Gliwicach nie będącego do tego upoważnionym, poprzez przełamanie zabezpieczeń lub ich ominięcie,

[234] Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 2 Ds. 1322.2019.

> zaszyfrowania danych znajdujących się na serwerze o nazwie /…/ firmy /…/ z siedzibą w Gliwicach, czym utrudniono do nich dostęp, ich automatyczne przetwarzanie, gromadzenie, żądając za odblokowanie od wyżej wymienionego podmiotu zapłaty kwoty nieustalonej wartości w postaci krypto-waluty bitcoin, na szkodę firmy /…/ , tj. o czyn z art. 268a § 1 k.k., art. 267 § 1 k.k. i inne[235]

W treści decyzji ustalono, że po zaszyfrowaniu serwera na pulpicie komputerów wyświetliła się instrukcja, jak należy postąpić, aby odzyskać dane, tj. wpłacić okup w BTC na podany przez sprawcę kryptowalutowy adres publiczny. Przedstawiciel firmy poinformował o zdarzeniu policję, a jego informatycy przywrócili w kolejnych dniach większość utraconych treści z tzw. beckup'ów (kopii zapasowych serwera). Wynika z tego, że „zaszyfrowanie danych znajdujących się na serwerze" miało stosunkowo krótki charakter, nie spowodowało w istotnym stopniu zakłócenia pracy systemu informatycznego i zapewne dlatego nie przyjęto w podstawie prawnej umorzenia art. 269a k.k., tylko art. 268a § 1 k.k. W omawianym aspekcie ciekawa do rozstrzygnięcia pozostaje kwestia: Czy zapłacenie przez pokrzywdzonego okupu za odszyfrowanie danych i odzyskanie utraconych zasobów powoduje, że doszło do zakłócenia w stopniu istotnym pracy systemu lub sieci?

Sytuacja taka miała miejsce w sprawie nadzorowanej przez Prokuraturę Rejonową Gliwice-Zachód w Gliwicach, gdzie prokurator umorzył postępowanie w sprawie:

> utrudnienia w dniu 17 lipca 2018 r. w Gliwicach i nieustalonym miejscu, przez osobę nieuprawnioną dostępu do danych informatycznych spółki /…/ z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w /…/ i zakłócenie w ten sposób pracy systemu informatycznego spółki w okresie od 17 do 20 lipca 2018 r. poprzez zainstalowanie na serwerze spółki oprogramowania szyfrującego, tj. o czyn z art. 268a § 1 k.k., i art. 269a k.k. w zw. z art. 11 § 2 k.k.[236]

W uzasadnieniu do postanowienia napisano, że nieustalony sprawca wysłał z adresu mailowego server123@scryptmail.com żądanie uiszczenia przez spółkę okupu w kryptowalucie w zamian za udostępnienie hasła odblokowującego zasoby serwera i po otrzymaniu 0,45 BTC 20 lipca 2018 r. dane odszyfrował. Wcześniej zostało już rozstrzygnięte, że w podobnych sprawach art. 268a § 1 k.k. i art. 269a k.k. nie pozostają w zbiegu realnym, a o wyborze jednego z tych przepisów decyduje przedmiot czynności wykonawczej (dane informatyczne lub informacje). Fakt zapłacenia bitcoinów atakującemu i w konsekwencji odblokowanie systemu lub sieci pozostaje ambiwalentny dla

[235] Akta Prokuratury Rejonowej Gliwice-Zachód w Gliwicach o sygn. PR Ds. 339.2018.
[236] Akta Prokuratury Rejonowej Gliwice-Zachód w Gliwicach o sygn. PR Ds. 579.2018.

przypisania sprawcy skutku w postaci „zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej", jeśli rzeczywiście takie zakłócenie wystąpiło. Zapłata okupu nie stanowi bowiem standardowego postępowania związanego z „naprawieniem" systemu lub sieci i żaden pokrzywdzony nie jest zobowiązany do jego uiszczenia; przeciwnie, chodzi o świadczenie uzyskane w sposób niegodziwy przez sprawcę, a polityka cyberbezpieczeństwa mówi, aby okupów nie płacić, gdyż generuje to tylko kolejne ataki.

3.7. Wytwarzanie programów komputerowych (art. 269b § 1 k.k.)

Przepis art. 269a k.k. budzi chyba największe kontrowersje, spośród wszystkich regulacji rozdziału XXXIII k.k., co do zakresu jego stosowania, a ponadto rzadko znajduje on zastosowanie w pracy organów ścigania. Warto zatem szczegółowo przeanalizować, co leży u podstaw takiej sytuacji.

> Art. 269b. [Wytwarzanie programów komputerowych]
> § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej,
> podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
> § 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.
> § 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Treść art. 269b k.k. nie wkomponowuje się w kształt całego rozdziału XXXIII k.k., ale też sprawia trudności w stosowaniu przepisów części ogólnej kodeksu do czynów określanych mianem przestępczości teleinformatycznej. Czytając art. 269b § 1 k.k., odnosi się wrażenie, że jest on zbyt pojemny i penalizuje zachowania, co do których oceny funkcjonuje instytucja pomocnictwa (art. 18 § 3 k.k.). W literaturze przedmiotu konstrukcja prawna omawianej regulacji jest krytykowana, m.in. autor dawno już podnosił zastrzeżenia dotyczące treści przepisu sankcjonującego bezprawne wykorzystanie programów i danych, zarzucając mu zbyt daleko idącą kryminalizację zachowań leżących na przedpolu wymienionych w art. 269b § 1 k.k. czynów zabronionych,

niedookreśloność znamion czasownikowych w kontekście specyfiki komunikowania się w sieci (czy z „udostępnieniem" mamy już do czynienia w momencie zamieszczenia w sieci linku do strony z programem hakerskim?), karalność przekazania narzędzi i urządzeń „innym osobom", podczas gdy taki sam czyn w stosunku do „jednej osoby" pozostaje bezkarny[237]. Obawy budzi nieprecyzyjny zwrot „urządzenie lub program komputerowy przystosowany do popełnienia przestępstwa". Zdecydowana większość programów dostępnych w sieci nadaje się do legalnych działań, ale posiada ponadto funkcje wykorzystywane przez cyberprzestępców (tzw. narzędzia o podwójnym zastosowaniu). Nawet najzwyklejszy software w nieodpowiednich rękach może stać się bardzo niebezpiecznym instrumentem hakerskim. Ustalenie zatem, czy konkretne urządzenie lub program jest przystosowany do popełnienia przestępstwa, wiąże się z poważnymi trudnościami dowodowymi; powstaje m.in. pytanie, czy weryfikacja urządzenia lub programu pod kątem znamion z art. 269b § 1 k.k. powinna być dokonywana *in abstracto*, a może należy dopasować ją ściśle do okoliczności konkretnej sprawy[238]. A. Adamski pisze, że inkryminowanie urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstw stanowi

> znamię wieloznaczne, które nie rozwiązuje w płaszczyźnie semantycznej problemu narzędzi podwójnego przeznaczenia i jest to problem w sensie technicznym trudny do rozwiązania ponieważ wielu narzędzi hakerskich nie sposób odróżnić od oprogramowania narzędziowego, które jest wykorzystywane do obsługi technicznej i utrzymania bezpieczeństwa komputerów i sieci[239]. Program komputerowy lub urządzenie, pisze dalej A. Adamski, powinny być obiektywnie przeznaczone lub przystosowane do popełniania przestępstw, natomiast sprawca powinien mieć zamiar popełnienia określonego przestępstwa z wykorzystaniem takiego urządzenia lub programu komputerowego[240].

Cytowany autor powołał się na stanowisko Sądu Konstytucyjnego Niemiec, który uznał, że pierwszy z tych warunków nie jest spełniony, gdy użyty przez sprawcę program komputerowy nie został w tym celu napisany. Taki cel powinien bowiem znaleźć odbicie w strukturze programu komputerowego[241]. A. Adamski prawidłowo zdiagnozował problem wykładniczy, pisząc, że:

---

[237] P. Opitek, *Legalny haking w Polsce*…, s. 121.

[238] Tamże.

[239] A. Adamski, *Kryminalizacja narzędzi hakerskich w europejskim i polskim prawie karnym*, [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018, s. 107.

[240] Tamże.

[241] Podobne stanowisko na temat art. 269b § 1 k.k. wyrazili W. Wróbel i D. Zając; autorzy zwrócili uwagę, że chociaż art. 269b § 1 k.k. nie wskazuje na to, by wymienione w nim urządzenia lub programy komputerowe musiały charakteryzować się szczególnymi cechami, należy przyjąć, że przepis ten dotyczy tylko takich urządzeń lub programów, które celowo zostały przystosowane do popełnienia wymienionych w tym przepisie przestępstw. W przeciwnym wypadku zakres karalności przewidziany w tym przepisie znacznie wykraczałby poza racje kryminalnopolityczne stojące u podstaw jego wprowadzenia do Kodeksu karnego, [w:] W. Wróbel, D. Zając, *Art. 269(b), teza 6*, [w:] *Kodeks karny. Część szczególna*, t. 2, cz. 2, *Komentarz do art. art. 212–277d*, red. W. Wróbel, A. Zoll, WKP 2017, LEX.

> projektodawca, działając w słusznym celu, użył niewłaściwych określeń. Nie zwrócił uwagi na okoliczność, że obiektywnie nie istnieje nic takiego jak hasło komputerowe „przeznaczone do uzyskania nieuprawnionego dostępu". Z natury rzeczy, każde hasło lub kod dostępu mają umożliwiać dostęp do systemu komputerowego wyłącznie osobom do tego uprawnionym. Hasła komputerowe, tak jak klucz do zamka w drzwiach, pasuje bądź nie. Jest właściwe albo niewłaściwe, poprawne bądź niepoprawne. W pierwszym przypadku umożliwia dostęp do systemu, w drugim nie[242].

Wszystkie wspomniane trudności sprawiają, że kwalifikacja prawna z art. 269b § 1 k.k. incydentalnie jest stosowana przez prokuratorów, a wyroki skazujące dotyczące przestępstwa z tego artykułu to prawdziwa rzadkość. W okresie od 2013 r. do połowy 2023 r. zarejestrowano we wszystkich powszechnych jednostkach organizacyjnych prokuratury w Polsce zaledwie 159 takich przypadków, co stanowi nikły procent spraw w porównaniu z tysiącami postępowań karnych dotyczących innych przestępstw teleinformatycznych. Z liczby 159 spraw aktem oskarżenia zakończyło się zaledwie 10 postępowań: najwięcej (3) w 2020 r., a w latach 2016–2018 żaden z prokuratorów nie wystosował skargi publicznej dotyczącej przestępstwa kwalifikowanego z art. 269b § 1 k.k. Powracając do postępowania przygotowawczego, to na 159 zarejestrowanych spraw, aż 85, tj. ponad 56%, zakończyła się umorzeniem z powodu niewykrycia sprawcy czynu zabronionego[243]. Przywołane statystyki dowodzą, że omawiane przestępstwo ma wybitnie niszowy charakter, a poza tym ściganie sprawców wytwarzających nielegalne programy jest niezwykle trudne, o czym świadczą dane o zakończeniu postępowań przygotowawczych na podstawie art. 322 § 1 k.p.k., a z drugiej strony bardzo mała liczba wniesionych do sądów aktów oskarżenia w takich sprawach.

Chcąc odkodować zamysł ustawodawcy, dlaczego wprowadził określoną regulację prawną, analizuje się m.in. uzasadnienie projektu ustawy dotyczącego danego przepisu. W tym przypadku, czytając ustawę z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[244], można odnieść wrażenie, że wynikało to jedynie z konieczności spełnienia przez Polskę

[242] A. Adamski, *Kryminalizacja narzędzi hakerskich*…, s. 91 i 94.

[243] Dane pochodzą z wewnętrznego systemu elektronicznego prokuratury PROK – SYS [dostęp: 12.07.2023].

[244] Dz. U. z 2004 r. Nr 69, poz. 626; w pierwotnym kształcie art. 269b k.k. brzmiał następująco:
§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.
§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.
Obowiązujący kształt przepis ten uzyskał na mocy ustawy z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw zob. przypis 210.

zobowiązań wynikających z Konwencji o cyberprzestępczości i implementacji do wewnętrznego porządku prawnego art. 6 ust. 1 tej Konwencji[245] w brzmieniu:

> Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych:
> a. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:
> i. urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5;
> ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna,
> z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5; oraz
> b. posiadania elementu wymienionego powyżej w punktach a. i. lub ii. z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5. Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek.

W projekcie z 2004 r.[246] uzupełnienie Kodeksu karnego o art. 269b k.k. argumentowano faktem, że przepis ten

> wskazuje na konkretne przestępstwa określone w Rozdziale XXXIII, które można popełnić przy użyciu programów i urządzeń, o których mowa w tym przepisie. Ponadto penalizuje on wytwarzanie, pozyskiwanie, zbywanie i udostępnianie innym osobom haseł komputerowych i kodów dostępu, jak również innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym. Ze względu na fakt, że hasła komputerowe i kody dostępu mają praktycznie tylko jedno zastosowanie (tj. uzyskanie dostępu do systemu komputerowego), zrezygnowano tu ze wskazywania przestępstw, których popełnieniu mogłyby służyć. Kody i hasła komputerowe dostępu służą bowiem jedynie ochronie informacji zawartych w systemie komputerowym i nieuprawniony obrót nimi należy uznać za społecznie szkodliwy w stopniu uzasadniającym penalizację.

Sporo mylących twierdzeń zawarto w przytoczonym uzasadnieniu, a zarazem brakuje w nim przekonujących argumentów o konieczności implementacji do systemu prawa karnego art. 269b § 1 k.k. Nieprawdziwa jest teza, jakoby hasła komputerowe i kody dostępu miały praktyczne zastosowanie tylko do uzyskania akcesu do systemu komputerowego, skoro hasła takie stanowią składowe np. elektronicznych zamków

[245] Konwencja Rady Europy o cyberprzestępczości.

[246] Druk nr 2031. Rządowy projekt ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń, https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/2031 [dostęp: 23.06.2023], dalej jako: Druk nr 2031.

(kłódki cyfrowe), a manualnie wprowadzane kody używane są w systemach dostępu do skrzynek bagażowych lub otwierają drzwi. Zresztą nie wiadomo, po co w art. 269b § 1 k.k. wymieniono „kody dostępu" i „hasła", skoro chodzi o wyrazy bliskoznaczne i trudno, nawet odwołując się do nauki informatyki lub teorii zarządzania informacją, postawić sensowne rozgraniczenie między nimi na gruncie przestępczości teleinformatycznej[247]. W uzasadnieniu do projektu mowa jest o tym, że art. 269b § 1 k.k. chroni jedynie „dostęp do informacji przechowywanych w systemie komputerowym", a przecież dobrem chronionym w regulacjach rozdziału XXXIII k.k. jest także akces do danych informatycznych. Zresztą widać tutaj niekonsekwencję ustawodawcy, który w znamionach art. 267–269a k.k. rozgranicza przedmiot czynności wykonawczej na „informacje" i „dane informatyczne". W art. 269b § 1 k.k. mowa jest tylko o „nieuprawnionym dostępie do informacji", a przecież systemy informatyczne, systemy teleinformatyczne lub sieci teleinformatyczne przechowują także dane informatyczne jako „rewers" informacji (przetworzone przez system komputerowy dane cyfrowe przyjmują postać informacji, a informacja może być przedstawiona w formie danych cyfrowych). Trzeba zatem odwołać się do wykładni funkcjonalnej i systemowej, żeby stwierdzić, iż art. 269b § 1 k.k. *in fine* penalizuje także nieuprawniony dostęp w zakresie danych informatycznych, bo inaczej „wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom" haseł i kodów, które umożliwiałyby dostęp tylko do danych informatycznych, nie stanowiłoby ww. przestępstwa. Zdaniem autora, jednak takie rozszerzające podejście nie jest dopuszczalne, mając na względzie przejęty w monografii zdecydowany prymat wykładni językowo-logicznej.

Jednak najtrudniejsze zadanie to rozgraniczenie sytuacji, kiedy stosuje się art. 269b § 1 k.k., a kiedy sprawca wypełni znamiona pomocnictwa do popełnienia przestępstwa z art. 165 § 1 pkt 4 k.k., art. 267 § 3 k.k., 268a § 1 albo 2 k.k. w zw. z § 1, art. 269 § 2 k.k. albo art. 269a k.k. W. Wróbel i D. Zając, a za nimi pozostali komentatorzy, twierdzą, że zbycie lub udostępnienie urządzeń lub programów przystosowanych do popełnienia ww. przestępstw może realizować znamiona pomocnictwa do ich popełnienia. W zależności od wysokości sankcji karnej sprawca będzie odpowiadać wówczas albo z art. 269b § 1 k.k. albo za pomocnictwo do przestępstwa, zagrożonego równą lub wyższą karą[248]. Taka konstatacja W. Wróbla i D. Zająca, pod względem działań legislatora, niepokoi. Wynika z niej, że jeden czyn może idealnie zrealizować znamiona dwóch przestępstw, np. udostępnienia przez sprawcę innej osobie skimmera w celu kopiowania zawartości pamięci kart płatniczych wypełni znamiona zarówno art. 269b § 1 k.k., jak i art. 18 § 3 k.k. w zw. z art. 267 § 3 k.k. Jako rozwiązanie problemu, który z tych przepisów

[247] Po wpisaniu w słowniku synonimów nazwy „kod" jako pierwszy wyraz bliskoznaczny pojawia się „hasło" (zob. https://synonim.net/synonim/kod [dostęp: 23.06.2023]).

[248] W. Wróbel, D. Zając, *Art. 269(b), teza 15*… Na pogląd tych autorów powołują się w komentarzach do Kodeksu karnego: A. Lach i P. Kozłowska-Kalisz; zob. A. Lach, *Art. 269(b)*, *tezy 5 i 16*, [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Wolters Kluwer Polska 2020, oraz P. Kozłowska-Kalisz, *Art. 269(b)*, *teza 8*, [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2023.

zastosować *in concreto*, wspomniani autorzy twierdzą, że powinna decydować „wysokość sankcji karnej". Nie sposób jednak zaaprobować takiej „dyrektywy" w procesie wykładni przepisów prawa, jakoby zagrożenie karą miało decydować o subsumpcji którejś z dwóch alternatywnych norm prawnych. Brak racjonalnych argumentów przemawiających za tym, jak chcieliby W. Wróbel i D. Zając, że w przypadku takiego samego zagrożenia karą należy przyjąć konstrukcję pomocnictwa, a nie art. 269b § 1 k.k.

Inny z komentatorów, J. Giezek, podnosi, że art. 269b § 1 k.k. jest w istocie przejawem kryminalizacji zachowań leżących na przedpolu wymienionych w nim czynów zabronionych i w taki sposób ustawodawca tworzy z czynności mających w istocie charakter przygotowawczy, w prawie polskim z reguły niekryminalizowanych, przestępstwa *sui generis*, ze wszystkimi wynikającymi z takiej regulacji konsekwencjami. Przepis art. 269b k.k. – pisze J. Giezek – może pozostawać w zbiegu jednoczynowym z pomocnictwem do przestępstw, które wymienione zostały w jego dyspozycji. W oderwaniu od okoliczności konkretnej sytuacji trudno ocenić, czy zbieg taki powinien mieć charakter zbiegu kumulatywnego, czy może raczej pomijalnego lub nawet pozornego. Z uwagi na to, że bezpośredni przedmiot ochrony potencjalnie zbiegających się przepisów nieco się jednak różni, nawet jeśli nie są to różnice znaczące, to można by zaakceptować potrzebę ich kumulatywnego zastosowania[249]. Zatem J. Giezek dopuszcza, aby udostępnienie przez sprawcę innej osobie skimmera do kopiowania kart płatniczych zakwalifikować z art. 269b § 1 k.k. i art. 18 § 3 k.k. w zw. z art. 267 § 3 k.k. w zw. z art. 11 § 2 k.k., chociaż sam nie jest do końca przekonany o słuszności takiego stanowiska, o czym świadczy użycie przez niego niekategorycznego zwrotu „można by zaakceptować". Koncepcja taka nie wytrzymuje jednak krytyki, gdyż zawarta w art. 11 § 1 k.k. zasada jednorodności czynu stoi na przeszkodzie mnożenia bytów przez przyjmowanie fikcji, że sprawca dopuścił się dwóch przestępstw z tego względu, że popełniony przez niego czyn może być zakwalifikowany z więcej niż jednego przepisu części szczególnej Kodeksu karnego. W prawie karnym obowiązuje bowiem zakaz multiplikacji przestępstw, wynikający z mnożenia ocen odnoszonych do tego samego czynu[250]. Jeżeli w ocenie osoby trzeciej, bezstronnego obserwatora, zachowanie sprawcy przedstawia się jednoczynowo, a tak jest w przypadku udostępnienie przez sprawcę, na platformie darknetowej, innym osobom skimmera w celu kopiowania zawartości pamięci kart płatniczych, to jedności takiej nie należy rozbijać na mniejsze elementy.

Widać zatem, że w komentarzach do art. 269b § 1 k.k. pojawiają się różne, niekiedy wzajemnie sprzeczne koncepcje jego wykładni, przy czym brak w egzegezach Kodeksu karnego szczegółowej analizy najbardziej kontrowersyjnych znamion art. 269b § 1 k.k., a dodatkowo większość poglądów doktryny odwołuje się w tym zakresie do utartych i powierzchownych stanowisk wyrażonych pierwotnie przez któregoś z prawników albo

[249] J. Giezek, *Art. 269(b). Wytwarzanie programów komputerowych, tezy 2 i 15*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Wolters Kluwer Polska 2021, LEX.

[250] Wyrok Sądu Apelacyjnego w Katowicach z dnia 4 lipca 2019 r., II AKa 70/19, LEX nr 2747930.

wcale nie wspomina o trudnościach z wykładnią art. 269b § 1 k.k. dotyczących m.in. relacji jego znamion do form stadialnych (usiłowanie) i zjawiskowych (pomocnictwo) przestępstw wymienionych w tym przepisie.

W celu „oczyszczenia przedpola" do dalszej dyskusji o zakresie penalizacji art. 269b § 1 k.k. należy wykluczyć sytuacje, kiedy sprawca, realizując znamiona innego przestępstwa, sam „pozyskuje" hasła lub programy komputerowe. Nie będzie podlegała odpowiedzialności z art. 269b § 1 k.k. osoba, jeśli zakupiła w Internecie skimmer, a potem wykorzystała go do kopiowania kart w bankomacie, lub haker, który wyczerpując znamiona opisane w art. 267 § 2 k.k., bez uprawnienia uzyskał dostęp do systemu informatycznego i przejął cudze hasła po to, aby uzyskać autoryzację do kolejnych poziomów systemu. Chodzi o to, że jeśli w art. 267 k.k. – 269a k.k. penalizowane są zachowania polegające na bezpośrednim oddziaływaniu na dane lub informacje, to wykładnia językowa, celowościowa i systemowa art. 269b § 1 k.k. wskazuje, że sprawca popełnia to przestępstwo w oderwaniu od realizacji znamion czynności opisanych w art. 267–269a k.k. Nic natomiast nie stoi na przeszkodzie, aby hasła i kody uzyskane przez niego w wyniku popełnienia innych przestępstw teleinformatycznych, np. włamania do systemu przedsiębiorstwa, posłużyły do realizacji czynu zabronionego opisanego w art. 269b § 1 k.k., tj. zostały udostępnione do pobrania na platformie cyfrowej lub sprzedane innej grupie hakerów.

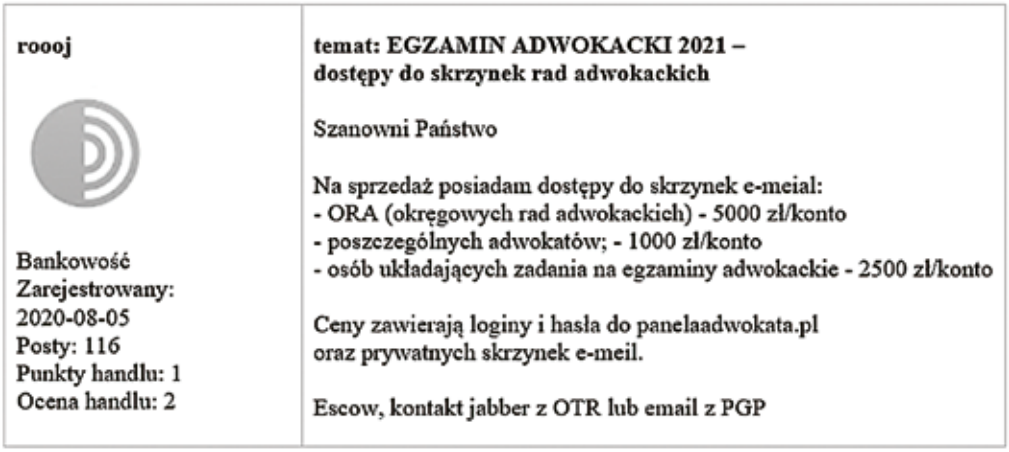
Przestępstwo nazywane „wytwarzaniem programów komputerowych" i stypizowane w art. 269b § 1 k.k. z założenia dotyczy działalności profesjonalnych przestępców tworzących rynek określany mianem crime as a service. Chodzi o specjalne platformy internetowe, najczęściej działające w sieci TOR, oferujące narzędzia do popełniania przestępstw w postaci haseł dostępu do baz danych, programów komputerowych przełamujących informatyczne zabezpieczenia systemów i sieci, numery kart płatniczych wraz z PIN-ami, oprogramowanie typu malware czy ransomware. Administrator takiej platformy nie uczestniczy w nielegalnych czynnościach związanych z wykorzystaniem sprzedanego „towaru"; nie musi nawet wiedzieć, kto, kiedy i w jaki dokładnie sposób go zastosował, ale ma świadomość, do czego innym osobom posłużą jego produkty i usługi. Można także wyobrazić sobie sytuację, że sprawca wypełni znamiona art. 269b § 1 k.k., kiedy sam wyprodukuje skimmer lub napisze złośliwe oprogramowanie w celu umieszczenia go na platformie sprzedażowej lub też pozyska takie urządzenie lub malware'a od innej osoby, aby następnie sprzedać w prowadzonym przez siebie wirtualnym sklepie. We wspomnianym już uzasadnieniu do projektu ustawy nowelizującej Kodeks karny z 2004 r. napisano, że chodzi o karalność „nieuprawnionego obrotu" kodami i hasłami komputerowymi, gdyż jest on „społecznie szkodliwy w stopniu uzasadniającym penalizację"[251].

Autor w 2017 r. pisał, że „Handel na 'czarnym rynku' w Internecie programami i danymi umożliwiającymi popełnienie przestępstw teleinformatycznych jest objęty penalizacją

[251] Druk nr 2031.

z art. 269b § 1 k.k."[252]. Za taką interpretacją tego przepisu, w warstwie językowej, przemawia także zastosowana przez ustawodawcę liczba mnoga w znamionach czynu: „udostępnia innym osobom" oraz „urządzenia lub programy komputerowe", „hasła komputerowe, kody dostępu" – działalność sprawcy ma bowiem charakteryzować się pewnym rozmachem (obrót wieloma narzędziami służącymi do popełniania przestępstw, przeznaczonymi dla społeczności cyberprzestępców) i zazwyczaj będzie rozciągnięta w czasie. Podobnie A. Adamski, komentując art. 269b § 1 k.k., stwierdził, że penalizuje on działalność „twórców wyrafinowanych narzędzi 'softwarowych' do okradania rachunków bankowych online", którzy „czerpią zyski głównie ze sprzedaży wytworów swojej pracy, czyli tzw. trojanów bankowych"; w tym kontekście A. Adamski wspomniał o producencie nielegalnego oprogramowania SpyEye, który w latach 2010–2012 sprzedał je 120 klientom, zarabiając na tym ponad milion dolarów[253].

Przykłady działalności penalizowanej z art. 269b § 1 k.k. można odnaleźć na polskim portalu cyberprzestępców o nazwie Cebulka działającym w darknecie. Jest to elektroniczna tablica ogłoszeń, gdzie zamieszczony anons wyglądał następująco:



Grafika nr 11. Ogłoszenie zamieszczone na Cebulce, darknetowym portalu dla polskich cyberprzestępców, oferujące do sprzedaży dane osobowe i hasła uwierzytelniające

Jedna z nielicznych spraw, która zakończyła się zatrzymaniem sprawcy przestępstwa z art. 269b § 1 k.k. oraz jego prawomocnym skazaniem, dotyczyła K. C., a zarzut z aktu oskarżenia brzmiał:

[252] P. Opitek, *Kodeksowe prawo materialne oraz procesowe*, [w:] *Przegląd polskiego prawa w kontekście zastosowania technologii rozproszonych rejestrów oraz walut cyfrowych, 19 stycznia 2017 r., przygotowany przez Zespół Prawo i Regulacje „Strumienia Blockchain i kryptowaluty" przy Ministerstwie Cyfryzacji*, red. K. Piech, www.mc.gov.pl [dostęp: 23.07.2023]; podobnie: P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2, s. 146.

[253] A. Adamski, *Kryminalizacja narzędzi hakerskich*…, s. 96.

w okresie od 22 lutego 2017 roku do dnia 14 maja 2017 roku wytworzył złośliwe oprogramowanie typu ransomware przystosowane do popełnienia przestępstwa określonego w art. 268a § 1 k.k., i art. 268a § 2 k.k., utrudniające dostęp do danych informatycznych poprzez zaszyfrowanie danych informatycznych znajdujących się na komputerze pokrzywdzonego, które następnie udostępnił odpłatnie T. T. tj. o czyn z art. 269b § 1 k.k.[254]

Charakter sprawy, w tym m.in. wykształcenie i sposób działania K. C., potwierdzają, że sprawcami omawianej przestępczości są osoby obeznane z nowymi technologiami, działające na zamówienie lub oferujące do sprzedaży szczególny rodzaj oprogramowania lub usługi, zagrażający cyberbezpieczeństwu informacji, systemów i danych. W sprawie tej oskarżony przyjął od ustalonego mężczyzny zlecenie napisania programu do przeprowadzania ataków ransomware. K. C. miał wykształcenie wyższe magistra inżyniera informatyki i wykonywał zawód informatyka, a posiadane umiejętności wykorzystał dla celów zarobkowych, mając pełną świadomość, do czego zostanie użyte stworzone przez niego oprogramowanie. W akcie oskarżenia wskazano: „Nie możemy bowiem tracić z pola widzenia faktu, że oskarżony jest ekspertem w swojej dziedzinie. Tym bardziej musiał mieć świadomość jakie cechy ma tworzony przez niego program, skoro cechy te są na tyle oczywiste, że widoczne dla osoby, która posiada jedynie podstawową wiedzę z zakresu metod działania złośliwego oprogramowania". Udoskonalanie oprogramowania, zgodnie z wytycznymi T. T., polegało na jego dostosowywaniu do popełniania przestępstw i oskarżony podejmował wszelkie kroki, aby malware jak najlepiej posłużył wyznaczonemu celowi. W ocenie oskarżyciela, K. C. chciał stworzyć software umożliwiające popełnianie cyberprzestępstw i udostępnił program T. T. w tym celu, a zatem działał w zamiarze bezpośrednim[255].

W niniejszej sprawie doszło do udostępnienia innej osobie przez oskarżonego programu komputerowego, tj. złośliwego oprogramowania typu ransomware. W doktrynie jest kwestią sporną, czy udostępnienie programu komputerowego tylko jednej osobie wypełnia znamiona przestępstwa z rt.. 269b § 1 k.k. Przedstawiciele poglądu uznającego, że zwrot „innym osobom" odnosi się także do jednej osoby, powołują się na uchwałę Sądu Najwyższego z dnia 21 listopada 2001 r.[256], automatycznie przekładając samą tezę orzeczenia do oceny znamienia „innym osobom" na gruncie art. 269b § 1 k.k. Uchwała odnosiła

[254] Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.

[255] Tamże.

[256] Uchwała Sądu Najwyższego z dnia 21 listopada 2001 r., I KZP 26/01, OSNKW 2002, nr 1–2, poz. 4; teza uchwały głosi: „Samo tylko użycie w treści normy prawnej liczby mnogiej dla określenia przedmiotu bezpośredniej ochrony, przedmiotu czynności sprawczej lub środka służącego do popełnienia przestępstwa nie oznacza, że ustawodawca używa jej w znaczeniu zwrotu: ‚co najmniej dwa', a więc w celu ograniczenia podstawy odpowiedzialności – zawarty zatem w art. 52 pkt 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie (t.j. Dz. U. z 2023 r. poz. 1082) zwrot ‚charty rasowe lub ich mieszańce' obejmuje także jednego psa tej rasy lub jego mieszańca".

się natomiast do zupełnie innego stanu faktycznego i prawnego, tj. do art. 52 pkt 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie. W realiach tamtej sprawy Sąd Najwyższy ustalił, że umieszczenie w treści normy prawnej liczby mnogiej dla określenia przedmiotu bezpośredniej ochrony nie oznacza, że ustawodawca używa jej w znaczeniu: „co najmniej dwa", a więc w celu ograniczenia podstawy odpowiedzialności, a zwrot „charty rasowe lub ich mieszańce" obejmuje także jednego psa tej rasy lub jego mieszańca. Jednak uzasadniając swoje rozstrzygnięcie, sąd napisał, że zawartą w ustawie cechę liczebną podmiotu lub przedmiotu, warunkującą realizację znamienia czynu zabronionego, należy rozpatrywać indywidualnie na gruncie konkretnego przepisu. We współczesnych realiach – napisał Sąd Najwyższy – stanowienie, stosowanie i dokonywanie wykładni prawa wymaga przede wszystkim racjonalnego używania i odczytywania języka, ale nie można ignorować ponadto innych dostępnych reguł interpretacyjnych, aby kompetentnie rozpoznać rzeczywistą treść normy prawnej. Analiza treści dyspozycji norm prawnych zawartych w przepisach Kodeksu karnego, a także w przepisach ustawy, ujawnia rozbieżność w używaniu gramatycznej formy określenia liczby przedmiotu, do którego odnosi się czynność czasownikowa. W takim przypadku należy ocenić, czy intencją ustawodawcy rzeczywiście było zawężenie podstawy odpowiedzialności przez wyłączenie z jej granic przypadku wystąpienia tylko jednej osoby, rzeczy lub czynności czasownikowej, czy też ustawodawca przypisuje użyciu liczby mnogiej takie samo znaczenie normatywne, jak w wypadku użycia liczby pojedynczej[257]. Przekładając rozważania Sądu Najwyższego na treść art. 269b § 1 k.k., stwierdzić należy, że charakter tego przestępstwa przemawia za użyciem liczby mnogiej jako uzasadnionej językowo i logicznie. Na takim stanowisku stoi A. Marek, twierdząc, że art. 269b § 1 k.k. w odniesieniu do „zbywania lub udostępniania" wyraźnie odnosi się do liczby mnogiej[258]. Podobnie znamię „innym osobom" wykłada P. Kozłowska-Kalisz, wskazując, że „ze względu na wyrażenie znamienia 'innym osobom' w liczbie mnogiej wydaje się, że zbycie czy udostępnienie np. programu komputerowego tylko jednej osobie nie wystarczy do dokonania omawianego przestępstwa"[259].

[257] Zob. Uzasadnienie do uchwały Sądu Najwyższego z dnia 21 listopada 2001 r., I KZP 26/01, OSNKW 2002, nr 1–2, poz. 4.

[258] A. Marek, *Art. 269(b). Bezprawne wykorzystanie programów lub danych informatycznych*, *teza 2*, [w:] tegoż, *Kodeks karny. Komentarz*, LEX 2010.

[259] P. Kozłowska-Kalisz, *Art. 269(b)..., tezy 4 i 8*. Nie do końca jasne jest w tym kontekście stanowisko J. Giezka, który wpierw, powołując się na uchwałę Sądu Najwyższego z 21 listopada 2001 r., pisze: „Niezależnie od użycia liczby mnogiej w odniesieniu do przedmiotów wykonawczych (urządzenia, programy, hasła, kody) kryminalizacją objęte jest również udostępnienie np. tylko jednego hasła komputerowego lub sporządzenie tylko jednego programu", ale w następnym zdaniu, powołując się na P. Kozłowską-Kalisz, dodaje: „Trafne jest jednak dokonane w tym kontekście spostrzeżenie, że ze względu na użycie liczby mnogiej w odniesieniu do znamienia ‚innym osobom' zbycie czy udostępnienie np. programu komputerowego tylko jednej osobie nie wystarczy do dokonania omawianego przestępstwa. Przekonuje bowiem argument, że gdyby wystarczające było dopuszczenie się czynności sprawczej określonej w omawianym przepisie wobec jednej tylko osoby, to ustawodawca posłużyłby się liczbą pojedynczą, tak jak to uczynił w art. 267 § 4, art. 266 § 2 czy art. 265 § 2" [w:] J. Giezek, *Art. 269(b). Wytwarzanie programów komputerowych*, *teza 9*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Wolters Kluwer Polska 2021.

Znamienia „innym osobom", podobnie jak użytej przez ustawodawcę liczby mnogiej określającej hasła, kody, programy i urządzenia, nie powinno się interpretować *contra legem* oraz wbrew zasadzie określoności i pewności ustawowych znamion czynu zabronionego dokonywać rozszerzającej wykładni tego określenia. Stanowisko takie zaaprobował Sąd Rejonowy dla Krakowa-Podgórza w Krakowie, rozpoznając sprawę mężczyzny oskarżonego o uzyskanie hasła, które bank wydał innej osobie, a które służyło do uwierzytelnienia dostępu do panelu klienta.

> Żadnemu z oskarżonych nie można przypisać popełnienia czynu z art. 269b § 1 k.k. Przepis ten penalizuje m.in. pozyskiwanie haseł komputerowych. Należy przy tym zwrócić uwagę, że opisując stronę przedmiotową powyższego czynu zabronionego, ustawodawca posłużył się liczbą mnogą. W przypadku typów czynów zabronionych, których znamiona zostają zrealizowane przy wykonaniu czynności sprawczych w odniesieniu do pojedynczego przedmiotu, jest to wyraźnie wskazane, tak jak w art. 278 § 1 k.k. opisującym kradzież polegającą na zaborze cudzej rzeczy ruchomej. Z tego powodu, opierając się na wykładni literalnej przedmiotowego przepisu, a także mając na uwadze bezwzględny zakaz stosowania wykładni rozszerzającej do przepisów materialnych prawa karnego należy przyjąć, że pozyskanie wyłącznie jednego hasła komputerowego nie realizuje wszystkich znamion czynu zabronionego z art. 269b § 1 k.k.[260]

W tym miejscu zostanie tylko zasygnalizowane, że chociaż zaprezentowana przez sąd wykładnia znamienia „innym osobom" była trafna, to jednak dokonana przez organ orzekający subsumpcja ustalonego stanu faktycznego – chybiona. Sprawca czynu nie wypełnił bowiem swoim zachowaniem znamion przestępstwa z art. 269b § 1 k.k.

Powracając do głównego problemu i stosując wykładnię celowościową, która zmierza do ustalenia treści przepisu ze względu na cel, jakiemu ma służy, to art. 269b § 1 k.k. ma penalizować działanie profesjonalnych dostarczycieli produktów i usług służących do szeroko rozumianego hakingu. Jest wiele takich osób w sieci TOR i stanowią one podstawowy element zjawiska nazwanego cyberprzestępczością. Natomiast jednostkowe przypadki związane z uzyskaniem hasła czy oprogramowania w odmiennym celu, aniżeli ich udostępnianie innym osobom, będą zazwyczaj kwalifikowane z art. 267 § 1 lub 2 k.k. Mylą się zatem M. Małecki i P. Dudek, twierdząc, że znamiona art. 269b k.k. wypełni sprawca, który uzyska nieuprawniony dostęp do portfela kryptowalutowego „na drodze zdobycia lub wygenerowania loginu i hasła do takiej aplikacji", gdyż chodzi tu o „pozyskiwanie kodów dostępu umożliwiających dostęp do informacji przechowywanych w systemie komputerowym". M. Małecki i P. Dudek piszą, że tutaj

[260] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.

> ochrona wysunięta zostaje na przedpole bezprawnego wpływania na zapis danych informatycznych. Warto podkreślić, że chodzi w tym przypadku o dostęp do aplikacji, nie zaś o dostęp do jednostek, gdyż wszystkie transakcje jednostkami w systemie informatycznym, takim jak otwarty łańcuch bloków systemu Bitcoin, są widoczne dla każdego (publicznie dostępne)[261].

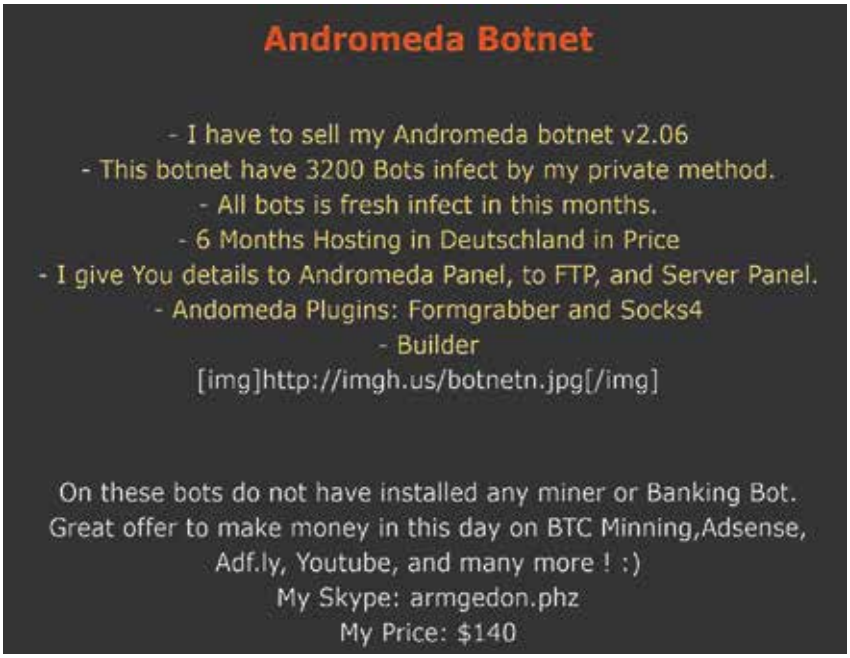
Porządkując poruszone kwestie, to nielegalne użycie oprogramowania w celu poznania zapisów portfela kryptowalutowego było potrzebne przestępcy po to, aby przetransferować środki z aplikacji na anonimowy adres i wypełniało znamiona art. 267 § 3 k.k., a nie art. 269b k.k. Sprawca „zdobył lub wygenerował loginy i hasła do takiej aplikacji" nie po to, aby „pozyskać" je do popełnienia „jakichś" przestępstw w przyszłości, ale owo „pozyskanie" stanowiło warunek *sine qua non* realizacji czynu polegającego na włamaniu się do portfela kryptowalutowego i przetransferowania kryptowaluty, tj. przest. z art. 267 § 1 k.k. i art. 267 § 3 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. Przyjmując stanowisko ww. autorów, należałoby postawić sprawcy zarzut z art. 269b k.k. w każdym przypadku, gdy za pomocą złośliwego oprogramowania uzyskuje dane autoryzacyjne do aplikacji bankowości mobilnej i wykorzystuje je do otwarcia aplikacji oraz kradzieży znajdujących się na rachunku bankowym środków; oczywiste jest, że w takim przypadku przestępca dopuszcza się „tylko" czynu karalnego z art. 279 § 1 k.k.

Za profesjonalnym charakterem działalności sprawcy przestępstwa z art. 269b § 1 k.k. przemawia także wykładnia systemowa, tj. umiejscowienie ww. jednostki redakcyjnej tekstu na końcu rozdziału XXXIII k.k., a więc stanowi ona niejako tło dla pozostałych przepisów karnych zawartych w tym rozdziale. Ponadto w § 2 art. 269b znajduje się kontratyp działania tzw. pentesterów, czyli bardzo wysokiej klasy specjalistów z zakresu informatyki i komputerów[262]. Skoro ich działanie ustawodawca porównuje, od strony technicznej, do czynności realizowanych przez sprawcę przestępstwa opisanego w art. 269b § 1 k.k., to chodzi w obu przypadkach o grupę osób posiadających szczegółową wiedzę i najwyższe kompetencje w świecie „cyber". Podsumowując zatem, przepis art. 269b § 1 k.k. stanowi ostatni typ przestępstwa teleinformatycznego opisanego w rozdziale XXXIII k.k. w jego najbardziej wyrafinowanej i zaawansowanej formie, gdyż mówi o dostarczaniu programów i narzędzi do realizacji innych cyberprzestępstw. Mówiąc obrazowo, stanowi on „wisienkę na torcie" dopełniającą obraz współczesnej cyberprzestępczości.

Zarzut o kwalifikacji prawnej z 13 § 1 k.k. w zw. z art. 269b § 1 k.k. znalazł się w akcie oskarżenia Prokuratury Okręgowej w Warszawie w sprawie legendarnego polskiego hakera T. T., tytułującego się nickiem Armaged0n; wśród kilkudziesięciu zarzutów został on oskarżony m.in. o to, że:

[261] M. Małecki, P.M. Dudek, *Uzyskanie cudzego bitcoina…*
[262] Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.

w dniu 17 sierpnia 2013 r. w miejscu nieustalonym, a ujawnionym w Warszawie usiłował zbyć program komputerowy przystosowany do popełnienia przestępstwa z art. 269a w ten sposób, że posługując się Nickiem Armaged0n na forum internetowym www.hackforums.net wystawił na sprzedaż botnet Andromeda służący do przeprowadzania ataków DDos za kwotę 140 dolarów – tj. o czyn z 13 § 1 k.k. w zw. z art. 269b § 1 k.k. przy zastosowaniu art. 4 §1 k.k. w brzmieniu obowiązującym w dacie czynu



Grafika nr 12. Ogłoszenie zamieszczone w darknecie przez cyberprzestępcę o nicku Armaged0n, w którym oferował do sprzedaży złośliwe oprogramowanie typu botnet o nazwie Andromeda i zachwalał jego parametry dotyczące m.in. możliwości wykorzystania do nielegalnych działań 3200 „zainfekowanych" komputerów

Oprogramowanie typu RAT służyło do organizowania ataków DDoS na strony internetowe poprzez „infekowanie" komputerów pokrzywdzonych osób malware'em. T. T. rozsyłał złośliwy kod przez torrenty, czyli programy do darmowego pobierania gier i filmów albo wysyłając fałszywe wiadomości mailowe, zawierające „robaka", do skrzynek potencjalnych ofiar. Przejęte maszyny podłączano do botnetu o nazwie Andromeda i wówczas sprawca mógł nimi zdalnie sterować. Stworzona w taki sposób infrastruktura pozwalała przestępcy m.in. podmieniać numery rachunków bankowych w przejętych komputerach, a więc ich użytkownicy nieświadomie wpłacali pieniądze na konta zarządzane przez administratora Andromedy. Sprawca poddawał także analizie pliki zgromadzone w przejętych komputerach i weryfikował, czy znajdują się w nich

dane, za których odzyskanie właściciel zaszyfrowanego komputera chciałby zapłacić okup. Następnie Armaged0n „infekował" złośliwym oprogramowaniem wytypowane komputery, a po zaszyfrowaniu danych zgromadzonych na dysku, pokrzywdzonemu wyświetlał się komunikat, jak zapłacić za odszyfrowanie treści. Oprogramowanie takie działało w powiązaniu z innymi malwere'ami, np. VB Clip, zmieniającym numery rachunków w schowku systemowym w momencie, gdy użytkownik aplikacji bankowej powielał numer konta za pomocą funkcji „kopiuj", a następnie funkcją systemu operacyjnego „wklej" umieszczał go na stronie mobilnej aplikacji bankowej, z której wykonywał przelew. W taki sposób pokrzywdzony nieświadomie przelewał pieniądze na konta zarządzane przez Armaged0na.

Warto wspomnieć jeszcze, że czarny rynek w Internecie nie jest idealny i bywa, że oferta sprzedaży narzędzia lub oprogramowania „podwójnego zastosowania" może mieć oszukańczy charakter; działo się tak w sprawie rozpoznawanej przez Prokuraturę Rejonową w Lidzbarku Warmińskim, gdzie prokurator zatwierdził na podstawie art. 17 **§** 1 k.p.k. postanowienie o umorzeniu dochodzenia w sprawie:

> Zaistniałego w dniu 24.11.2017 r. w bliżej nieustalonym miejscu, w celu osiągnięcia korzyści majątkowej, doprowadzenia M. K. do niekorzystnego rozporządzania mieniem w kwocie 2100,0 przez wprowadzenie w błąd co do zamiaru wywiązania się umowy kupna-sprzedaży programu komputerowego BOT, tj. o czyn z art. 286 § 1 k.k.[263].

Badania pokazały, że zdecydowana większość orzeczeń odwołujących się do art. 269b § 1 k.k. zawiera błędy, a podstawowa i najczęściej spotykana nieprawidłowość wynika z niezrozumienia roli, jaką pełni podmiot tego przestępstwa w cyberprzestępczości. Sytuacja taka dotyczyła np. wyroku Sądu Rejonowego dla Krakowa-Podgórza w Krakowie, w którym skazano oskarżonego za to, że:

> działając w krótkich odstępach czasu w ramach z góry powziętego zamiaru po uprzednim pozyskaniu w nieustalonym dniu, nie później niż 25 października 2012 r. w Krakowie hasła dostępu do internetowego konta bankowego K. B. uzyskała po jego wykorzystaniu w dniu 25 października 2012 r. bez uprawnienia dostęp do wyżej wymienionego konta bankowego, zawierającego informacje dla niej nie przeznaczone, tj. o przest. z art. 269b § 1 k.k. i art. 267 § 1 i 2 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[264]

[263] Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 2 Ds. 15.2018.
[264] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.

W opisanym stanie faktycznym ewentualnej odpowiedzialności karnej z art. 269b § 1 k.k. mogłaby podlegać osoba, która oferowała hasła dostępu do internetowych kont bankowych, a nie oskarżona, u której uzyskanie takiego hasła było częścią realizacji znamion przestępstwa hakingu, też zresztą nieprawidłowo zakwalifikowanego z art. 267 § 1 i 2 k.k., zamiast samego § 1. Poniżej autor zredagował treść zarzutów dotyczących sytuacji, w których udostępniane są hasła służące do nieuprawnionego dostępu do informacji zgromadzonych przez osobę trzecią na jej koncie Facebook, ale każdy z przypadków będzie odmiennie kwalifikowany prawnie.

W pierwszej sytuacji J. K. poinformował w rozmowie swojego kolegę P. N., że pokłócił się z żoną A. K., podejrzewa ją o zdradę i planuje włamać się na jej konto na Facebooku. Wiedząc, że P. N. wykonuje zawód informatyka, J. K. poprosił go o napisanie i przekazanie mu prostego programu do „łamania" haseł służących zalogowaniu się na konto założone na portalu społecznościowym. P. N., bacząc na długoletnią znajomość koleżeńską, napisał taki program, nazwał go roboczo *cracker* i 15 kwietnia 2023 r. sprzedał J. K. za kwotę 20 tys. zł, a ponadto udostępnił program do darmowego pobrania na forum internetowym, którego był moderatorem o nazwie witryny: www.dark_/.../. J. K. następnego dnia wykorzystał program do włamania na konto żony i zapoznał się z umieszczonymi tam informacjami, z których tylko część była dostępna publicznie. W takim przypadku sąd powinien uznać P. N. i J. K. za winnego tego, że:

(P. N.) w dniu 1 stycznia 2023 r. w Krakowie zbył na rzecz J. K. za kwotę 20 000 zł, wcześniej przez siebie wytworzony, program komputerowy o nazwie „cracker" przystosowany do popełnienia przestępstwa polegającego na przełamywaniu zabezpieczeń ustanowionych dla konta na platformie Facebook w postaci loginu oraz hasła i zapoznaniu się z zapisanymi na koncie informacjami oraz w tym samym dniu i miejscu udostępnił innym osobom ten sam program komputerowy poprzez umieszczenie go na platformie internetowej o nazwie www.dark_/.../. J. K., tj. o przestępstwo z art. 269b § 1 k.k.

(J. K.) w dniu 2 stycznia 2023 r. w Krakowie działając w celu uzyskania informacji, do której nie był uprawniony, posłużył się programem komputerowym o nazwie „cracker" przystosowanym do popełnienia przestępstwa polegającego na przełamywaniu zabezpieczeń ustanowionych dla konta na platformie Facebook w postaci loginu oraz hasła i uzyskał dostęp do informacji dla niego nie przeznaczonej w postaci zapisów rozmów, filmów i zdjęć umieszczonych na koncie A. K. o nazwie „anka_k@ /…/", działając na szkodę A. K., tj. o przestępstwo z art. 267 § 1 k.k. i art. 267 § 3 k.k. w zw. z art. 11 § 2 k.k.

Inna, hipotetyczna sytuacja, dotyczy P. N., utalentowanego informatyka, który postanowił zarobić kryptowalutę. 1 stycznia 2023 r. założył konto na działającym w darknecie portalu o nazwie Cebulka, a następnie napisał i oferował do sprzedaży programy hakerskie służące do przełamywania zabezpieczeń informatycznych i „łamania" haseł dostępu do kont założonych na portalu Facebook. W okresie od 10 stycznia do 15 maja 2023 r. wystawił do sprzedaży 5 exploitów o nazwach: *crack1*, *crack2*, *crack3*, *crack4* i *crack5* i sprzedał ich kod programistyczny za łączną kwotę 0,1 BTC ośmiu osobom korzystającym z narzędzi anonimizujących ruch w sieci TOR. W toku śledztwa udało się ustalić imię i nazwisko tylko jednego kupującego; okazał się nim być J. K., który kupił *crack1* 15 kwietnia 2023 r., a następnego dnia wykorzystał go do włamania się na Facebooka żony A. K. i zapoznania z umieszczonymi tam informacjami, z których część była dostępna tylko po zalogowaniu się na konto. W takim przypadku sąd powinien uznać P. N. za winnego tego, że:

> w okresie od 1 stycznia 2023 r. do 9 stycznia 2023 r. w Krakowie wytworzył pięć programów komputerowych typu exploit o nazwie crack1, ctack2, crack3, crack4 i crack5 umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym poprzez przełamywanie haseł dostępu do kont założonych na platformie Facebook, a następnie w okresie od 10 stycznia 2023 r. do 15 maja 2023 r. zaoferował je do sprzedaży na platformie internetowej „Cebulka" i w dniu 15 kwietnia 2023 r. zbył „crack1" J. K. oraz w tym samym czasie zbył pozostałe programy siedmiu nieustalonym osobą za łączną kwotę 0,1 bitcoina, tj. popełnienia przestępstwa z art. 269b § 1 k.k.

W sprawie prowadzonej przed Sądem Rejonowym w Mikołowie A. P. został oskarżony przez prokuratora o to, że:

> w nieustalonym dniu i w nieustalony sposób oraz bez uprawnienia pozyskał hasło komputerowe umożliwiające dostęp do serwisu internetowego /…/ do konta M. B. i D. P., a następnie w dniu 18 września 2018 r. w M. ul. /…/ o godz. 09:19 za pomocą tego hasła i bez uprawnienia uzyskał dostęp do systemu informatycznego /…/ przy użyciu numeru klienta M. B. i D. P., skąd pobrał informacje tam przechowywane, a dla niego nieprzeznaczone, dotyczące historii przelewów tego rachunku, które to informacje następnie wykorzystał, składając jako dowód przed Sądem Okręgowym w Katowicach w sprawie z jego powództwa o sygnaturze akt: XVII C 78/18, tj. o czyn z art. 267 § 1 k.k. i art. 269b § 1 k.k. przy zast. art. 11 § 2 k.k. [265]

[265] Wyrok Sądu Rejonowego w Mikołowie z dnia 30 marca 2021 r., II K 1/21, LEX nr 3232310.

W opisie czynu, o którego popełnienie został oskarżony A. P., słusznie zastosowano art. 267 § 1 k.k., ale nieprawidłowo określono jego znamiona. Sprawca powinien być oskarżony o to, że bez uprawnienia uzyskał dostęp do informacji dla niego nieprzeznaczonej w postaci zapisów znajdujących się w aplikacji bankowości elektronicznej poprzez ominięcie procedury zabezpieczającej w postaci uwierzytelniania i posłużenie się hasłem należącym do innej osoby, a nie za „bez uprawnienia pozyskanie hasła komputerowego umożliwiającego dostęp do serwisu internetowego". Sąd pomylił znamiona z art. 267 § 2 k.k. z zapisanymi w § 1 tego artykułu: sprawca uzyskał dostęp do informacji, a nie do systemu informatycznego. Fakt, że A. P. pobrane „informacje następnie wykorzystał, składając jako dowód przed Sądem Okręgowym w Katowicach w sprawie z jego powództwa o sygnaturze akt: XVII C 78/18", należy do znamion przestępstwa z art. 267 § 4 k.k. Wskazanie przez sąd, że czyn miał miejsce „w nieustalonym dniu", jest irracjonalne, bo z całą pewnością można było określić rok popełnienia przestępstwa i przedział czasowy limitowany miesiącami; zastosowane przez sąd określenie „w nieustalonym dniu", bez podania orientacyjnego czasu, nie pozwala np. ustalić daty przedawnienia karalności czynu, nie mówiąc już o zastosowaniu takich instytucji, jak wyrok łączny czy recydywa, gdyby wchodziły w grę. Sąd Rejonowy w Mikołowie tymczasem bez żadnego głębszego namysłu wyrokiem z dnia 30 marca 2021 r. uznał oskarżonego za winnego tego, że:

> działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru w nieustalonym dniu i w nieustalony sposób oraz bez uprawnienia pozyskał hasło komputerowe umożliwiające dostęp do serwisu internetowego /…/ do konta M. B. i D. P., a następnie w dniu 18 września 2018 r. w M. ul. /…/ o godz. 09:19 za pomocą tego hasła i bez uprawnienia uzyskał dostęp do systemu informatycznego /.../ przy użyciu numeru klienta M. B. i D. P., skąd pobrał informacje tam przechowywane, a dla niego nieprzeznaczone, dotyczące historii przelewów tego rachunku, które to informacje następnie wykorzystał, składając jako dowód przed Sądem Okręgowym w Katowicach w sprawie z jego powództwa o sygnaturze akt: XVII C 78/18, czym wyczerpał znamiona występku art. 267 § 1 k.k. i art. 269b § 1 k.k. przy zast. art. 11 § 2 k.k. w zw. z art. 12 § 1 k.k.

W analizowanej sprawie treść zarzutu i wyroku skazującego oraz kwalifikacja prawna czynu powinny brzmieć następująco:

> Uznaje A. P. za winnego tego, że w bliżej nieustalonym dniu /…/ roku, nie później, niż /…/ w nieustalonym miejscu bez uprawnienia uzyskał dostęp do informacji dla niego nieprzeznaczonych w postaci zapisów znajdujących się w aplikacji bankowości mobilnej Banku /…/, której uprawnionymi przez Bank użytkownikami byli M. B. i D. P., poprzez ominięcie procedury zabezpieczającej dostęp do aplikacji w postaci

uwierzytelniania i posłużenie się hasłem i loginem należącym do M. B. i D. P., a informacje uzyskane w ten sposób w dniu /…/ ujawnił innymi osobom, tj. uczestnikom postępowania toczącego się przed Sądem Okręgowym w Katowicach o sygnaturze akt: XVII C 78/18, działając na szkodę M. B. i D. P., tj. o czyn art. 267 § 1 k.k. i art. 267 § 4 k.k. w zw. z art. 11 § 2 k.k.[266]

W praktyce zdarzają się sytuacje, kiedy w postępowaniu karnym lub cywilnym strona lub przedstawiciel procesowy składa wniosek dowodowy o dopuszczenie w charakterze dowodów informacji zgromadzonych za pomocą własnych działań albo przekazanych przez klienta lub inną osobę, a uzyskanych wcześniej za pomocą czynu zabronionego. Zakładając, że wnioskodawca ma świadomość uzyskania informacji w sposób wskazany w art. 267 § 1–3 k.k., powstaje pytanie o jego odpowiedzialność karną. Dochodzi tu do ujawnienia informacji uzyskanych w sposób wskazany ww. przepisach. Zgodzić się należy ze stanowiskiem A. Lacha, że skład orzekający oraz uczestników postępowania można także uznać za „inne osoby" w rozumieniu art. 267 § 4 k.k. W tym kontekście pozostaje do rozważenia społeczna szkodliwość czynu oraz ewentualnie działanie w stanie wyższej konieczności[267].

Na zakończenie niniejszego podrozdziału warto dodać, że obowiązujący stan prawny, dotyczący legalnego hakingu, jeszcze bardziej skomplikowało wprowadzenie art. 269b § 1a k.k. Zakres przedmiotowy i podmiotowy kontratypu jest następujący:

1. dotyczy czterech znamion czasownikowych: wytwarzania, pozyskiwania, zbywania lub udostępniania innym osobom urządzeń lub programów komputerowych;
2. urządzenia i programy muszą być przystosowane do popełnienia ściśle określonych przestępstw, opisanych w art. 165 § 1 pkt 4 k.k., art. 267 § 3 k.k., art. 268a § 1 albo § 2 w związku z § 1 k.k., art. 269 § 1 lub 2 k.k. albo art. 269a k.k.;
3. liczy się ponadto zamiar sprawcy:

a. działa on wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w art. 269b § 1 k.k. albo
b. działa wyłącznie w celu opracowania metody zabezpieczenia teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie.

Art. 269b § 1a k.k. dotyczy sytuacji, kiedy pomimo spełnienia ustawowych znamion sankcjonujących, nie realizują się wszystkie warunki konieczne do przyjęcia przestępczości czynu i przypisania sprawcy odpowiedzialności karnej. Wskazany w art. 269b

[266] Zachowanie polegające na bezprawnym uzyskaniu dostępu do informacji, a następnie jej ujawnieniu, zdaniem K. Lipińskiego, prowadzić będzie do kumulatywnej kwalifikacji prawnej z art. 267 § 1 lub 3 oraz § 4 k.k.; K. Lipiński, *Art. 267*, *teza 39*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Wolters Kluwer Polska 2021; odmiennego zdania jest B. Kunicka-Michalska, [w:] *System prawa karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, t. 8, red. L. Gardocki, Warszawa 2018, s. 1016.

[267] A. Lach, *Art. 267*...

§ 1a k.k. „cel zabezpieczenia systemu" sprawia, że podejmowane działania służą ochronie dobra prawnego, a wobec tego nie zasługują na określenie ich mianem działań społecznie szkodliwych, nie wyczerpują więc w ogóle znamion „bazowego" typu czynu zabronionego pod groźbą kary. W takich okolicznościach ustawodawca niejako usprawiedliwia postępowanie osoby, która de facto naruszyła chronione dobro prawne wbrew woli jego dysponenta (administratora sieci lub systemu)[268].

Nowelizacja Kodeksu karnego z 27 marca 2017 r. dopuszcza produkcję i obrót nawet najbardziej niebezpiecznymi urządzeniami i programami komputerowymi, jeśli tylko osoba spełni warunki opisane w art. 269b § 1a k.k. W praktyce otwiera to możliwość bezkarnego wytwarzania, pozyskiwania, zbywania lub udostępniania urządzeń lub programów komputerowych ściśle przeznaczonych do popełniania przestępstw w cyberprzestrzeni. Wystarczy oświadczyć, że podejmuje się działania wyłącznie w celu zabezpieczenia systemu i sieci. Ponieważ nikt nie musi dostarczać dowodów na swoją niewinność, a ciężar udowodnienia winy leży po stronie prokuratora, to zanegowanie prawdziwości oświadczenia, niezależnie od prawdziwych intencji sprawcy, w większości przypadków będzie niemożliwe. Konieczne byłoby uzyskanie jednoznacznych dowodów świadczących, że wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie realizowane było w innych celach, aniżeli opisane w art. 269b § 1a k.k. Oprócz obciążających wyjaśnień samego sprawcy chodzi np. o treść korespondencji mailowej pomiędzy producentem a nabywcą, świadczącej, że narzędzia miały służyć do nielegalnych ataków hakerskich. Należy się spodziewać, że przestępcy będą bardziej ostrożni w praktyce i uzyskanie podobnych dowodów jest wątpliwe. Inna rzecz, że nawet osoby produkujące i udostępniające akcesoria do „etycznego hakingu" w dobrych intencjach nie są w stanie przewidzieć, czy nie nabędą ich przestępcy. Kolejna wątpliwość sprowadza się do stwierdzenia, że skoro art. 269b § 1a k.k. gwarantuje bezkarność obrotu tylko oprzyrządowaniem przystosowanym do popełnienia enumeratywnie wymienionych w § 1 przestępstw, to zachowanie osób wytwarzających lub udostępniających aplikacje do walki z przestępczością internetową w postaci np. oszustwa (art. 286 § 1 k.k.) czy tzw. oszustwa komputerowego (art. 287 § 1 k.k.) – nadal podlegać będzie odpowiedzialności karnej na podstawie art. 269b § 1 k.k. Brak zatem logiki w tym, że nie można produkować i udostępniać urządzeń lub programów do walki z cyberprzestępczością, których działanie nie polega na bezpośredniej ingerencji w zapis danych cyfrowych[269].

[268] P. Opitek, *Legalny haking w Polsce*…, s. 122.
[269] Tamże, s. 123.

Rozdział 4
Przestępstwa ukierunkowane na bankowość elektroniczną

4.1. Środek pieniężny zapisany na rachunku

Infrastruktura instytucji finansowych, na której zapisane są bezgotówkowe środki pieniężne, stanowi jeden z głównych celów działalności przestępczej. Ataki dotyczą najczęściej aplikacji elektronicznych, czytników kart płatniczych, bankomatów, a także serwerów oraz pozostałych urządzeń użytkowanych przez podmioty komercyjne i osoby indywidualne. Badania pokazały, że zdecydowanie największa liczba przestępstw teleinformatycznych polega na wypłacie gotówki z bankomatów i transakcjach zbliżeniowych oraz na włamaniach do aplikacji bankowych i kradzieżach zdeponowanych tam środków. Chodzi zatem o przestępstwa przeciwko mieniu, gdyż sprawcy działają w celu wzbogacenia się. Chociaż uzupełnienie w 2017 r. definicji legalnej „rzeczy ruchomej lub przedmiotu" (art. 115 § 9 k.k.) o zwrot „środek pieniężny zapisany na rachunku" wyjaśniło wiele kontrowersji dotyczących opisu i kwalifikacji prawnej wspomnianych czynów karalnych, to jednak wciąż istnieją w orzecznictwie na tym tle rozbieżności; o tym właśnie traktuje niniejszy rozdział książki.

Jeszcze kilka lat temu rozbieżności w orzecznictwie budziła kwestia kwalifikacji prawnej zachowania polegającego na bezprawnym przejęciu środków pieniężnych zgromadzonych na rachunku bakowym poprzez m.in. włamania do aplikacji bankowości elektronicznej czy wypłatę gotówki z bankomatu przy użyciu skradzionej karty płatniczej[270]. Sytuacja wyjaśniła się 27 kwietnia 2017 r., kiedy wszedł w życie art. 1 pkt 5 ustawy z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[271] poszerzający definicję legalną z art. 115 § 9 k.k. o zwrot „środki pieniężne zapisane na rachunku". Obecnie wspomniana definicja brzmi następująco:

> „Rzeczą ruchomą lub przedmiotem jest także polski albo obcy pieniądz lub inny środek płatniczy, środek pieniężny zapisany na rachunku oraz dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce".

Z art. 115 § 9 k.k. wynika, że w prawie karnym materialnym dla uznania bankowego pieniądza bezgotówkowego za „rzecz", zapis taki musi posiadać łącznie dwie cechy:

[270] Problem został szczegółowo opisany w artykule: P. Opitek, *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017, nr 2, LEX.
[271] Zob. przypis 210.

być środkiem pieniężnym oraz funkcjonować w formie zapisu na rachunku. Zgodnie z art. 3 ust. 1 pkt 25 ustawy z dnia 29 września 1994 r. o rachunkowości[272] aktywa pieniężne stanowią:

1. krajowe środki płatnicze, a więc walutę polską oraz papiery wartościowe i inne dokumenty, pełniące funkcję środka płatniczego, wystawione w walucie polskiej (art. 2 ust. 1 pkt 6 ustawy z dnia 27 lipca 2002 r. – Prawo dewizowe[273]);
2. waluty obce; są nimi znaki pieniężne (banknoty i monety) będące prawnym środkiem płatniczym, a także wycofane z obiegu, lecz podlegające wymianie; na równi z walutami obcymi traktuje się wymienialne rozrachunkowe jednostki pieniężne stosowane w rozliczeniach międzynarodowych, w szczególności jednostkę rozrachunkową Międzynarodowego Funduszu Walutowego (art. 2 ust. 1 pkt 10 ustawy Prawo dewizowe);
3. dewizy, którymi są papiery wartościowe i inne dokumenty pełniące funkcję środka płatniczego, wystawione w walutach obcych (art. 2 ust. 12 pkt 25 ustawy Prawo dewizowe);
4. inne aktywa finansowe, w szczególności naliczone odsetki od aktywów finansowych, jeśli spełniają warunki określone w ustawie o rachunkowości.

Wymienione w pkt 1–3 aktywa pieniężne można zrównać z „polskim albo obcym pieniądzem lub innym środkiem płatniczym" (art. 115 § 9 k.k.), co wynika z faktu, że sam ustawodawca używa tego pojęcia, dokonując wyliczenia zawartego w art. 3 ust. 1 pkt 25 ustawy o rachunkowości. Zdaniem T. Oczkowskiego, „środki płatnicze" to dokumenty lub przedmioty, które mają analogicznie do pieniądza funkcję płatniczą, ale służą do rozliczeń bezgotówkowych. Trafnie podkreśla się, że chodzi o walory będące surogatem pieniądza w obiegu, a więc powszechnie akceptowanym środkiem płatniczym w obrocie ekonomicznym[274].

Katalog wartości majątkowych z pkt 4 powyższego wyliczenia, stanowiących „inne aktywa finansowe", jest otwarty. W ekonomii i rachunkowości przyjmuje się, że chodzi o wszystkie rodzaje majątku wykorzystywanego do osiągnięcia określonego celu, mogącego mieć postać materialną (np. złoto, srebro) lub niematerialną (np. obligacje, akcje). Aktywa finansowe służą do inwestowania, generowania przepływów pieniężnych po to, aby uzyskać zysk. W. Więcław jako ich przykład podaje instrumenty kapitałowe wyemitowane przez inne jednostki i prawo do wymiany instrumentów finansowych z inną jednostką na korzystnych warunkach[275]. E. Walińska, J. Gad i A. Wencel podkreślają,

[272] Zmiana art. 115 § 9 k.k. została wprowadzona ustawą z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (zob. przypis 210), która weszła w życie dnia 27 kwietnia 2017 r.

[273] T.j. Dz. U. z 2022 r. poz. 309, dalej jako: u.p.d.

[274] T. Oczkowski, *Art. 310. Fałszowanie pieniędzy, innych środków płatniczych oraz papierów wartościowych*, *teza 4*, [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Wolters Kluwer Polska 2022, LEX.

[275] W. Więcław, *Inwestycje krótkoterminowe – definicje, podstawowe pojęcia, komentarze praktyczne*, ABC, LEX. Jak zauważa Z. Ćwiąkalski, „problematyka ‚innego środka płatniczego' jest wprawdzie podejmowana w wielu publikacjach, ale nie doczekała się jednej, powszechnie przyjętej definicji" [w:] Z. Ćwiąkalski, *Art. 310*, *teza 41*, [w:] *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2022, LEX.

że art. 3 ust. 1 pkt 25 ustawy o rachunkowości stanowi wskazówkę dla jednostek sporządzających rachunek przepływów pieniężnych w odniesieniu do zakresu uznawania określonych składników aktywów finansowych za środki pieniężne. Oznacza to, że do środków pieniężnych nie zalicza się wyłącznie gotówki, czyli „pieniądza" w najbardziej płynnej postaci, ale także wiele innych aktywów finansowych, w przypadku których ustawodawca uznaje, że stopień ich płynność niemal całkowicie usuwa ryzyko utraty wartości[276]. „Innymi aktywami finansowymi" nie są natomiast kryptowaluty, charakteryzujące się dużym ryzykiem kursowym i podatnością na manipulacje cenowe, a ponadto nie pełnią one roli surogatu pieniądza oraz nie są powszechnie akceptowane w obrocie gospodarczym.

Jak zatem w omawianym kontekście wygląda instytucja „pieniądza elektronicznego", którego nazwa mylona jest w decyzjach procesowych z pojęciem „środki pieniężne zapisane na rachunku"? Jego definicję legalną zapisano w art. 2 pkt 21a u.u.p.[277]; jest to wartość pieniężna przechowywana elektronicznie, w tym magnetycznie, wydawana, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowana przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego. Upraszczając nieco tę definicję, można stwierdzić, że chodzi o zbiór danych informatycznych zapisanych na karcie magnetycznej (karta pre-paid) lub w wirtualnej „portmonetce" działającej w Internecie w celu dokonywania transakcji płatniczych akceptowanych przez inne podmioty. Jednostki pieniądza elektronicznego zapisane są na serwerze jego emitenta i korzysta się z nich np. w trakcie dokonywania zakupów. System nie pobiera bezpośrednio pieniędzy zapisanych na rachunku bankowym, ale wpierw rozliczenie odbywa się w jednostkach pieniądza elektronicznego i dlatego stanowi on inny środek płatniczy, o którym mowa w art. 115 § 9 k.k. Taki nośnik wartości, np. w postaci specjalnej karty magnetycznej, nie jest powiązany z kontem bankowym użytkownika pieniądza elektronicznego, a umieszczone na nośniku jednostki rozliczeniowe różnią się pod względem technicznym od pieniądza bezgotówkowego, ale wyrażane są w takich samych jednostkach jak ten pieniądz, tj. polskich złotówkach. Pierwsze zezwolenie Komisji Nadzoru Finansowego na wydawanie pieniądza elektronicznego oraz świadczenie usług płatniczych w charakterze krajowej instytucji pieniądza elektronicznego udzielone zostało spółce Billon Solutions Sp. z o.o. Działający w Polsce przestępcy często wykorzystują usługi świadczone przez transgraniczne unijne instytucje pieniądza elektronicznego takie, jak np. Revolut czy PayPal do transferu i prania pieniędzy pochodzących z nielegalnych źródeł. Z drugiej strony technologia funkcjonowania pieniądza elektronicznego,

[276] J. Gad, E. Walińska, A. Wencel, *Art. 2. Zakres podmiotowy ustawy*, *teza 25*, [w:] *Ustawa o rachunkowości. Komentarz*, red. E. Walińska, Wolters Kluwer Polska 2023, LEX.

[277] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2021 r. poz. 1907, 1814, 2140), dalej jako: u.u.p. albo ustawa o usługach płatniczych. Definicja pieniądza elektronicznego została wprowadzona do ustawy o usługach płatniczych nowelizacją z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. z 2013 r. Nr 1036), która weszła w życiu w dniu 7 października 2013 r.; przed tą datą kwestie pieniądza elektronicznego regulowała ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych.

tj. fakt, że zarządzanie nim odbywa się na serwerach, w chmurze obliczeniowej czy mikroprocesorze plastikowej karty, powoduje, że stanowi on przedmiot różnych zagrożeń związanych z cyberprzestępczością.

Jak rozumieć natomiast zastosowane przez ustawodawcę pojęcie „rachunek", na którym zapisano środek pieniężny? W języku polskim „rachunek" stanowi podsumowany spis należności za towar lub usługi lub wyrażony w liczbach stan majątku albo kapitału jako rezultat obrotów finansowych; także zapis wpływów i wydatków[278]. Jednak odszyfrowując ten zwrot, nie można opierać się tylko na wykładni językowej, bowiem w art. 115 § 9 k.k. mowa jest o rachunku, na którym zapisano środki pieniężne. Wykładnia systemowa i historyczna omawianej regulacji prowadzi do wniosku, że chodzi o zapis środków pieniężnych w formie elektronicznej, a nie rachunek „papierowy". W uzasadnieniu do projektu ustawy, która znowelizowała art. 115 § 9 k.k., wskazano, że rozszerzenie zakresu pojęcia „rzeczy" w prawie karnym miało na celu usunięcie wątpliwości odnośnie tego, czy środki pieniężne znajdujące się na rachunku płatniczym lub bankowym można uznać za rzecz ruchomą, a tym samym za dowód rzeczowy. Wcześniej istniały na tym tle rozbieżności, chociaż jedna z linii orzeczniczej wskazywała, że dopuszczalne jest uznanie wymienionych środków, tj. w formie zapisu na rachunku bankowym, za rzecz ruchomą. W związku z powyższym zaproponowano, aby wskazać wprost w art. 115 § 9 k.k., że jako rzeczy ruchome przyjmuje się także środki pieniężne zapisane na rachunku bankowym, płatniczym czy jakimkolwiek innym[279].

Chodzi przede wszystkim o rachunek bankowy jako przedmiot umowy opisanej w art. 725 k.c.[280]; zgodnie z tym przepisem „Przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych". Mowa zatem o „urządzeniu" księgowym prowadzonym przez bank, służącym do ewidencjonowania należności między stronami relacji prawnej: bankiem i posiadaczem rachunku. Należności te powstają w wyniku realizacji wpłat, transferów i wypłat pieniędzy z rachunku. Wspomniane „urządzenie" obrazuje – w ujęciu dynamicznym – stan świadczeń pieniężnych w ramach takiej relacji. W znaczeniu księgowym wpis na rachunku płatniczym polega na dokonaniu – na podstawie dowodu księgowego – technicznej operacji zmieniającej stan należności ujawniony na rachunku: zwiększeniu (uznaniu) albo zmniejszeniu (obciążeniu). Rachunek ma charakter dwustronny i służy do ewidencjonowania należności, jakie przysługują posiadaczowi wobec banku: gdy występują takie należności, saldo

[278] https://sjp.pwn.pl/slowniki/rachunek.html [dostęp: 23.07.2023].

[279] Uzasadnienie do projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, wdrażającej dyrektywę Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.04.2014, str. 39), LEX.

[280] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2022 r., poz. 1360 z późn. zm.), dalej jako: k.c. lub Kodeks cywilny.

rachunku jest dodatnie. Może być także wykorzystywany do księgowania należności banku wobec posiadacza: na rachunku powstaje wtedy saldo ujemne (debet), które wskazuje na istnienie rodzaju roszczeń (np. dotyczących naliczonych opłat lub prowizji)[281]. Podstawę prawną funkcjonowania takich rachunków stanowi wspomniany już art. 725 k.c., regulujący konstrukcję umowy nazwanej, której podstawową treść wyznaczają przepisy prawa cywilnego i zawieraną przez banki w ramach wykonywania czynności bankowych.

Rachunek bankowy zawiera się w szerszym pojęciu, jakim jest rachunek płatniczy. Przepis art. 2 pkt 25 u.u.p. definiuje go jako „rachunek prowadzony dla jednego lub większej liczby użytkowników służący do wykonywania transakcji płatniczych, przy czym przez rachunek płatniczy rozumie się także rachunek bankowy oraz rachunek członka spółdzielczej kasy oszczędnościowo-kredytowej, jeżeli rachunki te służą do wykonywania transakcji płatniczych". Transakcja płatnicza z kolei, to zainicjowana przez płatnika lub odbiorcę wpłata, transfer lub wypłata środków pieniężnych (art. 2 pkt 29 u.u.p.). Zatem przewidziane przez Prawo bankowe[282] jeszcze inne rodzaje rachunków bankowych, tj. rachunki lokat terminowych, rachunki oszczędnościowe, rachunki oszczędnościowo-rozliczeniowe, w tym rachunki rodzinne, oraz rachunki terminowych lokat oszczędnościowych, a ponadto rachunki powiernicze, a także stanowiące podkategorie rachunku bankowego: rachunek VAT oraz rachunek escrow służący do nadzorowania rozliczenia transakcji między stronami – będą rachunkami płatniczymi, jeśli wykorzystywane są do płatności pieniężnych.

Oprócz banków, rachunek płatniczy może prowadzić także krajowa i unijna instytucja płatnicza (art. 2 pkt 11 u.u.p.). Pierwsza z wymienionych to osoba prawna z siedzibą na terytorium Rzeczypospolitej Polskiej, świadcząca wszystkie lub wybrane usługi płatnicze; chodzi m.in. o przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego, realizację transferów środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia zapłaty przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, wykonywanie transakcji płatniczych, w przypadku których zgoda płatnika na wykonanie transakcji udzielana jest przy użyciu urządzenia telekomunikacyjnego, cyfrowego lub informatycznego, a płatność przekazuje się dostawcy usług telekomunikacyjnych, cyfrowych lub informatycznych, działającemu jedynie jako pośrednik pomiędzy użytkownikiem zlecającym transakcję płatniczą a odbiorcą. Krajowa instytucja płatnicza, pod warunkiem posiadania odpowiedniego poziomu funduszy własnych, może także świadczyć usługi w zakresie emisji pieniądza elektronicznego. Napisano już, że tenże pieniądz elektroniczny często mylnie utożsamiany jest, nawet przez sędziów i prokuratorów, ze środkami pieniężnymi przechowywanymi na rachunku bankowym, a błędy w tym zakresie przenikają do

[281] T. Czech, *Wpis na rachunek płatniczy*, „Monitor Prawa Bankowego" 2019, nr 10, LEX.

[282] Zob. art. 49 ust. 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439, 2447), dalej jako: Prawo bankowe.

orzeczeń sądowych. Stało się tak w przypadku wyroku Sądu Rejonowego w Jeleniej Górze, który w uzasadnieniu orzeczenia z dnia 21 kwietnia 2015 r. stwierdził, jakoby karta płatnicza dawała dostęp do pieniądza elektronicznego, który w rozpoznawanej sprawie „stanowił kwotę 1000 zł"[283]. Sąd Okręgowy w Lublinie w orzeczeniu datowanym na 28 czerwca 2017 r. ustalił, że pieniądz elektroniczny stanowi jeden z rodzajów występującego w postaci niematerialnej pieniądza identycznego jak ten zapisany na rachunku bankowym[284]. Podobnie Sąd Okręgowy w Białymstoku w wyroku z dnia 28 maja 2021 r. popełnił błąd, twierdząc, iż sprawca, włamując się na rachunek bankowy pokrzywdzonego, uzyskał dostęp do mienia w postaci pieniądza elektronicznego[285]. W dwóch ostatnich przypadkach dokonana przez sądy niewłaściwa subsumpcja normy prawnej na podstawie błędnych ustaleń faktycznych nastąpiła z powołaniem się na poglądy M. Mozgawy, który w komentarzu do art. 115 § 9 k.k. stwierdził, że pieniądz elektroniczny to jedna z postaci pieniądza, tak samo jak pieniądz zapisany na rachunku czy też występujący w jakiejkolwiek postaci niematerialnej[286].

Działalność krajowych instytucji płatniczych ma charakter koncesjonowany, co oznacza, że wymaga uprzedniego uzyskania zezwolenia Komisji Nadzoru Finansowego oraz wpisu do prowadzonego przez KNF rejestru dostawców usług płatniczych. Komisja prowadzi rejestr, do którego wpisywane są krajowe instytucje płatnicze, biura usług płatniczych, spółdzielcze kasy oszczędnościowo-kredytowe i Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa, krajowe instytucje pieniądza elektronicznego oraz oddziały zagranicznych instytucji takiego pieniądza. Jest on jawny i dostępny na stronie internetowej KNF (https://e-rup.knf.gov.pl/); sędzia lub prokurator może skorzystać z rejestru w razie wątpliwości, czy przestępstwo dotyczy „środka pieniężnego zgromadzonego na rachunku" w myśl art. 115 § 9 k.k.[287], czy jednak innego, niesformalizowanego prawnie, cyfrowego aktywa.

Na podstawie dotychczas przeprowadzonej analizy nasuwa się pytanie: Czy środki pieniężne zgromadzone na rachunkach bankowych, które nie są rachunkami płatniczymi i nie służą do wykonywania transakcji płatniczych (art. 2 pkt 25 u.p.p. in fine), będą spełniały definicję rzeczy w rozumieniu art. 115 § 9 k.k.?

Chodzi m.in. o niektóre rachunki oszczędnościowe służące, jak sama nazwa wskazuje, do gromadzenia oszczędności na warunkach korzystnych dla klienta banku, ale bez możliwości wykonywania transakcji płatniczych. Pytanie dotyczy także rachunku prowadzonego do obsługi kredytu, czyli ewidencjowania wpłat od kredytobiorcy tytułem spłaty zadłużenia – nie jest on rachunkiem płatniczym, gdyż prowadzony jest dla banku w związku z relacją kredytową. Ponieważ w definicji legalnej rzeczy jest mowa

[283] Wyrok Sądu Rejonowego w Jeleniej Górze z dnia 21 kwietnia 2015 r., II K 1177/14, LEX nr 1862061.
[284] Wyrok Sądu Okręgowego w Lublinie z dnia 28 czerwca 2017 r., IV K 65/13, LEX nr 2385636.
[285] Wyrok Sądu Okręgowego w Białymstoku z dnia 28 maja 2021 r., III K 7/21, LEX nr 3354429.
[286] Zob. M. Budyn-Kulik, P. Kozłowska-Kalisz, *Art. 115*, *teza 5*, [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2023.
[287] 30 lipca 2022 r. w rejestrze wpisanych było 1465 podmiotów, a rok później (4 lipca 2023 r.) już 1575.

o rachunku, a nie „rachunku płatniczym", to środki zgromadzone na rachunku oszczędnościowym lub hipotecznym mieszczą się w legalnej definicji rzeczy i mogą stanowić przedmiot przestępstwa opisanego w art. 278 § 1 k.k. lub 279 § 1 k.k.

4.2. Własność środków zgromadzonych na rachunku i podmiot pokrzywdzony przestępstwem

W umowie rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych. Na podstawie umowy bank otwiera rachunek bankowy, na którym nie są fizycznie przechowywane środki pieniężne, lecz dokonuje się wpisów odzwierciedlających operacje, zwiększające lub uszczuplające stan posiadania. Wpis pełni także funkcję konstytutywną, stanowiąc materialnoprawną przesłankę rozporządzania przez posiadacza zgromadzonymi środkami pieniężnymi. Znaczenie wpisu polega więc na tym, że określa on wierzytelność posiadacza rachunku do banku, który zobowiązany jest na jego żądanie wypłacić określoną kwotę pieniędzy lub wykonać polecenie przelewu, polecenie zapłaty, czy inne zlecenie. Inaczej rzecz ujmując, bank jest dłużnikiem posiadacza rachunku do wysokości zapisanej na rachunku kwoty. Zgodnie z art. 50 ust. 1 i 2 ustawy Prawo bankowe, posiadacz takiego rachunku ma prawo swobodnie dysponować środkami pieniężnymi zgromadzonymi na rachunku, chociaż w umowie z bankiem mogą być zawarte postanowienia ograniczające ową swobodę. Co bardzo ważne, po stronie banku leży obowiązek dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Jednocześnie, zgodnie z treścią przepisu art. 56 ust. 1 u.u.p., bank ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika, a w razie wystąpienia nieautoryzowanej transakcji – ma obowiązek dokonania niezwłocznego zwrotu kwoty transakcji i przywrócenia stanu poprzedniego na koncie. Zgromadzona na rachunku bankowym kwota stanowi zatem własność banku, a nie posiadacza rachunku, a tym bardziej nie jest własnością osoby trzeciej, na polecenie której określona kwota ten rachunek zasiliła, choćby nawet dokonała omyłkowej wpłaty. Dlatego przedmiotem zajęcia egzekucyjnego nie jest ani gotówka, ani sama kwota zapisana, inaczej mówiąc zaksięgowana, na rachunku bankowym, lecz wierzytelność posiadacza rachunku bankowego wobec banku o wypłatę tej kwoty[288].

Skoro z chwilą wpłacenia środków na rachunek bankowy posiadacz tych środków traci prawo własności do nich, a zyskuje roszczenie do banku o zwrot aktywów, to zasadne staje się pytanie: Kto jest podmiotem pokrzywdzonym w wypadku przestępstwa

[288] Wyrok Sądu Najwyższego z dnia 27 października 2016 r., V CSK 48/16, http://www.sn.pl/sites/orzecznictwo, [dostęp: 02.08.2022]. Podobnie: wyrok Sądu Najwyższego z dnia 18 lutego 2004 r., V CK 233/03, LEX nr 550934; wyrok Sądu Najwyższego z dnia 4 października 2007 r., V CSK 255/07, OSNC – ZD 2008, nr 3, poz. 79.

kradzieży środków z rachunku bankowego: klient banku, bank czy dwa podmioty łącznie?

Na temat instytucji „pokrzywdzonego przestępstwem" w literaturze przedmiotu napisano już bardzo wiele. Wymóg bezpośredniości pokrzywdzenia należy interpretować tak, aby krąg pokrzywdzonych mieścił się w zespole znamion czynu będącego przedmiotem postępowania. Nie ma przy tym znaczenia, czy dobro prawne naruszone lub zagrożone przestępstwem jest głównym, czy też ubocznym przedmiotem ochrony na tle konkretnej normy prawnej[289]. Owa bezpośredniość pokrzywdzenia zachodzi wówczas, gdy pomiędzy czynem zawierającym przedmiotowe znamiona przestępstwa a naruszeniem dobra danego podmiotu nie ma ogniw pośrednich. Dopiero zrealizowanie tego znamienia statuuje dany podmiot, przy wystąpieniu pozostałych przesłanek, jako pokrzywdzonego i w konsekwencji legitymuje go do możności zasądzenia na jego rzecz obowiązku naprawienia przez oskarżonego szkody wyrządzonej czynem zabronionym[290].

Wynika z tego, że w przypadku przestępstwa kradzieży środków pieniężnych zapisanych na rachunku, pokrzywdzonym jest bank jako ich właściciel, oraz klient banku, gdyż faktycznie traci on, przynajmniej czasowo, możliwość dysponowania środkami. Jednak w praktyce najczęściej dzieje się inaczej i od początku prowadzenia postępowania przygotowawczego jako pokrzywdzonego przestępstwem wskazuje się tylko posiadacza rachunku bankowego. Powoduje to, że cały „ciężar" aktywnego uczestniczenia w czynnościach procesowych spada na osobę fizyczną, podczas gdy bank dysponujący profesjonalnym zapleczem kadrowym, także prawników specjalizujących się w prawie karnym, sytuuje się w roli „biernego obserwatora" w toczącym się śledztwie. Sytuacja klienta banku, który w wyniku przestępstwa utracił środki zgromadzone na rachunku bankowym, staje się tym bardziej uciążliwa, że instytucje finansowe często nie poczuwają się do zwrotu utraconych przez niego środków, tylko czekają na zakończenie śledztwa, które przecież może ciągnąć się miesiącami. Jeśli dojdzie do kradzieży środków, to konsumentowi przysługuje co prawda uprawnienie dochodzenia od banku roszczenia o ich zwrot, ale zbyt często reklamacje zostają nieuznane. Banki twierdzą, że utrata środków nastąpiła z powodu niezachowania przez posiadacza rachunku środków cyberbezpieczeństwa w wyniku np. zainstalowania na komputerze niesprawdzonego oprogramowania albo kliknięcia przez posiadacza rachunku w link „fałszywej" wiadomości mailowej i uruchomienia malware'a. Tymczasem orzecznictwo sądowe uznaje, iż bank jako podmiot, który winien cieszyć się niezwykle wysokim zaufaniem publicznym, musi dołożyć należytej, szczególnej staranności i skutecznie zabezpieczyć powierzone mu środki. Tyle mówi prawo. Jednak praktyka pokazuje, że w zderzeniu z profesjonalną instytucją

[289] I. Zielinko, *Bezpośredniość jako element definicji pokrzywdzonego w procesie karnym*, „Przegląd Sądowy" 2014, nr 3, s. 88–99.

[290] Wyrok Sądu Najwyższego z dnia 10 lutego 2022 r., V KK 543/21, LEX nr 3348356.

finansową klient nierzadko pozostaje bezradny i osamotniony, gdy naprzeciwko niego w sądzie zasiadają wykwalifikowani prawnicy reprezentujący interesy banku.

Jedna ze spraw w której zdaniem autora, niesłusznie przerzucono na klienta banku odpowiedzialność za utratę środków pieniężnych w wyniku wyrafinowanego cyberataku, toczyła się przed Sądem Rejonowym dla Łodzi-Śródmieścia w Łodzi[291]. Sąd ustalił, że bank prowadził dla powódki A. S. indywidualny rachunek oszczędnościowo-rozliczeniowy i nie stawiał klientce szczególnych wymagań dotyczących sprzętu lub oprogramowania, a sugerował jedynie, by korzystała z programu antywirusowego oraz aktualnego systemu operacyjnego i przeglądarki. Aby uzyskać dostęp do usług elektronicznych instytucji finansowej, wystarczyło posługiwać się zwykłym komputerem i aktualnym systemem operacyjnym oraz przeglądarką. Powódka zainstalowała w komputerze program antywirusowy, a w smartfonie miała takie oprogramowanie wgrane przez operatora telefonii komórkowej. Regularnie czytała też komunikaty dotyczące bezpieczeństwa, pojawiające się na stronie internetowej banku, ale przed 17 sierpnia 2016 r. nie zapoznała się z informacją dotyczącą zagrożeń związanych z fałszywymi mailami. Procedura dostępu do konta za pośrednictwem Internetu wymagała podania danych identyfikacyjnych, a klient dokonywał autoryzacji dostępu za pomocą loginu nadawanego przez bank i statystycznego hasła znanego wyłącznie klientowi. Przelew wierzytelności na rachunek innego użytkownika wymagał autoryzacji transakcji dokonywanej poprzez kod wysyłany przez bank SMS-em.

17 sierpnia 2016 r. o godzinie 16:52 cyberprzestępca przeprowadził atak i powódka otrzymała mail z adresu „BZWBKbzwbk@informacje-wbk.com" o treści: „Natychmiastowa blokada rachunku Bank /…/! W trosce o bezpieczeństwo naszych konsumentów zablokowaliśmy konto w systemie /…/ Internet, powodem jest nieautoryzowany dostęp do konta. W celu uzyskania informacji, oraz odblokowania dostępu prosimy o weryfikację właściciela rachunku logując się na ‚weryfikacjazespółbankzachodniwbksa'.

Słowo „weryfikacja" opatrzone zostało hiperłączem, a powódka była przeświadczona, że nadawcą powyższej wiadomości był bank, gdyż we wcześniejszych okresach prowadziła korespondencję elektroniczną z instytucją finansową. A. S. podjęła zatem bezskuteczną próbę logowania do serwisu internetowego w celu uzyskania informacji o nieautoryzowanym dostępie do jej rachunku bankowego oraz odblokowania konta. Następnie skorzystała z hiperłącza znajdującego się w treści wiadomości i została przekierowana do domeny, na której zamieszczona została witryna internetowa łudząco podobna do serwisu bankowego. Powódka nie zauważyła żadnej różnicy w szacie graficznej, treści czy stosowanych zabezpieczeniach na tej stronie, podała swoje dane osobowe i hasło, a potem otrzymała SMS-a z komunikatem o przesłaniu kolejnym SMS-em kodu do dalszej weryfikacji. A. S. otrzymała na telefon kod, wpisała go we wskazanym polu; za chwilę dostała kolejne SMS-y wysyłane przez przestępcę, który podszywał się pod pracownika banku. Pomimo spełnienia wytycznych otrzymanych na telefon, A. S. nadal

[291] Wyrok Sądu Rejonowego dla Łodzi-Śródmieścia w Łodzi, XVIII C 4854/16, LEX nr 2538475.

nie mogła zalogować się do swojego konta, co wzbudziło jej podejrzenia, dlatego skontaktowała się z konsultantem instytucji finansowej. Wtedy dowiedziała się o kradzieży z jej rachunku kwoty 9800 zł oraz 9200 zł przelewami systemu bluecash.

Na skutek opisanego zdarzenia A. S. złożyła reklamację do banku o zwrot utraconych środków, która została negatywnie rozpoznana, i pismem z 31 sierpnia 2016 r. A. S. wezwała bank do naprawienia szkody poprzez przywrócenie obciążonego rachunku płatniczego do stanu sprzed wykonania nieautoryzowanych transakcji płatniczych; bank odrzucił żądanie. Pozwany poinformował powódkę, po analizie zdarzenia, że podała dane identyfikacyjne i hasło do usługi, logując się na fałszywej stronie banku, a wiadomość mailowa zawierająca prośbę o weryfikację danych została skierowana do niej przez podmiot podszywający się pod pozwanego. W śledztwie prowadzonym przez Prokuraturę Okręgową we Wrocławiu ujawniono 54 pokrzywdzonych cyberatakiem z 17 sierpnia 2016 r. Mając na uwadze powyższe, Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi, stosownie do art. 46 u.u.p., zasądził na rzecz powódki kwoty dochodzone pozwem jako pobrane na skutek nieautoryzowanych przez powódkę transakcji, wraz z odsetkami zasądzonymi na postawie art. 481 § 1 i 2 k.c.

Apelację od wyroku złożył pozwany, domagając się jego zmiany poprzez oddalenie powództwa, a Sąd Okręgowy w Łodzi w decyzji z dnia 27 marca 2018 r.[292] w całości podzielił stanowisko banku. W ocenie sądu odwoławczego A. S. wykazała się rażąco nienależytą starannością przy wypełnianiu wynikającego z umowy ramowej obowiązku nieudostępniania osobom nieuprawnionym indywidualnych zabezpieczeń instrumentów płatniczych, w tym kodu identyfikacyjnego umożliwiającego dostęp do konta. Choć powódka nie wiedziała, że podmiot, któremu dane udostępnia, nie jest instytucją finansową, to jednak jej przekonanie nie znajdowało jakiegokolwiek usprawiedliwienia w okolicznościach sprawy, zważywszy, że opierało się ono jedynie na niczym niepopartych zapewnieniach nadawcy wiadomości mailowej. Okolicznością taką nie mogło być też przekierowanie jej przez nadawcę maila na stronę, której witryna była łudząco podobna do witryny portalu banku, gdyż z równym powodzeniem mógł to być kolejny etap przestępczego planu zmierzającego do bezprawnego skłonienia klienta, aby udostępnił indywidualne zabezpieczenia instrumentów płatniczych. Według sądu, zarzut, jaki można było postawić A. S., polegał na lekkomyślnym powzięciu nieuzasadnionego przekonania, przy zaniedbaniu jakiejkolwiek jego weryfikacji, że podmiot podający się za bank jest nim rzeczywiście, ale równocześnie nie sposób pominąć, że gdyby w ramach wcześniejszych kontaktów z pozwanym powódka nie pomijała kierowanych do niej ostrzeżeń, powzięcie takiego przekonania, skutkującego rażącą nieostrożnością i podaniem osobie nieuprawnionej przedmiotowych danych, byłoby wykluczone, gdyż niezwłocznie rozpoznałaby ona metodę postępowania przestępców i byłoby dla niej jasne, że nie powinna ufać nadawcy fałszywych wiadomości. Podsumowując poczynione ustalenia, sąd stwierdził, że skoro powódka, jako płatnik w rozumieniu ustawy

[292] Wyrok Sądu Okręgowego w Łodzi z dnia 27 marca 2018 r., III Ca 51/18, LEX nr 2538475.

o usługach płatniczych naruszyła swe obowiązki wskutek rażącego niedbalstwa, czego konsekwencją były nieautoryzowane transakcje płatnicze, to przyjąć należy, iż to właśnie ona – w myśl art. 46 ust. 3 u.u.p. – odpowiada w pełnej wysokości za ich skutki. Z odpowiedzialności w tym zakresie zwolniony jest pozwany bank, co czyni niezasadnymi roszczenia dochodzone pozwem i powództwo winno zostać oddalone.

Wyrok Sądu Okręgowego w Łodzi stoi w sprzeczności z linią orzeczniczą sądów cywilnych wskazującą, iż w przypadku kradzieży środków z rachunku bankowego, podmiotem poszkodowanym winien być w zasadzie bank, a nie konsument. Z mocy umowy o otwarcie i utrzymanie rachunku bankowego, to bank staje się właścicielem środków zdeponowanych przez klienta na koncie, a osoba fizyczna posiada jedynie wymagalną wierzytelność względem banku dotyczącą natychmiastowej wypłaty środków na jej zlecenie. W przypadku wyłudzenia pieniędzy z rachunku szkoda powstaje po stronie banku, a nie po stronie klienta, albowiem bank nadal jest zobowiązany do wypłacenia środków klientowi zgodnie z zawartą umową. Jedynym wyjątkiem jest sytuacja, w której konsument – użytkownik rachunku bankowego - umyślnie doprowadza do kradzieży środków z rachunku albo dochodzi do niej w wyniku leżącego po stronie klienta rażącego niedbalstwa w zakresie naruszenia obowiązków wynikających z ustawy o usługach płatniczych. Trudno mówić o „rażącym niedbalstwie" w zachowaniu A. S., która stała się podmiotem wyrafinowanego cyberataku z wykorzystaniem zaawansowanych narzędzi technologicznych, łącznie ze stroną internetową doskonale imitującą faktyczną witrynę banku, oraz socjotechniki. Twierdzenie Sądu Okręgowego w Łodzi, że kobieta nie przeczytała jednego z wielu komunikatów ostrzegających o oszukańczej kampanii mailingowej prowadzonej przez przestępców, nic nie zmienia w ocenie sytuacji, gdyż obecnie każdy użytkownik bankowości elektronicznej regularnie zalewany jest takimi wiadomościami i nie sposób od niego wymagać, aby każdą przeczytał i na tej podstawie rozpoznawał zaawansowane działania cyberprzestępców. Ocena prawna zdarzenia kształtuje się zupełnie inaczej, gdy użytkownik rachunku bankowego świadomie przekazuje innej osobie dane dostępowe do tego rachunku lub nie zgłasza bankowi kradzieży karty płatniczej. Wówczas jego odpowiedzialność cywilna za kradzież środków z konta jest oczywista.

Przekładając wszystkie poczynione wyżej uwagi na prawo karne i praktyczne aspekty pracy prokuratora, należy postulować, aby przynajmniej na pierwszym etapie postępowania przygotowawczego dotyczącego kradzieży środków z rachunku bankowego jako pokrzywdzonych wskazywać zarówno bank, jak i posiadacza rachunku. Do takiego wniosku doszedł Sąd Apelacyjny w Warszawie w wyroku z dnia 29 października 2018 r. stwierdzając, że:

> Przyjęcie, że bank uzyskuje własność deponowanych pieniędzy – prowadzi do prostej konkluzji, że bank jest osobą bezpośrednio pokrzywdzoną w wypadku

bezprawnego przełamania zabezpieczeń i dokonania przelewu pieniędzy na rzecz osoby nieuprawnionej[293].

W takim przypadku pokrzywdzonym jest także klient banku, na co zwrócił uwagę Sąd Najwyższy w postanowieniu z dnia 28 kwietnia 2016 r., rozpatrując stan faktyczny, w którym środki pieniężne z rachunków bankowych zostały wyprowadzone poprzez nieuprawnioną zmianę, dokonaną przez nieustalonego hakera, danych informatycznych w aplikacji elektronicznej obsługiwanej przez klienta banku i przelane na inne konto. Sąd Najwyższy stwierdził:

Mimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Ochronę wierzytelności gwarantują posiadaczowi przepisy prawa cywilnego, finansowego i oparta na nich umowa z bankiem. To jednak, że posiadacz nie ponosi szkody, gdyż wartość aktywów podlegających zwrotowi na jego rzecz przez bank nie ulega zmianie po wypłacie osobie nieuprawnionej, nie oznacza automatycznie, że w żadnym konkretnym przypadku nie dochodzi do bezpośredniego naruszenia dobra prawnego posiadacza rachunku[294].

Sąd Najwyższy przyznał posiadaczowi rachunku bankowego, z którego dokonano wypłaty środków pieniężnych osobie nieuprawnionej, status pokrzywdzonego w rozumieniu art. 49 § 1 k.p.k. Zdaniem sądu, osoba taka posiadała legitymację do wystąpienia w roli oskarżyciela posiłkowego (subsydiarnego) w postępowaniu karnym w sytuacji, gdy doszło do wypłaty środków z jego konta na rzecz osoby nieuprawnionej. Wypłata środków pieniężnych takiej osobie, niekorzystna dla banku, może być uznana *in concreto* za rozporządzenie niekorzystne, w rozumieniu art. 286 § 1 k.k., także dla posiadacza rachunku. Jego dobro prawne, mające źródło w umowie rachunku bankowego, zostaje bezpośrednio naruszone wtedy, gdy uprawnienie do uzyskania zwrotu zdeponowanych środków pieniężnych na każde żądanie nie zostanie zrealizowane przed skorygowaniem przez bank stanu konta. Do tego czasu posiadacz rachunku nie dysponuje środkami, które wypłacono osobie nieuprawnionej, co może pociągnąć określone ujemne następstwa w jego majątku, także w zakresie *lucrum cessans*. Nie ma więc podstaw, by *a limine* odmówić posiadaczowi rachunku statusu pokrzywdzonego w rozumieniu art. 49 § 1 k.p.k., a w konsekwencji legitymacji do wniesienia aktu oskarżenia w trybie art. 55 § 1 k.p.k. wtedy, gdy osoba nieuprawniona, działając w celu osiągnięcia korzyści

[293] Wyrok Sądu Apelacyjnego w Warszawie z dnia 29 października 2018 r., II AKa 400/18, LEX nr 2593608.
[294] Postanowienie Sądu Najwyższego z dnia 28 kwietnia 2016 r., I KZP 3/16, OSNKW 2016/6/37.

majątkowej doprowadziła do wypłaty środków pieniężnych z jego konta przez wprowadzenie w błąd przedstawiciela banku. Powinność usunięcia przez bank skutków wypłaty środków pieniężnych osobie nieuprawnionej (skorygowanie stanu konta) nie zmienia tego, że przedmiot dokonanej wypłaty pozostaje czasowo poza zasięgiem dyspozycji posiadacza rachunku, a tym samym poza możliwością wejścia w jego posiadanie, aż do przywrócenia właściwego stanu konta[295]. Wynika z tego, że chociaż zaistnienie przestępstwa nie powoduje automatycznie powstania szkody po stronie posiadacza rachunku, gdyż bank jest zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości, to jednak posiadacz rachunku jest osobą pokrzywdzoną takim przestępstwem.

Kwestia statusu podmiotów pokrzywdzonych przestępstwem oszustwa była rozpoznawana w jeszcze innej sprawie przez Sąd Najwyższy. Znamieniem skutku przestępstwa z art. 286 § 1 k.k., jak stwierdził sąd, jest niekorzystne rozporządzenie mieniem, a wypłata środków pieniężnych przez bank osobie nieuprawnionej jest takim rozporządzeniem. Prowadzi ona wprost do straty w majątku będącym własnością banku, a równocześnie zmniejsza odpowiednio stan konta posiadacza rachunku, chociaż nie powoduje straty w prawie majątkowym posiadacza, gdyż nie zmniejsza jego wierzytelności wobec instytucji finansowej. Ale to, czy oszukańcza wypłata, obniżająca saldo środków, stanowi lub nie stanowi dla posiadacza niekorzystnego rozporządzenia mieniem w rozumieniu art. 286 § 1 k.k., jest już zagadnieniem odrębnym. W doktrynie przyjmuje się, że pojęcie rozporządzenia mieniem, należące do opisu strony przedmiotowej przestępstwa oszustwa, ma znaczenie autonomiczne, właściwe dla szeroko zakreślonego przedmiotu ochrony. Obejmuje wszelkie czynności prowadzące do zmiany stanu majątkowego, w tym również zmiany we władaniu mieniem. Te ostatnie mogą wynikać z czynności, które pozbawiają osobę uprawnioną posiadania mienia, co oznacza, że nie muszą one mieć jednoznacznie cywilistycznej konotacji. Rozporządzeniem w rozumieniu art. 286 § 1 k.k. może być każda czynność zadysponowania mieniem, kształtująca określony stan prawny, a także stan faktyczny w zakresie władania mieniem. Stosownie do szeroko pojmowanego doprowadzenia do rozporządzenia mieniem jako znamienia określającego skutek przestępstwa oszustwa, interpretuje się pojęcie „niekorzystności" rozporządzenia, doprecyzowującego to znamię. Sąd Najwyższy podkreślił, że w orzecznictwie karnym utrwalony jest pogląd, iż powstanie szkody nie jest warunkiem koniecznym uznania rozporządzenia mieniem za niekorzystne. Ogólnie ujmując, niekorzystne rozporządzenie pociąga zmianę, która pogarsza sytuację majątkową osoby rozporządzającej lub innej osoby pokrzywdzonej. Warunkiem uznania rozporządzenia za niekorzystne nie jest ani wyrządzenie rzeczywistej szkody, ani też jej niepowetowalność. W szerszym aspekcie rzecz ujmując, niekorzystność rozporządzenia to utrata prawa podmiotowego o charakterze majątkowym, a ponadto niemożność korzystania lub pogorszenie warunków korzystania z tego prawa. Stąd też za niekorzystne trzeba uznać i takie rozporządzenia mieniem, które osobę uprawnioną pozbawiają lub ograniczają

[295] Postanowienie Sądu Najwyższego z dnia 28 kwietnia 2016 r., I KZP 3/16, OSNKW 2016, nr 6, poz. 37.

w jego posiadaniu[296]. W wyniku kradzieży środków pieniężnych z rachunku bankowego następuje zmiana salda i posiadacz rachunku traci konieczną przesłankę skutecznego zrealizowania wierzytelności w części odpowiadającej kwocie wypłaconej przestępcy. Wstrzymana zostaje możliwość korzystania przez niego w tym zakresie z uprawnienia do swobodnego dysponowania środkami pieniężnymi, o którym mowa w art. 50 ustawy Prawo bankowe, przez uzyskanie ich zwrotu na każde żądanie (art. 726 k.c.), bądź przez wydanie bankowi innej dyspozycji przewidzianej umową. Powoduje to, że w przypadku oszustwa nie tylko bank, ale także posiadacz rachunku ma status pokrzywdzonego przestępstwem przynajmniej do momentu, aż rachunek ponownie zostanie zasilony do wysokości skradzionych pieniędzy.

Zatem w przypadku przestępstw ukierunkowanych na środki pieniężne zgromadzone na rachunku z reguły pokrzywdzonym jest bank i posiadacz rachunku. Może się zdarzyć, że równolegle do postępowania karnego toczy się spór między nimi, kto jest odpowiedzialny, w rozumieniu prawa finansowego, za powstanie szkody. Spór prawny między bankiem a posiadaczem depozytu może utrzymywać się do momentu rozstrzygnięcia w postępowaniu arbitrażowym albo w procesie cywilnym. W tym czasie prokurator powinien uznać zarówno bank, jak i posiadacza rachunku, za pokrzywdzonego w toczącej się sprawie karnej w rozumieniu art. 49 § 1 k.p.k. Takie stanowisko zaprezentował Sąd Apelacyjny w Katowicach, twierdząc:

> Niewątpliwie wypłata przez bank środków pieniężnych osobie nieuprawnionej rodzić może ujemne skutki dla posiadacza rachunku, który jakkolwiek nie traci swojego prawa obligacyjnego w postaci wierzytelności względem banku, to jednak możliwość jej realizacji zostaje zawieszona do czasu skorygowania stanu konta. Tylko wtedy, gdy bank wypełni żądanie posiadacza rachunku bez opóźnienia, interes majątkowy posiadacza konta nie dozna żadnego uszczerbku. Może jednak dojść, przy różnicy stanowisk stron umowy, do impasu, który przeistoczy się w spór prawny. Do czasu jego rozstrzygnięcia posiadacz rachunku nie dysponuje środkami, które wypłacono osobie nieuprawnionej (które stały się przedmiotem zaboru), co może pociągnąć ujemne następstwa w jego majątku. Stąd posiadaczowi rachunku przysługuje status pokrzywdzonego, a w konsekwencji oskarżyciela posiłkowego[297].

4.3. Relacje pomiędzy art. 267 § 1–3 k.k., art. 278 § 1 k.k., art. 279 § 1 k.k. i art. 287 § 1 k.k.

Zbieg, realny lub pomijalny, wymienionych w tytule podrozdziału przepisów to zagadnienie, z którym sędziowie i prokuratorzy mają często do czynienia, gdyż dotyczy on wielu postępowań karnych chroniących zarówno mienie, ale także integralność danych

[296] Tamże.
[297] Wyrok Sądu Apelacyjnego w Katowicach z dnia 29 czerwca 2017 r., II AKa 151/17, LEX nr 2440808.

informatycznych. Dlatego duże znaczenie ma analiza problemów rysujących się na tym polu.

Art. 278. [Kradzież]
§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 2. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.
§ 3. W wypadku mniejszej wagi, sprawca
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
§ 4. Jeżeli kradzież popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.
§ 5. Przepisy § 1, 3 i 4 stosuje się odpowiednio do kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego.

Art. 279. [Kradzież z włamaniem]
§ 1. Kto kradnie z włamaniem,
podlega karze pozbawienia wolności od roku do lat 10.
§ 2. Jeżeli kradzież z włamaniem popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 287. [Oszustwo komputerowe]
§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 2. W wypadku mniejszej wagi, sprawca
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Kradzież środków pieniężnych zgromadzonych na rachunku powoduje wyjęcie ich spod władania banku, a zatem wyklucza możliwość korzystania ze środków przez posiadacza konta. Realizując przestępstwo, sprawca zmienia zapisy danych w różnych miejscach systemu informatycznego i teleinformatycznego nazywanego ogólnie systemem płatności bezgotówkowych. Powstaje zatem pytanie: Czy kwalifikacja prawna kradzieży środków pieniężnych zapisanych na rachunku powinna uwzględniać tylko art. 278 § 1 k.k. lub art. 279 § 1 k.k., a może pozostawać w kumulatywnej kwalifikacji czynu z art. 287 § 1 k.k.?

W piśmiennictwie za drugim rozwiązaniem opowiedział się A. Wąsek, twierdząc, że przepis art. 287 § 1 k.k. może pozostawać w kumulatywnym zbiegu z przepisem art. 279 § 1 k.k.[298] Także sądy, wydając wyroki, a prokuratorzy, formułując treść zarzutów, często przyjmują zbieg realny pomiędzy art. 279 § 1 k.k. i art. 287 § 1 k.k.; poniżej zamieszczono kilka przykładów takich decyzji procesowych:

dnia 12 maja 2020 r. przy użyciu zbliżeniowo karty płatniczej /…/ Bank dotyczącej prowadzonego rachunku bankowego o numerze /…/, wpłynął na automatyczne przetwarzanie danych informatycznych dokonując płatności za artykuły w sklepie w kwocie 29,62 zł, czym działał na szkodę /…/ Bank, tj. o przest. z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[299]

w dniu 28 grudnia 2016 roku w Krakowie działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru w celu osiągnięcia korzyści majątkowej poprzez użycie w transakcjach zbliżeniowych karty płatniczej wydanej przez Bank Powszechna Kasa Oszczędności Bank Polski S.A. należącej do pokrzywdzonej J. B., bez upoważnienia pokonał elektroniczne zabezpieczenie banku, wpływając na automatyczne przetwarzanie, gromadzenie i przekazywanie danych informatycznych i dokonując 10 włamań do systemu bankowego, a następnie dokonał kradzieży pieniędzy w kwocie odpowiednio 6,99 zł, 6,99 zł, 6,99 zł, 13,20 zł, 14,07 zł, 7,80 zł, 15,20 zł, 20,99 zł, 19,99 zł, 7,28 zł, stanowiących płatność za zakupiony towar, czym działał na szkodę J. B. powodując straty w łącznej wysokości 119,50 zł, tj. o przestępstwo z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[300]

w dniu 14 lutego 2016 r. w miejscowości N., /…/ bez upoważnienia wpłynął na automatyczne przetwarzanie danych informatycznych i zmienił zapis danych informatycznych rachunku /…/ prowadzonego przez Bank /…/ S.A., zmieniając saldo dostępnych środków pieniężnych znajdujących się na tym rachunku w ten sposób, że po uprzednim wejściu w posiadanie karty bankomatowej VISA Elektron /…/*******5540 należącej do E. Z., dokonał włamania na powyższy rachunek poprzez wprowadzenie kodu PIN bez wiedzy i zgody ww. w bankomacie, a następnie dokonał kradzieży pieniędzy w kwocie 2000 zł na szkodę E. Z. tj. o czyn z art. 279 § 1 k.k. w zb. z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[301]

[298] A. Wąsek, *Glosa do wyroku Sądu Najwyższego z dnia 11 września 2002 r.*, V KKN 9/01, OSP 2003, nr 7–8, poz. 103. Warto jednak odnotować, że ww. glosie autor napisał „wydaje się, że przyjęcie takiego zbiegu jest dopuszczalne", a więc nie był kategoryczny w swoich sądach.

[299] Wyrok Sądu Rejonowego w Jeleniej Górze z dnia 28 września 2020 r., II K 739/20, LEX nr 3102107.

[300] Akta Sądu Rejonowego dla Krakowa Nowej-Huty w Krakowie o sygn. II K 724/17/N.

[301] Wyrok Sądu Rejonowego w Legionowie z dnia 7 czerwca 2017 r., II K 406/16, LEX nr 2340308.

Analizując problem dotyczący zbiegu realnego lub pomijalnego pomiędzy art. 279 § 1 k.k. (art. 278 § 1 k.k.) i art. 287 § 1 k.k. w przypadku przestępczych transakcji kartami płatniczymi, wskazać należy, że każda taka transakcja powoduje zmianę wielu danych informatycznych na różnym poziomie funkcjonowania systemu kart płatniczych poprzez automatyczne przetwarzanie, gromadzenie, przekazywanie i w konsekwencji wprowadzenie nowych zapisów w pamięci urządzeń i narzędzi do obsługi transakcji bezgotówkowych. Pod względem technicznym kolejne etapy realizacji płatności wyglądają następująco:

1. posiadacz karty, chcąc uiścić należność za towar/usługę albo wypłacić gotówkę, przykłada kartę do terminalu POS[302], sensora karty zainstalowanego na bankomacie (wpłatomacie) lub wkłada kartę do czytnika (tzw. slotu). Terminal automatycznie rozpoznaje rodzaj karty i sprawdza m.in. limity ustanowione dla rachunku;
2. informacje odczytane przez terminal, w ramach autoryzacji, przesyłane są do centrum rozliczeniowego (ang. *acquirer*) i za jego pośrednictwem otrzymuje je wystawca karty, który sprawdza kwotę dostępnych środków na koncie płatnika oraz pozostałe dane, np. datę ważności „plastiku". W przypadku pozytywnej weryfikacji do terminalu akceptanta wysyłany jest komunikat zwrotny o możliwości przeprowadzenia zadeklarowanej operacji i jednocześnie na rachunku posiadacza karty blokowana jest zadysponowana kwota;
3. posiadacz karty proszony jest o autoryzację transakcji kodem PIN, jeśli przekracza ona kwotę 100 zł, otrzymuje pokwitowanie i może odebrać zakupiony towar lub pieniądze z bankomatu;
4. po zakończeniu dnia roboczego terminal akceptanta łączy się z centrum rozliczeniowym i przekazuje agentowi rozliczeniowemu dane o wszystkich wykonanych w ciągu ostatnich 24 godzin operacjach. Za pośrednictwem Krajowego Systemu Rozliczeń podsumowuje się krajowe transakcje przy użyciu kart płatniczych wydanych przez polskie banki;
5. w przypadku transakcji dokonanej przez posiadacza polskiej karty płatniczej za granicą lub zagraniczną kartą płatniczą w Polsce, jej rozliczenie następuje w systemie międzynarodowym organizacji zrzeszającej bank – wydawcę karty;
6. w terminie umownym centrum rozliczeniowe uznaje na rachunku odbiorcy kwotę transakcji;
7. *acquirer* za pośrednictwem systemu rozliczeniowego otrzymuje od wydawcy karty kwotę, na jaką opiewała transakcja (notę obciążeniową), a bank obciąża tą kwotą rachunek płatnika. Uzyskane środki agent rozliczeniowy przekazuje na rzecz akceptanta na rachunek bankowy wskazany przez niego w umowie;
8. centrum rozliczeniowe uiszcza na rzecz banku opłatę interchange, właściciel systemu rozliczeniowego uzyskuje bowiem dochód z tytułu opłat za wydanie karty

[302] Terminal POS (z ang. *point of sale*) to nowoczesne urządzenie służące do przyjmowania płatności bezgotówkowych. Dzięki terminalowi płatniczemu klienci punktów handlowo-usługowych mogą uiszczać cenę za zakupiony towar lub usługi za pomocą karty, mobilnie lub przy użyciu BLIK-a.

pod jego auspicjami oraz opłat za uwierzytelnienie, uzgodnienie sald i rozliczenie transakcji[303].

Widać zatem, że przestępcza transakcja dokonana z wykorzystaniem karty płatniczej powoduje różnego rodzaju zmiany danych informatycznych zapisywanych na serwerach banków, centrów rozliczeniowych, Krajowego Systemu Rozliczeń, a także w infrastrukturach IT innych podmiotów, które uczestniczyły w transakcji. W wyniku popełnionego przestępstwa zmiany danych informatycznych następują też w pamięci urządzenia wykorzystanego do realizacji przestępstwa, tj. karty płatniczej (chipa), terminala POS lub bankomatu. Podobnie, w wyniku nieuprawnionej transakcji w Internecie, tj. bez fizycznego użycia czytnika instrumentu finansowego, zmiana danych dokonuje się wielopoziomowo: w aplikacji bankowości mobilnej, na serwerze dostarczyciela usług sieciowych itd.

Jednak sprawca, w zakresie znamion strony podmiotowej czynu, dokonując transakcji kartowej, obejmuje swoim zamiarem chęć uzyskania korzyści majątkowej, a nie manipulowania danymi informatycznymi. W przypadku typowych wypłat bankomatowych lub zbliżeniowych, oprócz wpisania kodu PIN i żądanej kwoty lub zbliżenia mikroprocesora do czytnika, nie podejmuje on żadnych szczególnych działań, ukierunkowanych na manipulowanie cyfrowymi artefaktami: nie zmienia danych osobowych posiadacza konta, nie przeformatowuje umyślnie dziennika logów „atakowanego" urządzenia, nie instaluje złośliwego oprogramowania. Swoją świadomością obejmuje jedynie zamiar zaboru cudzego mienia bez konieczności naruszenia integralności danych. Podobnie jak osoba oskarżona o kradzież środków zgromadzonych na rachunku bankowym, także sędzia i prokurator posiadają zazwyczaj tylko ogólną wiedzę o sposobie przetwarzania danych przez system kart płatniczych.

Jeśli chodzi o znamiona określające czynność sprawczą, to kradzież polega na zaborze cudzej rzeczy ruchomej w celu przywłaszczenia, a jej typ kwalifikowany opisany w art. 279 § 1 k.k. wymaga dodatkowo, aby zabór poprzedzało włamanie. W przypadku w art. 287 § 1 k.k. zachowanie sprawcy może przybierać sześć rodzajów czynności sprawczej, a więc wpływanie na automatyczne przetwarzanie danych informatycznych, gromadzenie danych informatycznych, przekazywanie takich danych; zmianę zapisów danych informatycznych, ich usuwanie albo na wprowadzaniu nowych cyfrowych artefaktów. W przypadku nieuprawnionych wypłat bankomatowych i płatności w terminalach POS, weryfikowanych kodem PIN, „włamanie" jako czynność czasownikowa z art. 279 § 1 k.k. stanowi przełamanie zabezpieczenia poprzez użycie kodu lub mikroprocesora, co powoduje równocześnie transfer środków pieniężnych. Niekiedy dodatkowy warunek owego transferu stanowi manualne wprowadzenie stosownej dyspozycji, np. wybranie i zaakceptowanie kwoty do wypłaty lub wpisanie rachunku do przelania środków. Tak więc „kradzież" oznacza wprowadzenie nowych zapisów w urządzeniu w celu przelania środków pieniężnych, ale bez przełamywania zabezpieczeń, gdyż do

[303] P. Opitek, *Skimming, Cyberprzestępczość w bankowości elektronicznej*…, s. 35–37.

przełamania zabezpieczeń odnosi się znamię „włamania". Zatem realizacja dyspozycji art. 278 § 1 k.k. będzie miała miejsce, gdy dostęp do systemu jest otwarty, np. pokrzywdzony nie wylogował się z aplikacji bankowości mobilnej i pod jego nieobecność, mając dostęp do aplikacji, sprawca wprowadza zlecenie transakcji środków z rachunku „ofiary" na własne konto.

Wynika z tego, że w przypadku kradzieży środków pieniężnych z rachunku bankowego działanie sprawcy ukierunkowane jest na zabór rzeczy, a czynności sprawcze podjęte w tym kierunku są tożsame z wpływaniem bez upoważnienia na automatyczne przetwarzanie danych, o którym mowa w art. 287 § 1 k.k. Doszło zatem do konkurencji dwóch przepisów, gdyż ten sam czyn może być poddany ocenie z punktu widzenia dwóch norm sankcjonujących. Mowa jednak o zbiegu pomijalnym, gdyż skazanie sprawcy za przestępstwo kradzieży z włamaniem oddaje w opisanym przypadku całą zawartość kryminalną czynu i zbędne jest odwołanie się do konstrukcji zbiegu realnego. Zatem stanowiące przestępstwo wypłaty pieniędzy z wykorzystaniem kart płatniczych powinny być kwalifikowane z art. 279 § 1 k.k. (art. 278 § 1 k.k.), a nie art. 279 § 1 k.k. (art. 278 § 1 k.k.) i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. W tego typu sprawach zachodzi bowiem pomijalny zbieg przestępstw i należy z opisu czynu i jego kwalifikacji prawnej wyeliminować art. 287 § 1 k.k. Co prawda przepis konsumujący (art. 279 § 1 k.k.), literalnie rzecz biorąc, nie powiela znamion ustawowych zawartych w przepisie konsumowanym (art. 287 § 1 k.k.), jednak poprzez „sztuczny" zabieg ustawodawcy polegający na uznaniu środków zapisanych na rachunku za rzecz ruchomą (art. 115 § 9 k.k.), kradzież bezgotówkowego pieniądza bankowy należy typizować z przepisów, w których przedmiotem czynności wykonawczej jest rzecz (art. 279 § 1 k.k.), a nie dane informatyczne (art. 287 § 1 k.k.). Ponadto kradzież z włamaniem charakteryzuje się o wiele większym stopniem społecznej szkodliwości, aniżeli sama manipulacja danymi. W literaturze wskazywano natomiast, że u podstaw wyłączenia wielości ocen w ramach czystej wielości czynów leży generalne wskazanie teleologiczne, zgodnie z którym ukaranie za czyn o większej zawartości bezprawia usuwa możliwość ukarania za czyn o mniejszej zawartości bezprawia[304]. Zgodzić należy się zatem z S. Tarapatą, który twierdzi, że nie ma racjonalnego powodu, by nie uznać, że zakwalifikowanie nieautoryzowanej zbliżeniowej transakcji kartowej z art. 279 § 1 k.k. w pełni odzwierciedla całą kryminalną zawartość bezprawia takiego zachowania. Zbędnym jest zatem kwalifikowanie takiego czynu również z art. 284 § 1 k.k. oraz art. 287 § 1 k.k. Przepisy te pozostają w relacji pomijalnego zbiegu ustawy z art. 279 § 1 k.k.[305]

Stanowisko o pomijalnym zbiegu art. 279 § 1 k.k. i art. 287 § 1 k.k. zaprezentował Sąd Okręgowy w Gliwicach. W sprawie tej prokurator oskarżył sprawcę o to, że dokonał

[304] W. Macior, *Z problematyki zbiegu przestępstw i przepisów ustawy (w sprawie pozornego zbiegu realnego przestępstw)*, „Państwo i Prawo" 1965, nr 1, s. 77.

[305] S. Tarapata, *Wybrane prawnokarne zagadnienia związane z dokonywaniem płatności zbliżeniowej za pomocą cudzej karty płatniczej bez zgody osoby uprawnionej – uwagi na marginesie wyroku Sądu Najwyższego z 22.3.2017, III KK 349/16*, „Kwartalnik Prawa Publicznego" 2017, nr 4, LEX.

transakcji zbliżeniowej kartą bankomatową utraconą przez inną osobę, działając dodatkowo w warunkach multirecydywy, tj. o piętnaście czynów kwalifikowanych z art. 279 § 1 k.k. w zw. z art. 283 k.k. przy zastosowaniu art. 64 § 2 k.k. Jednak Sąd Rejonowy w Rudzie Śląskiej wyrokiem z dnia 5 kwietnia 2017 r. zmienił kwalifikację przyjętą przez prokuratora i uznał oskarżonego G. K. za winnego popełnienia przestępstwa polegającego na tym, że:

> w okresie od 18 do 19 czerwca 2016 r. w R. i K. działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, bez upoważnienia wpłynął na automatyczne przekazywanie danych informatycznych w ten sposób, że posługując się utraconą przez A. W. kartą bankomatową do rachunku bankowego w /…/ piętnastokrotnie dokonał płatności na zasadzie odczytu zbliżeniowego za zakupy o łącznej wartości 412,18 złotych powodując tym zmniejszenie o tę kwotę salda na rachunku na szkodę A. W., przy czym czyn ten stanowi wypadek mniejszej wagi i dopuścił się go działając w warunkach recydywy, tj. o czyn z art. 287 § 1 k.k. w zw. z art. 12 k.k. w zw. z art. 64 § 1 k.k. [306]

Sąd Okręgowy w Gliwicach[307], rozpoznając apelację oskarżonego od powyższego wyroku, ustalił, że sprawca przestępstwa swoim każdorazowym zachowaniem nie tyle wpływał na proces obróbki danych informatycznych, co go uruchamiał (inicjował). Wprowadzał w ten sposób w systemie informatycznym banku nowe zapisy danych informatycznych, tzn. uzupełniał zapisy danych o nowe, niewystępujące w pierwotnej wersji elementy, które prowadziły do modyfikacji zapisu w całości lub jedynie zmiany jego części, przez umieszczenie w bankowym zapisie danych nie występujących wcześniej elementów. W taki sposób, zdaniem sądu, wyrażała się czynność sprawcza opisana w art. 287 § 1 k.k., realizowana poprzez dokonanie tzw. płatności zbliżeniowych. Nie może budzić zatem wątpliwości, że art. 287 § 1 k.k. ma zastosowanie do bezprawnie realizowanych transakcji kartowych bez udziału czynnika ludzkiego, gdyż w takiej sytuacji sprawca niewątpliwie ingeruje bez upoważnienia w dane informatyczne, przetworzeniu ulegają przecież dane zapisywane i archiwizowane na serwerach banku, a dotyczące dokonanych transakcji i salda na rachunku bankowym. Jednak w ustalonych okolicznościach faktycznych sprawca działał w celu osiągnięcia korzyści majątkowej, a manipulowanie danymi stanowi tylko środek do realizacji zasadniczego celu – kradzieży mienia chronionego zabezpieczeniem elektronicznym. Uzasadnia to tezę, wskazał Sąd Okręgowy w Gliwicach, o pozornym zbiegu przepisów art. 279 § 1 k.k. i art. 287 § 1 k.k. Sąd celnie stwierdził:

[306] Wyrok Sądu Rejonowego w Rudzie Śląskiej Wydział II Karny z dnia 5 kwietnia 2017 r., II K 580/17.
[307] Wyrok Sądu Okręgowego w Gliwicach z dnia 11 lipca 2017 r., VI Ka 461/17, LEX nr 2351893.

Zabezpieczenie elektroniczne nie chroni tutaj danych informatycznych dotyczących cudzego mienia, lecz konkretną rzecz ruchomą, którą włamywacz chce zabrać w celu przywłaszczenia. Pełni więc rolę przeszkody zabezpieczającej mienie przed jej zaborem. W rezultacie art. 287 § 1 k.k. zostawałby pochłonięty w ten sposób, że nie istniałaby potrzeba powoływania się na niego. Naruszenie bezpieczeństwa wspomnianych danych jest bowiem konieczną i logiczną, a poza tym typową konsekwencją kradzieży pieniędzy poprzez przełamanie zabezpieczenia elektronicznego. Nie miałoby znaczenia przy pominięciu art. 287 § 1 k.k., że oprócz przedmiotu ochrony typowego dla kradzieży z włamaniem (tj. mienia), znamiona oszustwa komputerowego chronią jeszcze dodatkową wartość – proces teleinformatycznego przetwarzania informacji.

W niniejszej sprawie sąd nie mógł jednak, ze względu na kierunek zaskarżenia wyroku na korzyść oskarżonego i niedopuszczalność wydania w postępowaniu odwoławczym orzeczenia surowszego względem zaskarżonego z powodu obowiązywania zakazu *reformationis in peius*, zakwalifikować czynu jako kradzieży z włamaniem. Sąd odstąpił zatem od zastosowania pomijalnego zbiegu przepisów i poprzestał na zakwalifikowaniu czynu przypisanego oskarżonemu z art. 287 § 1 k.k. Pokazuje to zarazem, jak błędy popełnione w subsumpcji stanu faktycznego pod odpowiednią normę prawną mają kolosalne oddziaływanie na orzekanie o winie i podstawie skazania. W tym przypadku spowodowały one, że osoba została prawomocnie skazana za nie to przestępstwo, które rzeczywiście popełniła.

Słuszności stanowisku wyrażonemu przez Sąd Okręgowy w Gliwicach nie umniejsza błędne przyjęcie przez ów sąd, że podczas dokonywania płatności na zasadzie odczytu zbliżeniowego nie dochodzi do wpłynięcia na automatyczne przekazywanie danych informatycznych. Sąd ustalił, że

> oskarżony swoim każdorazowym zachowaniem nie tyle wpływał na proces obróbki danych informatycznych, co go po prostu uruchamiał, inicjował. Wprowadzał jednak w ten sposób w systemie informatycznym banku nowe zapisy danych informatycznych, tzn. uzupełniał zapisy danych o nowe, niewystępujące w pierwotnej wersji elementy, które prowadziły do modyfikacji zapisu w całości lub jedynie zmiany jego części, przez umieszczenie w zapisie danych informatycznych nie występujących wcześniej w nim elementów.

Widać zatem sprzeczność w stanowisku sądu, że sprawca nie wpłynął na przetwarzanie i przekazywanie danych informatycznych, a jednocześnie wprowadzał nowe zapisy w systemie. W tym też wyrażała się na gruncie art. 287 § 1 k.k. realizowana przez przestępcę czynność sprawcza. Jednak, co podkreślił sąd, „sprawcy nie chodziło jedynie o zmianę zapisu danych informatycznych polegającą na przekształceniu zapisu tych

danych, modyfikacji treści tych zapisanych danych informatycznych", gdyż jego zamiar obejmował kradzież mienia, które dane informatyczne utożsamiały.

Niekiedy sądy same „komplikują sprawę" i w dość oczywistych oraz nietrudnych do oceny stanach faktycznych budują „barokowe" opisy czynów tak, jak zrobił to, przywołany już wcześniej, Sąd Rejonowy w Legionowie, skazując sprawcę za to, że:

> w dniu 14 lutego 2016 r. w miejscowości N., /…/ bez upoważnienia wpłynął na automatyczne przetwarzanie danych informatycznych i zmienił zapis danych informatycznych rachunku /…/ prowadzonego przez Bank /…/ S.A., zmieniając saldo dostępnych środków pieniężnych znajdujących się na tym rachunku w ten sposób, że po uprzednim wejściu w posiadanie karty bankomatowej VISA Elektron /…/*******5540 należącej do E. Z., dokonał włamania na powyższy rachunek poprzez wprowadzenie kodu PIN bez wiedzy i zgody ww. w bankomacie, a następnie dokonał kradzieży pieniędzy w kwocie 2000 zł na szkodę E. Z. tj. o czyn z art. 279 § 1 k.k. w zb. z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[308]

W sprawie tej nie doszło do popełnienia czynu z art. 287 § 1 k.k., a dla właściwego oddania całego bezprawia nie miała znaczenia wskazana przez sąd okoliczność, że sprawca wszedł uprzednio w posiadanie „karty bankomatowej VISA Elektron"; która to karta nota bene jest kartą płatniczą, a nie bankomatową. Mając powyższe na uwadze, wyrok skazujący mógł brzmieć następująco:

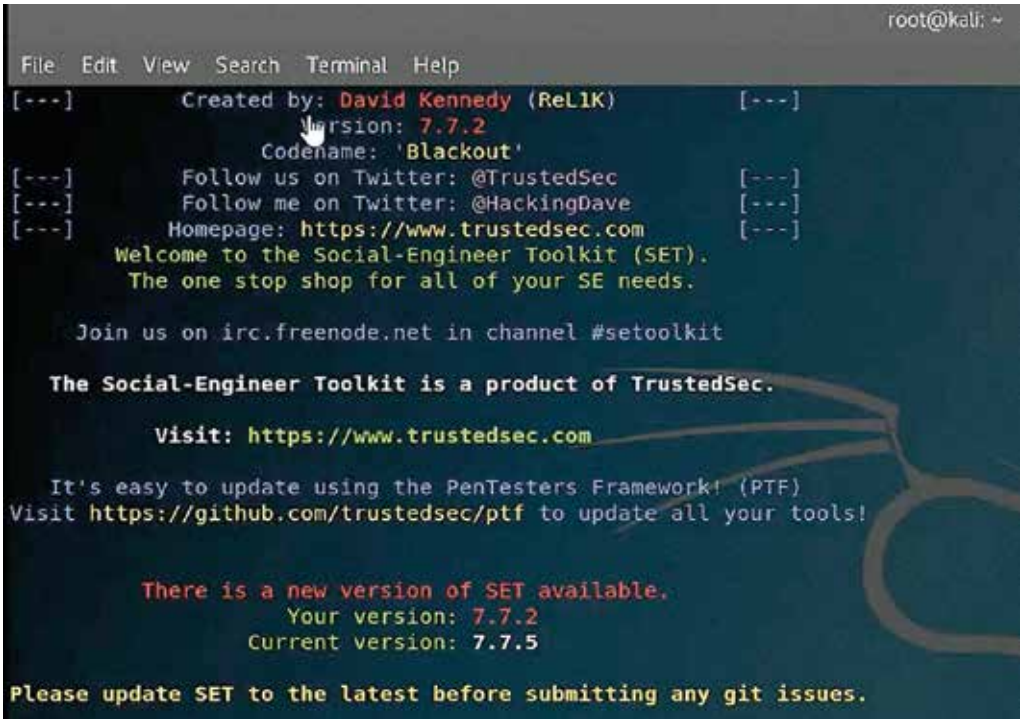
> w dniu 14 lutego 2016 r. w miejscowości N., /…/ przy użyciu karty płatniczej i kodu PIN, należących do E. Z., dokonał kradzieży z włamaniem do rachunku bankowego należącego do Banku /…/, którego posiadaczem był E. Z. oraz zaboru w celu przywłaszczenia środków pieniężnych zapisanych na rachunku w wysokości 2000 zł działając na szkodę Banku /…/ i E. Z.,tj. o przestępstwo z art. 279 § 1 k.k.

W momencie analizy przestępstwa kradzieży z włamaniem na rachunek bankowy pojawia się jeszcze jedno zagadnienie, dotyczące charakteru zbiegu przepisów: art. 267 § 1, 2 lub 3 k.k. i art. 279 § 1 k.k. Kradzież taka wygląda często w ten sposób, że sprawca najpierw przełamuje zabezpieczenia aplikacji do obsługi takiego rachunku zainstalowanej na smartfonie, laptopie czy komputerze stacjonarnym, a po zalogowaniu się do niej dokonuje przelewu zgromadzonych na rachunku środków na konto założone na „słupa". Podatność aplikacji i szerzej, systemu informatycznego i teleinformatycznego banku, na włamania może wynikać z następujących czynników:

[308] Wyrok Sądu Rejonowego w Legionowie z dnia 7 czerwca 2017 r., II K 406/16, LEX nr 2340308.

1. luk w zabezpieczeniach po stronie serwera instytucji finansowej, tj. poza aplikacją mobilną, m.in. w usługach sieciowych, czy konfiguracjach serwerów www powodujących „wyciek" danych do logowania;
2. niezabezpieczonego magazynu danych, gdy aplikacja przechowuje w urządzeniu mobilnym poufne treści w formacie zwykłego tekstu lub innej postaci łatwej do odczytania przez hakera;
3. niewystarczającej ochrony warstwy transportowej; ta kategoria ryzyka dotyczy ochrony ruchu sieciowego i może pojawić się w każdej sytuacji, w której dane są przekazywane w postaci zwykłego tekstu lub stosuje się nieprawidłowy sposób ich szyfrowania;
4. niezamierzonego wycieku danych, gdy programista przypadkowo umieszcza poufne informacje lub dane w miejscach urządzenia mobilnego, które są łatwo dostępne z poziomu innych aplikacji;
5. zawodnego mechanizmu autoryzacji i uwierzytelniania; dotyczy to nieprawidłowości związanych z logowaniem się na konto i potwierdzaniem przelewów środków pieniężnych; błąd w tym zakresie może występować w aplikacji mobilnej lub po stronie serwera;
6. nieprawidłowego stosowania kryptografii: aplikacja przechowująca dane w urządzeniu mobilnym powinna je szyfrować w celu zapewnienia poufności tych danych. Ryzyko pojawia się, gdy implementacja aplikacji zawiera „słabe" strony, np. z powodu wadliwego procesu zarządzania kluczem kryptograficznym;
7. możliwości przeprowadzenia ataku typu injection po stronie klienta, gdy aplikacja mobilna akceptuje dane wejściowe pochodzące z niezaufanych źródeł. Dotyczy to m.in. sytuacji, kiedy pobiera ona z witryny internetowej opublikowane przez innych użytkowników komunikaty ze złośliwym oprogramowaniem[309].

[309] D. Chell, T. Erasmus, S. Colley, O. Withehouse, *Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera*, Gliwice 2017, s. 37–39.



Grafika nr 13. Panel sterowania programu root@kali przeznaczonego do „etycznego hakowania"

Czy zatem taki czyn, tj. przełamanie zabezpieczenia aplikacji bankowej i kradzież środków pieniężnych zapisanych na rachunku, należy kwalifikować tylko z art. 279 § 1 k.k., czy w kumulatywnym w zbiegu z art. 267 § 1 k.k.? W takim przypadku dochodzi bowiem do przełamania lub ominięcia zabezpieczenia informatycznego, co jest charakterystyczne dla obu ww. przepisów. Jednak w omawianych sytuacjach art. 267 § 1 k.k. pozostaje w zbiegu pomijalnym w stosunku do art. 279 § 1 k.k., gdyż znamię „przełamanie lub ominięcie informatycznego zabezpieczenia" odpowiada czynności „włamania się", o której mowa w art. 279 § 1 k.k. Nadto, w doktrynie i orzecznictwie wspólne jest stanowisko, że wypłata pieniędzy z bankomatu przy wykorzystaniu bez uprawnienia cudzej karty płatniczej oraz przypisanego do niej PIN-u stanowi kradzież z włamaniem. Przykładowe wyroki zapadłe w tego typu sprawach brzmią następująco:

> w okresie od 27 do 28 marca 2020 r. w T. działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, dokonała włamania na rachunek bankowy A. W. w ten sposób, iż po uprzednim otrzymaniu od pokrzywdzonej karty bankomatowej banku /…/ – bez zgody i wiedzy pokrzywdzonej użyła ww. karty i dokonała

dwóch wypłat w bankomacie ww. kartą powodując straty w kwocie łącznej 400 zł czym działała na szkodę A. W., przy czym czynu tego dopuściła się w przeciągu 5 lat po odbyciu co najmniej 6 miesięcy kary pozbawienia wolności będąc skazaną wyrokiem Sądu Rejonowego w Toruniu II Wydział Karny sygn. akt II K 1469/14 z dnia 7 lipca 2015 r. za przestępstwo z art. 286 § 1 k.k. tj. o przestępstwo z art. 279 § 1 k.k. w zw. art. 12 § 1 k.k. w zw. z art. 64 § 1 k.k.[310]

w dniu 17 czerwca 2014 r., o godz. 20:55 w /…/ używając karty bankomatowej J. G. /…/ usiłował dokonać kradzieży z włamaniem kwoty łącznej 500 zł poprzez pokonanie zabezpieczeń karty w ten sposób, że wprowadził uzyskany wcześniej kod PIN, lecz zamierzonego celu nie osiągnął z uwagi na odrzucenie transakcji z powodu zgłoszenia kradzieży karty, czym działał na szkodę J. G., przy czym czynu tego dopuścił się będąc uprzednio skazanym wyrokiem Sądu Rejonowego w Sulęcinie z dnia 24 kwietnia 2008 r., sygn. II K 45/08, za umyślne przestępstwo podobne na karę pozbawienia wolności w wymiarze 8 miesięcy, którą odbył w okresie od 18 grudnia 2009 r. do 18 sierpnia 2010 r., a więc w ciągu 5 lat po odbyciu co najmniej 6 miesięcy kary, tj. o czyn z art. 13 § 1 k.k. w zw. z art. 279 § 1 k.k. w zw. z art. 12 k.k. w zw. z art. 64 § 1 k.k.[311]

Przełamanie zabezpieczenia i zabór rzeczy, szczególnie wtedy, gdy działania takie są zbieżne czasowo (jedno następuje zaraz po drugim), stanowią jeden czyn w rozumieniu prawa karnego i nie można ich rozdzielać. W opisanej poniżej sprawie Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie naruszył prawo materialne, tj. art. 279 § 1 k.k., kwalifikując dwa zachowania jako wypełniające znamiona art. 267 § 1 k.k. i art. 278 § 1 k.k., podczas gdy otwarcie paczkomatu za pomocą kodu stanowiło „włamanie", a dokonany po nim zabór rzeczy idealnie wpisywał się w treść art. 279 § 1 k.k.

w dniu 23 grudnia 2015 roku w Krakowie, na os. Piastów 60a, dokonał zaboru w celu przywłaszczenia przesyłki o numerze /…/ o wartości 531 złotych zawierającej zegarek marki Casio z paczkomatu o oznaczeniu /…/, należącego do przedsiębiorstwa InPost S.A., posługując się kodem do skrzynki w tym paczkomacie, który to kod uzyskał wykorzystując swoje stanowisko służbowe w firmie InPost, co pozwoliło rozliczyć fikcyjną opłatę za tą przesyłkę w systemie informatycznym tej spółki, czym działała na szkodę InPost S.A., tj. o przestępstwo z art. 278 § 1 k.k. i art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k.[312]

[310] Wyrok Sądu Rejonowego w Toruniu z dnia 26 sierpnia 2020 r., II K 777/20, LEX nr 3060595.
[311] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 26 kwietnia 2017 r., II AKa 191/16, LEX nr 2295144.
[312] Wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie, II K 228/17/N.

Przechodząc do analizy kolejnych orzeczeń sądowych, to w części spraw błędnie przyjmowano kumulatywną kwalifikację prawną z art. 279 § 1 k.k. i art. 287 § 1 k.k.; dotyczy to np. wyroku Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie uznającego oskarżoną za winną tego, że:

> w dniu 14 listopada 2016 roku w nieustalonym miejscu w celu osiągnięcia korzyści majątkowej znając hasło dostępu do konta bankowego M. Z. o numerze /…/ prowadzonego w Banku /…/ korzystając z nielegalnie uzyskanego kodu do tego rachunku umożliwiającego dokonanie transakcji drogą elektroniczną dokonała kradzieży z włamaniem na konto bankowe pokonując zabezpieczenie oraz bez upoważnienia wpłynęła na automatyczne przetwarzanie danych informatycznych w ten sposób, że dokonała przelewu z tego rachunku na rachunek /…/ kwoty 350 zł za pośrednictwem bankowości elektronicznej Banku /…/ zatwierdzonego przy pomocy kodu wysłanego na numer telefonu /…/ działając na szkodę M. Z. przy uznaniu, że czyn ten stanowi wypadek mniejszej wagi, tj. o czyn z art. 279 § 1 k.k. w zw. z art. 283 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[313]

Pomijając już kwestie błędnej kwalifikacji prawnej zdarzenia, to z lektury orzeczenia bije niefrasobliwość sądu w opisie znamion czynu zabronionego i ogólnie stylu języka, jakim opisano czyn karalny. Niepotrzebnie podano fakt, że transakcja została „zatwierdzona za pomocą kodu wysłanego na numer telefonu", a pominięto, które znamię czasownikowe czynności sprawczej, spośród sześciu alternatywnie wymienionych w art. 287 § 1 k.k., wypełniła swoim zachowaniem oskarżona. Odnotowano także sprawy, gdzie sądy w kwalifikacji prawnej omawianego rodzaju przestępczości prawidłowo uwzględniły tylko art. 279 § 1 k.k.; oto kilka z nich:

> w dniu 10 października 2014 r. w miejscowości S., /…/ działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru trzykrotnie dokonał włamania na konto E. G. w ten sposób, że używając karty bankomatowej przełamał elektroniczne zabezpieczenie wykorzystując numer PIN, po czym dokonał wpłaty z bankomatu /…/ w K. pieniędzy w kwocie łącznej 1.000 zł, które zabrał w celu przywłaszczenia na szkodę E. G., tj. o czyn art. 279 § 1 k.k. w zw. z art. 12 k.k.[314]

> w dniu 29 sierpnia 2018 r. w miejscowości J., /…/ działając w krótkich odstępach czasu w wykonaniu tego samego zamiaru dokonał kradzieży z włamaniem na konto bankowe należące do J. A. przy użyciu karty bankomatowej wielowalutowej i bez

[313] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 1666/17/N.
[314] Wyrok Sądu Okręgowego w Siedlcach z dnia 11 lipca 2016 r., II Ka 329/16, LEX nr 2074573.

wiedzy i zgody właściciela rachunku przy użyciu kodu /…/ wykonał cztery razy wypłaty po 241,78 Euro z bankomatu i wypłaty w kwocie 12,09 Euro z bankomatu z tytułu czego powstały koszty w kwocie 39,92 Euro związane z wykonywaniem wypłat i przewalutowaniem powodując straty w łącznej kwocie 1019,13 Euro (4369,11 zł) na rzecz J. A. to jest popełnienia czynu z art. 279 § 1 k.k. w zw. z art. 12 § 1 k.k.[315]

w dniu 8 kwietnia 2017 r. przy ul. /…/ w G. za pomocą skradzionej karty bankomatowej z indywidualnym kodem /…/ dokonał kradzieży z włamaniem do bankomatu, skąd dokonał wypłaty pieniędzy w kwocie 1000 zł czym działał na szkodę A. W. tj. o czyn z art. 279 § 1 k.k.[316]

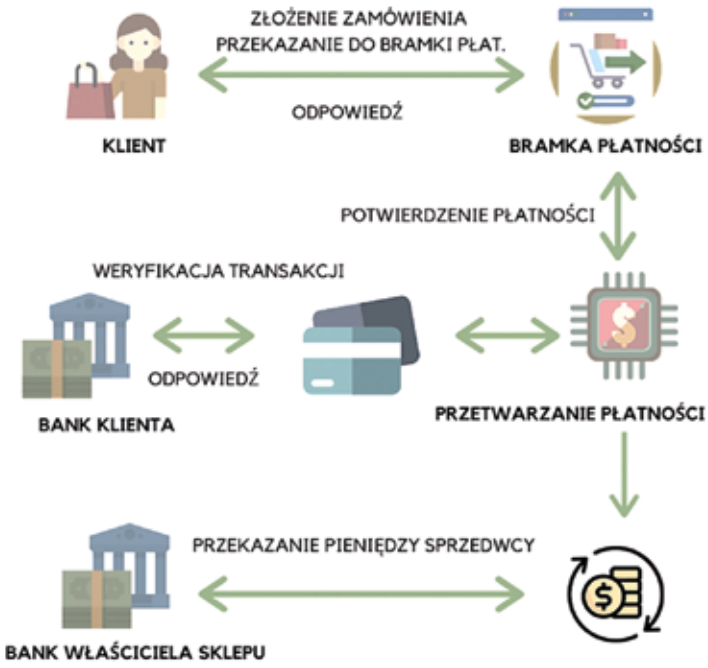
Zdarzają się jednak przestępstwa o bardziej skomplikowanym *modus operandi* sprawców, aniżeli opisane we wcześniejszych wyrokach, kiedy ich cel działania w postaci kradzieży środków zapisanych na rachunku bankowym jest poprzedzony umyślnym i znaczącym manipulowaniem danymi teleinformatycznymi, często przy wykorzystaniu złośliwego oprogramowania. Wtedy w grę wchodzi przyjęcie art. 287 § 1 k.k. w zbiegu realnym z art. 279 § 1 k.k., a nawet zakwalifikowanie manipulacji danymi jako całkiem odrębne przestępstwo od kradzieży, gdy nielegalny transfer środków i owa manipulacja zostały popełnione w różnym czasie. Przykładem takiego zaawansowanego ataku jest kreowanie w cyberprzestrzeni fałszywych systemów płatności w postaci tzw. bramek do dokonywania przez osoby pokrzywdzone przelewów środków finansowych na fałszywe rachunki bankowe. Działania takie, wykorzystujące np. mechanizm szybkich przelewów internetowych, można przedstawić w trzech etapach:

1. klient po wybraniu wspomnianej metody płatności jest przenoszony na stronę internetową swojego banku. Po zalogowaniu się na konto, czeka na niego wypełniony już wniosek przelewu na rzecz sprzedawcy i dokonuje jego autoryzacji;
2. klient przenoszony jest z powrotem na stronę internetową sprzedawcy, który jednocześnie dostaje od dostawcy płatności informację o dokonaniu zapłaty za towar lub usługę;
3. dostawca płatności otrzymuje przelew z banku klienta i przekazuje środki dalej na rachunek sprzedawcy albo sprzedawca otrzymuje przelew bezpośrednio z banku kupującego[317].

W schemacie tym występują „bramki płatności", czyli system pozwalający wykonywać szybkie przelewy online. Usługa ta świadczona jest przez agenta rozliczeniowego, który pozwala przyjmować przelewy środków pieniężnych sklepom internetowym oraz innym podmiotom pobierającym płatności w sieci. Narzędzie takie może być

[315] Wyrok Sądu Rejonowego w Legionowie z dnia 7 lutego 2020 r., II K 1247/18, LEX nr 3069347.
[316] Wyrok Sąd Rejonowy w Goleniowie z dnia 27 lutego 2018 r., II K 424/17, LEX nr 2730262.
[317] B. Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognoza,* publikacja Komisji Nadzoru Finansowego, Warszawa 2019, s. 9, https://www.knf.gov.pl/knf/pl/komponenty/ [dostęp: 23.07.2023].

dostarczone przez wyspecjalizowanego dostawcę usług finansowych (operatora płatności) lub udostępnione przez bank, a zlecenia dokonywane są zazwyczaj za pomocą kart płatniczych, szybkich przelewów bankowych (pay-by-link), BLIK, Apple Pay, Google Pay oraz innych metod płatniczych. Bramki bazują na tzw. koncie przejściowym i pobierają opłatę w postaci prowizji procentowej lub kwotowej w zależności od wysokości i liczby transakcji. Klienci sklepu, płacąc za towar lub usługę poza sklepem, logują się do swojego banku. W momencie finalizacji przelewu, pieniądze od klienta trafiają na przypisane do sklepu internetowego konto przejściowe[318].



Grafika nr 14. Działanie systemu płatności internetowych z wykorzystaniem tzw. bramek płatności

Przestępcy, przy wykorzystaniu różnych scenariuszy wirtualnych ataków na systemy informatyczne i teleinformatyczne oraz socjotechniki oddziałującej na świadomość człowieka, nakłaniają pokrzywdzonych do realizacji płatności online. Jeden ze sposobów działania polega na zamieszczaniu na platformach sprzedażowych w Internecie, takich jak OLX i Allegro lub portalach społecznościowych typu Facebook ofert sprzedaży towarów po atrakcyjnych cenach (np. telefonów, dronów) lub propozycji darmowego przekazania różnych produktów (np. zabawek lub artykułów pielęgnacyjnych dla dzieci). Kolejny scenariusz ataku opiera się na tworzeniu witryn fałszywych sklepów z atrakcyjnymi ofertami sprzedażowymi. Osoby zainteresowane dokonaniem zakupów

[318] https://thenewlook.pl/bramki – platnosci – online/ [dostęp: 23.07.2023].

na takiej platformie otrzymują od sprawców przesłaną pocztą elektroniczną, SMS-em lub komunikatorem typu Messenger wiadomość, w której znajduje się informacja o płatności oraz link prowadzący do fałszywej strony imitującej stronę agenta rozliczeniowego, a następnie banku. Osoba, która odpowiedziała na ogłoszenie o darowiźnie, otrzymuje następnie powiadomienie o konieczności opłacenia przesyłki, którą będą dostarczone rzeczy, wraz z hiperłączem do realizacji płatności, a hiperłącze także prowadzi do fałszywej strony internetowej. Tak więc w opisanym *modus operandi* sprawcy wysyłają wiadomości do osób, które same zainteresowały się ogłoszeniem z ofertą sprzedaży lub darowizny produktu[319].

Inne *modus operandi* stosowane przez przestępców ukierunkowane jest na internautów, którzy sami opublikowali różnego typu oferty sprzedażowe na platformach cyfrowych wraz z danymi kontaktowymi (numer telefonu, adres mailowy). W tym scenariuszu przestępcy wysyłają do nich powiadomienie o konieczności dopłaty za usługę lub uwolnienie konta zablokowanego z tytułu zadłużenia jego posiadacza, a kliknięcie przez pokrzywdzonego na podstawiony link powoduje, że potencjalna ofiara zostaje przekierowana na stronę imitującą prawdziwą bramkę płatności[320].

Funkcjonują także ataki masowe, gdy cyberprzestępcy hurtowo rozsyłają hiperłącza prowadzące do fałszywych stron płatności, bez indywidualnego dostosowania scenariusza ataku pod kątem konkretnego pokrzywdzonego. Sprawcy wysyłają najczęściej SMS-y z wezwaniem do realizacji płatności, a jako powód wskazują np. dopłatę do przesyłki, i podszywają się wówczas pod przedsiębiorców świadczących usługi przewozowe, spedycyjne lub pocztowe (DHL, DPD, InPost, Pocztę Polską). Poczynając od 2022 r., coraz częściej dystrybuowano SMS-y z informacją o konieczności dopłaty do rachunku za energię elektryczną i rzekomym działaniu w imieniu dostarczyciela typu PGE, ENEA lub Tauron[321].

Pokrzywdzony, który skorzystał z nadesłanego przez przestępców hiperłącza, kliknął w link dostarczony SMS-em lub innym kanałem komunikacji elektronicznej, jest przekierowywany na specjalnie przygotowaną stronę imitującą pośrednika płatności o przykładowym adresie https://placimy24.net. Osoba, po wyborze swojego banku, jest przekierowywana na kolejną fałszywą stronę podszywającą się tym razem pod witrynę instytucji finansowej, w której ofiara posiada rachunek płatniczy. Jeśli nieświadoma niczego wpisze na tej stronie login i hasło do swojej aplikacji bankowości elektronicznej, to przestępcy przejmują dane, momentalnie logują się do prawdziwej aplikacji bankowej pokrzywdzonego i dodają w niej tzw. zaufanego odbiorcę (rachunek założony na „słupa", który zostanie wykorzystany do prania skradzionych z innych rachunków pieniędzy).

[319] Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 17 stycznia 2022 r. dotyczące przestępstw związanych z fałszywymi panelami płatności i stronami podszywającymi się pod strony bankowości elektronicznej, sygn. 1001 – 7.024.1.2022 (zbiory własne autora), dalej jako: Pismo z 17 stycznia 2022 r.

[320] Tamże.

[321] Tamże.

Ponieważ atak obsługiwany jest w czasie rzeczywistym, to zaraz po tym, jak przestępca zaloguje się do cudzej aplikacji, nieświadomy niczego klient banku otrzymuje na swój telefon powiadomienie SMS-em z instytucji finansowej o poprawnym logowaniu, które faktycznie wykonał przestępca. Utwierdza to ofiarę w mylnym przekonaniu, że znajduje się na oryginalnej stronie swojej bankowości elektronicznej. Tymczasem sprawcy, aby zdefiniować zaufanego odbiorcę i wytransferować środki z cudzego rachunku, muszą otrzymać SMS-a z banku z kodem autoryzacyjnym do przelewu. W tym celu na fałszywej, obsługiwanej przez nich stronie, którą widzi na pulpicie swojego komputera pokrzywdzony, wyświetla się formularz ze skierowanym do niego żądaniem podania jednorazowego kodu autoryzacyjnego w celu potwierdzenia płatności tytułem (rzekomego) opłacenia przesyłki kurierskiej, usługi przewozowej, opłaty za energię elektryczną itp. Jeżeli zmanipulowana osoba nie przeczyta uważnie otrzymanego SMS-a i poda cyberprzestępcom kod na fałszywej stronie bankowości elektronicznej, to odczytują oni ten kod w panelu służącym do zarządzania fałszywą bramką płatności i wykorzystują go do autoryzacji dodanego do aplikacji zaufanego odbiorcy. Finalnie, po wykonaniu ww. czynności, oszust może dokonać przelewu środków pieniężnych z rachunku bankowego pokrzywdzonego bez konieczności potwierdzania kodami autoryzacyjnymi kolejnych transakcji[322].

Przestępstwa polegające na wyłudzeniu płatności przy wykorzystaniu fałszywych stron internetowych będą kwalifikowane przede wszystkim z art. 279 § 1 k.k. jako kradzież z włamaniem do aplikacji bankowości elektronicznej i zabór w celu przywłaszczenia znajdujących się tam środków. Jeśli chodzi o samo przełamanie zabezpieczenia aplikacji poprzez wpisanie uzyskanego podstępem hasła i uzyskanie bez uprawnienia dostępu do informacji dla sprawcy nieprzeznaczonej, to art. 267 § 1 k.k. będzie pozostawał w zbiegu pomijalnym z art. 279 § 1 k.k. i nie należy zamieszczać go w opisie czynu[323]. W takich sytuacjach dochodzi natomiast do kumulatywnej kwalifikacji prawnej kradzieży z włamaniem i „oszustwa komputerowego". *Modus operandi* sprawców omawianych czynów opiera się na manipulacji danymi, które przybierają o wiele bardziej rozległy i świadomy charakter, aniżeli tylko przyłożenia karty do czytnika lub wpisanie na klawiaturze PIN-u. Oszuści, za pomocą wyłudzonego loginu i hasła, logują się do aplikacji oferowanej pokrzywdzonemu, dodają do systemu tzw. zaufanego odbiorcę i definiują jego uprawnienia, wpisują podstępnie przejęte dane w celu uwierzytelnienia się, definiują przelewy środków, a niekiedy działają bardziej długofalowo i instalują w aplikacji złośliwe oprogramowanie, które będzie co jakiś czas pobierać z rachunku tylko niewielkie kwoty lub pozwoli sprawcom ponownie zalogować się do niej w przyszłości. Działanie takie jest ponadto rozciągnięte w czasie, gdyż zwabienie ofiary

[322] Tamże.

[323] Odmiennie wskazano w Piśmie z 17 stycznia 2022 r., argumentując, że „Z uwagi na to, że sprawcy podają login i hasło do bankowości elektronicznej i uzyskują nieuprawniony dostęp do informacji dla niech nieprzeznaczonej, w zbiegu z art. 279 § 1 k.k. będzie pozostawał art. 267 § 1 k.k.". Kwestia charakteru zbiegu tych przepisów stanowi przedmiot rozważań następnego podrozdziału monografii.

do fałszywej bramki płatności, a potem witryny imitującej stronę banku, wyłudzenie kodów, podstępne zarządzanie aplikacją pokrzywdzonego – wszystkie takie działania trwają o wiele dłużej, aniżeli płatność zbliżeniowa, czy podjęcie pieniędzy z bankomatu. Wynika z tego, że zarzut opisujący przestępstwo kradzieży pieniędzy w taki sposób, jak opisano powyżej, mógłby brzmień następująco:

> w dniu 1 stycznia 2023 r. w Krakowie dokonał kradzieży z włamaniem do aplikacji bankowości elektronicznej Banku /…/ obsługującej rachunek bankowy o numerze 2323**********, którego posiadaczem był J. K. w ten sposób, że przejął od pokrzywdzonego hasła dostępu do aplikacji za pomocą fałszywej „bramki" płatności i strony internetowej Banku i po zalogowaniu się do aplikacji, działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia wprowadził nowy zapis danych informatycznych dodając „zaufanego odbiorcę" i zabrał w celu przywłaszczenia kwotę 20 000 zł działając na szkodę J. K. i Banku /…/, tj. o przestępstwo z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

Analiza przestępczości z wykorzystaniem fałszywych bramek płatności pokazuje, że środki pieniężne ze skompromitowanych rachunków transferowane są w miejsca bezpieczne dla przestępców z wykorzystaniem różnych metod działania; często kierunek alokacji środków stanowią giełdy kryptowalutowe, gdzie zamieniane są na tokeny cyfrowe (najczęściej bitcoiny), innym razem przelewane są na konta założone na „słupy", a jeśli na rachunku pokrzywdzonego brak znaczących sum, to mniejsze kwoty można wypłacić w formie gotówki w bankomacie. Niektórzy ustaleni już operatorzy fałszywych bramek płatności za nielegalnie uzyskane środki dokonywali zakupu wirtualnych przedmiotów w grach komputerowych lub transferowali je na rachunki bankowe osób uprzednio zrekrutowanych tytułem zatrudnienia[324]. Działania dotyczące ukrycia przestępczego pochodzenia środków uzyskanych w wyniku opisanego *modus operandi* (przestępstwo bazowe) kwalifikuje się jako pranie pieniędzy z art. 299 § 1 k.k.

Podsumowując, skazanie sprawcy za przestępstwo wyczerpujące znamiona jednego przepisu, tj. kradzieży lub kradzieży z włamaniem, z reguły oddaje całą zawartość kryminalną czynu i zbędne jest w tym zakresie odwołanie się do konstrukcji zbiegu realnego i przywoływanie w opisie czynu i jego kwalifikacji prawnej art. 287 § 1 k.k. Może się jednak zdarzyć, że nastąpi zbieg realny pomiędzy przepisami art. 278 § 1 k.k. lub art. 279 § 1 k.k. i art. 287 § 1 k.k. szczególnie wtedy, gdy działanie sprawcy ukierunkowane jest nie tylko na kradzież środków pieniężnych zapisanych na rachunku bankowym, ale także świadomie manipuluje on danymi informatycznymi i powoduje skutki o wiele dalej idące, aniżeli tylko typowa zmiana zapisu danych w systemie płatniczym związana z transferem środków. W praktyce będą to jednak sytuacje stosunkowo

[324] Tamże.

rzadkie, mając na uwadze, że czyn przestępczy polega najczęściej na dokonaniu płatności kartą płatniczą innej osoby, przelaniu środków zgromadzonych na jej koncie lub na wypłacie pieniędzy z bankomatu.

4.4. Transakcje zbliżeniowe

Transakcje zbliżeniowe polegają na dokonywaniu kartą płatniczą opłaty za towar lub usługę z wykorzystaniem funkcji zbliżeniowej karty bazującej na działaniu mikroprocesora, gdyż po implementacji standardu EMV pasek magnetyczny na karcie rzadko wykorzystywany jest w Unii Europejskiej do autoryzacji transakcji. Obecnie karty są zaawansowanymi urządzeniami elektronicznymi, a zainstalowany w nich chip pełni rolę swego rodzaju komputera wyposażonego w wyspecjalizowany system operacyjny. Na powierzchni karty, za powłoką pokrytą cienką warstwą żywicy ochronnej, osadzono kilkudziesięciobitowy mikroprocesor oraz moduł z pamięcią do ponownego zapisu (EEPROM). Procesor wyposażony jest w oprogramowanie, które kontroluje odczyt i zapis danych zawartych w pamięci elektronicznej, a więc zajmuje się zarządzaniem pamięcią karty. Zawiera on wiele poufnych danych informatycznych i wykorzystuje zaawansowane algorytmu do autentykacji. W trakcie transakcji zapłaty metodą zbliżeniową lub wypłaty zbliżeniowo pieniędzy z bankomatu, następuje komunikacja oraz weryfikacja informacji pomiędzy kartą i odczytującym ją terminalem, a nie tylko bierny odczyt z chipa. Dzięki temu system identyfikuje klienta, sprawdza autentyczność karty, saldo rachunku i limity transakcji. Na końcu ma miejsce autoryzacja karty mikroprocesorowej przez system, co oznacza wyrażenie przez bank zgody na realizację zamierzonej operacji. Większość bankomatów funkcjonuje w trybie online, co daje możliwość monitorowania transakcji w czasie rzeczywistym, odnajdywania anomalii i reagowania na nieprawidłowości. Dane z mikroprocesora wprowadzone do komputera bankomatu lub terminalu POS są od razu porównywane z danymi znajdującymi się w bazie centralnej banku lub agenta rozliczeniowego i na bieżąco sprawdza się, czy karta nie została zastrzeżona[325].

Pokazuje to, że w procesie autoryzacji transakcji kartowej podstawowa rola czuwania nad jej bezpieczeństwem przypada mikroprocesorowi. Do transakcji dochodzi bowiem w momencie, kiedy mikroprocesor umieszczony w karcie lub innym urządzeniu przenośnym (np. smartfonie) nawiązuje, poprzez fizyczne zetknięcie lub bezstykowo, kontakt z terminalem. Chip przechowuje informacje o rachunku bankowym posiadacza karty i za pomocą specjalnej aplikacji wykonuje kryptograficzne przetworzenie danych dla potwierdzenia prawidłowości, m.in. numeru karty. Specyfikacje EMV, czyli systemu kart płatniczych z mikroprocesorem, bazują na normie ISO i określają wzajemne zależności fizyczne, elektryczne i aplikacyjne warunkujące współpracę pomiędzy kartami z chipem i urządzeniami „czytającymi" takie karty w trakcie realizacji różnego rodzaju operacji. Chodzi w pierwszej kolejności o proces autoryzowania i uwierzytelnienia

[325] P. Opitek, *Skimming, Cyberprzestępczość w bankowości elektronicznej*…, s. 23–25.

płatności z fizycznym użyciem karty na podstawie danych zawartych w pamięci chipa zatopionego w plastiku[326]. Autoryzacja oznacza w tym przypadku udzielenie zgody na wykonanie transakcji przez płatnika, podczas gdy uwierzytelnienie jest techniczną procedurą weryfikacji realizowaną przez dostawcę usługi. Moment zapłaty kartą za towar/usługę jest najbardziej newralgiczny pod względem bezpieczeństwa: dochodzi wtedy równocześnie do złożenia zlecenia płatniczego, uwierzytelnienia i autoryzacji[327].

Jeszcze przed dokonaną w kwietniu 2017 r. zmianą art. 115 § 9 k.k. i rozszerzeniem definicji „rzeczy" o pojęcie „środka pieniężnego zapisanego na rachunku" toczył się w doktrynie spór, czy nieuprawniona transakcja zbliżeniowa dokonana kartą płatniczą bez użycia kodu PIN, powinna być kwalifikowana z art. 278 § 1 k.k. (ewentualnie art. 119 k.k.w.[328]), art. 279 § 1 k.k. lub art. 287 § 1 k.k. Zdarzały się też wyroki, w których sądy przyjmowały realny zbieg tych przepisów; postąpił tak Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie, skazując sprawcę za to, że:

> w dniu 28 grudnia 2016 roku w Krakowie działając w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru w celu osiągnięcia korzyści majątkowej poprzez użycie w transakcjach zbliżeniowych karty płatniczej wydanej przez Bank /…/ S.A. należącej do pokrzywdzonej J. B., bez upoważnienia pokonał elektroniczne zabezpieczenie banku, wpływając na automatyczne przetwarzanie, gromadzenie i przekazywanie danych informatycznych i dokonując 10 włamań do systemu bankowego, a następnie dokonał kradzieży pieniędzy w kwocie odpowiednio 6,99 zł, 6,99 zł, 6,99 zł, 13,20 zł, 14,07 zł, 7,80 zł, 15,20 zł, 20,99 zł, 19,99 zł, 7,28 zł, stanowiących płatność za zakupiony towar, czym działał na szkodę J. B. powodując straty w łącznej wysokości 119,50 zł, tj. o przestępstwo z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[329]

W publikacji poświęconej zagadnieniu kwalifikacji prawnej przestępstw związanych z nieautoryzowanym użyciem karty płatniczej z lutego 2017 r.[330] autor książki wyraził pogląd, że kwalifikacja ta zależy od tego, czy w transakcji pośredniczyła inna osoba, czy też zrealizowano ją w terminalu samoobsługowym. W pierwszym wypadku należało wziąć pod uwagę przepis art. 286 k.k., gdyż w płatnościach manualnych przy użyciu sklepowych czytników POS sprawca posługujący się kartą płatniczą oddziałuje

[326] J. Biegański, *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, [w:] *Przestępczość teleinformatyczna*, red. J. Kosiński, Szczytno 2012, s 19.

[327] P. Opitek, *Wpływ standardu EMV na nielegalne działania z wykorzystaniem kart płatniczych w kontekście przestępstwa skimmingu*, „Bezpieczny Bank" 2016, nr 1, s. 136–137.

[328] Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (t.j. Dz. U. z 2022 r. poz. 2151 z późn. zm.), dalej jako: k.w. Zgodnie z art. 119 § 1 k.w. „Kto kradnie lub przywłaszcza sobie cudzą rzecz ruchomą, jeżeli jej wartość nie przekracza 800 złotych, podlega karze aresztu, ograniczenia wolności albo grzywny".

[329] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 724/17/N.

[330] P. Opitek, *Kwalifikacja prawna przestępstw*…

na proces decyzyjny osoby obsługującej terminal, aby wykonała ona konkretne czynności faktyczne warunkujące realizację sprzedaży: uruchomiła urządzenie, wpisała na klawiaturze czytnika lub połączonego z nim komputera cenę towaru/usługi i zatwierdziła ją. Dopiero wtedy terminal sygnalizuje możliwość płatności zbliżeniowej i przykłada się kartę do czytnika mikroprocesora. Ponieważ na akceptancie ciąży prawny obowiązek czuwania nad bezpiecznym przebiegiem usługi płatniczej, w tym weryfikowania osoby posługującej się kartą, przestępca musi go oszukać, zazwyczaj dać do zrozumienia sprzedawcy, że jest prawowitym posiadaczem karty lub wyzyskać błąd powstały w jego świadomości (fałszywe wyobrażenie o rzeczywistości), że osoba posługująca się kartą ma do tego prawne umocowanie. Można to porównać do sytuacji w salonie sprzedaży telefonów komórkowych, kiedy przestępca, podszywając się pod inną osobę, zawiera umowę o świadczenie usług telekomunikacyjnych i z tego tytułu otrzymuje telefon na kredyt, którego potem nikt nie spłaca. Sprzedawca obsługujący w takim salonie reprezentuje firmę telekomunikacyjną i działa w jej imieniu, podobnie jak sprzedawca sklepowy zawiera w imieniu akceptanta umowę sprzedaży towaru.

Bazując na kształcie art. 115 § 9 k.k. sprzed 27 kwietnia 2017 r., autor stwierdził ponadto, że przepis art. 287 § 1 k.k. będzie miał zastosowanie do nieautoryzowanych transakcji kartowych realizowanych bez udziału „czynnika ludzkiego". W takim wypadku element wprowadzenia innej osoby w błąd lub wykorzystania jej błędu nie występuje, gdyż sprawca, posługując się bezprawnie danymi autoryzacyjnymi, oddziałuje na urządzenia i uruchamia algorytmy przetwarzające dane informatyczne związane z ich „obiegiem" w systemie płatności kartowych, nie zaś na psychikę człowieka. Chodziło m.in. o realizację transakcji zbliżeniowych w terminalach samoobsługowych, a więc przy użyciu czytników przyjmujących płatności automatycznie, zlokalizowanych np. w samoobsługowych kasach sklepowych, na stacjach benzynowych, w urzędach pocztowych, na autostradach i w innych miejscach użyteczności publicznej[331]. Przykład

[331] Na marginesie wskazać należy na błędne twierdzenia A. Czesnowickiej jakoby, przed nowelizacją Kodeksu karnego i rozszerzeniem definicji „rzecz ruchoma" o „środek pieniężny zapisany na rachunku", osoba wykonująca przestępczą transakcję zbliżeniową nie wypełniała swoim działaniem znamienia „wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych", gdyż w przypadku płatności zbliżeniowej nie sposób uznać, aby sprawca „wpływał", dokonując zniekształcenia bądź innej transformacji automatycznego procesu rozliczeniowego. Ten proces, zdaniem Autorki, przebiegać bowiem będzie dokładnie w ten sam sposób jak w przypadku dokonania płatności przez osobę uprawnioną, a mechanizm płatności, w tym uwierzytelniania i autoryzacji, nie ulegnie zmianie. A. Czesnowicka zapomina jednak, że przypisanie konkretnej osobie winy za popełnione przestępstwo wymaga, aby wypełniła ona swoim działaniem wszystkie znamiona czynu zabronionego. Sprawca przestępstwa nie tylko wpływa na automatyczne przetwarzanie danych informatycznych, ale ponadto robi to bez upoważnienia. Przyrównać można to do sytuacji, kiedy dwie osoby tłuką o podłogę ten sam drogocenny wazon, przy czym jedna z nich byłaby właścicielem rzeczy, a druga nie. Oczywiście, chociaż obydwoje realizują taki sam czyn w sensie zmiany, jaką powoduje on w otaczającej rzeczywistości, ale prawo własności do wazonu przysługujące jego właścicielowi, powoduje, że nie popełnia on przestępstwa, ale już druga osoba może odpowiedzieć za zniszczenie mienia (art. 288 § 1 k.k.); zob. A. Czesnowicka, *Transakcja nieautoryzowana z perspektywy prawnokarnej – kwalifikacja prawna dokonania tzw. płatności zbliżeniowej za pomocą cudzej karty płatniczej*, „Palestra" 2022, nr 7–8, wydanie internetowe: https://palestra.pl/pl/czasopismo/wydanie/7 – 8 – 2022 [dostęp: 08.07.2023].

takiego podejścia i kwalifikacji prawnej czynu na podstawie art. 287 § 1 k.k. stanowi wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie z 2016 r.:

> w okresie od 7 października 2016 r. do 8 października 2016r w Krakowie działając w celu osiągnięcia korzyści majątkowej oraz w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, używając karty bankomatowej banku Millenium własności P. Z., bez upoważnienia wpłynął na automatyczne przetwarzane, gromadzenie i przekazywanie danych informatycznych, dokonując nieuprawnionej transakcji bezgotówkowych i transakcji zbliżeniowych, powodując w ten sposób szkodę majątkową w mieniu P. Z. w łącznej kwocie 322.68 zł przy czym czynu tego dopuścił się w ciągu pięciu lat, po odbyciu w okresie od 2 listopada 2011r do 18 kwietnia 2014 – przy zaliczeniu okresów rzeczywistego pozbawienia wolności od 19 marca 2008r do 27 czerwca 2008r i od 3 marca 2009r do 8 czerwca 2009t – kary trzech lat pozbawienia wolności orzeczonej wyrokiem Sądu Rejonowego dla Krakowa – Nowej Huty Wydział II karny w Krakowie z dnia 27 czerwca 2008r sygn. II K 675/08/N za umyślne przestępstwo podobne spenalizowane w art. 280 § 1 k.k. – tj. o przest. z art. 287 § 1 k.k. w zw. z art. 12 k.k. w zw. z art. 64 § 1 k.k.[332]

Obowiązująca od 27 kwietnia 2017 r. zmiana art. 115 § 9 k.k. poprzez rozszerzenie definicji „rzecz ruchoma lub przedmiot" o „środek pieniężny zapisany na rachunku" dużo wyjaśniła w wykładni i stosowaniu prawa, a płatności zbliżeniowe słusznie zaczęto traktować jak kradzież. Problematyczna natomiast stała się kwestia, czy chodzi o zwykłą kradzież (art. 278 § 1 k.k.), czy też kradzież z włamaniem (art. 279 § 1 k.k.). Rozwiązanie tego problemu zależy od tego, jak potraktuje się na gruncie prawa karnego techniczne aspekty realizacji transakcji zbliżeniowych.

Stanowisko, że ma się do czynienia z art. 278 § 1 k.k., wyraził Sąd Apelacyjny w Gdańsku w wyroku z dnia 27 listopada 2018 r.[333] w którym oceniał wyrok Sądu Okręgowego w Bydgoszczy uznający oskarżonego za winnego tego, że:

---

[332] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 503/17/N.

[333] Wyrok Sądu Apelacyjnego w Gdańsku z dnia 27 listopada 2018 r., II AKa 307/18, KSAG 2019/1/197 – 213. Identyczne stanowisko, opierając się na przytoczonym orzeczeniu Sądu Najwyższego, zajął P. Szajna: „W świetle poczynionych rozważań czyn polegający na zrealizowaniu transakcji finansowej kartą z funkcją płatniczą w formie tzw. płatności zbliżeniowej (do kwoty niewymagającej autoryzacji kodem PIN) przez osobę nieuprawnioną, która weszła w jej posiadanie wbrew woli właściciela, stanowi kradzież. Jednakże – co wymaga wyraźnego podkreślenia – w sytuacji gdy nastąpi autoryzacja poprzez wprowadzenie kodu PIN, to dochodzi do przełamania zabezpieczenia i wówczas tego rodzaju czyn należy oceniać przez pryzmat znamion typu czynu zabronionego jakim jest kradzież z włamaniem", [w:] P. Szajna, *Transakcja zbliżeniowa zrealizowana cudzą kartą płatniczą do kwoty niewymagającej autoryzacji kodem PIN – kradzież (art. 278 § 1 k.k., art. 119 § 1 k.w.) czy kradzież z włamaniem (art. 279 § 1 k.k.)?*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1, s. 23.

w dniu 27 listopada 2017 r. w S., działając w krótkich odstępach czasu i ze z góry powziętym zamiarem poprzez trzykrotne użycie w transakcji zbliżeniowej karty bankomatowej należącej do pokrzywdzonej K. D., pokonał zabezpieczenia elektroniczne, włamując się do systemu bankowego, a następnie dokonał kradzieży pieniędzy w kwocie łącznej 57,40 zł, stanowiących płatność za zakupiony towar, to jest przestępstwa z art. 279 § 1 k.k.

W ocenie sądu, prawidłowość takiego poglądu, tj. wyczerpania przez oskarżonego znamion przestępstwa kradzieży z włamaniem, nasuwała daleko idące wątpliwości. Sąd stwierdził, że mikroprocesor znajdujący się na karcie stanowi jedynie indyferentny z punktu widzenia znamion określonych w art. 279 § 1 k.k. mechanizm umożliwiający komunikowanie się z systemem informatycznym banku, który wydał kartę, i realizację płatności. Mikroprocesor sam w sobie nie stanowi natomiast zabezpieczenia przed nieuprawnionym dostępem do środków pieniężnych. Z punktu widzenia zawartości bezprawności kryminalnej czynu – napisał sąd – nie można na jednej szali stawiać zachowania polegającego na dokonaniu za pomocą karty płatniczej płatności zbliżeniowej bez konieczności podawania kodu PIN z dokonaniem płatności przy użyciu tej samej karty z PIN-em. W pierwszym przypadku właściciel karty, wyrażając zgodę przy zawarciu umowy z bankiem, że do określonej, ustalonej wcześniej kwoty, możliwe będzie dokonywanie płatności zbliżeniowo przez każdą osobę bez konieczności autoryzowania jej za pomocą kodu PIN, do pewnego przynajmniej stopnia akceptuje zwiększone ryzyko, że w razie dostania się karty w ręce nieuprawnionej osoby możliwe będzie dokonywanie tych płatności, a przez to łatwiejsza kradzież środków pieniężnych znajdujących się na rachunku bankowym. Reasumując, napisał sąd, transakcja kartą płatniczą w formie płatności zbliżeniowej przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, stanowiło, w zależności od przywłaszczonej kwoty, przestępstwo kradzieży zwykłej określone art. 278 § 1 k.k. lub też wykroczenie z art. 119 § 1 k.w.[334] Identyczne stanowisko jak Sąd Apelacyjny w Gdańsku zajął P. Szajna, twierdząc, że czyn polegający na zrealizowaniu transakcji zbliżeniowej kartą do kwoty niewymagającej autoryzacji kodem PIN przez osobę nieuprawnioną to kradzież. Jednakże – co wymaga podkreślenia – w sytuacji, gdy nastąpi autoryzacja poprzez wprowadzenie PIN-u, to następuje przełamanie zabezpieczenia i wówczas tego rodzaju działanie należy oceniać przez pryzmat kradzieży z włamaniem[335]. Za przyjęciem w spornej kwestii

[334] Wyrok Sądu Apelacyjnego w Gdańsku z dnia 27 listopada 2018 r., II AKa 307/18, KSAG 2019/1/197 – 213; P. Szajna, *Transakcja zbliżeniowa zrealizowana*…, s. 23.

[335] Także zdaniem A. Adamskiego, uzyskanie pieniędzy z bankomatu za pomocą skradzionej lub sfałszowanej karty płatniczej jest zwykłą kradzieżą (art. 278 § 1 kk), [w:] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000 r., s. 120–121; podobnie J. Wojciechowski uważa, że pokonanie kodu zabezpieczającego rzecz przed dostępem do niej osób nieuprawnionych nie stanowi włamania w znaczeniu art. 279 § 1 kk, termin ten odnosi się bowiem do zabezpieczeń fizycznych, [w:] J. Wojciechowski, *Kodeks karny. Komentarz. Orzecznictwo*, Warszawa 2000, s. 523.

przestępstwa kradzieży, a nie kradzieży z włamaniem, opowiedziała się także A. Czesnowicka, chociaż jak sama przyznała, aktualnie dominujący okazał się pogląd przyjmowania w przypadku dokonania przez osobę nieuprawnioną płatności zbliżeniowej kwalifikacji prawnej z art. 279 § 1 k.k. Niewątpliwie, podsumowała A. Czesnowicka, wpłynął na to autorytet Sądu Najwyższego, ale sama autorka nie zgadzała się z takim stanowiskiem[336].

Prawdą jest, że Sąd Najwyższy zajął jednoznaczne stanowisko w sprawie transakcji zbliżeniowych w wyroku z dnia 22 marca 2017 r.[337], a orzeczenie to stanowiło ważny etap w ujednoliceniu stosowanej przez sądy i prokuratorów kwalifikacji prawnej czynów dotyczących transakcji zbliżeniowych. Sąd, odwołując się do tradycyjnego rozumienia pojęcia „włamanie" jako przełamanie zabezpieczeń, stwierdził, że pierwotne zabezpieczenie karty płatniczej stanowi jej konstrukcja, która zawiera mikroprocesor umożliwiający dokonywanie wszelkich transakcji, także zbliżeniowych, bez autoryzacji PIN-em. Przybliżenie karty płatniczej do terminalu skutkuje uzyskaniem dostępu do rachunku bankowego właściciela karty, dochodzi zatem do przełamania bariery elektronicznej w systemie bankowej płatności bezgotówkowej. Jeżeli czyni to osoba nieuprawniona, która weszła w posiadanie karty wbrew woli jej właściciela [powinno być „prawowitego posiadacza" – przyp. autora], w celu dokonania płatności za określony towar lub usługę, to w ocenie Sądu Najwyższego dokonuje ona kradzieży z włamaniem.

W glosie do ww. orzeczenia odmienne stanowisko zajął A. Lach[338], wskazując, że w funkcji zbliżeniowej nie można wyodrębnić czynności sprawczej polegającej na „włamaniu się" tak, jak ma to miejsce w przypadku wprowadzenia PIN-u przez osobę nieuprawnioną. „Zbliżając kartę do czytnika – pisze A. Lach – sprawca dokonuje rozporządzenia mieniem, nie sposób natomiast ani od strony semantycznej ani technicznej uznać, że dokonuje on włamania". Glosator odwołuje się do przykładu otwarcia drzwi do pokoju hotelowego poprzez naciśnięcie klamki, co nie wyczerpuje znamion „włamania", o którym mowa w art. 279 § 1 k.k. Jego zdaniem, podobnie ma się sprawa z odblokowaniem pokojowego zamka elektronicznego zabezpieczonego kartą z chipem, ale bez autoryzacji kodem[339]. A. Lach nie zauważa jednak podstawowej różnicy: każda osoba potrafi otworzyć drzwi klamką i nie potrzebuje do tego żadnego specjalnego narzędzia lub programu. Inaczej jest w przypadku zabezpieczenia drzwi zamkiem elektronicznym i kartą dostępu, kiedy wejście do pomieszczenia warunkowane jest posiadaniem karty z indywidualnym kodem. Ów system kontroli dostępu ma ograniczyć dostęp do pomieszczenia osobom nieuprawnionym, które np. mają pokój usytuowany naprzeciwko oraz identyczną wizualnie kartę dostępu, ale działającą tylko w czytniku drzwi ich pokoju. W hotelu system składa się z zamka dostępu do pokoju w postaci czytnika kart

[336] A. Czesnowicka, *Transakcja nieautoryzowana z perspektywy prawnokarnej…*
[337] Wyrok Sądu Najwyższego z dnia 22 marca 2017 r., III KK 349/16 OSNKW 2017, z. 9, poz. 50.
[338] A. Lach, *Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r., III KK 349/16*, „Prokuratura i Prawo" 2018, nr 5, s. 170–175.
[339] Tamże, s. 172.

lub skanera. Za pomocą oprogramowania operator systemu może dowolnie nadawać i zmieniać uprawnienia implementowane w pamięć hotelowej karty z nadrukowanym kodem kreskowym, karty magnetycznej, zbliżeniowej lub mikroprocesorowej. Analizowany problem przypomina sytuację z kluczem do zamka: przestępca musi najpierw wejść w jego posiadanie, aby otworzyć hotelowy pokój i ukraść z niego rzeczy. Czyn taki będzie kwalifikowany z art. 279 § 1 k.k.

A. Lach myli się, twierdząc, że w przypadku funkcji zbliżeniowej karty nie można wyodrębnić dwóch znamion czasownikowych, niezbędnych do przyjęcia kradzieży z włamaniem, tj. przełamania zabezpieczenia i zaboru rzeczy[340]. Powracając do przykładu hotelowego pokoju, to sprawca wpierw przełamuje zabezpieczenie (otwarcie drzwi kartą), a następnie wchodzi w posiadanie rzeczy stanowiących cudzą własność i oddala się z nimi (zabór rzeczy w celu ich przywłaszczenia). Zamiar sprawcy (strona podmiotowa przestępstwa) ma tutaj podstawowe znaczenie, gdyż identycznie wyglądające zachowanie człowieka w momencie pokonywania zabezpieczenia może generować odmienną kwalifikację prawną czynu. Przykładowo, jeśli sprawca otworzy drzwi cudzą kartą zbliżeniową z zamiarem sprawdzenia, kto zajmuje pokój, a następnie zostanie zatrzymany w progu mieszkania, to jego czyn stanowić będzie usiłowanie naruszenia miru domowego (art. 13 § 1 k.k. w zw. z art. 193 k.k.). W innym przypadku, gdy osoba zatrzymana przyszła z zamiarem kradzieży rzeczy, kwalifikacja prawna otrzyma postać art. 13 § 1 k.k. w zw. z art. 279 § 1 k.k.

Z. Kukuła braku znamion przestępstwa z art. 279 § 1 k.k. w posłużeniu się kartą płatniczą do transakcji zbliżeniowej upatruje w stwierdzeniu, że takim działaniem „żadnych zabezpieczeń przełamać nie sposób z przyczyn obiektywnych". Jego zdaniem, typowe włamanie powiązane jest „z jakąś formą użycia przemocy wobec zabezpieczeń", a omawiane zachowanie nie wymaga „podjęcia żadnego wysiłku, a jedynie przyłożenia karty do czytnika, przy którym nie ma żadnej najmniejszej nawet ingerencji zewnętrznej w system elektroniczny"[341]. Odnosząc się do argumentacji Z. Kukuły, warto zadać pytania: Czy rzeczywiście większego wysiłku, aniżeli przyłożenie mikroprocesora do czytnika, wymaga włożenie klucza do zamka w drzwiach i przekręcenie przez włamywacza tegoż zamka w celu otwarcia pokoju? Czy ma znaczenie dla kwalifikacji prawnej czynu jako kradzieży z włamaniem, że jeden złodziej otworzy sejf z pieniędzmi za pomocą specjalnego klucza ślusarskiego ze „szpilkami", a drugi wysadzi drzwi dynamitem?

Oczywiście, że oba czyny będą penalizowane z art. 279 § 1 k.k. Nadto, sprzeczne z prawami fizyki jest twierdzenie, że w przypadku płatności zbliżeniowej „nie ma żadnej najmniejszej nawet ingerencji zewnętrznej w system elektroniczny"; jest wręcz przeciwnie, gdyż mikroprocesor lub pasek magnetyczny „dogaduje się" z terminalem POS, a dokładniej z centrum autoryzacyjno-rozliczeniowym, które to urządzenia wymieniają

[340] Tamże.

[341] Z. Kukuła, *Dokonanie płatności skradzioną kartą bankomatową. Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r., sygn. III KK 349/16*, „Przegląd Sądowy" 2018, nr 7–8, s. 174–179.

między sobą pakiety danych. System działania kart płatniczych, oparty na indywidualnej, niepowtarzalnej informacji zapisanej w pamięci umieszczonej na plastiku, stanowi zabezpieczenie konkretnej karty przed jej nieuprawnionym użyciem. Gdyby było inaczej, to każdą funkcjonującą w obiegu kartą płatniczą można by realizować transakcje z dowolnego rachunku bankowego. Oczywiście, tak nie jest, gdyż spowodowałoby to dysfunkcjonalność rynku płatności kartowych. Mikroprocesorem i unikalnym, niepowtarzalnym kodem zaimplementowanym w kartę, ma prawo posługiwać się tylko posiadacz rachunku bankowego przypisanego do tej karty, co stanowi zabezpieczenie przed oszukańczymi transakcjami płatniczymi.

Powracając jeszcze do Z. Kukuły i podniesionego przez tego autora argumentu „wysiłku fizycznego" jako koniecznego elementu „włamania", to w orzecznictwie Sądu Najwyższego dawno już porzucono teorię niebezpieczeństwa (teorię siły fizycznej), odwołującą się do wykładni słownikowej (semantycznej) pojęcia „włamanie", na rzecz teorii zabezpieczenia. Wynikało to ze słusznego założenia, iż kryterium użycia siły fizycznej jako warunku *sine qua non* włamania, powodowałoby niczym nieuzasadnione premiowanie sprawców działających w sposób bardziej wyrafinowany i wysublimowany. Słusznie wskazuje się, że w zasadzie to, czy ktoś dokonuje włamania za pomocą łomu, powodując przy tej okazji nieraz znaczne zniszczenia, czy też zaledwie otwiera zamek dorobionym kluczem wbrew woli właściciela mieszkania, wymaga w obu przypadkach użycia jakieś siły fizycznej; w drugim przypadku nieporównywalnie mniejszej, ale jednak użycia siły. Kryterium siły nie stanowi więc żadnego charakterystycznego wyróżnika dla kradzieży z włamaniem[342]. Istotę rozumienia „siły fizycznej", towarzyszącej włamaniu, trafnie ujął T. Tyburcy, wskazując, że położenie każdego przedmiotu zostaje zmienione tylko przy użyciu takiej siły, co wynika z praw fizyki. Konkretne zabezpieczenie można pokonać przy większym (wyważenie drzwi) lub mniejszym jej natężeniu (otwarcie drzwi wytrychem lub kodem elektronicznym). Włamanie do zabezpieczenia informatycznego chroniącego przed kradzieżą następuje przy użyciu minimalnej siły fizycznej, będącej w tym wypadku także środkiem do uzewnętrznienia umiejętności złodzieja. Przy użyciu takiej siły może nastąpić ponadto podłączenie odpowiedniego urządzenia (programu) umożliwiającego włamanie[343]. Podobnie zaakceptowanie transakcji poprzez wpisanie czterocyfrowego kodu BLIK w aplikacji bankowości elektronicznej, ale już bez fizycznego użycia karty, wymaga określonej pracy wykonanej przez człowieka i liczonej w dżulach, co w języku prawniczym nazywa się „włamaniem". Podsumowując, zgodnie z utartą linią orzeczniczą i poglądami doktryny, dominuje obecnie teoria zabezpieczenia, która kładzie akcent na zamanifestowaną wolę właściciela rzeczy dotyczącą ich ochrony przed innymi osobami, zatem o bycie przestępstwa

[342] P. Nowak, *Wykładnia znamienia „włamanie" na gruncie art. 279 § 1 Kodeksu karnego*, „Palestra" 2013, nr 7–8, wydanie internetowe: https://palestra.pl/pl/czasopismo [dostęp: 05.08.2022].

[343] T. Tyburcy, *Treść i zakres znamienia „włamanie" (art. 279 § 1 k.k.) – czy kradzież z włamaniem może nastąpić tylko z pomieszczenia zamkniętego?*, „Acta Iuris Stetinensis" 2019, nr 25, s. 160.

stypizowanego w art. 279 § 1 k.k. nie świadczy siła fizyczna jako decydujący elementu kradzieży z włamaniem[344].

W celu dopełnienia analizy charakteru prawnego nieautoryzowanych transakcji zbliżeniowych, należy odwołać się jeszcze do teorii „klucza kryptograficznego" jako szczególnego rodzaju zabezpieczenia mienia. Z. Kukuła[345], ale także R. Sosik[346], podają argument, jakoby zabezpieczenie w postaci PIN-u było czymś więcej aniżeli systemem dostępu opartym na mikroprocesorze karty płatniczej.

> W przypadku włamania – pisze Z. Kukuła – sprawca musi posłużyć się kluczem – narzędziem umożliwiającym otwarcie zabezpieczenia /…/. Użycie karty płatniczej do dokonywania alternatywnych płatności zbliżeniowych nie jest zdolne przełamać jakiegokolwiek zabezpieczenia, bowiem dla takich transakcji zabezpieczeń nie przewidziano[347].

To błędny pogląd, gdyż przyłożenie karty do czytnika da się przyrównać do przekręcenia oryginalnego klucza w drzwiach cudzego mieszkania w celu dokonania kradzieży z włamaniem. Jeśli specjalne zabezpieczenie zamka stanowi oryginalny, niepowtarzalny kształt klucza pasujący tylko do tego jednego zamka, to ochronę środków pieniężnych zgromadzonych na rachunku bankowym stanowi oryginalny „klucz" cyfrowy pasujący tylko i wyłącznie do jednego rachunku bankowego. Stanowisko kwalifikujące zarówno transakcje płatnicze z wykorzystaniem PIN-u oraz bez wpisywania kodu jako kradzież z włamaniem odpowiada także postulatowi prowadzenia sprawiedliwej i racjonalnej polityki karnej. Skoro oba zabezpieczenia chronią dostęp do bankowego pieniądza bezgotówkowego, to nielogiczne oraz niesprawiedliwe byłoby, w przypadku przełamania zabezpieczenia PIN-em, pociągnięcie sprawcy do odpowiedzialności karnej z art. 279 § 1 k.k., a w przypadku transakcji zbliżeniowych tylko z art. 119 § 1 k.w. Należy przyjąć, że racjonalny ustawodawca nie dopuszcza takiej „penalnej dysharmonii" szczególnie dzisiaj, kiedy największa liczba nieautoryzowanych transakcji, wypełniających znamiona przestępstwa, dotyczy transferów zbliżeniowych.

Gdy analizuje się poglądy sprzeciwiające się kwalifikacji transakcji zbliżeniowych z art. 279 § 1 k.k., widać niekiedy brak konsekwencji ich autorów. Z jednej strony podkreślają oni obserwowany od pewnego już czasu rozwój technologii informatycznych, który nakazuje inaczej spojrzeć na charakter działania nowoczesnych systemów i urządzeń zabezpieczających mienie i w związku z tym „pojęcie włamania w rozumieniu art. 279 § 1 k.k. powinno ewoluować w kontekście rozwoju technicznego i nowych form popełnienia przestępstw"[348]. Jednak komentując płatności zbliżeniowe, zapominają o tym fakcie. W konsekwencji, aby

[344] P. Nowak, *Wykładnia znamienia „włamanie"…*
[345] Z. Kukuła, *Dokonanie płatności skradzioną kartą…*, s. 174–179.
[346] R. Sosik, *Wykorzystanie skradzionej karty płatniczej do wykonania płatności zbliżeniowych. Glosa do wyroku SN z dnia 22 marca 2017 r., III KK 349/16,* „Prokuratura i Prawo" 2017, nr 2, s. 124–125.
[347] Z. Kukuła, *Dokonanie płatności skradzioną kartą…*, s. 174–179.
[348] A. Lach, *Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r…*, s. 171.

uznać czyn za kradzież z włamaniem, chcą widzieć w ręce złodzieje symboliczny „łom", a nie subtelny klucz kryptograficzny, jaki stanowi system mikroprocesora. W kontrze do takiego stanowiska S. Tarapata prawidłowo określił samą kartę płatniczą jako narzędzie pozwalające na dostęp do środków pieniężnych zgromadzonych na rachunku bankowym tylko podmiotom do tego upoważnionym i porównał ją do klucza od sejfu, w którym przechowywane są pieniądze. Jeżeli dana osoba używa karty bez uprawnienia, to przełamuje środki chroniące mienie przed jego bezprawnym zadysponowaniem[349].

Najlepszy, bo empiryczny dowód na to, że mikroprocesor nie służy tylko do realizacji transakcji, ale stanowi efektywne, elektroniczne zabezpieczenie systemu kart płatniczych przed przestępstwami, stanowi historia wprowadzenia EMV. Ów termin oznacza globalny standard obsługi płatności przy użyciu kart z mikroprocesorem. Składają się na niego kolejne serie specyfikacji, procesów ich wdrażania i procedur testowych dla mikroprocesorowych kart płatniczych i urządzeń je akceptujących takich, jak punkty sprzedaży POS i bankomaty. Poczynając od końca lat 90. ubiegłego stulecia, kraje Europy Zachodniej zmagały się z plagą przestępczości kartowej polegającej na pozyskiwaniu w terminalach płatniczych numerów kart i wykorzystywaniu ich do oszukańczych transakcji. Dzięki datowanej od 2004 r. systematycznej migracji środowiska bankowego do EMV, w całej Europie odnotowano stały spadek liczby transakcji związanych z wypłatą środków pieniężnych z bankomatów przy użyciu „białego plastiku" (karty podrobione przez skimmerów). Mikroprocesor pozwala także na zastosowanie przez instytucje finansowe coraz bardziej wyrafinowanego oprogramowania i procedur wykrywających oraz przeciwdziałających oszustwom kartowym, m.in. informatycznych systemów detekcji danych, które w rzeczywistym czasie monitorują i rozpoznają podejrzane operacje. Wynika z tego, że założenia techniczne oparte na płatnościach z wykorzystaniem mikroprocesora gwarantują kompatybilność kart i przeznaczonych do ich obsługi terminali na całym świecie[350].

Kradzież pieniędzy w wyniku przeprowadzenia transakcji zbliżeniowej przez sprawcę przestępstwa została prawidłowo zakwalifikowana z art. 279 § 1 k.k. w wyroku Sądu Okręgowego w Radomiu oraz w orzeczeniach Sądu Rejonowego Gdańsk-Południe w Gdańsku. Podkreślenia natomiast wymaga, że w opisie czynów jako pokrzywdzonego wskazano tylko posiadacza rachunku bankowego. Pominięto natomiast właściciela tego rachunku i zgromadzonych (przed kradzieżą) na nim pieniędzy, co było błędem zgodnie ze wcześniejszymi ustaleniami. W obu przypadkach podstawą skazania był art. 279 § 1 k.k., a sprawcy zostali uznani za winnych tego, że:

[349] S. Tarapata, *Wybrane prawnokarne zagadnienia...*
[350] P. Opitek, *Wpływ standardu EMV...*, s. 136–137.

w dniu 03 stycznia 2018 roku w K., działając w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru i wspólnie i w porozumieniu, pokonując elektroniczne zabezpieczenia należącej do K. C. karty płatniczej w Banku /…/ dokonali na jej szkodę kradzieży pieniędzy o łącznej wartości 200,26 (dwieście 26/100) złotych, dokonując pięciokrotnie przy użyciu tejże karty płatności:
— w sklepie /…/ sp. z o.o. o wartości 37,98 złotych,
— w sklepie stacji paliw /…/ o wartości 28,88 złotych,
— w sklepie /…/ o wartości 46,28 złotych,
— w przedsiębiorstwie /…/ s.c. o wartości 48,15 złotych,
— w przedsiębiorstwie P.H.U. GIG A. G. o wartości 38,97 złotych, przy czym P. K. czynu tego dopuścił się w ciągu 5 lat po odbyciu co najmniej 6 miesięcy kary pozbawienia wolności orzeczonej za umyślne przestępstwo podobne, tj. za winnych czynu z art. 279 § 1 k.k. w zw. z art. 12 k.k. w zw. z art. 64 § 1 k.k. w stosunku do P. K., zaś art. 279 § 1 k.k. w zw. z art. 12 k.k. w stosunku do I. L.[351]

w dniu 30 sierpnia 2018 r. w G. w sklepie warzywno-owocowym działając wspólnie i w porozumieniu z D. N. dokonali kradzieży z włamaniem w ten sposób, że bez zgody osoby uprawnionej, poprzez pokonanie zabezpieczenia elektronicznego chroniącego dostęp do karty bankomatowej banku /…/ **** **** /…/ wystawione na dane T. S., dokonali w sposób zbliżeniowy płatności w kwocie 25,80 zł, czym działali na szkodę T. S., tj. o czyn z art. 279 § 1 k.k.[352]

w dniu 10 marca 2018 r. w miejscowości T. wszedł w posiadanie karty bankomatowej z banku /…/ S.A. należącej do E. P. po czym poprzez użycie w transakcji karty zbliżeniowej z banku /…/ S.A. należącej do ww. pokonał zabezpieczenie elektroniczne włamując się do systemu bankowego, a następnie dokonał kradzieży pieniędzy w kwocie 35 PLN stanowiące płatność za zakupiony towar w sklepie /…/ przy ul. /…/ w miejscowości T. działając na szkodę E. P., tj. o przestępstwo art. 279 § 1 k.k.[353]

Podsumowując, należy przyjąć pogląd jako słuszny i zgodny z przeważającą linią orzeczniczą, że uiszczenie ceny w formie płatności zbliżeniowej przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela i/lub prawowitego posiadacza, stanowi przestępstwo kradzieży z włamaniem (art. 279 § 1 k.k.)[354]. Tak samo jak transakcje kartowe wymagające podania PIN-u uznawane są za kradzież z włamaniem,

[351] Wyrok Sądu Okręgowego w Radomiu z dnia 8 marca 2019 r., II K 82/18, LEX nr 3077417.
[352] Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 30 lipca 2019 r., X K 146/19, LEX nr 2785597.
[353] Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 11 października 2018 r., X K 499/18, LEX nr 2622492.
[354] Wyrok Sądu Apelacyjnego w Lublinie z dnia 20 grudnia 2019 r., II AKa 235/19, LEX nr 3077417.

to kod jest tylko zabezpieczeniem dodatkowym, a pierwotną ochronę przed nadużyciami stanowi konstrukcja karty płatniczej z wbudowanym mikroprocesorem. W chipie zapisany jest niepowtarzalny klucz bezpieczeństwa umożliwiający dostęp do konkretnego rachunku bankowego i dokonywanie transakcji, w tym również zbliżeniowych, bez użycia PIN-u. Przybliżenie karty płatniczej do terminalu skutkuje uzyskaniem dostępu do rachunku bankowego właściciela karty, dochodzi zatem do przełamania bariery elektronicznej w systemie bankowych płatności bezgotówkowych. Jeżeli czyni to osoba nieuprawniona, to popełnia przestępstwo kradzieży z włamaniem[355]. Trafnie ujął to Sąd Apelacyjny w Lublinie:

> W orzecznictwie sądów przez długi czas występowały rozbieżności co do kwalifikacji prawnej działania polegającego na posłużeniu się kartą płatniczą wbrew woli jej właściciela. Ostatecznie dominującym okazał się pogląd, iż dokonanie płatności kartą płatniczą w formie tzw. płatności zbliżeniowej przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, stanowi przestępstwo kradzieży z włamaniem (art. 279 § 1 k.k.)[356].

4. 5. Dodatkowe uwagi o kwalifikacji prawnej czynu z art. 287 § 1 k.k.

Przedmiotem ochrony art. 287 k.k. są dane informatyczne, a więc bezpieczne funkcjonowanie urządzeń i systemów działających w oparciu o takie dane. Przewidziana ochrona nie jest różnicowana w zależności od rodzaju komputera, bo w istocie każde urządzenie cyfrowe służące do przetwarzania informacji to komputer. Nie znajdują zatem podstaw w obowiązujących przepisach prawa wątpliwości wyrażone przez M. Siwickiego: Czy przedmiotem ochrony przepisu art. 287 k.k. są wszystkie systemy przetwarzania danych (np. prosty sprzęt AGD, elektroniczne kasowniki biletów), czy tylko te, które pełnią znaczące (ważne) funkcje związane z przetwarzaniem danych, np. bankomaty, internetowe portale aukcyjne, serwisy internetowe banków?

Ostatecznie jednak ww. autor słusznie stwierdza, że przepis art. 287 k.k.

> nie wprowadza jakiejkolwiek klasyfikacji danych informatycznych i nie różnicuje odpowiedzialności karnej od ich charakteru lub treści. Aby sprawiedliwie ocenić zachowanie danej osoby i uniknąć zbytniej punitywności prawa karnego, przy ocenie

[355] Postanowienie Sądu Najwyższego z dnia 18 maja 2021 r., III KK 102/21, LEX nr 3177284. Innym razem Sąd Najwyższy zauważył, że kod jako swoisty i niepowtarzalny klucz elektroniczny zabezpieczający dostęp do rachunku bankowego za pośrednictwem ATM-u wraz z kartą bankomatową stanowią przeszkodę do zawładnięcia mieniem innej osoby. Jej pokonanie w wyniku posłużenia się skradzioną kartą i PIN-em (kluczem elektronicznym) w celu pobrania pieniędzy z bankomatu, wyczerpuje znamiona kradzieży z włamaniem, tj. art. 279 § 1 k.k., [w:] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 9 lipca 2014 r., II AKa 180/14, LEX nr 1506771. Podobnie: postanowienie Sądu Najwyższego z dnia 2 grudnia 2020 r., III KK 358/20, LEX nr 3183271; wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.

[356] Wyrok Sądu Apelacyjnego w Lublinie z dnia 20 grudnia 2019 r., II AKa 235/19, LEX nr 3077417.

> prawnej czynu zawsze należy posiłkować się materialną definicją przestępstwa, zgodnie z którą warunkiem odpowiedzialności karnej jest większy niż znikomy stopień społecznej szkodliwości czynu[357].

Warto dodać, że spełnienie warunku społecznej szkodliwości czynu nie jest czymś „posiłkowym" przy ocenie bytu przestępstwa, ale obligatoryjnie waży się go w okolicznościach faktycznych sprawy. Oczywiste jest zatem, że nie popełni przestępstwa osoba, która chcąc komuś dokuczyć, przeprogramuje telewizor w taki sposób, że „pokrzywdzony" nie oglądnie ulubionego programu albo wbrew jego woli rozreguluje cyfrowy moduł sterujący pralką po to, aby utrudnić pranie. Jeśli natomiast wgranie złośliwego oprogramowania do modułu urządzenia spowodowałoby, że telewizor lub pralka stałyby się trwale bezużyteczne, to wówczas można mówić o zrealizowaniu przez sprawcę znamion art. 287 § 1 k.k. Trudno bowiem *in abstracto* uznać, jak chciałby M. Siwicki, że omawiane przestępstwo dotyczy

> operacji przetwarzania danych odnoszące się jedynie do takich systemów, które dokonują skomplikowanych operacji arytmetycznych na danych informatycznych. W przypadku, gdy „proces decyzyjny komputera" nie ma takiego charakteru, a więc przebiega na przykład w sposób czysto mechaniczny, np. w przypadku automatów rozmieniających pieniądze, które oceniają ich nominał po wadze, art. 287 k.k. nie znajdzie zastosowania[358].

Jeśli ów automat działa w oparciu o przetwarzanie danych informatycznych, a jego złośliwe uszkodzenie spowoduje, że np. duża grupa osób przez dłuższy okres czasu nie będzie mogła korzystać z ważnej usługi opłacanej rozmienionymi w urządzeniu monetami, to wcale nie jest powiedziane, że sprawca unieruchomienia automatu uniknie odpowiedzialności karnej z art. 287 § 1 k.k., szczególnie że w § 2 tego przepisu ustawodawca przewidział „wypadek mniejszej wagi".

Omówione wyżej przykłady dotyczą sytuacji nietypowych i wyjątkowych, bowiem do realizacji znamion „oszustwa komputerowego" dojdzie najczęściej wtedy, gdy osoba ma dostęp do danych informatycznych w systemie podmiotu prowadzącego działalność gospodarczą i z jakichś powodów realizuje znamiona czynu karalnego. Stosunkowo często dzieje się tak, gdy sprawca, z tytułu wykonywanego zawodu i powierzonych mu przez pracodawcę obowiązków, posiada akces do elektronicznej bazy danych i manipuluje danymi informatycznymi w celu osiągnięcia korzyści majątkowej. Wyroki skazujące nierzadko odnosiły się do pracowników banków, którzy realizowali znamiona art. 287 § 1 k.k., np. P. B. został skazany wyrokiem Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 21 lutego 2019 r. za to, że

[357] Zob. M. Siwicki, *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018, s. 175.
[358] Tamże.

w okresie od dnia 5 lipca 2011 r. do dnia 23 października 2015 r. w P., działając w celu osiągnięcia korzyści majątkowej, w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, pełniąc funkcję Dyrektora działającego w P. Oddziału /…/ Banku S. w R., wprowadzając nowe zapisy oraz zmiany dotychczasowych danych informatycznych w elektronicznym systemie bankowym polegające na uruchamianiu kredytów i pożyczek oraz zwiększaniu limitu zadłużeń na rachunkach bankowych klientów, bez upoważnienia i wiedzy innych pracowników Banku oraz bez zgody i wiedzy osób, których dotyczyły ww. czynności, przywłaszczył sobie uzyskane w ten sposób środki pieniężne w łącznej wysokości 34.697.247,00 złotych należące do /…/ Banku S. w R. i powierzone mu z racji wykonywanych obowiązków, i tak:
1. w dniu 5 lipca 2011 r. przywłaszczył kwotę 35.000,00 złotych pochodzącą z uruchomionego przez siebie kredytu na dane A. S.
/w opisie wymieniono 148 działań sprawcy noszących znamiona przywłaszczenia mienia/
powodując szkodę w łącznej wysokości 7.478.317,36 złotych, stanowiącą różnicę pomiędzy wartością przywłaszczonych środków pieniężnych z tytułu fikcyjnych kredytów i pożyczek oraz zwiększeń limitów kredytowych a wysokością spłat i pokryć owych kredytów, pożyczek i limitów zadłużeń, których dokonał ze środków uzyskanych z kolejnych fikcyjnych, wyżej opisanych czynności bankowych, pomniejszoną o wartość odsetek, nadto zaś – w zakresie nieuprawnionej ingerencji w dane informatyczne – działając na szkodę P. W., O. M. i G. M., tj. o przestępstwo z art. 284 § 2 k.k. w zw. z art. 294 § 1 k.k. i z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[359]

Warto zwrócić uwagę, że chociaż w art. 287 § 1 k.k. mowa jest o „danych informatycznych" jako przedmiocie czynności wykonawczej, to w orzecznictwie powszechnie stosuje się ów przepis do penalizacji nielegalnych zachowań ukierunkowanych na informacje. W opisie czynu zamieszczonym w wyroku Sądu Okręgowego w Piotrkowie Trybunalskim wskazano, że dyrektor oddziału banku „wprowadził nowe zapisy oraz zmiany dotychczasowych danych informatycznych w elektronicznym systemie bankowym polegające na uruchamianiu kredytów i pożyczek oraz zwiększaniu limitu zadłużeń na rachunkach bankowych klientów". Nie ulega wątpliwości, że oskarżony operował na informacjach zamieszczonych w systemie bankowym, a nie na danych informatycznych. Mówiąc wprost: w momencie popełnienia czynu zabronionego na monitorze komputera wprowadzał sensowną treść dotyczącą imienia i nazwiska fikcyjnego kredytobiorcy, wysokości kredytu, okresu jego spłaty itd., a więc wprowadzał w systemie banku nowy zapis informacji, a nie danych informatycznych. Także wskazuje na to treść uzasadnienia do wyroku; sąd ustalił, że oskarżony „wchodził" na konta

[359] Wyrok Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 21 lutego 2019 r., III K 73/18, LEX nr 2635086.

P. W., O. i G. M. uruchamiał na ich rachunkach kredyty, dokonywał przelewów", „zamykał jeden fikcyjny kredyt innym fikcyjnym kredytem". Dopiero wtórnym skutkiem wprowadzenia ww. informacji było przekonwertowanie ich przez algorytm komputerowy na dane informatyczne i przetwarzanie w informatycznym systemie bankowym. Oskarżony nie działał zatem na „surowych" danych informatycznych, reprezentowanych w formie cyfrowej, bo zapewne nie znał się i nie rozumiał znaczenia języka programowania.

Jak zatem znaleźć rozwiązanie w takiej sytuacji, skoro podstawowym założeniem wykładni znamion przestępstw teleinformatycznych jest odróżnienie informacji od danych informatycznych, i czy dokonane przez Sąd Okręgowy w Piotrkowie Trybunalskim opis i kwalifikacja prawna czynu były prawidłowe? Można przyjąć, że „wpłynięcie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianę, usunięcie albo wprowadzenie nowych zapisów danych informatycznych" stanowi skutek działania sprawcy, który może być poprzedzony zmianą lub usunięciem informacji w systemie albo wprowadzeniem nowych informacji do systemu. Takie zachowanie sprawcy powoduje konwersję sensownej treści na jej postać zapisu binarnego i uruchomienie procesu automatycznego przetwarzania, gromadzenia i przekazywania danych. Uporządkowaniem sytuacji mogłaby być nowelizacja art. 287 k.k. poprzez wprowadzenie nowego art. 1a w brzmieniu[360]:

> § 2a. Jeżeli czyn określony w § 1 dotyczy informacji, sprawca podlega karze pozbawienia wolności /…/.

Manipulowanie danymi dotyczy niekiedy kont na platformach społecznościowych lub aukcyjnych i wynika z konfliktów na tle obyczajowym pomiędzy prawowitym użytkownikiem konta a sprawcą przestępstwa. Często dzieje się tak na tle toczącej się sprawy rozwodowej, w wyniku zdrady małżeńskiej czy zakończenia nieformalnego związku. Podobna sytuacja zaistniała w sprawie prowadzonej przez Sąd Rejonowy dla Krakowa-Krowodrzy w Krakowie, w której mężczyzna została skazany za to, że:

> w dniu 16 grudnia 2011 roku w Krakowie działając w celu wyrządzenia szkody A. /…/ bez upoważnienia wpływał na automatyczne przekazywanie danych informatycznych poprzez zalogowanie się przy wykorzystaniu hasła na konto A. /…/ w portalu www.allegro.pl i złożenie oferty zakupu samochodu Audi A8 oraz krawatki Swarowski zawierając w ten sposób bez jej wiedzy i zgody umowy kupna-sprzedaży, tj. o przestępstwo z art. 287 § 1 k.k.[361]

[360] Podobny zabieg legislacyjny zastosowano przy redakcji art. 268. k.k., gdzie w § 1 mowa jest o „informacji", a § 2 brzmi: „Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3".

[361] Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie Wydział II Karny o sygn. II K 549/12/K.

Oskarżony wyjaśnił, że znał hasło żony do jej konta na platformie Allegro; powiedział: „przecież byliśmy małżeństwem wiele lat i zasada tworzenia haseł w trakcie małżeństwa była taka sama" (małżonkowie byli w trakcie sprawy rozwodowej). Zalogował się na jej konto, gdyż chciał sprawdzić, jakie rzeczy kupuje, i „przypadkiem kliknął na te dwie oferty", wygrywając licytację sprzedaży samochodu za kwotę 60000 zł i krawatki „Svarowski" za 4,40 zł. Opłata za towar nie została uiszczona i jak zeznała kobieta: „jakiś mężczyzna" miał do niej pretensje, że nie zapłaciła za pojazd.

Z treści zarzutu wynika, że oskarżony zalogował się bez uprawnienia do konta, a więc wypełnił także znamiona przestępstwa z art. 267 § 1 k.k., czego zabrakło w opisie i kwalifikacji prawnej czynu. Pokrzywdzona sama złożyła wiosek o „ściganie i ukaranie osoby za włamanie na jej konto". Ponadto w Kodeksie cywilnym jest mowa o „umowie sprzedaży", a nie „kupna-sprzedaży", a więc pierwsza z wymienionych nazw powinna zostać użyta w tekście prawnym. W wyroku napisano niepoprawną nazwę firmy: „Swarowski" zamiast „Swarovski". To kolejny dowód na to, że sądy zbyt często publikują wadliwe wyroki nie tylko pod względem subsumpcji norm prawa, ale także lingwistyki prawniczej i zasad poprawnej polszczyzny. W tej sprawie prawidłowy opis czynu i jego kwalifikacja prawna powinny brzmieć następująco:

> w dniu 16 grudnia 2011 roku w Krakowie bez uprawnienia, omijając zabezpieczenie informatyczne w postaci hasła dostępu, uzyskał dostęp do informacji znajdujących się na koncie A. /…/ założonym na portalu www.allegro.pl i działając w celu wyrządzenia A. /…/ szkody bez upoważnienia wprowadził nowy zapisy danych informatycznych na koncie, co spowodowało ich automatyczne przetwarzania przez system informatyczny,
>
> w postaci przystąpienia do licytacji na internetowej aukcji i zawarcia umowy sprzedaży samochodu osobowego marki Audi A8 za kwotę 60 000 zł i krawatki firmy „Swarovski" za kwotę 4,40 zł, co spowodowało roszczenia po stronie sprzedających o zapłatę ceny za wylicytowany towar skierowane do A. /…/, tj. o przestępstwo z art. 267 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

Warto zwrócić uwagę na subtelną różnicę w określeniach: „bez uprawnienia" (art. 267 § 1 k.k.) i „bez upoważnienia" (art. 287 § 1 k.k.); wynika z nich, że w przypadku przestępstwa hakingu sprawca w ogóle nie ma prawa do zapoznania się z informacją, a osoba popełniająca „oszustwo komputerowe" posiada legalny dostęp do danych informatycznych, ale łamie prawo, manipulując nimi. Kwestionuje się dopuszczalność zbiegu realnego pomiędzy art. 267 § 1 k.k. i art. 287 § 1 k.k. W akcie oskarżenia Prokuratury Rejonowej dla Krakowa-Podgórza w Krakowie z dnia 28 czerwca 2013 r. podsądny został oskarżony o to, że:

działając w krótkich odstępach czasu, w ramach z góry powziętego zamiaru w celu osiągnięcia korzyści majątkowej, po uprzednim pozyskaniu w nieustalonym dniu, nie później niż 25 października 2012 r. w Krakowie hasła dostępu do internetowego konta bankowego K. B. o nr /…/ i po jego wykorzystaniu bez zgody pokrzywdzonej oraz wprowadzeniu bez jej upoważnienia nowego zapisu danych informatycznych na przedmiotowym koncie w dniu 25 października 2012 r. dokonał zaboru w celu przywłaszczenia kwoty 27 000 zł na szkodę K. B., tj. o przest. z art. 269b § 1 k.k. i art. 287 § 1 k.k. i art. 279 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[362]

Sąd wyrokiem z dnia 20 kwietnia 2016 r., który dotyczył jednego z dwóch współsprawców przestępstwa, zmienił kwalifikację prawną i opis zarzuconego mężczyźnie czynu i uznał oskarżonego za winnego tego, że:

uznaje oskarżonego W. K. w ramach zarzucanego mu czynu za winnego tego, że w dniu 25 października 2012 r. w Krakowie, w celu osiągnięcia korzyści majątkowe, wykorzystując bez jej zgody hasło i login pokrzywdzonej K. B., uzyskał bez uprawnienia dostęp do panelu klienta systemu bankowości internetowej BRE Bank S.A. w części służącej do obsługi rachunku bankowego nr /…/ i następnie bez uprawnienia wprowadził do powyższego systemu informatycznego nowy zapis danych informatycznych w formie zaksięgowania obciążenia rachunku bankowego pokrzywdzonej K. B. nr /…/ na rzecz rachunku bankowego nr /…/, prowadzonego dla /…/ na kwotę 27 000 zł, co stanowi występek z art. 287 § 1 k.k. /…/[363]

W uzasadnieniu do wyroku sąd wskazał, iż:

> art. 287 § 1 k.k. penalizuje wywarcie, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, wpływu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianę, usuwanie lub wprowadzenie nowego zapisu danych informatycznych. Polecenie przelewu wprowadzane do systemu informatycznego banku za pomocą panelu klienta systemu bankowości internetowej należy zakwalifikować jako wprowadzenie nowego zapisu danych informatycznych, powodujące automatyczne przetwarzanie danych informatycznych w postaci obciążenia rachunku bankowego nadawcy przelewem na rzecz rachunku bankowego odbiorcy przelewu.[364]

Dalej sąd napisał:

[362] Akta Prokuratury Rejonowej dla Krakowa-Podgórza w Krakowie o sygn. 2 Ds. 1880/12/D.
[363] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.
[364] Tamże.

> /…/ w przypadku czynu W. K. należy ponadto rozważyć relację pomiędzy art. 267 § 2 k.k. i art. 287 § 1 k.k., tj. czy pomiędzy tymi przepisami zachodzi zbieg właściwy czy tez zbieg niewłaściwy. Zgodnie z regułą konsumpcji zbieg niewłaściwy, czyli pomijalny, zachodzi wtedy, gdy zakwalifikowanie zachowania z jednego ze zbiegających się przepisów czyni kwalifikowanie czynu z drugiego przepisu zbędnym z punktu widzenia potrzeby oddania zawartości kryminalnej danego zachowania /…/. W niniejszej sprawie oskarżony, aby móc bez uprawnienia dokonać przelewu z rachunku bankowego pokrzywdzonej, musiał uzyskać nieuprawniony dostęp do panelu klienta systemu bankowości internetowej /…/ Głównym celem zamachu oskarżonego było mienie oskarżonej, natomiast sam dostęp do systemu informatycznego był dla oskarżonego jedynie środkiem do osiągnięcia tego celu, a czynności sprawcze przemawiające za zakwalifikowaniem zachowania oskarżonego z obu zbiegających się przepisów pozostają ściśle ze sobą powiązane. Ponadto popełnienie czyny z art. 287 § 1 k.k. godzi jednocześnie w dwa dobra prawnie chronione w postaci mienia i bezpieczeństwa informacji, a właśnie bezpieczeństwo informacji jest przedmiotem ochrony art. 267 § 2 k.k.[365]

Mając powyższe na względzie, sąd przyjął, że w rozpatrywanym stanie faktycznym nieuprawnione uzyskanie dostępu do panelu klienta jest czynem współukaranym uprzednim w stosunku do czynu z art. 287 § 1 k.k., ponieważ zakwalifikowanie działania W. K. z art. 287 § 1 k.k. oddaje całą zawartość kryminalna jego zachowania. Samo wprowadzenie nowego zapisu danych informatycznych w postaci dyspozycji przelewu i spowodowanie przez to szkody materialnej u K. B. stanowi o realizacji wszystkich znamion powołanego przepisu.

Na wstępie rozważań nad wyrokiem Sądu Rejonowego dla Krakowa-Podgórza w Krakowie oraz argumentami zamieszczonymi w uzasadnieniu orzeczenia należy zaznaczyć, że po zmianie definicji „rzecz ruchoma" w 2017 r. rozpatrywany przez sąd stan faktyczny należałoby zakwalifikować jako kradzież z włamaniem. Niemniej, problematyka zbiegu realnego art. 267 § 1 lub 2 k.k. i art. 287 § 1 k.k. nadal ma praktyczne znaczenie, ponieważ istnieją wartości majątkowe, np. artefakty w grach lub kryptowaluty, których tzw. kradzież będzie kwalifikowana z art. 287 § 1 k.k. Nie sposób dlatego zgodzić się z przywołanym stanowiskiem sądu, że „zakwalifikowanie czynu W. K. z art. 287 § 1 k.k. oddaje całą zawartość kryminalną jego zachowania", gdyż artykuł ten nie zawiera znamienia przełamywania zabezpieczeń, a oskarżony „zhakował" zabezpieczenie cudzego internetowego konta bankowego, posługując się bez uprawnienia hasłami wydanymi przez bank posiadaczowi konta. Sytuację tę można porównać z kradzieżą zwykłą (art. 278 § 1 k.k.) i kradzieżą z włamaniem (art. 279 § 1 k.k.): sprawca podlega surowszej odpowiedzialności karnej, jeśli przełamie zabezpieczenie mobilnej aplikacji bankowej i dostanie się do jej środka, a następnie dokona zaboru w celu przywłaszczenia pieniędzy (kradzież z włamaniem), aniżeli wykorzystałby tylko

[365] Tamże.

otwartą aplikację na pulpicie komputera i wyprowadził z niej środki (kradzież). Tak samo czymś więcej, aniżeli tylko manipulowaniem danymi informatycznymi, jest włamanie się do konta gry lub portfela kryptowalutowego i przetransferowanie stamtąd wartości cyfrowych, aniżeli uczynienie takiego transferu bez hakowania konta czy portfela. Taki punkt widzenia przyjął prokurator, oskarżając sprawcę o przełamanie elektronicznego zabezpieczenia, a następnie osiągnięcie korzyści majątkowej poprzez zmianę bez upoważnienia zapisu danych informatycznych i przejęcie awatara w grze komputerowej, tj. o czyn z art. 267 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[366] Sądy obu instancji nie zakwestionowały takiej kwalifikacji prawnej zdarzenia, ale uniewinniły oskarżonego, gdyż inne okoliczności nie przesądzały w sposób jednoznaczny o jego sprawstwie i powodowały „stan wątpliwości co do winy R. N.". Poglądy doktryny w tej kwestii są natomiast zróżnicowane. B. Kunicka-Michalska twierdzi, że w opisanej sytuacji art. 267 § 1 k.k. zostaje pochłonięty przez art. 287 k.k.[367], ale przywołuje także stanowisko B. Michalskiego, który wyraził stanowisko, że dokonanie oszustwa komputerowego możliwe jest dopiero po pokonaniu przez sprawcę zabezpieczeń w postaci haseł, kodów itp., a więc sprawca wpierw musi rozszyfrować hasła lub kody zabezpieczające system, aby zrealizować znamiona czasownikowe występku z art. 287 k.k. Czyn taki należy zatem kwalifikować dodatkowo na podstawie art. 267 § 1 k.k., który pozostaje wtedy w kumulatywnym zbiegu z oszustwem komputerowym[368]. R. Korczyński i R. Koszut także stoją na stanowisku, że jeśli realizacja znamion art. 287 § 1 k.k. poprzedzona jest dodatkowo przełamywaniem przez sprawcę specjalnych zabezpieczeń, to jego zachowanie narusza także dyspozycję art. 267 § 1 k.k., penalizującego przestępstwo hakingu[369].

Na przykładzie wyroku Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 21 lutego 2019 r. pokazano już, że często zdarzają się sytuacje, kiedy osoba z tytułu świadczenia pracy lub sprawowania funkcji posiada uprawniony dostęp do systemu informatycznego przeznaczonego do rozliczeń finansowych i chcąc się wzbogacić, bez upoważnienia wprowadza w nim nowe zapisy. W podobnej sprawie Sąd Rejonowy dla Krakowa-Podgórza w Krakowie uznał oskarżoną za winną popełnienia szeregu podobnych przestępstw, a jeden z czynów miał postać:

> w dniu 9 października 2016 roku w Krakowie doprowadził /…/ S. A. w celu osiągnięcia korzyści majątkowej, do niekorzystnego rozporządzenia mieniem w kwocie 218,87 zł przy dokonaniu wpłaty od L. S. poprzez wpłynięcie bez upoważnienia na automatyczne przetwarzanie danych informatycznie w systemie operacyjnym /…/ poprzez skasowanie w/w wpłaty tj. o czyn z art. 287 § 1 k.k.[370]

[366] Wyrok Sądu Okręgowego w Poznaniu z dnia 7 marca 2017 r., IV Ka 111/17, LEX nr 2280584.
[367] B. Michalski, *Przestępstwa przeciwko mieniu. Rozdział XXXV Kodeksu karnego. Komentarz*, Warszawa 1999, s. 224, [za:] B. Kunicka-Michalska, *Oszustwo komputerowe. Regulacje prawa polskiego*, „Studia Prawnicze" 2006, nr 4, s. 116–117.
[368] B. Kunicka-Michalska, *Oszustwo komputerowe...*, s. 117.
[369] R. Korczyński, R. Koszut, *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2022, nr 2, s. 23.
[370] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 418/18/P.

W sprawie ustalono, że kobieta obsługiwała klientów w placówce pocztowej i z tego tytułu użytkowała program komputerowy do rozliczania przyjętych przez nią wpłat gotówki. Przestępstwa popełniała w ten sposób, że w obecności interesantów wprowadzała zapisy do systemu informatycznego o przyjętej wpłacie, a potem usuwała dane, aby niezewidencjonowane środki wykorzystać na własne cele. Na dobrą sprawę zatem zachowanie takie odpowiada znamionom art. 284 § 1 k.k., tj. przywłaszczeniu mienia w postaci wpłaconych przez osoby trzecie pieniędzy w formie gotówki. Aby ukryć ten nielegalny proceder, oskarżona, działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia usuwała zapis danych informatycznych dokumentujących wpłaty dokonane przez klientów instytucji pośredniczącej w rozliczeniach. Warto podkreślić, że dane w tym przypadku nie utożsamiały „środków pieniężnych zapisanych na rachunku" (art. 115 § 9 k.k.), gdyż system komputerowy ewidencjonował tylko wpłaty, ale nie stanowił rachunku, na którym zgromadzone były środki pieniężne w formie elektronicznej. Gdyby w dacie popełnienia czynu obowiązywała nawet definicja legalna „rzeczy ruchomej" w obecnym jej kształcie, to i tak nie byłoby mowy o kwalifikowaniu opisanego zachowania jako kradzieży z art. 278 § 1 k.k. Odmienna sytuacja miała miejsce w wyroku skazującym wydanym przez Sąd Rejonowy dla Krakowa-Podgórza w Krakowie, gdy sprawca:

> działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia, wpłynęła na automatyczne przetwarzanie danych informatycznych w ten sposób, że dokonała dyspozycji wypłaty z rachunków bankowych należących do pokrzywdzonych /…/ prowadzonych przez bank /…/ S.A. na ustalone kwoty, podrabiając dokument w postaci potwierdzenia wpłaty gotówkowej z rachunków ustalonych klientów nakreślając ich podpisy fałszywie wskazujące na odbiór gotówki przez pokrzywdzonych i użyła tych dokumentów jako autentycznych, tj. o czyn z art. 287 § 1 k.k. i art. 270 § 1 k.k. w zw. z art. 11 § 2 k.k.[371]

Charakter przestępstwa dokonanego w 2019 r. jednoznacznie wskazuje, że sprawca był winny popełnienia czynu z art. 278 § 1 k.k., a nie art. 287 § 1 k.k. Chodziło bowiem o kradzież środków pieniężnych zgromadzonych na rachunku, a nie manipulację danymi informatycznymi. Owszem, sprawca musiał wprowadzić określone dyspozycje w systemie informatycznym banku, ale dotyczyły one tylko użycia mechanizmu przelewu bez dalszej, szczególnej ingerencji w elektroniczne repetytorium. Doszło więc do zbiegu pomijalnego i art. 287 § 1 k.k. nie powinien pozostać w subsumpcji stanu faktycznego sprawy. Sytuację tę można porównać do naruszenia nietykalności cielesnej w przypadku rozboju. Zabór cudzej rzeczy ruchomej, poprzez np. wyrwanie torebki z ręki i lekkie odepchnięcie pokrzywdzonego, połączony jest niekiedy z naruszeniem

[371] Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 289/19/P.

jego nietykalności cielesnej i najczęściej takie naruszenie, jeśli nie przekroczyło minimalnego stopnia dolegliwości, jest traktowane jako czyn pomijalny, a zarzut ogłoszony sprawcy dotyczy art. 280 § 1 k.k. Natomiast przełamanie zabezpieczenia rzeczy poprzez zniszczenie ochraniającej rzecz przeszkody kwalifikuje się jako realny zbieg przepisu art. 279 § 1 k.k. i art. 288 § 1 k.k. tylko wówczas, gdy zniszczone zabezpieczenie posiadało dużą wartość. Podobnie jest w przypadku kradzieży środków pieniężnych zgromadzonych na rachunku, która siłą rzeczy prowadzi do wywołania, bez upoważnienia, procesu przetwarzania danych informatycznych w elektronicznym systemie płatniczym. Jeżeli jednak sprawca ogranicza swoje działanie wyłącznie do skorzystania z funkcji zapłaty lub przelewu, bez instalowania złośliwego oprogramowania czy zmieniania w aplikacji danych osobowych posiadacza rachunku, to zakwalifikowanie jego zachowania tylko z art. 278 § 1 k.k. lub art. 279 § 1 k.k. oddaje całe kryminalne bezprawie czynu. Dlatego zbędne było przywoływanie znamion z art. 287 § 1 k.k. w treści wyroku wydanego przez Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie, uznającego podsądnego za winnego tego, że:

> w dniu 10 września 2014 roku w Krakowie, działając w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru oraz w celu osiągnięcia korzyści majątkowej, wykonując bez upoważnienia pięć autoryzowanych przelewów środków pieniężnych na swoje konto bankowe, wykorzystując komputer J. B. i zapisane w przeglądarce dane do jego konta wprowadził nowy zapis danych informatycznych na koncie bankowym o numerze /…/, prowadzonym przez PKO BP SA, skąd następnie zabrał w celu przywłaszczenia pieniądze w łącznej kwocie 101.635 złotych na szkodę J. B. tj. o przestępstwo z art. 287 § 1 k.k., art. 278 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k."[372]

W sprawie ustalono, że przestępstwa dokonała osoba, której przekazano komputer w celu zainstalowania oprogramowania antywirusowego. Oskarżony, przebywając w biurze pokrzywdzonego, zabrał z szuflady kody („karty-zdrapki") do autoryzacji transakcji bankowych, a w przeglądarce serwisowanego komputera odnalazł pozostałe dane weryfikacyjne, tj. login i hasło do aplikacji bankowej. W tym samym dniu wykonał pięć przelewów w kwotach: 22 140 zł, 21 525 zł, 23 370 zł, 10 000 zł i 24 600 zł o łącznej wartości 101 635 zł z rachunku J. B. na trzy inne, administrowane przez siebie konta. Jak już wspomniano, sąd popełnił błąd, przyjmując realny zbieg art. 287 § 1 k.k. i art. 278 § 1 k.k., gdyż całość zachowania sprawcy zawierała się w znamionach kradzieży z włamaniem w ujęciu czynu ciągłego. Gdyby organ orzekający był konsekwentny w mnożeniu, de facto prawnie ambiwalentnych, zachowań oskarżonego, to powinien także wskazać na wypełnienie przez niego znamion art. 267 § 1 k.k., bowiem mężczyzna

[372] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 45/15/N.

uzyskał dostęp do informacji dla niego nieprzeznaczonych, tj. zapisów w aplikacji bankowej, poprzez ominięcie ich informatycznych zabezpieczeń – wpisanie odzyskanego z przeglądarki hasła.

W przypadku nieuprawnionych transakcji kartowych pojawił się problem, jak kwalifikować zabór karty, co poprzedza zazwyczaj takie transakcje, a ponadto z jakim rodzajem karty ma się do czynienia. W wyroku z dnia 17 listopada 2016 r. Sąd Rejonowy w Radomsku uznał oskarżonego za winnego tego, że:

> w okresie czasu od dnia 31 sierpnia 2009 r. do dnia 4 grudnia 2009 r. w R., działając w wykonaniu z góry powziętego zamiaru dokonania włamania do konta bankowego pokrzywdzonego E. M. i kradzieży z niego pieniędzy, w krótkich odstępach czasu, a więc w warunkach przestępstwa ciągłego wykorzystując posiadaną kartę płatniczą Maestro należącą do E. M., do której /…/ uzyskała po wcześniejszym sporządzeniu wniosku o jego przesłanie do Banku /…/ S.A. w R., bez zgody i wiedzy właściciela karty, po uprzednim złamaniu zabezpieczenia kodem /…/ tej karty wypłaciła przy jej użyciu z bankomatów na terenie R. pieniądze w łącznej kwocie 23.500 zł na szkodę E. M.; tj. o przestępstwo z art. 278 § 1 k.k. i art. 278 § 5 k.k. w zw. z art. 279 § 1 k.k. w zw. z art. 12 k.k.[373]

Obecnie, zgodnie z art. 278 § 5 k.k., przepisy dotyczące kradzieży rzeczy stosuje się odpowiednio do kradzieży karty uprawniającej do podjęcia pieniędzy z automatu bankowego, ale od 1 października 2023 r. ma zacząć obowiązywać art. 278 § 1a k.k. stanowiący, że „Tej samej karze podlega [jak za kradzież – przypis autora], kto zabiera w celu przywłaszczenia cudzą kartę uprawniająca do podjęcia pieniędzy z automatu bankowego". W treści zacytowanego wyroku Sąd Rejonowy w Radomsku uznał, że „karta płatnicza Maestro" stanowi przedmiot czynności wykonawczej, o którym mowa w art. 278 § 5 k.k.[374] Jednak w prawie karnym należy precyzyjnie posługiwać się pojęciem „karta płatnicza" i „karta bankomatowa", uwzględniając, że legalna definicja pierwszej z nich znajduje się w ustawie o usługach płatniczych.

Zgodnie z art. 2 pkt 15a u.u.p.: kartę płatniczą definiuje się jako „kartę uprawniającą do wypłaty gotówki lub umożliwiającą złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, akceptowaną przez akceptanta w celu otrzymania przez niego należnych mu środków, w tym kartę płatniczą w rozumieniu art. 2 pkt 15 rozporządzenia (UE) 2015/751". Decydujące znaczenie ma zastosowanie przez

[373] Wyrok Sądu Rejonowego w Radomsku z dnia 17 listopada 2016 r., VI K 288/16, LEX nr 2342576.

[374] W artykule pt. *Odpowiedzialność karna za kradzież karty płatniczej* z 2017 r. autor dokonał szczegółowej analizy przepisów i wyraził pogląd, że kradzież karty bankomatowej *sensu stricto*, a więc pozwalającej tylko i wyłącznie podejmować pieniądze z maszyny, należy kwalifikować z art. 278 § 5 k.k., a karty bankomatowo-płatniczej lub tylko z funkcją płatniczą z art. 278 § 1 k.k. lub z art. 119 § 1 k.w. Zob. P. Opitek, *Odpowiedzialność karna za kradzież karty płatniczej*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2017, nr 4, s. 55 i nast.

ustawodawcę przyimka „lub" pomiędzy podaniem dwóch kategorii kart, którym można przypisać przymiotnik „płatnicze". W konsekwencji, na gruncie ustawy o usługach płatniczych, funkcjonują trzy grupy kart płatniczych:

1. karty uprawniające tylko do wypłaty gotówki (karta bankomatowa *sensu stricto*);
2. karty umożliwiające złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, zatwierdzanego przez akceptanta w celu otrzymania przez niego należnych mu środków, np. karta kredytowa i debetowa (karta płatnicza *sensu largo*);

— kartami płatniczymi będą ponadto karty uprawniające do wypłaty gotówki i umożliwiające złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, zatwierdzanego przez akceptanta w celu otrzymania przez niego należnych mu środków (karta bankomatowo-płatnicza).

Artykuł 2 pkt 15a u.u.p. wskazuje na funkcję karty płatniczej, która pozwala podejmować pieniądze w bankomatach, składać zlecenia płatnicze za pośrednictwem ustalonych w ustawie podmiotów oraz dokonywać płatności w punktach usługowo-handlowych, które akceptują taką formę umarzania zobowiązań. Zwrot „zlecenie płatnicze" doprecyzowuje art. 2 pkt 36 u.u.p.; chodzi o „oświadczenie płatnika lub odbiorcy skierowane do jego dostawcy zawierające polecenie wykonania transakcji płatniczej". Zgodnie natomiast z pkt 29 omawianego artykułu, przez transakcję płatniczą należy rozumieć zainicjowaną przez płatnika lub odbiorcę wpłatę, transfer lub wypłatę środków pieniężnych. Z przywołanych regulacji wynika, że ustawodawca do „transakcji płatniczych" zalicza m.in. podejmowanie gotówki z ATM-u.

Definicja zawarta w art. 2 pkt 15a u.u.p. ma charakter uniwersalny w tym sensie, że zawiera w sobie wszystkie karty płatnicze dostępne na rynku (nie ma innego rodzaju kart pozostających poza jej zakresem). Potwierdza to art. 4 pkt 4 Prawa bankowego, który w zakresie definicji karty płatniczej odsyła do wspomnianego artykułu. Wynika z tego, że chociaż przymiotnik „płatnicza" kojarzy się z funkcją płacenia kartą za zobowiązania wyrażone w pieniądzu polskim, to na gruncie ustawy o usługach płatniczych, w obrębie art. 2 pkt 15a, mieszczą się także typowe karty bankomatowe. Dlatego nie pokrywa się idealnie zakres znaczeniowy terminu „karta płatnicza" (15a u.u.p.) i „środek płatniczy" (art. 115 § 9 k.k., art. 310 k.k.) w tym sensie, że „karty płatnicze" to zarówno „inne środki płatnicze", a ponadto „karty uprawniające do podjęcia pieniędzy z automatu bankowego". Wnioski takie opierają się na założeniu spójności systemu prawa, z którego wynika, że używając pomocniczo – do interpretacji przedmiotu przestępstwa – terminu „karta płatnicza" na gruncie prawa karnego, należy przypisywać mu znaczenie z ustawy o usługach płatniczych. Doniosła rola definicji legalnej przejawia się bowiem w tym, że jest ona niezwykle silną dyrektywą wykładni narzuconą przez ustawodawcę i sformułowane przez nią znaczenie nie niweluje się nawet w sytuacji, gdyby treść językowa tej definicji podważała inne założenia o racjonalnym prawodawcy[375].

[375] M. Zieliński, *Wykładnia prawa...*, s. 190–191.

Mając powyższe na uwadze, żadnego logicznego uzasadnienia nie znajduje wyodrębnienie przez ustawodawcę specjalnej jednostki redakcyjnej Kodeksu karnego poświęconej kradzieży „karty uprawniającej do podjęcia pieniędzy z automatu bankowego" (art. 278 § 1a k.k.). Autor postulował o zamianę przepisów Kodeksu karnego w zakresie penalizacji kradzieży kart płatniczych, bowiem regulacja z art. 278 § 1a k.k. jest rozwiązaniem archaicznym. Odrębnemu wyszczególnieniu karty bankomatowej *sensu stricto* jako przedmiotu przestępstwa, przyświecał zamiar specjalnego zabezpieczenia przed kradzieżą wszystkich kart przeznaczonych do obrotu bezgotówkowego, a w pierwszej fazie kształtowania się rynku transakcji elektronicznych w Polsce podstawowymi operacjami pieniądzem bezgotówkowym były wypłaty bankomatowe. Dlatego w momencie wejścia w życie Kodeksu karnego, „kartę uprawniającą do podjęcia pieniędzy z automatu bankowego" utożsamiano z jednozadaniową kartą do wypłat. Od tego czasu wiele się jednak zmieniło i obecnie prawie wszystkie karty posiadają funkcję płatniczą, a typowe karty bankomatowe praktycznie przestały funkcjonować. W tym stanie rzeczy szczególna ochrona przyznana im w art. 278 § 1a k.k. stała się zbędna i nieadekwatna do realiów współczesnego rynku. Co gorsze jednak, obowiązujące regulacje powodują niepotrzebny zamęt w penalizacji kradzieży kart płatniczych i brak spójności w ich ochronie. *De lege ferenda* konieczna jest zmiana uregulowań Kodeksu karnego w omawianym zakresie, a jedno z rozwiązań polega na rezygnacji z indywidualnej penalizacji kradzieży karty bankomatowej i podjęciu przez ustawodawcę decyzji, czy zamierza traktować kradzież karty płatniczej w sposób szczególny, czy też na takich samych zasadach, jak kradzież rzeczy ruchomej. W tym pierwszym przypadku art. 278 § 1a k.k. należałoby nadać brzmienie: „Tej samej karze podlega, kto zabiera w celu przywłaszczenia cudzą kartę płatniczą". Rozwiązanie takie byłoby słuszne, gdyż kradzież karty płatniczej jest dużym obciążeniem dla jej prawowitego posiadacza, a karanie za to na podstawie art. 119 § 1–3 k.w., to stanowczo zbyt mało.

Przechodząc do kwestii oceny dwóch czynów, tj. kradzieży karty, a następnie wykorzystania jej do transakcji płatniczej, to zasadniczo dochodzi do popełnienia dwóch odrębnych przestępstw z art. 278 § 1a k.k. oraz art. 279 § 1 k.k. Inaczej orzekł Sąd Apelacyjny we Wrocławiu, stwierdzając, że „usiłowanie wypłaty pieniędzy na podstawie karty bankomatowej skradzionej podczas napadu rabunkowego, a także przy wykorzystaniu kodu, którego ujawnienia domagał się sprawca w trakcie rozboju, stanowi czyn współukarany następczy przestępstwa z art. 280 § 2 k.k., a nie odrębne przestępstwo z art. 13 § 1 k.k. w zw. z art. 279 § 1 k.k."[376]. Jednak Sąd Rejonowy w Kielcach, skazał sprawcę za to, że:

[376] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 9 lipca 2014 r., II AKa 180/14, LEX nr 1506771.

1. w dniu 16 sierpnia 2018 r. w miejscowości O. gmina C. dokonał zaboru w celu przywłaszczenia karty kredytowej /…/ Bank SA na szkodę J. S., tj. o przestępstwo z art. 278 § 5 k.k.
2. w dniu 16 sierpnia 2018 r. w miejscowości B. gmina M. dokonał wypłaty z bankomatu poprzez przełamanie zabezpieczenia w postaci kodu /…/ pieniędzy w kwocie 290 złotych na szkodę J. S., tj. o przestępstwo z art. 279 § 1 k.k.[377]

Oskarżony dokonał kradzieży karty bankomatowej swojego ojca, znajdującej się w kieszeni marynarki. Znał do niej kod PIN, bo pokrzywdzony zapisał go na kartce schowanej w kurtce wiszącej w tej samej szafie co marynarka z kartą. W uzasadnieniu wyroku sąd stwierdził, że pokrzywdzony nie wyrażał nigdy zgody na to, aby syn dysponował jego kodem do karty i nie udostępniał mu PIN-u. Możliwości przypisania sprawcy przestępstwa kradzieży z włamaniem nie wyklucza fakt, że oskarżony w uzyskaniu dostępu do karty bankomatowej i kodu nie musiał pokonywać jakiś specjalistycznych zabezpieczeń. Innymi słowy, nie ma żadnych podstaw do tego, aby wymagać od pokrzywdzonego stosowania jakiś szczególnych zabezpieczeń w dostępie do rzeczy, która zostaje skradziona. Istotne jest to, żeby pokrzywdzony w sposób oczywisty zamanifestował swoją wolę braku dostępu do jego rzeczy osobom nieuprawnionym i taka sytuacja miała miejsce w niniejszej sprawie: nigdy nie udostępniał on karty swojemu synowi i nie wyrażał zgody na korzystanie przez syna z tej karty. J. S. kartę i PIN przechowywał w takim miejscu, które w sposób wyraźny stanowiło dla otoczenia informację o braku woli dostępu do tych rzeczy przez inne osoby.

4.6. Oszustwa w cyberprzestrzeni (art. 286 § 1 k.k.)

Pisząc o przestępstwach teleinformatycznych, nie sposób pominąć czynów mających znamiona oszustwa, gdyż kwalifikacja prawna z art. 286 § 1 k.k. stale jest obecna w ściganiu takich przestępstw. Autor już kilka lat temu wskazywał, że chociaż cyberprzestępczość kojarzy się z nowoczesnymi, wyrafinowanymi narzędziami teleinformatycznymi, przy użyciu których sprawcy włamują się do baz danych, kradną środki pieniężne lub przejmują konta internetowe, to w praktyce do nielegalnych działań w wirtualnym świecie nadają się także najprostsze, ale bardzo skuteczne, metody socjotechniki i manipulowania wolą człowieka. W książce z 2002 r. pt. *Sztuka podstępu* Kevin Mitnick, najsłynniejszy haker świata, użył określenia: „Łamałem ludzi, nie hasła", chcąc przez to powiedzieć, że najsłabszym ogniwem każdego systemu jest człowiek, a przestępcy wyznają zasadę: „Im prościej, tym lepiej" nielegalnie się wzbogacić. Jeśli firma prywatna lub instytucja publiczna zainwestuje w swoje cyberbezpieczeństwo duże środki, zakupi najnowocześniejsze urządzenia i oprogramowanie, wdroży prawidłowe procedury, ale

[377] Wyrok Sądu Rejonowego w Kielcach z dnia 27 maja 2019 r., IX K 1680/18, LEX nr 2764110.

nie przeszkoli odpowiednio wszystkich pracowników, to dalej będzie podatna na cyberataki. Wszystko może zawieść z powodu, wydawałoby się, mało znaczącego błędu ludzkiego[378]. Po pięciu latach od napisania tych słów wciąż pozostają one aktualne.

Jednym ze sposobów nielegalnego działania sprawców jest tzw. marketing sprzedażowy, którego pewien etap realizacji opiera się na środkach łączności elektronicznej, zazwyczaj telefonach. Znajomość między przestępcą i pokrzywdzonym zawiązuje się w trakcie rozmowy telefonicznej, gdy potencjalna „ofiara" zostaje zaproszona na spotkanie lub prezentuje się jej ofertę nabycia atrakcyjnego towaru. Oszuści dzwonią przede wszystkim do ludzi, którzy z powodu podeszłego wieku lub braku rozeznania w przepisach prawa nie są w stanie samodzielnie ocenić charakteru sytuacji. Pokrzywdzeni są często „stymulowani" do podjęcia niekorzystnych decyzji finansowych wywołaną przez przestępców atmosferą znacznych korzyści płynących z oferowanych zakupów, zwłaszcza jeśli są one powiązane z rzekomo wylosowanymi nagrodami lub wyjątkowymi upustami cenowymi. Decyzje pokrzywdzonych o nabyciu towaru lub usługi zapadają pod presją czasu i różnego rodzaju technik marketingowych bez możliwości zapoznania się z rzeczywistą treścią umowy i wynikającymi z niej zobowiązaniami. Niekiedy zamiast marketingu telefonicznego osoby zapraszane są na prezentację produktów bez świadomości, że łączy się ona ze sprzedażą towarów i podejmują „na gorąco" nieprzemyślane decyzje. Dopiero po jakimś czasie orientują się, jakie są właściwości nabytej rzeczy i warunki uiszczenia opłaty, a przede wszystkim, jakie poniosą rzeczywiste, z reguły bardzo wysokie i rozciągnięte w czasie, koszty „inwestycji". *Modus operandi* sprawców omawianych przestępstw charakteryzuje się zatem stosowaniem schematów psychologicznego oddziaływania na potencjalne ofiary, wyrafinowaną socjotechniką i agresywnym marketingiem, co powoduje, że wielokrotnie uzyskują oni wysokie korzyści kosztem ludzi pokrzywdzonych przestępstwem[379].

Prowadzenie postępowań karnych dotyczących ww. praktyk jest trudne z uwagi na skomplikowany charakter spraw, w tym konieczność udowodnienia sprawcy przestępstwa zamiaru kierunkowego bezpośredniego, wykazania znamienia wprowadzenia w błąd pokrzywdzonych, wyzyskania błędu lub niezdolności do należytego pojmowania przez nich przedsiębranego działania (art. 286 § 1 k.k.). Pokrzywdzonego przesłuchuje się z zachowaniem szczególnej staranności i dokładności na okoliczności zdarzenia, m.in. kiedy i w jaki sposób otrzymał zaproszenie na prezentację, co miało być jej przedmiotem, czy na spotkaniu sprzedawano towary oraz w jakich okolicznościach doszło do zawarcia umowy sprzedaży, jakie cechy miała posiadać zakupiona rzecz i czy różniła się od faktycznie otrzymanego produktu, czy zakup towaru lub usługi był związany z zaciągnięciem kredytu lub pożyczki i na jakich warunkach,

[378] P. Opitek, *Cyberprzestępczość w pracy prokuratora*…, s. 49.

[379] Zalecenia Prokuratora Krajowego z dnia 15 września 2022 r. w sprawie zasad prowadzenia postępowań przygotowawczych o przestępstwa prowadzone w drodze oszukańczych sprzedaży przedmiotów i usług, w szczególności w drodze sprzedaży bezpośredniej połączonej z ich prezentacją, sygn. 1001 – 1.024.18.2022 (zbiory własne autora), dalej jako: Zalecenia z 15 września 2022 r.

czy tytułem zawarcia umowy sprzedaży pokrzywdzony otrzymał prezenty lub nagrody. W trakcie przesłuchania należy ustalić także, jaki był stan zdrowia pokrzywdzonego w momencie zaciągania zobowiązania, gdyż okoliczności z tym związane decydują m.in. o możliwości wprowadzenia w błąd kupującego przez sprzedawcę. W śledztwie należy ponadto zabezpieczyć kryminalistycznie i procesowo całość dokumentacji związanej ze zdarzeniem oraz otrzymany przez pokrzywdzonego towar, a następnie zweryfikować, czy jest on zgodny z zapisami umowy. Ważne jest ustalenie, jak podmiot organizujący marketing sprzedażowy wszedł w posiadanie danych osobowych ludzi, z którymi się skontaktował, pod kątem wypełnienia znamion art. 107 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[380]. W przypadku stwierdzenia, że zakupu przedmiotów dokonano na podstawie udzielonego pokrzywdzonemu instrumentu finansowego, to należy zweryfikować, czy podmiot oferujący kredyt lub pożyczkę nie naruszył art. 59a ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim[381]. W wytycznych skierowanych do prokuratorów podkreślono także, iż warunkiem skutecznego ścigania sprawców opisanych przestępstw jest pociągnięcie do odpowiedzialności karnej osób odgrywających wiodącą rolę w organizowaniu sprzedaży marketingowej, a nie jedynie tych, które wykonują czynności na podstawie umów agencyjnych lub zlecenia. Dlatego śledztwo powinno zmierzać do ustalenia struktury grupy przestępczej, zasad jej funkcjonowania, nazwisk osób decyzyjnych w grupie oraz ich wzajemnych powiązań osobowo-kapitałowych. W takich sprawach przydatna okazuje się współpraca prokuratora z Urzędem Ochrony Konkurencji i Konsumentów (pod kątem naruszenia zbiorowych interesów konsumentów), Krajową Administracją Skarbową (sprawdzenie realizacji przez podmiot obowiązków podatkowych i składania deklaracji w tym zakresie, a ostatecznie zainicjowanie kontroli karno-skarbowej) i Generalnym Inspektorem Informacji Finansowej (analiza danych objętych tajemnicą bankową). Dalsze wytyczne dotyczą konieczności zabezpieczenia w śledztwie różnego rodzaju dowodów, które pozwolą na ustalenie istotnych okoliczności faktycznych sprawy, m.in. dokumentacji fiskalno-księgowej znajdującej się w posiadaniu „podejrzanej" firmy, sprzętu elektronicznego ze śladami cyfrowymi (szczególnie, jeśli kontakt między klientem i przedsiębiorcą odbywał się „na odległość"). W przypadkach, gdy zakup rzeczy przez pokrzywdzonego podyktowany był jego przeświadczeniem o szczególnych cechach nabywanego przedmiotu, podawanych w jego reklamie, a ich istnienie budzi wątpliwości, zasięgnąć należy opinii biegłego rzeczoznawcy w celu stwierdzenia, czy towar rzeczywiście takie cechy posiada[382].

Wytyczne zawierają ponadto informacje co do oceny prawno-karnej zachowania sprawców prowadzących marketing sprzedażowy. W tym zakresie, oprócz przepisów Kodeksu karnego (art. 286 § 1 k.k., art. 258 k.k. i art. 65 § 1 k.k.), należy wziąć pod

[380] T.j. Dz. U. z 2019 r. poz. 1781.
[381] T.j. Dz. U. z 2023 r. poz. 1028.
[382] Zalecenia z 15 września 2022 r.

uwagę art. 24a ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[383], art. 15 ust. 1 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym[384] oraz zastosowanie środków określonych ustawą z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary[385]. Niezależnie od czynności podejmowanych w postępowaniu karnym, rozważyć należy także inicjowanie działań na gruncie prawa cywilnego zmierzających do ochrony interesów osób pokrzywdzonych przestępstwem[386].

Jeśli mowa o oszustwach, to największa liczba przestępstw teleinformatycznych, kwalifikowanych z art. 286 § 1 k.k., dotyczy bankowości internetowej. W jednej ze spraw M. B. posiadała trzy rachunki w różnych instytucjach finansowych. W połowie kwietnia 2013 r. oskarżona poprosiła ją o możliwość skorzystania z jednego rachunku bankowego, tłumacząc, że będą wpływały na niego środki pieniężne od jej brata. Pokrzywdzona zgodziła się i udostępniła kartę płatniczą, kod PIN oraz swoją aplikację bankowości elektronicznej. W okresie od 11 do 30 kwietnia 2013 r. oskarżona bez wiedzy i zgody M. B., korzystając z ww. aplikacji i podszywając się pod pokrzywdzoną, zawarła szereg umów pożyczkowych tzw. chwilówek, których nie spłaciła. Sformułowany wobec kobiety zarzut brzmiał:

> w dniu 11 kwietnia 2013 r. w Krakowie, w celu osiągnięcia korzyści majątkowej, bez upoważnienia wprowadziła nowy zapis danych informatycznych poprzez wykonanie za pośrednictwem systemu informatycznego bankowości internetowej /…/ Bank z konta o nr /…/ należącym do M. B. operacji przelewu w celu weryfikacji danych pożyczkobiorcy, a następnie doprowadziła /…/ Sp. z o.o. z siedzibą w Warszawie do niekorzystnego rozporządzania mieniem w postaci pieniędzy w kwocie 1.200 zł, poprzez wprowadzenie w błąd przedstawiciela pokrzywdzonej spółki co do tożsamości osoby zawierającej umowę pożyczki o nr /… oraz zamiaru jej spłaty, tj. o przest. z art. 286 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[387]

Sąd Okręgowy w Krakowie, orzekając w zakresie jedenastu czynów dotyczących wyłudzenia pożyczek „chwilówek", uznał oskarżoną za winną tego, że:

> w dniach od 11 kwietnia 2013 r. do 30 kwietnia 2013 r. w Krakowie działając w krótkich odstępach czasu, z wykorzystaniem tej samej sposobności, podszywając się pod M. B. w celu wyrządzenia jej szkody majątkowej i jednoczesnego osiągnięcia korzyści

[383] T.j. Dz. U. z 2022 r. poz. 1233.
[384] T.j. Dz. U. z 2023 r. poz. 845.
[385] T.j. Dz. U. z 2023 r. poz. 659.
[386] Zalecenia z 15 września 2022 r.
[387] Akta Sądu Okręgowego w Krakowie o sygn. III K 106/17.

majątkowej, wykorzystała jej dane osobowe w ten sposób, że za pośrednictwem systemu informatycznego bankowości internetowej /…/ Banku z rachunku o nr /…/ należącego do M. B. dokonywała operacji przelewu w celu weryfikacji danych pożyczkobiorcy, przez co wprowadzając w błąd przedstawicieli rozmaitych spółek co do tożsamości pożyczkobiorcy oraz zamiaru spłaty doprowadziła bądź usiłowała doprowadzić różne spółki pożyczkowe do niekorzystnego rozporządzenia mieniem w postaci pieniędzy przelanych na podstawie umów pożyczek, a w szczególności /…/ co stanowiło występek z art. 13 § 1 k.k. w zw. z art. 286 § 1 k.k. i art. 190a § 2 k.k. w zw. z art. 11 § 2 k.k.[388]

Oskarżona postanowiła ponadto uzyskać dostęp do środków pieniężnych zgromadzonych na drugim rachunku M. B. i poprosiła ją o możliwość skorzystania z konta w celu załatwiania spraw finansowych związanych ze spadkobraniem po zmarłym członku rodziny. M. B. przekazała oszustce dane do rachunku i w okresie od 8 września 2013 r. do 11 października 2013 r. oskarżona, korzystając z bankowości elektronicznej, wykonała siedem przelewów z konta M. B. na własny rachunek bankowy o łącznej wartości środków 3938 zł; na podstawie tak ustalonych okoliczności faktycznych prokurator oskarżył sprawcę o to, że:

w dniu 8 września 2013 r. w Krakowie, w celu osiągnięcia korzyści majątkowej, bez upoważnienia wprowadziła nowy zapis danych informatycznych poprzez wykonanie za pośrednictwem systemu informatycznego bankowości internetowej /…/ Banku z konta o nr /…/ należącym do M. B. siedem operacji przelewu środków finansowych, a następnie przywłaszczyła pieniądze w kwocie 385 zł na szkodę M. B., tj. o przest. z art. 287 § 1 k.k. w zw. z art. 284 § 1 k.k. w zw. z art. 11 § 2 k.k.[389]

Rozpoznający sprawę, Sąd Okręgowy w Krakowie zakwalifikował każdy z czynów przy zastosowaniu art. 91 § 1 k.k. jako występek z art. 278 § 1 k.k. i art. 190a § 2 k.k. w zw. z art. 11 § 2 k.k.[390] W uzasadnieniu wyroku napisano: „Zachowanie oskarżonej polegające na posługiwaniu się imieniem, nazwiskiem oraz numerem rachunku pokrzywdzonych /…/ właśnie po to, by wytworzyć u adresata mylne przekonanie, że koresponduje z inna osobą, w pełni wyczerpało wszelkie znamiona tzw. kradzieży tożsamości". Sąd wskazał ponadto, że podając dane osobowe pokrzywdzonych, oskarżona niewątpliwie działała w celu wyrządzenia określonym osobom szkody majątkowej. „Sąd nie podzielił jednak propozycji prokuratora sprowadzającej się do kwalifikacji jej czynów z art. 287

[388] Tamże.
[389] Tamże.
[390] Tamże.

§ 1 k.k.", gdyż działanie oskarżonej nie wpłynęło na automatyczne przetwarzanie danych informatycznych, ale wykorzystała Internet do wprowadzenia w błąd firm pożyczkowych tak samo, jakby osobiście stawiła się w oddziale i posłużyła cudzym dokumentem tożsamości albo ubiegała się o pożyczkę pocztą lub telefonicznie. „Nie ma podstaw by surowiej kwalifikować czyn oskarżonej tylko z tego powodu, że do jego popełnienia wykorzystała elektroniczny system przesyłania informacji" – napisał sąd. W innej sprawie, ale dotyczącej podobnego stanu faktycznego, Sąd Okręgowy w Krakowie zakwalifikował czyn jako przestępstwo z art. 278 § 1 k.k. i art. 287 § 1 k.k. i art. 270 § 1 k.k. i art. 270 § 2 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 294 § 1 k.k. w zw. z art. 12 k.k.[391] Ustalono bowiem, że oskarżona podrabiała podpisy innych osób na umowach kredytowych oraz dyspozycjach przelewów bankowych i w ten sposób „zabrała w celu przywłaszczenia z rachunków bankowych" prowadzonych dla ustalonych w sprawie klientów pieniądze w łącznej kwocie 754 530,31 zł".

W pierwszej kolejności odnieść się należy do przypisania przez sąd oskarżonej sprawstwa przestępstwa z art. 190a § 2 k.k. w zbiegu z art. art. 286 § 1 k.k., a następnie z art. 278 § 1 k.k. Przepis art. 190a § 2 k.k. stanowi, że odpowiedzialności karnej podlega ten, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana w celu wyrządzenia jej szkody majątkowej lub osobistej. Przestępstwo to może być popełnione wyłącznie w zamiarze bezpośrednim, tak więc dla realizacji znamion art. 190a § 2 k.k. nie jest wystarczające, aby sprawca jedynie godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa, wykorzystując jej wizerunek lub dane osobowe[392]. Przyrównując ustawowe znamiona przestępstwa „kradzieży tożsamości" do okoliczności faktycznych analizowanej sprawy, to z rozstrzygnięciem sądu nie sposób się zgodzić, gdyż oskarżona nie działała ze szczególnym zamiarem kierunkowym wyrządzenia M. B., pod którą się podszywała, szkody majątkowej lub osobistej, ale cel sprawcy stanowiła chęć wzbogacenia się kosztem M. B. Przestępstwo określone w art. 190a § 2 k.k. może być popełnione wyłącznie w zamiarze bezpośrednim, tak więc dla realizacji jego znamion nie jest wystarczające, aby sprawca tylko godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa, wykorzystując jej wizerunek lub dane osobowe. W jednej z rozpoznawanych spraw Sąd Najwyższy podkreślił, że:

> K. P. dopuściła się zarzucanych jej przestępstw wyłącznie dla własnej korzyści (dzięki przestępczemu procederowi uzyskiwała pożyczki, karty kredytowe, aparaty telefoniczne, umowę abonencką z telewizją cyfrową) jednak nie znała osobiście osoby, której zaszkodzi. Podczas przesłuchania, w którym A. P. finalnie poddała się karze stwierdziła, że od początku zdawała sobie sprawę z negatywnych konsekwencji, jakie przyniesie pokrzywdzonej jej działanie, ale głębsza refleksja przyszła później[393].

[391] Akta Sądu Okręgowego w Krakowie o sygn. III K 193/17.
[392] Wyrok Sądu Najwyższego z dnia 27 stycznia 2017 r., V KK 347/16, LEX nr 2269116.
[393] Tamże.

Takie ustalenia uniemożliwiły, zdaniem Sądu Najwyższego, przypisania skazanej wypełnienia znamion przestępstwa z art. 190a § 2 k.k.

Poza tym czynność sprawcza opisana w art. 190a § 2 k.k. musi być w jakiś sposób zademonstrowana wobec innej osoby lub grupy osób; jak słusznie pisze A. Lach: „Ważne jest aby dla odbiorcy powstało wrażenie, że ma do czynienia z inną osobą, niż nią jest rzeczywiście sprawca”[394]. Tymczasem w sprawie rozpoznawanej przez Sąd Okręgowy w Krakowie oskarżona „podszyła się” pod inną osobę wobec, mówiąc obrazowo, programu komputerowego, gdyż wprowadzane przez nią nowe zapisy w aplikacji bankowości elektronicznej nie były następnie weryfikowane przez pracownika banku, ale automatycznie przetwarzane w informatycznym systemie bankowym. Prawdą jest, jak pisze A. Zoll, że możliwy jest zbieg kumulatywny pomiędzy art. 190a § 2 k.k. i art. 286 § 1 k.k.[395], ale nie w opisanej sytuacji. Doszłoby do niego, gdyby np. sprawca, posługując się danymi osobowymi pokrzywdzonego, zawarł umowę pożyczki przy „okienku bankowym”, wprowadzając w błąd pracownika instytucji finansowej co do zamiaru spłaty świadczenia (art. 286 § 1 k.k.), a nadto, działając w celu wyrządzenia szkody osobie, pod którą się podszywa, złośliwie wypowiedział zawartą z bankiem przez pokrzywdzonego umowę kredytu hipotecznego i naraził go w ten sposób na brak płynności w regulowaniu zobowiązań za roboty budowlane świadczone na jego rzecz w związku z prowadzoną inwestycją (art. 190a § 2 k.k.)[396].

Powracając do zbiegu realnego art. 287 § 1 k.k. i art. 286 § 1 k.k., warto przytoczyć kolejną decyzję procesową, która dotyczyła oszustwa bankowego. Prokuratura Rejonowa Olsztyn-Południe w Olsztynie wszczęła śledztwo w sprawie:

> doprowadzenia w okresie od 17.02.2015 r. do 25.02.2015 r. w Zielone Górze, Katowicach, Wrocławiu, Iławie i innych miejscowościach na terenie Polski, M. C., / wskazano pozostałych pokrzywdzonych – przypis autora/, w celu osiągnięcia korzyści majątkowej, w krótkich odstępach czasu i w wykonaniu z góry powziętego zamiaru, po uprzednim zainstalowaniu przez sprawcę złośliwego oprogramowania na komputerach pokrzywdzonych, służącego do zmiany rachunków bankowych, do niekorzystnego rozporządzenia mieniem w łącznej kwocie 172.623,23 PLN za

[394] A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo” 2012, nr 3, s. 34.

[395] A. Zoll, *Art. 190a k.k.*, *teza 28*, [w:] *Kodeks karny. Część szczególna*, t. 2, cz. 1, *Komentarz do art. 117–211a*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2017, LEX.

[396] Przeciwne stanowisko zajął Sąd Apelacyjny w Krakowie; zdaniem sądu, skorzystanie z automatycznych procesów realizacji przelewu płatności i posłużenie się danymi osobowymi kogoś innego może wypełniać znamiona art. 190a § 2 k.k.; sąd zawyrokował, że „Przepis art. 190a § 2 k.k. nie warunkuje odpowiedzialności karnej sprawcy od jednoczesnego wykorzystania wizerunku innej osoby i jej danych osobowych. Przepis posługuje się alternatywą rozłączną tych zachowań, zatem wystarczające jest tylko wykorzystanie danych osobowych innej osoby, jak to stwierdzono w realiach sprawy. Logując się do bankowości internetowej i konta pokrzywdzonej, oskarżona wykorzystała jej dane osobowe, podszywając się pod nią i dokonując następnie przypisanych jej wyłudzeń”; zob. wyrok Sądu Apelacyjnego w Krakowie z dnia 8 stycznia 2019 r., II AKa 194/17.

pomocą wprowadzenia pokrzywdzonych w błąd, iż przelewy na wskazane wyżej kwoty nastąpiły na wybrane przez nich rachunki bankowe, podczas gdy w rzeczywistości beneficjentem uzyskanych za pośrednictwem tych przelewów środków pieniężnych była osoba, która posiadała dostęp do rachunku bankowego o nr /…/, założonego w /…/ na fikcyjną osobę o nazwisku /…/, czym działał na szkodę wyżej wymienionych pokrzywdzonych oraz innych, tj. o przestępstwo z art. 287 § 1 kk i art. 286 § 1 kk w zw. z art. 12 kk[397]

Opis czynu sformułowany w prokuratorskim postanowieniu nie współgra z jego kwalifikacją prawną. Wskazać należy, że art. 287 § 1 k.k. i art. 286 § 1 k.k. dotyczą dwóch zupełnie innych sytuacji i ogólnie rzecz biorąc, nie będą pozostawać w zbiegu realnym. Z treści postanowienia wynika, że przestępca nie oddziaływał na psychikę pokrzywdzonego lub osoby reprezentującej pokrzywdzoną instytucję (bank), ale poufnie zainstalował w użytkowanej przez siebie aplikacji bankowości elektronicznej złośliwe oprogramowanie, które automatycznie przekierowywało przelewy na podstawione rachunki bankowe. Prawidłowa zatem kwalifikacja prawna czynu w dacie orzekania wyczerpywała znamiona art. 287 § 1 k.k., a biorąc pod uwagę stan prawny obowiązujący od 27 kwietnia 2017 r., to w grę wchodziłby art. 278 § 1 k.k. (ewentualnie art. 279 § 1 k.k. jeśli aplikacja została „zhakowana"). Pozostaje kwestią otwartą, w jaki sposób przestępca uzyskał nieuprawniony dostęp do zasobów, jak uruchomił złośliwe oprogramowanie i czy posiadało ono cechy programu szpiegującego. Ustalenie wszystkich wspomnianych okoliczności czyniłoby koniecznym uzupełnienie kwalifikacji prawnej przestępstwa lub sformułowanie odrębnego czynu z art. 267 § 1 k.k. lub art. 267 § 2 k.k. i ewentualnie z art. 267 § 3 k.k.

Może zajść sytuacja, gdy sprawca wypełni swoim zachowaniem znamiona przestępstwa kradzieży (lub kradzieży z włamaniem) środków zapisanych na rachunku, ale jednocześnie manipuluje danymi w celu wykonania przelewów. Powstaje pytanie: Czy czynność sprawcza nosząca znamiona art. 287 § 1 k.k. pozostanie w zbiegu pomijalnym z art. 278 § 1 k.k. (ewentualnie art. 279 § 1 k.k.); czy też właściwe będzie przyjęcie kumulatywnej kwalifikacji prawnej tych dwóch przestępstw?

Zagadnienie to zostało już poruszone w podrozdziale dotyczącym zbiegu realnego ww. przepisów w przypadku przestępczych transakcji kartami płatniczymi, a analiza poglądów doktryny stoi na stanowisku, że zbieg realny art. 287 § 1 k.k. i art. 279 § 1 k.k. „może zachodzić, ale nie musi". Rzeczywiście tak jest, ale warto uściślić takie twierdzenie. M. Dąbrowska-Kardas i P. Kardas piszą:

> Zasadnie podkreśla się w orzecznictwie, że zbieg przepisów art. 287 § 1 i art. 279 § 1 wymaga aktualizacji określonych okoliczności, w konsekwencji przepisy te mogą

[397] Akta Prokuratury Rejonowej Olsztyn-Południe w Olsztynie o sygn. PR 2 Ds. 242.2016.

> stanowić podstawę kwalifikacji prawnej tylko w odniesieniu do pewnej kategorii przypadków. W szczególności zaś nie jest trafny pogląd jakoby przepis art. 287 § 1 nigdy nie mógł samodzielnie stanowić podstawy kwalifikacji prawnej, zawsze zaś występował w zbiegu z art. 279 § 1. Zbieg przepisów art. 279 § 1 i art. 287 § 1 występuje m.in. wówczas, gdy „wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianie, usunięciu albo wprowadzeniu nowych zapisów danych informatycznych towarzyszyć będzie wyjście jednostek pieniężnych z władztwa dotychczasowego posiadacza i ich włączenie do majątku sprawcy”[398].

W tym zakresie ww. autorzy powołują się na orzeczenie Sądu Apelacyjnego w Szczecinie[399]:

> Przestępstwo określone w art. 279 § 1 – piszą dalej M. Dąbrowska-Kardas, P. Kardas – charakteryzuje bowiem nie tylko zachowanie polegające na przełamaniu m.in. elektronicznego zabezpieczenia dostępu do mienia odzwierciedlonego przez odpowiednie zapisy na nośnikach elektronicznych, lecz także zabór zabezpieczonej rzeczy ruchomej w celu przywłaszczenia. Zatem dla wykorzystania jako ewentualnej podstawy kumulatywnej kwalifikacji art. 279 § 1 niezbędne jest wypełnienie przez zachowanie sprawcy ingerującego w sposób opisany w art. 287 § 1 w proces automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych wszystkich znamion typu przewidzianych w art. 279 § 1. Kumulatywnej kwalifikacji nie uzasadnia zatem samo przełamanie elektronicznego zabezpieczenia danych informatycznych[400].

Otóż realizowana przez przestępcę transakcja środków zapisanych na rachunku bankowym zawsze będzie tożsama z wpłynięciem bez upoważnienia na automatyczne przetwarzanie i przekazywanie danych informatycznych oraz z wprowadzeniem nowego zapisu w systemie banku, gdyż taka jest natura techniczna realizacji przelewu. Skoro jednak immanentną cechą kradzieży jest czynność wykonawcza polegająca na zaborze mienia w celu jego przywłaszczenia, to w operacjach na bankowym pieniądzu bezgotówkowym ów zabór jest tożsamy z czynnościami związanymi z wywołaniem transakcji i przetwarzaniem danych po to, aby przypisane do rachunku środki wyjąć spod władztwa ich właściciela (banku) oraz prawowitego posiadacza (klienta) a więc sprawić, że pieniądze przejmuje przestępca. W typowej zatem kradzieży środków zapisanych na rachunku bankowym art. 287 § 1 k.k. pozostanie w pomijalnym zbiegu z art. 279 § 1 k.k. Może się jednak zdarzyć, że sprawca kradzieży takich środków zrobi „coś więcej” w systemie bankowym, aniżeli tylko dokona zlecenia przelewu. Może np.

[398] M. Dąbrowska-Kardas, P. Kardas, *Art. 287*, *teza 86,* [w:], *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. A. Zoll, W. Wróbel, LEX 2022.
[399] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.
[400] M. Dąbrowska-Kardas, P. Kardas, *Art. 287, tezy 13 i 15*…

złośliwie zmienić ustawienia aplikacji bankowości elektronicznej tak, aby pokrzywdzony nie mógł sprawdzić historii transakcji i korespondencji prowadzonej z instytucją finansową. Albo włamując się i kradnąc pieniądze, tak ustawi algorytmy zarządzające aplikacją, że nawet po wylogowaniu się przestępcy z systemu aplikacja nadal będzie przesyłała środki pieniężne na wskazany przez niego rachunek. W takich przypadkach w grę wchodzi kumulatywna kwalifikacja prawna z art. 278 § 1 k.k. (art. 279 § 1 k.k.) i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. bowiem oprócz wypełnienia znamion kradzieży, sprawca wykonał jeszcze inne czynności wykraczające poza to, co należało zrobić, aby transferować pieniądze.

Powracając do przykładów *modus operandi*, to stosunkowo prosty sposób na popełnienie przestępstwa z wykorzystaniem telefonu często jest najefektywniejszy w dokonywaniu oszustw i „zarabianiu" pieniędzy. Na taki pomysł wpadł B. Z.; w śledztwie prowadzonym przez Prokuraturę Rejonową w Chorzowie ustalono, że sprawca oszukał 57 osób, dzwoniąc do sklepów, gdzie pracowały, i podając się za dostawcę rozwiązań dla płatności mobilnych prosił sprzedawców o dokonanie określonych czynności na terminalu płatniczym, związanych rzekomo z serwisowaniem POS-ów. Jedna z pokrzywdzonych zeznała:

> Kazał mi w terminalu wejść na opcje „moje rachunki" i tam miałam poszukać opcji *paysafecard* /…/ tam pisało „paysafecard 300" i miałam na to nacisnąć, co też zrobiłam. Wtedy na terminalu wyświetliło mi się, że do zapłaty jest kwota 300 zł i należy ją zaakceptować. Ja to powiedziałam temu mężczyźnie, na co on powiedział, że tym nie mam się co martwić bo na wydrukach są kody testowe i kazał przedyktować sobie kod podany na wydruku z terminala.

Sprawca stwierdził, że z kodami jest „coś nie w porządku" i operację trzeba powtórzyć, a nieświadoma niczego ekspedientka pomogła oszustowi zrealizować kolejny przelew do jego wirtualnej portmonetki. B. Z. został oskarżony o to, że:

> w dniu 2 lutego 2016 r. w Świętochłowicach i Chorzowie, działając w celu uzyskania korzyści majątkowej, po uprzednim wprowadzeniu pracowników sklepów ogólnospożywczych prowadzonych przez A. T. w błąd co do faktu działania w imieniu firmy /…/ i konieczności zaktualizowania systemu w terminalu płatniczym, uzyskał 14 kodów uzupełniających do karty paysafecard o nominałach 300 zł każdy, czym doprowadził A. T. do niekorzystnego rozporządzenia mieniem w łącznej kwocie 4200 zł przy czym z popełnienia przestępstwa uczynił sobie stałe źródło dochodu, tj. o przestępstwo z art. 286 § 1 k.k. w zw. z art. 65 § 1 k.k.[401]

[401] Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 2 Ds. 424.2016.

W sprawie tej ustalono ponadto, że sprawca zakładał fikcyjne konta mailowe wykorzystywane do kreacji rachunków na platformach płatności Skrill, na które wpływały środki z oszukańczych doładowań sklepowych. Następnie środki te przestępca przeznaczał na zakup biletów turniejowych na portalu internetowych gier hazardowych PokerStars[402], po ukończeniu turnieju w pokera nagroda była przelewana na wskazany przez niego rachunek bankowy, a pieniądze podejmowane w bankomacie. B. Z. popełnił zatem przestępstwo prania pieniędzy, a sformułowany przez prokuratora zarzut brzmiał:

> w okresie od września 2015 r. do kwietnia 2016 r. w Siedlcach, Poznaniu, Warszawie i Łukowie, działając w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru, dokonywał transferu środków płatniczych uzyskiwanych z doładowań do kart paysafecard na założone przez siebie fikcyjne konta skrill i pokerstrars, z których przedmiotowe środki były następnie wykorzystywane do udziału w turniejach pokerowych rozgrywanych pomiędzy uczestnikami posługującymi się założonymi uprzednio przez niego kontami, co gwarantowało uzyskanie nagrody za ukończenie turnieju, która następnie była przelewana na konta bankowe, w tym otwarte na dane /…/ i wypłacana za pomocą kart bankomatowych, przez co utrudniał stwierdzenie przestępczego pochodzenia środków związanych z doprowadzaniem osób fizycznych i innych podmiotów do niekorzystnego rozporządzania mieniem, przy czym z popełnienia przestępstwa uczynił sobie stałe źródło dochodu, tj. o przestępstwo z art. 299 § 1 k.k. w zw. z art. 12 k.k. przy zast. art. 65 § 1 k.k.[403]

Paysafecard to wirtualny środek płatniczy w postaci karty przedpłaconej, której kod składa się z 16 znaków. Umożliwia on płacenie w Internecie za towar i usługi bez podawania danych osobowych oraz innych danych „wrażliwych", takich jak numer rachunku bankowego czy karty kredytowej. Karty Paysafecard zakładane są w usłudze o tej samej nazwie, a następnie ich użytkownik anonimowo doładowuje swoje indywidualne konto pieniędzmi. W systemie płaci się podobnie jak kartą płatniczą, ale dane wpłacającego nie są podawane do wiadomości sklepów czy aplikacji. Wspomniane karty najczęściej wykorzystywane są przez usługi związane z branżą gier mobilnych, konsolowych i komputerowych; można nimi płacić m.in. na Steamie, PlayStation Store, Wargaming.net albo bezpośrednio w grach z mikropłatnościami. Podobnie aplikacja

[402] PokerStars to jeden z najpopularniejszych na świecie wirtualnych salonów internetowych do urządzania gier w pokera online. Zgodnie z art. 5 ust. 1b ustawy z dnia 19 listopada 2009 r. o grach hazardowych, takie urządzenie, do których zalicza się poker, z wyjątkiem loterii promocyjnych oraz zakładów bukmacherskich objęte jest monopolem państwa. W związku z tym, wszystkie strony internetowe, oferujące możliwość brania udziału w takich rozgrywkach, podlegają wpisowi do Rejestru Domen Służących do Oferowania Gier Hazardowych Niezgodnie z ustawą (tzw. rejestr domen zakazanych), a następnie są blokowane. Zgodnie z art. 107 § 2 k.k.s. „Kto na terytorium Rzeczypospolitej Polskiej uczestniczy w zagranicznej grze hazardowej, podlega karze grzywny do 120 stawek dziennych".

[403] Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 2 Ds. 424.2016.

Skrill utożsamia wirtualny portfel służący tylko do realizacji płatności online lub transferów pieniędzy pomiędzy uczestnikami systemu.

Od pewnego już czasu plaga oszustw w Internecie powiązana jest z działalnością platform inwestycyjnych, które proponują zakup różnego rodzaju produktów finansowych, często mających postać kryptoaktywów, za pieniądz fiducjarny. Oszukańcze oferty dotyczą przede wszystkim detalicznego rynku Forex działającego jako rynek instrumentów pochodnych, na którym inwestuje się pieniądze, aby zarobić na różnicy kursów walorów. Firmy oferują swoim klientom do inwestowania instrumenty pochodne, m.in.:

1. kontrakty na różnice będące dwustronną umową, w której strony zobowiązują się do rozliczenia kwoty równej różnicy pomiędzy ceną otwarcia a zamknięcia pozycji. Kontrakt CFD stanowi zatem umowę pomiędzy „nabywcą" a „sprzedawcą", dotyczącą wymiany różnicy w aktualnej cenie instrumentu bazowego (np. akcji, walut, towarów, wskaźników itp.) a jego ceną w momencie zamknięcia kontraktu z mechanizmami lewarowania. CFD umożliwiają inwestorom wykorzystanie wzrostu cen instrumentu bazowego (przyjęcie długiej pozycji) lub spadku tych cen (przyjęcie krótkiej pozycji). W momencie zamknięcia kontraktu inwestor otrzymuje lub musi zapłacić różnicę pomiędzy ceną zamknięcia a ceną otwarcia instrumentu i/lub aktywów bazowych, a gdy różnica jest dodatnia, to dostawca CFD płaci inwestorowi[404];
2. opcje binarne to spekulacja służąca zarabianiu na zmianie kursu kontraktów terminowych. Mówi się, że kontrakty terminowe to „gra o sumie zero", ponieważ kwota zysku jednej ze stron odzwierciedla kwotę straty inwestora, który zajmuje pozycję przeciwną. Klasyczna opcja binarna stanowi przykład relacji pomiędzy nabywcą a wystawcą, gdzie pierwszy z nich oczekuje sytuacji, w której cena przyjętego instrumentu będzie niższa od ceny realizacji, natomiast nabywca spodziewa się sytuacji odwrotnej, tj. gdy cena instrumentu bazowego przewyższy kurs realizacji[405];
3. instrumenty oparte na cenach walut dotyczą bardzo popularnego wśród posiadaczy kryptowalut tzw. trading na Forex – chodzi o spekulację na wartości wybranego pieniądza lub waluty wirtualnej w stosunku do ceny podobnego rodzajowo aktywa. Kiedy dwie waluty są zestawione i wycenione względem siebie, nazywa się je parą walutową.

Ogólnie rzecz biorąc, oferowanie instrumentów finansowych nie jest zabronione, jednak zbyt wiele platform sieciowych ma z założenia oszukańczy charakter. Scenariuszy takich przestępstw jest kilka. W najprostszym z nich sprawcy gromadzą środki wpłacone przez inwestorów i w pewnym momencie „znikają", a prowadzona przez nich platforma cyfrowa przestaje działać. W innym scenariuszu długi wobec wcześniejszych inwestorów spłacają z funduszy pozyskanych od nowych uczestników platformy, tworząc w ten sposób piramidę finansową.

[404] https://www.esma.europa.eu/sites/default/files/library/2015/11/investor_warning_-_cfds_-_esma_2013_00070000_pl_cor.pdf [dostęp: 28.07.2023].

[405] https://mfiles.pl/pl/index.php/Opcje_binarne [dostęp: 28.07.2023].

Jeśli chodzi o podejście do indywidualnego inwestora, to przestępcy nawiązują z nim kontakt na stronach internetowych promujących przedsięwzięcie biznesowe. Oferty tam umieszczone wyglądają bardzo atrakcyjnie pod względem marketingowym i brzmią wiarygodnie, strona jest prosta w obsłudze, zawiera pozytywne komentarze podstawionych osób, a ponadto dopuszcza się wiele metod transferu i konwersji środków finansowych. W dłuższej perspektywie kontakt przestępcy z inwestorami odbywa się w trakcie rozmów telefonicznych, ale dochodzi także do przejęcia przez sprawcę kontroli nad komputerem potencjalnego pokrzywdzonego z wykorzystaniem tzw. zdalnego pulpitu (programy AnyDesk, TeamViewer, VNC Viewer, AreoAdmin, Radmin, SupRemo, Chrome Remote Desktop, PuTTY, TightVNC), umożliwiającego z dowolnego miejsca na świecie zarządzanie jego aktywami i decyzjami inwestorskimi. W jednej ze spraw kobieta zeznała przed sądem, że padła ofiarą oszustwa, gdyż na prośbę osoby, która przedstawiła się jako pracownik banku, zainstalowała na swoim telefonie aplikację typu *quick support*, co umożliwiło sprawcom zawarcie w jej imieniu umowy pożyczki, a następnie pobranie z jej konta środków pieniężnych[406].

Oszuści promują oferowane produkty, wykorzystując nowoczesne środki komunikacji, media społecznościowe, a ponadto znanych internetowych blogerów, którzy reklamują inwestycje, zachwalają możliwość szybkiego wzbogacenia się i udzielają (niekoniecznie rzetelnych) porad. Stosując metody socjotechniczne, wsparte narzędziami teleinformatycznymi, przestępcy namawiają fundatora do instalacji określonej aplikacji, założenia konta na wskazanej przez nich giełdzie i przelania na podany adres jednostek kryptowaluty, czy po prostu przekazania im pieniędzy na inwestycję. „Biznesowy doradca" udziela wskazówek, jak inwestować, gdzie oraz ile środków lokować, w którym momencie dokonać zakupu kryptowalut lub zamienić tokeny na złotówki. W tym samym czasie, w sposób oficjalny lub zakamuflowany, przejmuje on kontrolę nad aktywami pokrzywdzonego i przywłaszcza je. Niekiedy, aby podtrzymać więź z oszukiwaną osobą, przekazuje jej niewielkie środki i obiecuje coraz większe zyski oraz przesyła fikcyjne algorytmy obrazujące rzekome, rosnące wpływy z inwestycji[407].

Autor, jako konsultant, uczestniczył w przygotowaniu *Algorytmu podstawowych czynności realizowanych przez funkcjonariuszy Policji związanych z oszustwami inwestycyjnymi z wykorzystaniem walut wirtualnych*. W metodyce wskazano m.in., jak przesłuchiwać osobę, która składa zawiadomienie o podejrzeniu popełnienia omawianego oszustwa, bazując na regule 7 pytań wykrywczych:

— Co się wydarzyło?
— Gdzie?
— Kiedy?
— Jakimi środkami?

[406] Wyrok Sądu Okręgowego w Olsztynie z dnia 25 kwietnia 2022 r., I C 536/21, LEX nr 3357331.

[407] E. Przewłoka, *Algorytm podstawowych czynności realizowanych przez funkcjonariuszy Policji związanych z oszustwami inwestycyjnymi z wykorzystaniem walut wirtualnych*, Wydział do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Bydgoszczy, Bydgoszcz 2023, s. 2 (zbiory własne autora).

— W jaki sposób?
— Kto?
— Dlaczego?

Algorytm opisuje także, że funkcjonariusz przyjmujący zawiadomienie powinien dążyć do zabezpieczenia śladów i dowodów cyfrowych związanych z *modus operandi* sprawców w postaci m.in.:

1. korespondencji prowadzonej przez pokrzywdzonego ze sprawcą drogą mailową, łącznie z nagłówkami wiadomości elektronicznych (korespondencję w miarę możliwości należy zabezpieczyć w wersji elektronicznej);
2. korespondencji prowadzonej przez komunikator internetowy poprzez wyeksportowanie czatu związanego z popełnionym przestępstwem i przekazanie go na służbowy adres mailowy funkcjonariusza przyjmującego zawiadomienie lub na fizycznym nośniku danych;
3. parametrów kont utworzonych za pomocą aplikacji pozwalających na zdalne przejęcie kontroli nad urządzeniem;
4. pełnej treści ze strony html, poprzez którą został nawiązany kontakt z oszustem;
5. korespondencji prowadzonej SMS-ami w postaci zrzutów ekranu z uszczegółowieniem czasu trwania rozmowy, liczby połączeń, numerów telefonów z których kontaktował się sprawca z pokrzywdzonym;
6. historii przeglądarki internetowej za okres, kiedy pokrzywdzony nawiązał kontakt ze sprawcą;
7. historii rachunków bankowych oraz potwierdzeń przelewów z bankowości internetowej poprzez eksport danych np. do pliku PDF, celem ustalenia szczegółów transakcji. Jeśli nie będzie to możliwe, należy uzyskać zgodę od pokrzywdzonego na wystąpienie w jego imieniu do banku o przekazanie informacji mających związek z przestępstwem, w tym daty i godziny, adresów IP oraz numerów portów, z których następowały logowania do panelu bankowości elektronicznej pokrzywdzonego;
8. nagrań postów i informacji zamieszczanych na platformach społecznościowych, za pomocą których sprawcy przestępstwa reklamowali nielegalną inwestycję;
9. rozważenie konieczności zabezpieczenia sprzętu komputerowego lub innych urządzeń wykorzystywanych przez pokrzywdzonego do kontaktowania się z oszustami[408].

Niezgodna z prawem działalność inwestycyjna w zakresie kontraktów Forex lub w jeszcze innym zakresie naruszająca przepisy regulujące rynek kapitałowy, oprócz malwersacji finansowych, często połączona jest z naruszeniem prawa dotyczącego przyjmowania środków pieniężnych pod tytułem zwrotnym, udzielania pożyczek lub emisji pochodnych instrumentów finansowych bez uzyskania stosownych zgód lub zezwoleń u publicznych organów sprawujących nadzór nad rynkiem kapitałowym. Działania takie mogą być penalizowane na gruncie przepisów ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[409] lub ustawy o usługach płatniczych; drugi przypadek

[408] Tamże.
[409] T.j. Dz. U. z 2023 r. poz. 646, 825.

miał miejsce w postępowaniu prowadzonym przez Prokuraturę Rejonową Katowice-Północ w Katowicach w sprawie:

> mającego miejsce w okresie od nieustalonego dnia do dnia 27 marca 2019 r. w Katowicach działania polegającego na prowadzenia działalności w zakresie wydawania pieniądza elektronicznego bez wymaganej licencji przez osobę działającą w imieniu i w interesie osoby prawnej spółki /…/, tj. o czyn z art. 150 ust. 3 w zw. z ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[410].

Materiał dowodowy gromadzony w śledztwie dotyczącym nielegalnych ofert inwestycyjnych ma niekiedy dość nietypowy charakter i obejmuje m.in. nagrania z platform społecznościowych typu YouTube, Facebook czy Twitter, gdzie osoby podejrzewane reklamowały swoje produkty. Ustalenia poczynione w tym zakresie są przydatne m.in. dla biegłego z zakresu ekonomii w udzieleniu odpowiedzi na pytania dotyczące „podejrzanych" planów inwestycyjnych:

1. Czy oferty inwestycyjne ustalonego podmiotu były ekonomicznie uzasadnione?
2. Czy stopa zysków oferowana przez podmiot była oparta na racjonalnych podstawach ekonomicznych?
3. Czy nabycie produktów podmiotu wiązało się z ryzykiem szkody dla inwestora oraz jaka była jego skala?
4. Czy mechanizm funkcjonowania podmiotu:
   a. wykazywał cechy systemu sprzedaży lawinowej w kontekście art. 17c ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,
   b. wykazywał cechy systemów typu piramida o jakich mowa w ustawie z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym,
   c. marketingu wielopoziomowego (MLM)[411]?

Często zdarza się bowiem, że twórcy oszukańczych programów oferują potencjalnym inwestorom wysokie stopy zysków, które nie pochodzą z typowej działalności gospodarczej, ale opłat uiszczanych przez nowych inwestorów, tj. kolejnych ofiar oszukańczego procederu, noszącego pozory legalnej działalności. Przestępcy, na początku dla uwiarygodnienia się, wypłacają zyski (prowizje) pierwszym uczestnikom platformy lub sprzedają im realnie istniejące produkty. Jednakże u podstaw każdej piramidy finansowej leży nieustanne pozyskiwanie nowych dostawców kapitału. Osoby takie mamione są wizją nie tylko wysokich i szybkich zysków, ale także brakiem ryzyka. Dochodzi do tego zatajanie obiektywnych informacji, umów, faktur oraz używanie licznych technik manipulacji. W przygotowanych przez Prokuraturę Krajową wytycznych dla prokuratorów wskazano, że w toku prowadzonych postępowań należy w pierwszej kolejności ustalić, czy dany podmiot rzeczywiście prowadził działalność np. na rynku Forex, czy

[410] Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 1 Ds. 67.2019.
[411] Akta Prokuratury Regionalnej w Katowicach o sygn. PR I Ds. 16.2018.

też, pod pozorem dokonywania inwestycji w instrumenty pochodne, oszukiwał swoich klientów co do charakteru realizowanej działalności i niekorzystnie rozporządzał mieniem pokrzywdzonych. W taki sposób zachowywał się T. O., który został oskarżony przez Prokuraturę Regionalną w Katowicach o kilkadziesiąt oszustw popełnionych na szkodę pokrzywdzonych inwestorów. Jeden z zarzutów brzmiał:

> w okresie od 19 kwietnia do 30 maja 2017 roku, w /…/, czyniąc sobie z popełniania przestępstwa stałe źródło dochodu, działając w celu osiągnięcia korzyści majątkowej, doprowadził M. K. do niekorzystnego rozporządzenia mieniem w kwocie 40.378,10 zł poprzez wprowadzenie pokrzywdzonej w błąd, co do zamiaru zwrotu przekazanej kryptowaluty Bitcoin i wypłaty uzyskanego zysku z obrotu na giełdzie kryptowalutowej, w ten sposób, że działając w ramach firmy Crypto Academy /…/ z siedzibą w /…/ przyjął od M. K.:
> - w dniu 19 kwietnia 2017 roku 2 Bitcoiny przesłane na adres publiczny 1JhZGCW/…/,
> - w dniu 19 maja 2017 roku 2 Bitcoiny przesłane na adres publiczny NEWrgcHK2/…/,
> - w dniu 30 maja 2017 roku 2 Bitcoiny przesłane na adres publiczny 75i6xeie/…/
> - których kluczami prywatnymi dysponował pod pozorem dalszego inwestowania na giełdach kryptowalutowych, w wyniku czego miał zwracać przesłane Bitcoiny i wypłacać z góry określony zysk, co jednak nie nastąpiło i następnie zerwał kontrakt z pokrzywdzonymi i opuścił granice Polski,
> tj. o przst. z art. 286 § 1 k.k. przy zast. art. 65 § 1 k.k.[412].

W prokuratorskim śledztwie ustalono, że oskarżony interesował się nowymi technologiami i posiadał wiedzę dotyczącą blockchainów i kryptowalut, którą upowszechniał, działając jako firma CryptoAcademy, prowadząc szkolenia i organizując społeczność na Facebooku. T. O. od lutego 2017 r. zaczął proponować obserwującym go osobom w Internecie inwestowanie za jego pośrednictwem na zasadach tradingu w kryptowaluty, zapewniając wysokie odsetki z powierzonych środków. Chętni do skorzystania z oferty musieli przystąpić do społeczności na zamkniętym koncie Facebooka i przekazać na rzecz oskarżonego wstępną opłatę w wysokości co najmniej 0,1 BTC. T. O. obiecał zwrócić przekazane mu aktywa po upływie ustalonego w umowie terminu wraz z wysokimi odsetkami, a standardowy okres inwestycji wynosił 90 dni z oprocentowaniem zainwestowanego kapitału na poziomie 180% (w pierwszych 60 dniach było to 60%). Po pewnym czasie okazało się, że T. O. nie realizuje przyjętych na siebie zobowiązań finansowych, nie zwraca inwestorom przekazanych przez nich środków, a ostatecznie

[412] Tamże.

„zniknął" i nie można było się z nim skontaktować. W śledztwie ustalono, że sprawca oszukał 45 pokrzywdzonych na łączną kwotę kilkuset tysięcy złotych.

W sprawie T. O., oprócz dokonania zabezpieczenia majątkowego na kryptowalutach w formie portfela papierowego, prokurator wydał decyzję o przeszukaniu systemów informatycznych na podstawie z art. 217 § 1 i 2 k.p.k. i art. 219 § 1 k.p.k., art. 220 § 1 k.p.k. w zw. z art. 236a k.p.k. i postanowił:

1. zażądać od T. O. wydania wszelkich danych informatycznych, korespondencji elektronicznej oraz plików znajdujących się na skrzynce pocztowej /…/@gmail.com,
2. w przypadku nie wydania dobrowolnie wskazanych wyżej danych polecić funkcjonariuszom /…/ przeprowadzenie przeszukania skrzynki /…/@gmail.com, w celu zabezpieczenia tych danych informatycznych, korespondencji i plików[413].

Termin „przeszukanie na odległość" dotyczy, najogólniej rzecz biorąc, czynności związanych z zapoznawaniem się przez organ procesowy z treściami określonych zasobów cyfrowych dostępnych w Internecie w celu ujawnienia śladów i dowodów popełnionych przestępstw lub zabezpieczenia mienia. Prokuratorzy i funkcjonariusze organów ścigania prawie nie korzystają z możliwości realizacji takiej formy przeszukania, gdyż wydaje się ona trudna pod względem technicznym i kontrowersyjna pod względem prawnym. Tymczasem przepis art. 236a k.p.k. w obecnym kształcie daje pełną podstawę do prowadzenia przeszukania na odległość i elastycznie odsyła do odpowiedniego stosowania w tym zakresie pozostałych regulacji rozdziału 25 k.p.k. Kształt odesłania stanowi, że do omawianego przeszukania należy stosować rygory zabezpieczające prawa osoby, której przeszukanie dotyczy. W takim duchu dokonuje się zresztą wykładni wszystkich przepisów umiejscowionych w Kodeksie postępowania karnego: jeżeli przepis stanowi, że inne przepisy stosuje się odpowiednio do zakresu regulacji, to odpowiednie stosowanie nie może być mniej korzystne dla świadka lub podejrzanego, aniżeli wynika to ze wzorca pierwotnego. Kwestie podstawowe, takie jak prawo do udziału w czynności określonych osób, jej zaskarżalność, czy dopuszczalność na podstawie decyzji uprawnionego organu, pozostają niezmienne. Patrząc z drugiej strony, to przeszukanie online ma specyficzny charakter i siłą rzeczy pewne normy muszą ulec modyfikacji, aby można było przeprowadzić takie działanie. Uprawnione jest stanowisko, że zbyt kazuistyczna regulacja omawianej czynności procesowej mogłaby przynieść skutek odmienny od założonego i przyczynić się do powstania jeszcze większej liczby problemów i wątpliwości, kiedy można, a kiedy nie można realizować „zdalnego przeszukania" lub zbytnio zawęzić sytuacje, w których jest ono dozwolone. Lepiej wyznaczać

[413] Tamże.

i wytyczać w doktrynie i orzecznictwie pewne uniwersalne przepisy pasujące do szybko zmieniającej się taktyki i techniki działań w cyberprzestrzeni, aniżeli bardzo szczegółowo określać hipotetyczne stany faktyczne, kiedy czynność jest dopuszczalna[414].

Analiza spraw karnych pokazała, że podobnych oszustw było więcej i dotyczyły one także zagranicznych platform internetowych oferujących pozornie bardzo intratne inwestycje. Prokuratura Rejonowa Warszawa-Mokotów w Warszawie wydała postanowienie o umorzeniu śledztwa z powodu niewykrycia sprawcy przestępstwa w dwóch tego rodzaju sprawach:

> doprowadzenia M. C. B. do niekorzystnego rozporządzenia mieniem w celu osiągnięcia korzyści majątkowej w postaci pieniędzy w kwocie 26 700,00 euro stanowiących równowartość 111 594,93 zł za pośrednictwem platformy internetowej www.crypto-banque.com poprzez wprowadzenie w błąd co do zamiaru wywiązania się z usług inwestycyjnych oraz zwrotu wpłaconych środków, tj. o czyn z art. 286 § 1 k.k.[415].

> w sprawie doprowadzenia /…/ w dniu 20 października 2017r. w nieustalonym miejscu do niekorzystnego rozporządzenia mieniem znacznej wartości, tj. w kwocie 51 000 EURO w celu osiągnięcia korzyści majątkowej poprzez wprowadzenie w błąd /…/ co do wywiązania się z umowy inwestycyjnej, tj. o czyn z art. 286 § 1 kk w zw. z art. 294 §1 kk[416]

Ustalenie sprawcy takich przestępstw jest bardzo trudne i śledztwa/dochodzenia kończą się najczęściej na etapie postępowania przygotowawczego, wydaniem postanowienia bazującego na art. 322 § 1 k.p.k. Tak było w dochodzeniu Prokuratury Rejonowej w Lidzbarku Warmińskim, gdzie prokurator umorzył postępowanie w sprawie:

> zaistniałego w dniu 11 maja 2018 r. w bliżej nieustalonym miejscu w celu osiągnięcie korzyści majątkowej – doprowadzenia P. O. do niekorzystnego rozporządzenia mieniem w postaci pieniędzy w kwocie 500 EU, tj. 2.325,21 PLN za pomocą wprowadzenia w błąd co do zamiaru zwrotu zainwestowanych pieniędzy za pośrednictwem platformy internetowej służącej do obrotu https://kryptonextgroup kryptowalutami, tj. o czyn z art. 286 § 1 k.k.[417].

Na zakończenie niniejszego podrozdziału warto wspomnieć jeszcze o dodatkowej metodzie wykorzystywanej przez sprawców, której celem są zarówno oszustwa finansowe,

[414] P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2020, nr 9, s. 125–126.
[415] Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 2 Ds. 1614.2018.
[416] Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 5 Ds. 297.2018.
[417] Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 1 Ds. 460.2018.

ale także działania ukierunkowane na zagrożenie bezpieczeństwa powszechnego, a nawet zdrowia i życia ludzkiego; mowa tu o spoofingu. Polega on na wykonywaniu połączeń telefonicznych przy użyciu nieprawdziwego identyfikatora inicjującego połączenie (tzw. caller ID). Umożliwia to podszywanie się pod numer MSISDN (przechowywany na karcie SIM numer abonenta sieci komórkowej) przy wykorzystaniu infrastruktury operatorów i naruszając integralność sieci. Sprawca może zaprogramować dowolny numer telefonu, który ma się wyświetlić na ekranie urządzenia końcowego, obsługiwanego przez osobę odbierającą połączenie. Operatorzy sieci telekomunikacyjnych działają bowiem na zasadzie zaufania do swoich klientów i nie weryfikują numerów MSISDN. Usługi umożliwiające podszywanie się pod identyfikator inicjującego połączenie są łatwo dostępne w Internecie oraz tanie, zatem sprawca nie musi posiadać szczególnej wiedzy z zakresu funkcjonowania sieci telekomunikacyjnej, aby zastosować metodę spoofingu[418].

Jeden z takich ataków polega na podszywaniu się przez sprawcę pod pracownika infolinii banku i ostrzeganiu klientów instytucji finansowych o rzekomym wykryciu próby włamania na konta. Oszust prosi o podanie haseł uwierzytelniających dostęp do aplikacji płatności mobilnych lub zainstalowanie programu zdalnego pulpitu, co rzekomo ma pomóc w obsłudze informatycznej banku w neutralizacji zagrożenia z poziomu urządzenia końcowego klienta. W podobnym scenariuszu sprawcy podszywają się pod numer telefonu jednostki policji lub prokuratury, dzwonią i ostrzegają zmanipulowane osoby o rzekomym włamaniu na ich konto i konieczności dokonania przelewu środków finansowych na inny, podstawiony przez oszustów, rachunek, aby uniknąć ataku hakera. Stosując werbalną socjotechnikę, sprzęt techniczny (skrzynka SimBox) i oprogramowanie do fałszowania numerów telefonów, przestępcy chcą podnieść swoją wiarygodność w świadomości ofiar, a zatem zwiększyć efektywność działania, którego cel stanowi kradzież środków zapisanych na rachunku[419]. Podobną sprawę rozpoznał Sąd Okręgowy w Olsztynie, gdzie dzwoniący manipulowali przez telefon świadomością ludzi, bazując na ich niewiedzy i łatwowierności. Po uzyskaniu danych wrażliwych zamierzali w najprostszy sposób pokonać zabezpieczenia systemów informatycznych bez konieczności szukania luk w tych zabezpieczeniach lub stosowania zaawansowanej wiedzy technicznej do przełamywania haseł. W tym przypadku zastosowany przez nich spoofing miał postać vishingu: podając się za pracownika banku, bez fałszowania numerów telefonu, próbowali wzbudzić zaufanie rozmówców, że chronią ich pieniądze, i wywołując u pokrzywdzonych emocje i obawy o bezpieczeństwo oszczędności, wydobyć jak najwięcej poufnych danych[420]. Zachowanie takie należało zakwalifikować jako oszustwo z art. 286 § 1 k.k., a sprawcy uzyskane w ten sposób środki starali się natychmiast „wyprać" z wykorzystaniem „mułów" finansowych. Nieczęsto udaje się ustalić organom ścigania osoby pomagające w procederze prania pieniędzy, gdyż mogą one np. przebywać

[418] Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 10 stycznia 2022 r. dotyczące przestępstw spoofingu, sygn. 1001 – 7.024.1.2022 (zbiory własne autora), dalej jako: Pismo z 10 stycznia 2022 r.

[419] Tamże.

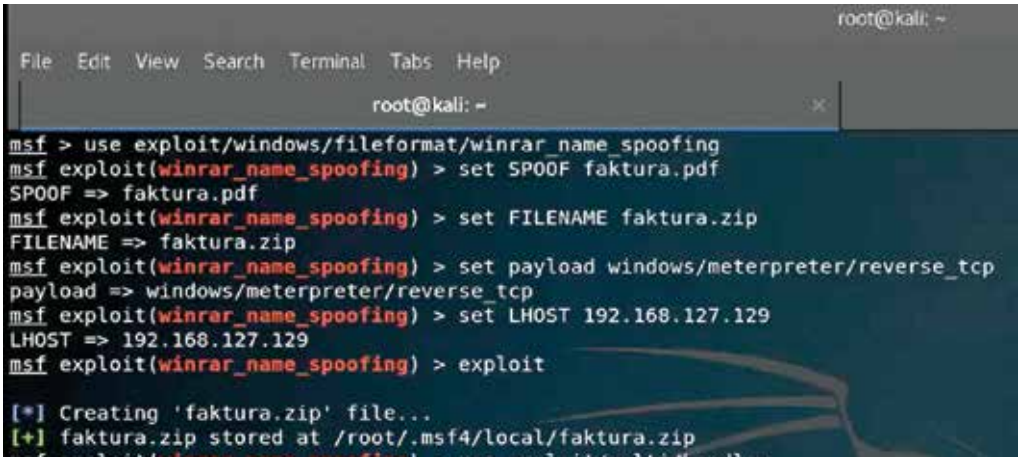
[420] Wyrok Sądu Okręgowego w Olsztynie z dnia 25 kwietnia 2022 r., I C 536/21, LEX nr 3357331.

w innej części świata, aniżeli działał sprawca przestępstwa lub nastąpił jego skutek. Nawet jeśli osoba taka zostanie ujawniona, to wykazanie jej umyślności w realizacji znamion art. 299 § 1 k.k. stanowi trudne wyzwanie dla prokuratora. Można się zastanawiać, czy R. S., która została oskarżona o pomoc w oszustwie, nie popełniła także przestępstwa z art. 299 § 1 k.k., gdyż opis zarzucanego jej czynu brzmiał następująco:

> w dniu 13 maja 2013 roku w Krakowie, w celu osiągnięcia korzyści majątkowej, działając z zamiarem, by osoba trzecia, dotychczas nie ustalona, dokonała czynu zabronionego w postaci wyłudzenia, przy wykorzystaniu łącza internetowego, na szkodę firmy /…/, pieniędzy w kwocie 49.090. złotych, udzieliła pomocy do popełnienia tego czynu użyczając swojego rachunku bankowego o numerze PL /…/ prowadzonego przez /…/ Bank, do transferu pieniędzy pochodzących z wyłudzenia, czym działała na szkodę wskazanej powyżej firmy, to jest o czyn z artykułu 18 § 3 kodeksu karnego w związku z artykułem 286 § 1 kodeksu karnego i artykułu 287 § 1 kodeksu karnego w związku z artykułem 11 § 2 kodeksu karnego[421]

Przesłuchana w charakterze podejrzanej R. S. wyjaśniła, że otrzymała wiadomość mailową, w której zagraniczna firma zaproponowała jej atrakcyjną ofertę zatrudnienia. Na początku zobowiązano ją do przesłania numeru posiadanego przez nią rachunku bankowego i skanu dowodu osobistego. Dalej jej „praca" polegała na przyjmowaniu pieniędzy na konto bankowe, w związku z czym 14 i 15 maja 2017 r. dokonała szeregu wypłat bankomatowych, w tym 11-krotnie kwoty 4000 zł. Otrzymane pieniądze przelała za pośrednictwem Western Union na adresy trzech osób otrzymane w SMS-ach. O tym, jak ma postępować, poinformował ją telefonicznie nieznany mężczyzna posługujący się „topornym" językiem polskim. Podejrzana nie przyznała się do popełnienia zarzucanego jej czynu, powiedziała, że nie znała mechanizmu przestępstwa. Ustalono natomiast, że pieniądze przelewane na jej konto pochodziło z rachunku osoby, która stała się ofiarą ataku phishingowego i nieświadomie wykonała transakcję w kwocie 11 809 euro.

[421] Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 1629/17/N.



Grafika nr 15. Konsola programu root@kali ukazująca działanie złośliwego oprogramowania typu exploit do przejęcie metodą spoofingu sesji prowadzonej przez inny adres IP i podszycia się pod osobę trzecią (na ekranie widać preparowanie załącznika pdf o nazwie „faktura.zip", który będzie dystrybuował malware'a)

Inną postacią spoofingu, której znamiona wyczerpują art. 224a k.k., są tzw. kaskadowe alarmy bombowe, gdy dzwoniący informują pracowników instytucji publicznych o podłożeniu ładunków wybuchowych w urzędach, szpitalach, szkołach i prokuraturach, podszywając się także pod numery telefonów osób publicznych, redaktorów serwisów o cyberbezpieczeństwie lub pracowników NASK. Począwszy od 2018 r., liczba takich przestępstw stale rośnie; np. w okresie egzaminów maturalnych w 2019 r. w wyniku fałszywych alarmów bombowych ewakuowano uczniów z 227 szkół w całej Polsce, a w kilku placówkach przerwano egzaminy dojrzałości. Jeśli chodzi o szczegóły *modus operandi* sprawców, to wysyłane przez nich zawiadomienia odczytywane są w słuchawce telefonu przez narzędzia przekształcające tekst na mowę syntetyczną (np. syntezator mowy Ivona), a innym razem wysyłane z opóźnieniem od momentu ich zaprogramowania. W innym scenariuszu przestępcy rozsyłali fałszywe powiadomienia w formie wiadomości mailowej, zakładając do tego anonimowe skrzynki pocztowe w zagranicznych, niszowych domenach. Sprawcy, rozsyłając wiadomości lub logując się do kont na platformach społecznościowych, anonimizują swój ruch sieciowy z wykorzystaniem sieci TOR, VPN-ów i PROXY oraz komputerów zainfekowanych złośliwym oprogramowaniem i podłączonych do botnetu. Dlatego dokonane przez organy ścigania pierwsze ustalenia adresu IP mogą być mylące i wskazywać, że alarm bombowy wysłała osoba, która w rzeczywistości nie ma nic wspólnego z popełnieniem przestępstwa[422].

Cel przeprowadzonych ataków spoofingu był różny: niektóre miały zdestabilizować funkcjonowanie instytucji publicznych i być może odciągnąć uwagę organów ścigania od innego rodzaju nielegalnej działalności realizowanej jednocześnie przez cyberprzestępców. Niektórzy sprawcy kierowali się chęcią zaistnienia w wirtualnym świecie, wywołania

[422] Pismo z 10 stycznia 2022 r.

zdarzenia, które szeroko komentowane jest w mediach, lub zdyskredytowania osób publicznych, których dane zostały wykorzystane do ataków. W wytycznych Prokuratury Krajowej[423] wskazano, że osoby, pod które podszył się „atakujący", są pokrzywdzonymi przestępstwem z art. 190a § 2 k.k., a nie art. 190 § 1 k.k.; w przypadku „ataków bombowych" w grę wchodzi kwalifikacja prawna z art. 224a k.k. Dla ustalenia, czy inicjującym połączenie była osoba lub podmiot, którego numer MSISDN wyświetlił się na ekranie odbiorcy, konieczne jest pozyskanie danych bilingowych dotyczących numeru telefonu pokrzywdzonego podmiotu oraz numeru inicjującego połączenie. Od dostarczycieli usług telekomunikacyjnych powinno się uzyskać informacje, o których mowa w art. 180c ustawy Prawo telekomunikacyjne, m.in. lokalizację stacji przekaźnikowych BTS, numery IMEI urządzeń, z którymi współpracował „podejrzany" telefon w okresie popełnienia przestępstwa, a zgromadzony materiał dowodowy poddaje się analizie kryminalnej w celu ustalenia powiązań zachodzących pomiędzy osobami i wykorzystywanymi do ataku urządzeniami. W takich sprawach pomocne mogą okazać się informacje uzyskane dzięki analizie OSINT, gdyż cyberprzestępcy zostawiają ślady cyfrowe swojej działalności w otwartym Internecie.

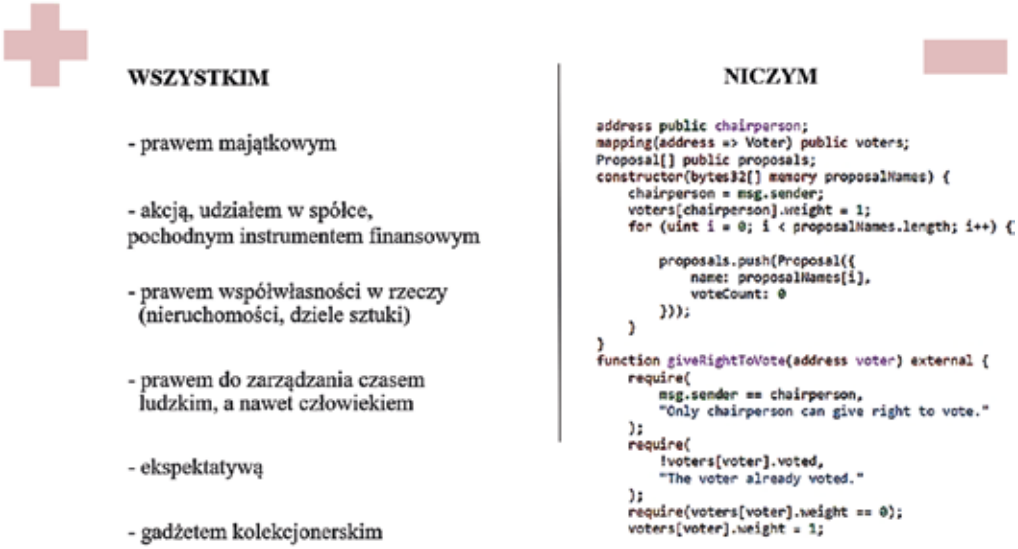
[423] Tamże.

Rozdział 5.
Przestępstwa z wykorzystaniem kryptoaktywów

5.1. Tokeny cyfrowe

Pojęcia: „kryptowaluty", „waluty wirtualne" i „kryptoaktywa" to intensywnie eksploatowane tematy w dyskursie prawniczym, co wynika z faktu migracji aktywności ludzkiej, a wraz z nią różnych form wartości majątkowych, do cyberprzestrzeni. Ponieważ jednym z przejawów takiej aktywności jest handel, to za otrzymane dobra lub usługi w Internecie należy w jakiś sposób zapłacić. Dla niektórych ludzi, szczególnie młodych, rozliczenia z wykorzystaniem tradycyjnego bankowego pieniądza bezgotówkowego stały się nieatrakcyjne, a więc poszukują oni nowych form płatności, nadających się do szybkich i łatwo dostępnych transferów wartości majątkowych w formie binarnej. Przyjmują one najczęściej postać tokenów cyfrowych. Kryptoaktywami interesują się także podmioty instytucjonalne, takie jak chociażby banki, które zainwestowały duże środki w tzw. stablecoiny. Tokeny mają zatem „jakąś" wartość i chociaż pod względem technicznym stanowią tylko część kodu cyfrowego przynależnego do określonego programu komputerowego, to obwarowanie tego kodu przepisami powszechnie obowiązującymi, postanowieniami umów lub po prostu zaufaniem inwestorów powoduje, że posiadanie tokenów utożsamiane jest z wymierną wartością finansową. Mówiąc najprościej: bitcoin (BTC), którego cena 12 lipca 2023 r. oscylowała w granicach 122540 zł, to wycinek protokołu Bitcoina, któremu realną wartość nadało wyłącznie przekonanie użytkowników protokołu, że jest on godnym uwagi projektem. BTC nie posiada funduszu gwarancyjnego, rekompensującego ewentualne straty wynikające z załamania kursu bitcoina, żaden centralny organ nie kreuje polityki jego emisji lub skupu, posiadaczowi bitcoina nie przysługuje prawo podmiotowe, które uprawniałoby go *orga omnes* do wymiany tokena na pieniądze lub złoto. Na przeciwnym krańcu usytuowane są stablecoiny utrzymujące, jak sama nazwa mówi, stabilny kurs w stosunku do określonych walorów, zakotwiczonych w „realnym" świecie lub posiadających ugruntowaną pozycję na rynku. Najczęściej chodzi o tradycyjne waluty, na czele z dolarem amerykańskim. W przypadku większości stablecoinów, typu tether i USDcoin, za ich stabilizowanie odpowiada gwarancja wymiany tokenów na walutę wzorcową w stosunku „1 do 1". Oznacza to, że w każdym momencie użytkownik „stabilnej monety" ma prawo zażądać od jej emitenta konwersji stablecoina na pieniądz fiducjarny. Do parytetu złota odwołuje się z kolei DigixDAO. Jest to zdecentralizowana organizacja na Ethereum typu DAO tworząca, listowaną na giełdzie, kryptowalutę DGD jako natywny token ERC20 zarządzający siecią Digix Golden Token (DGX)[424].

[424] P. Opitek, *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Instytut Ekspertyz Ekonomicznych i Finansowych w Łodzi, Łódź 2022, s. 163–164.



Grafika nr 16. Czym jest cyfrowy token?

Wynika z tego, że tokeny mają niejednorodny charakter prawny: mogą być „tylko" przedmiotem wymiany (np. bitcoin), aktywem reprezentującym prawo własności rzeczy albo dobra niematerialne (tokeny DGD i DGX), a nawet instrumentem finansowym (tokeny ETH20SMACO). Token przyznaje niekiedy prawo dostępu do fizycznych zasobów określonego towaru (złota, ropy, energii elektrycznej), a innym razem stanowi cyfrową tożsamość lub zaawansowany produkt będący elementem konstrukcyjnym „inteligentnych umów". Jeśli algorytm funkcjonowania określonych tokenów przypomina rolę, jaką spełniają instrumenty finansowe na rynku kapitałowym, to takie kryptoaktywa pozostają w obszarze zainteresowania Komisji Nadzoru Finansowego, a emisja i obrót nimi podlegają szczególnemu reżimowi prawnemu dotyczącemu np. konieczności uzyskania zezwolenia lub uprawnienia bądź sporządzenia dokumentu informacyjnego w związku z ich „wypuszczeniem" na rynek. Dodatkowo, dwa tokeny wyemitowane na tym samym blockchainie i identyczne pod względem technologicznym, potencjalnie mogą być odmiennie zakwalifikowane, np. jeden jako znak legitymacyjny, o którym mowa w art. 921[15] k.c., a drugi będzie stanowił instrument inkorporujący prawa tożsame do praw zawartych w papierze wartościowym lub instrumencie finansowym[425].

W dyskusji o tokenach cyfrowych często pojawia się słowo blockchain, ponieważ technologia rozproszonych rejestrów stanowi fundament działania walut wirtualnych. Najlepiej omówić ją na przykładzie protokołu Bitcoina, gdyż bitcoin stanowi pierwszą wyemitowaną na świecie kryptowalutę, jest najpopularniejszy na rynku walut

[425] Stanowisko Urząd Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf, s. 5, [dostęp: 27.07.2022].

wirtualnych, ale także najczęściej wykorzystywany do popełniania przestępstw. Można z łatwością odnaleźć chociażby w Internecie wiele pozycji naukowych charakteryzujących techniczne aspekty funkcjonowania blockchainów[426], a opisywanie ich wszystkich w monografii mijałoby się z celem książki i znacznie przekraczało ramy objętościowe opracowania. Dlatego poniżej przedstawione zostaną tylko ogólne zasady funkcjonowania technologii publicznego blockchaina, które przekładają się na opis czynów karalnych oraz ich kwalifikację prawną, a ponadto na zasady poszukiwania i wykorzystania śladów cyfrowych związanych z użytkowaniem kryptowalut przez przestępców oraz realizację zabezpieczenia majątkowego.

Blockchain, najprościej rzecz ujmując, to elektroniczna księga rozrachunkowa zawierająca listę transakcji dokonywanych w określonej kryptowalucie, a jednocześnie system rozrachunkowy tychże transakcji. W literaturze przedmiotu można spotkać obrazowe porównania działania blockchaina do idei wielkich kamieni nazywanych Rai, znajdujących się na wyspie Yap. Mieszkańcy wyspy wykonywali na tych kamieniach własne, niepowtarzalne znaki, czyli podpisywali je, i każdy tubylec oznaczał głazy stanowiące jego własność. Realizacja płatności polegała na zmazaniu podpisu przez osobę, która go naniosła, i umieszczeniu w tym miejscu identyfikatora nowego właściciela głazu[427]. Podobnie wygląda transakcja kryptowalutowa: token przesyłany jest z adresu X (kupującego) na adres Y (sprzedawcy), a w sieci publikuje się komunikat informujący o tym, kto jest nadawcą i odbiorcą tokena oraz co stanowi jego treść. Adres to unikalny ciąg alfanumeryczny, pozwalający na odbieranie i wysyłanie danej kryptowaluty. Może on być prezentowany w kilku formatach: zaczynając od wspomnianej, ale trudnej w codziennym użytkowaniu, adnotacji alfanumerycznej, a kończąc na wygodnych kodach QR do skanowania. Szukając analogii do adresu w świecie tradycyjnej bankowości elektronicznej, można porównać go z numerem rachunku bankowego. Podobnie jak osoba indywidualna posiada konta w kilku bankach, a na tych kontach uruchomionych jest kilka rachunków bankowych, tak samo w przypadku kryptowalut ich użytkownicy mogą dysponować wieloma portfelami, w których przechowywanych jest wiele adresów. Każda kryptowaluta posiada swój własny „przepis" (algorytm) na generowanie adresu publicznego z klucza prywatnego[428].

Skoro transakcja polega na przesłaniu danych z jednego adresu na drugi adres, to ktoś musi wesprzeć taki proces zapleczem technologicznym i energią elektryczną. W celu realizacji bezgotówkowego przelewu pieniężnego, bank zatrudnia pracowników i utrzymuje serwery z danymi informatycznymi, łącza telekomunikacyjne, aplikacje bankowe itp. Wszystkie te urządzenia czerpią energię elektryczną, a poszczególne procesy operacyjne nadzorują pracownicy instytucji finansowej. W systemie Bitcoina

[426] Zob. m.in. P. Opitek, *Kryptowaluta jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6, s. 41–44.

[427] S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluta jako elektroniczny instrument płatniczy bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wrocław 2016, s. 111–112.

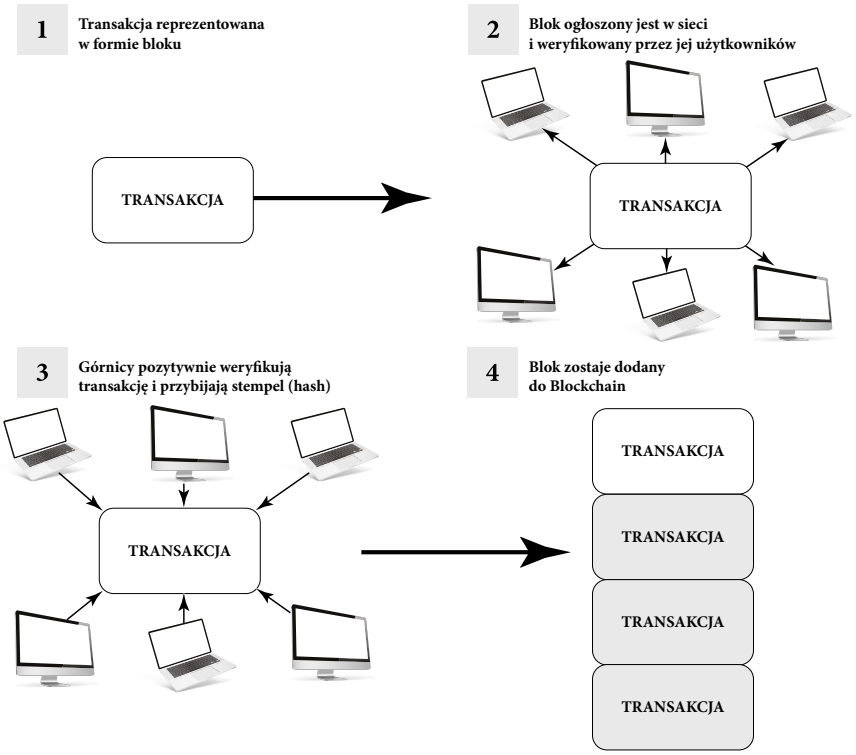
[428] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, Gdynia 2021, s. 37.

opisane zadania spełniają „górnicy" i budowane przez nich „kopalnie". „Górnicy" to osoby, które angażują swój sprzęt komputerowy po to, aby generował moc obliczeniową do wspierania pracy systemu blockchaina. W ich komputerach zapisana jest cała historia operacji związanych z przesyłaniem tokenów z jednego adresu na drugi. Każdy pełny węzeł blockchaina (ang. *full nodes*) stanowi kompletną bazę danych, a 16 lipca 2023 r. działały 16 724[429] węzły rozlokowane na całym świecie, głównie w Europie Zachodniej i Stanach Zjednoczonych. Węzeł, czyli de facto komputer sterowany przez specjalne oprogramowanie, magazynuje całą kopię blockchaina i powiększa ją samodzielnie wraz z pojawieniem się nowych operacji zatwierdzonych przez system. Każdy komputer podtrzymuje pracę sieci poprzez walidację transakcji, tj. zatwierdzanie przesyłów BTC w blokach, a więc kolejnych, powiązanych ze sobą bazach danych, zgodnie z zasadą konsensusu obowiązującą w systemie; pełne węzły są również odpowiedzialne za przekazywanie nowych transakcji i bloków do sieci[430]. Podsumowując, należy stwierdzić, iż w ramach sieci wiele komputerów łączy się ze sobą i realizuje proces konsensusu zarządzający obiegiem informacji w programie blockchain, a wszelkie interakcje między nimi są weryfikowane kryptograficznie. Za każdym razem, gdy zostanie osiągnięty konsensus, transakcja rejestruje się w bloku będącym repozytorium danych. Z fizycznego punktu widzenia faktyczny napęd dla łańcuchów bloków stanowią połączone w jedną sieć serwery wielu komputerów, które czerpią moc z energii elektrycznej[431].

[429] https://bitnodes.io/ [dostęp: 16.07.2023].

[430] Obok „pełnych węzłów" sieci, zdecydowana większość osób korzystających z tego protokołu ma status „lekkich klientów", którzy nie przechowują lokalnej kopii całej historii łańcucha bloków i nie weryfikują transakcji.

[431] P. Opitek, K. Lenczowska-Soboń, *Tokeny NFT jako dzieło sztuki wykorzystywane do popełniania przestępstw*, [w:] *Taktyka i technika kryminalistyczna w zmieniającym się świecie,* [w:] *Kryminalistyka w zmieniającym się świecie. Wybrane zagadnienia,* red. D. Wilk, Wydawnictwo Naukowe FNCE, 2023, s. 123.



Grafika nr 17. System Bitcoina i realizacja transakcji przesyłania danych statuujących jednostki kryptowaluty o nazwie bitcoin z jednego adresu na drugi adres

Ze strony indywidualnego użytkownika sieci Bitcoin, narzędziem do zarządzania tokenami jest wspomniany już portfel. Nazwa ta zwiera w sobie oprogramowanie w formie prostej do obsługi aplikacji przechowującej klucze prywatne, a więc zapisy liczb umożliwiające transferowanie posiadanych jednostek waluty wirtualnej poprzez tworzenie podpisu cyfrowego. Najbezpieczniejszy dla użytkownika jest portfel sprzętowy, mający postać pendrive'a podłączanego do komputera tylko w momencie wysyłania posiadanych bitcoinów na inne adresy, gdyż transfer tokenów na adres tego portfela nie wymaga, aby działał on w trybie online (po podłączeniu do Internetu uaktualni on stan swojego adresu). Odmienną postać ma portfel papierowy, na którym zapisuje się dane do uwierzytelnienia transakcji. Tak więc osoba chcąca przelać bitcoina na inny adres i dysponująca portfelem elektronicznym, wpierw dokonuje odpowiednich ustawień w aplikacji (podaje docelowy adres, wartość waluty wirtualnej do przesłania, opłatę transakcyjną) i naciska funkcję „wyślij". Informacja o transakcji jest „rozgłaszana" w sieci, a zatem wiedzę o niej uzyskują wszystkie węzły protokołu Bitcoina, które następnie muszą zatwierdzić zlecenie, aby zmiana właściciela BTC doszła do skutku. W tym celu stosowany jest model osiągania konsensusu, w którym do ustalania najdłuższego

łańcucha, a tym samym aktualnego stanu rozliczeń w protokole, budowane są kolejne bloki, stanowiące historię wszystkich przepływów tokenów pomiędzy adresami od momentu powstania sieci aż do chwili obecnej[432]. Bloki zorganizowane są w takiej formie, że każdy z nich połączony jest nierozerwalnym, cyfrowym „węzłem" z poprzednim (wcześniejszym) i późniejszym blokiem, tworząc w ten sposób blockchain – nierozerwalny łańcuch bloków.

Chociaż w uproszczeniu mówi się, że transakcja dotyczy przekazania pewnej liczby danej jednostki kryptowaluty z jednego adresu lub wielu adresów na inny adres lub adresy[433], to w rzeczywistości między adresami przekazywane są klucze do zarządzania tokenami, a zapis danych informatycznych utożsamiających bitcoiny znajduje się w blokach. Na skutek zatwierdzonej transakcji, same jednostki kryptowaluty nie przemieszczają się pomiędzy portfelami (adresami) w sieci, ale operacje rozliczane są we wspólnej dla wszystkich, transparentnej cyfrowej księdze nazywanej blockchainem (stan adresu portfela faktycznie odzwierciedla tylko zapisy znajdujące się w łańcuchu bloków). Zatem, teoretycznie rzecz biorąc, gdyby rejestr bloków został zniszczony, to portfele użytkowników łańcucha stałyby się bezużyteczne, a przesyłanie między nimi kryptowaluty niemożliwe. Przypomina to sytuację anihilacji wszystkich serwerów systemu bankowego, na których zapisane są środki pieniężne, co spowodowałoby unicestwienie architektury transakcyjnej pieniądza bezgotówkowego.

Poczynione wyżej ustalenia determinują specyficzny opis czynu zabronionego, którego przedmiotem jest „kradzież" kryptowaluty, o czym będzie jeszcze mowa. Z punktu widzenia pracy prokuratora natomiast bardzo ważne jest ustalenie, jakim portfelem dysponuje sprawca przestępstwa i gdzie go przechowuje, gdyż pozwala to na realizację zabezpieczenia majątkowego na kryptowalutach oraz (być może) ustalanie źródła pochodzenia i transferu zgromadzonych w aplikacji środków. Zasadą cyberprzestępców jest posiadanie wielu adresów, co zapobiega w pewien sposób możliwości śledzenia i kojarzenia realizowanych przez nich operacji. W sytuacji korzystania z wielu adresów jeden użytkownik widziany jest w systemie jako działanie wielu uczestników protokołu, co zwiększa jego anonimowość przez niwelowanie możliwości kojarzenia przelewów[434]. Oczywiście, w przypadku organów ścigania taka „wieloadresowość" przepływu środków znacznie utrudnia analizę kryminalną. Dlatego czynności postępowania przygotowawczego powinny być ukierunkowane na ujawnienia portfela użytkowanego przez przestępcę, a działania w tym kierunku zaczynają się już na etapie czynności operacyjno-rozpoznawczych. Komfortowa jest sytuacja, gdy sprawca podejmuje współpracę z organami ścigania i umożliwia dostęp do posiadanych zasobów tokenów. W przeciwnym razie odzyskanie waluty wirtualnej, którą dysponuje, może okazać się niemożliwe. Nigdy nie powinno się rezygnować z możliwości wykrywczych; w jednej sprawie

[432] Tamże, s. 123.
[433] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*…, s. 17.
[434] S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluta jako elektroniczny instrument płatniczy*…, s. 112–113.

okazało się np., że zatrzymany cyberprzestępca ukrył portfel sprzętowy w myszce do komputera i dopiero szczegółowe oględziny zabezpieczonego sprzętu pozwoliły na ujawnienie tego portfela.

5.2. Status prawny kryptoaktywów

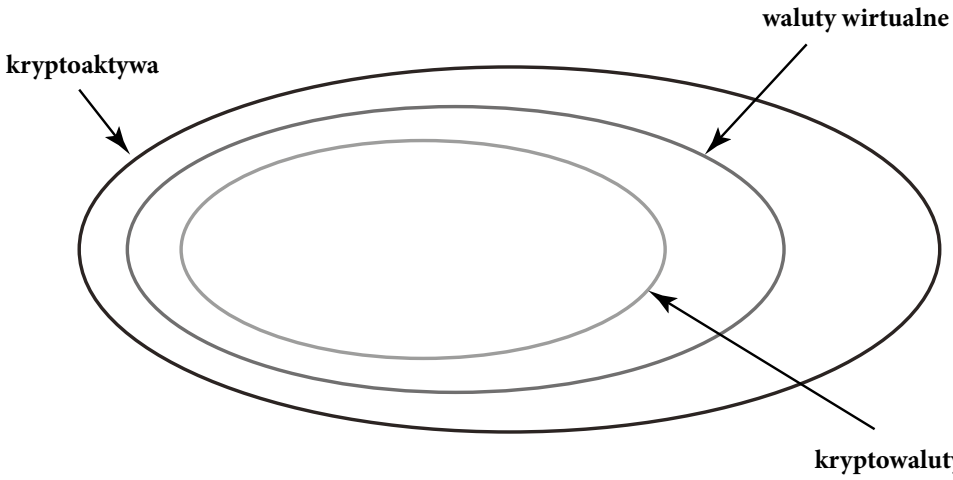
Określenie statusu tokenów cyfrowych na gruncie prawa karnego może być niekiedy problematyczne, ale z drugiej strony trudności z tym związane są wyolbrzymiane przez karnistów. Pojawiają się nawet głosy optujące za wprowadzeniem legalnej definicji kryptowalut lub kryptoaktywów, co zdaniem formułujących je osób, mogłoby przyczynić się do uproszczenia kwalifikacji prawnej przestępstw popełnianych z wykorzystaniem kryptoaktywów oraz stosowania instytucji prawa karnego procesowego w cyberprzestępczości[435]. Jednak w praktyce zabieg taki tylko zwielokrotniłby problemy z wykładnią i stosowaniem przepisów. Być może status prawny tokenów najbardziej zaawansowanych pod względem technologicznym i ekonomicznym, stanowiących pochodne instrumenty finansowe oparte na *smart contract*, wymaga pogłębionej analizy, jednak w większości przypadków tokeny cyfrowe, które pojawiają się w postępowaniach karnych, to bitcoiny oraz inne altcoiny, i prokuratorzy potrafią sobie z nimi radzić. Jeśli nawet w Internecie odnaleźć można setki, a nawet tysiące „coinów" o różnych nazwach, to funkcjonowanie większości z nich opiera się na zmodyfikowanym blockchainie Bitcoina i traktowane są na gruncie prawa karnego jako dane informatyczne. Warto natomiast określić, jaką stosować terminologię w nazewnictwie tokenów, gdyż w dyskursie prawniczym ważna jest unifikacja pojęć, których zakres determinowany jest przez regulacje prawne.

Najbardziej rozpoznawalną i najszerszą grupą kryptoaktywów są kryptowaluty na czele z bitcoinem i pozostałymi altcoinami: etherum, monero, dash, litecoin, zcash i inne. Szerszy zbiór desygnatów obejmuje pojęcie „waluty wirtualne", gdyż zawiera np. tokeny NFT, które nie są uważane za kryptowalutę. Dochodzą do tego tokeny niedziałające w oparciu o blockchain, np. skiny w grze Counter Strike czy cyfrowe artefakty bohaterów gier komputerowych. Najszersza jest nazwa „kryptoaktywa", do których zalicza się m.in. pochodne instrumenty finansowe funkcjonujące na rynkach regulowanych i nieregulowanych. Według serwisu coinlore.com[436] na dzień 22 lipca 2022 r. łączna liczba wszystkich kryptoaktywów umieszczonych na mniej lub bardziej zdecentralizowanych rejestrach

[435] M. Mariański twierdzi np., że „Ustawodawca powinien jednak, mając na względzie coraz bardziej postępującą wirtualizację życia gospodarczego, zmierzać do wytworzenia definicji terminologicznie neutralnych i uniwersalnych oraz na tyle pojemnych, aby mogły one obejmować swoim zakresem również te formy działalności, które jedynie w sensie funkcjonalnym do tworzonych definicji przystają". Zob. M. Mariański, *Ryzyka związane z rozwojem obrotu wirtualnymi walutami. Analiza na gruncie obecnie obowiązujących przepisów*, [w:] *Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania*, red. W. Pływaczewski, LEX 2015.

[436] https://www.coinlore.com/pl/all_coins [dostęp: 22.07.2022].

bloków wynosiła 10 442[437], kryptowalut przypominających bitcoina odnotowano 352, a pozostałych tokenów 4238. Rynek kryptoaktywów był wyceniony na łączną kwotę 1 105 494 358 138 dolarów amerykańskich. Faktem jest natomiast, że Unia Europejska zamierza pierwszy raz w historii objąć ramami prawnymi kryptoaktywa, ich emitentów oraz dostawców usług (np. administratorów portfeli przeznaczonych do przechowywania kluczy kryptograficznych). Parlament Europejski osiągnął porozumienie co do rozporządzenia w sprawie rynków kryptoaktywów (MiCA), a nowe regulacje, wprowadzające m.in. definicję legalną instytucji rynku kryptoaktywów, będą obowiązywać od 2024 r.



Grafika nr 18. Zakres wzajemnych relacji pomiędzy cyfrowymi tokenami określanymi jako: kryptowaluty, waluty wirtualne i kryptoaktywa

Analiza akt postępowań karnych ujawniła, że sędziowie i prokuratorzy w wydawanych decyzjach procesowych zamiennie stosują słowa: „kryptowaluty", „waluty wirtualne" i „kryptoaktywa", chociaż ich znaczenie jest różne[438]. Zdarzają się jeszcze inne „wytwory terminologiczne", jak chociażby określenie „waluty cyfrowe" w piśmie instruktażowym Prokuratury Krajowej dotyczącym zabezpieczenia majątkowego na

[437] Szybki wzrost liczny dostępnych w Internecie kryptoaktywów potwierdza fakt, że w 2019 r. platforma coinlore.com odnotowała ich około trzech tysięcy, a więc trzykrotnie mniej aniżeli w 2022 r.; źródło: P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*…, s. 15.

[438] Właściwe definiowanie rodzaju aktywa, o którym się pisze pod względem prawnym, jest zadaniem ważnym, ale nie zawsze przestrzeganym przez komentatorów; np. D. Skowron w rozdziale II *Definicja waluty cyfrowej* opracowania pt. *Bitcoin jako przedmiot zabezpieczenia w postępowaniu karnym* pisze, jakoby na gruncie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu obowiązywała definicja „walut cyfrowych", podczas gdy od początku obowiązywania tej ustawy mowa w niej o „walutach wirtualnych" (D. Skowron, *Bitcoin jako przedmiot zabezpieczenia w postępowaniu karnym*, „Prawo Karne i Kryminologia", Warszawa 2018, wydanie internetowe: https://iws.gov.pl/analizy – i – raporty/raporty/#prawokarne2018 [dostęp: 12.07.2022]).

walutach wirtualnych[439]. Warto zatem opisać, czym jest waluta wirtualna, a następnie, jaki status w prawie karnym mają jednostki kryptowaluty.

Spośród takich nazw, jak „waluty wirtualne", „kryptowaluty" czy „bitcoin", tylko pierwsza z wymienionych doczekała się definicji legalnej. Zgodnie z art. 2 ust. 2 pkt 26 u.p.p.p.[440] pod tym pojęciem rozumie się cyfrowe odwzorowanie wartości, które nie jest:

1. prawnym środkiem płatniczym emitowanym przez NBP[441], zagraniczne banki centralne lub inne organy administracji publicznej;
2. międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące;
3. pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[442];
4. instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi;
5. wekslem lub czekiem

— oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego.

Ustawowa definicja walut wirtualnych stanowi dosłowne tłumaczenie z języka angielskiego terminu *virtual currencies* (VA) wprowadzonego przez Financial Action Task Force (FATF[443]) i przeniesionego do projektu V dyrektywy Unii Europejskiej z dnia 30 maja 2018 r. dotyczącej uregulowań AML/CFT[444]. FATF w swoich rekomendacjach podkreśla, że owa definicja powinna być interpretowana szeroko, a wchodzące w jej skład pojęcia mają otwarty charakter po to, aby uwzględniały postęp technologiczny

[439] Pismo Zastępcy Dyrektora Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z czerwca 2023 r. dotyczące zabezpieczenia majątkowego na kryptowalutach, znak: 1001 – 12.024.4.2023 (zbiory własne autora).

[440] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124. 1285), dalej jako: u.p.p.p.

[441] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.). Zgodnie z art. 32 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz. U. z 2022 r. poz. 492, 655) „Znaki pieniężne emitowane przez NBP są prawnymi środkami płatniczymi na obszarze Rzeczypospolitej Polskiej".

[442] Zgodnie z art. 2 pkt 21a) ustawy pieniądz elektroniczny to wartość pieniężna przechowywana elektronicznie, w tym magnetycznie, wydawany, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowany przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego.

[443] Financial Action Task Force (FATF) utworzył w 1989 r. Międzynarodowy Fundusz Walutowy i skupia obecnie 37 krajów członkowskich. Celem Grupy jest definiowanie standardów i promowanie środków prawnych do zwalczania prania pieniędzy, finansowania terroryzmu i innych poważnych zagrożeń dla integralności globalnego systemu finansowego. Chociaż FATF nie decyduje wprost o przyjętych przez poszczególne kraje rozwiązaniach w zakresie AML/CFT, to de facto ma zasadniczy wpływ na ich kształt.

[444] Uzasadnienie do rządowego projektu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, s. 12–13, https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2233 [dostęp: 30.10.2022]. Skrót „AML/CFT" (ang. *Anti Money Laundering/Counter Financing of Terrorism*) stanowi zbiorcze określenie przepisów i zasad, które muszą stosować instytucje obowiązane w celu zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu.

i innowacyjne modele biznesowe związane z cyfrowymi prawami majątkowymi. Stanowi to zaletę wspomnianej definicji, ale z drugiej strony powoduje w praktyce wątpliwości interpretacyjne, na co wskazał Trybunał Sprawiedliwości UE[445]. Ponadto formuła VA bazuje na zasadzie „neutralności technologicznej", co oznacza, że interpretacja pojęcia *virtual currencies* powinna być stosowana w oparciu o właściwości, jakie oferuje komercyjna usługa, a nie pod kątem technologii zastosowanej do jej uruchomienia[446].

Przechodząc na grunt krajowy, to definicja z art. 2 ust. 2 pkt 26 u.p.p.p. wyraźnie oddziela pojęcie walut wirtualnych od „tradycyjnych" aktywów typu pieniądze, akcje czy obligacje, nadając takim walutom nowy charakter prawny. I chociaż zgodnie z „Zasadami techniki prawodawczej"[447] przepisy ustawy redaguje się zwięźle i syntetycznie, unikając nadmiernej szczegółowości, a zarazem w sposób, w jaki opisuje się typowe sytuacje występujące w dziedzinie spraw regulowanych tą ustawą (§ 5); ponadto przepisy powinny być redagowane tak, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy (§ 6), to w przypadku definicji legalnej walut wirtualnych dokładne spełnienie tych postulatów było zadaniem bardzo trudnym, a wręcz niewykonalnym. Zbyt duża jest bowiem różnorodność wspomnianych walut pod względem technicznym, ekonomicznym i prawnym, aby „zamknąć" je w prostej definicji, tym bardziej że polski ustawodawca, wprowadzając do porządku prawnego art. 2 ust. 2 pkt 26 u.p.p.p., był zobowiązany kierować się pojęciem *virtual currencies*.

Przechodząc do szczegółowej analizy art. 2 ust. 2 pkt 26 u.p.p.p.[448], najciekawsze, ale także najtrudniejsze zadanie stanowi ustalenie znaczenia następujących zwrotów zawartych w definicji walut wirtualnych:

1. „cyfrowe odwzorowanie wartości",
2. „wymienialne w obrocie gospodarczym na prawne środki płatnicze",
3. „akceptowane jako środek wymiany",
4. wartość „może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego".

„Odwzorować" znaczy tyle, co „odtworzyć według wzoru"; natomiast „wartość" oznacza: „to, ile coś jest warte pod względem materialnym", ale też „cechę tego, co jest dobre pod jakimś względem", „posiada zalety"[449]. Zatem „cyfrowe odwzorowanie wartości" walut wirtualnych to cyfrowe odtworzenie według wzoru posiadanych przez te

[445] Wyrok Trybunału Sprawiedliwości z dnia 22 października 2015 r., C – 264/14, Skatteverket przeciwko Davidowi Hedqvistowi, https://eur – lex.europa.eu/legal – content/pl/ALL/?uri=CELEX:62014CJ0264 [dostęp: 23.09.2022].

[446] *Virtual Assets and Virtual Asset Service Providers. Updated guidance for a risk – based approach*, October 2021, s. 23 (dokument w zbiorach autora).

[447] Obwieszczenie Prezesa Rady Ministrów z dnia 29 lutego 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie „Zasad techniki prawodawczej" (Dz. U. z 2016 r. poz. 283).

[448] Autor uznał, że zbędne jest pisanie o tym, czym jest prawny środek płatniczy emitowany przez NBP, pieniądz elektroniczny, weksel, czek itd., gdyż dokładnie opisują to właściwe ustawy i komentarze do tych ustaw.

[449] https://sjp.pwn.pl/szukaj/warto%C5%9B%C4%87.html [dostęp: 30.10.2022].

waluty cech, a patrząc pod kątem subiektywnym – także ich niedoskonałości i/lub zalet. Z treści przepisu wynika, że waluty wirtualne *per se* są „jakąś" wartością, podobnie jak pieniądze, instrumenty finansowe czy pieniądz elektroniczny, ale nie taką samą wartością jak inne, wymienione w definicji aktywa. Chodzi o pewien rodzaj dobra ekonomicznego rozumianego jako usługa zaspokajająca potrzeby człowieka (np. kapitałowe, inwestycyjne) i będąca rezultatem procesu szeroko rozumianej produkcji (realizacja crowdfundingu w ramach start-upu, emisja stablecoina przez instytucję finansową, zamieszczenie otwartego protokołu blockchainowego w sieci itp.)[450]. Z komentowanego przepisu wynika ponadto, że waluty wirtualne, owo dobro ekonomiczne, mają postać cyfrową. Jak słusznie zauważa K. Stolarski, tzw. własność wirtualna zawsze będzie w istocie pewną formą cyfrowej reprezentacji kodu komputerowego, a więc nie powinno się jej interpretować w tradycyjnych kategoriach rozumienia prawa własności czy też władztwa[451].

Bitcoin pod względem technicznym stanowi „jedynie" kawałek kodu programu komputerowego. Nie ma w nim żadnego zapisu wskazującego na cenę tokena lub innej informacji, która mówiłaby o jego wartości rynkowej. Niezależnie, czy BTC kosztowałby kilkaset tysięcy złotych, czy nie posiadałby żadnej wartości, jego cyfrowy zapis będzie zawsze wyglądał tak samo. Zatem „odwzorowanie wartości", o którym mowa w art. 2 ust. 2 pkt 26 u.p.p.p., nie dotyczy ceny waluty wirtualnej, ale mechanizmu (algorytmu) funkcjonowania tych walut, pośrednio wpływającego na ich cenę. Niemniej, praktycznie rzecz biorąc, waluty wirtualne posiadają realną wartość rynkową, co wiąże się z pozostałymi ich cechami: uczestnictwem w obrocie gospodarczym i akceptowalnością. Mówiąc wprost: nikt nie interesowałby się daną „wartością", gdyby nie posiadała zalet ekonomicznych. Jednak w przypadku walut wirtualnych chodzi o realne dobro mające substrat majątkowy, gdyż odnosi się do nich instytucja wstrzymywania transakcji i blokady rachunków, o której mowa w rozdziale 8 u.p.p.p.: zgodnie z art. 2 ust. 2 pkt 27 u.p.p.p. przez wartość majątkową rozumie się m.in. waluty wirtualne. Stanowią one także przedmiot transakcji, o której mowa w art. 2 ust. 2 pkt 21 u.p.p.p.; w jej wyniku dokonuje się przeniesienia własności lub posiadania wartości majątkowych. Poczynione rozważania prowadzą do wniosku, że chociaż zapis: „cyfrowe odwzorowanie wartości" nie odnosi się do terminu „wartość" w znaczeniu „to, ile coś jest warte pod względem materialnym", ale do *essential features* danej waluty wirtualnej, a więc uzyskanie statusu waluty wirtualnej nie jest uzależnione od posiadania przez walutę konkretnej ceny

[450] P. Opitek, G. Ocieczek, *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum. Kwartalnik Naukowy Krajowej Rady Sądownictwa" 2022, nr 3–4, s. 129.

[451] K. Stolarski, *Prawny i podatkowy status walut wirtualnych w kontekście wprowadzenia do prawa polskiego definicji legalnej waluty wirtualne*, „Monitor Podatkowy" 2018, nr 9, wydanie internetowe: https://czasopisma.beck.pl [dostęp: 07.06.2023].

rynkowej, to de facto waluty wirtualne są traktowane przez ustawodawcę jako prawo majątkowe o niejednoznacznym charakterze[452].

Waluty wirtualne są „wymienialne w obrocie gospodarczym na prawne środki płatnicze". Zakres znaczeniowy określenia „środki płatnicze" jest regulowany przez ustawę z dnia 27 lipca 2002 r. – Prawo dewizowe. Zgodnie z nią:

1. krajowymi środkami płatniczymi są waluta polska oraz papiery wartościowe i inne dokumenty pełniące funkcję środka płatniczego, wystawione w walucie polskiej (art. 2 ust. 1 pkt 6 u.p.d.);
2. zagranicznymi środkami płatniczymi są waluty obce i dewizy (art. 2 ust. 1 pkt 9 u.p.d.); z kolei:
   a. walutami obcymi są znaki pieniężne (banknoty i monety) będące poza krajem prawnym środkiem płatniczym, a także wycofane z obiegu, lecz podlegające wymianie; na równi z walutami obcymi traktuje się wymienialne rozrachunkowe jednostki pieniężne stosowane w rozliczeniach międzynarodowych (art. 2 ust. 1 pkt 10 u.p.d.);
   b. dewizami są papiery wartościowe i inne dokumenty pełniące funkcję środka płatniczego, wystawione w walutach obcych (art. 2 ust. 1 pkt 12 u.p.d.).

Nie jest konieczne omawianie w tym miejscu każdego z prawnych desygnatów pojęcia „środek płatniczy", ale uwagę należy skupić, w aspekcie definicji „walut wirtualnych", na ich atrybucie: „wymienialne w obrocie gospodarczym", o którym mowa w art. 2 ust. 2 pkt 26 u.p.p.p.

Pojęcie obrotu gospodarczego nie ma charakteru normatywnego, wobec czego jego wyjaśnienie pozostawiono doktrynie prawniczej. Zjawisko obrotu gospodarczego należy do świata pojęć ekonomii – stosunki wymiany dóbr i usług, będące przejawem prowadzonej przez przedsiębiorców działalności, podlegają bowiem prawom rynku. W tym sensie prawo gospodarcze prywatne ma swoje korzenie w ekonomicznej aktywności jednostek oraz grup społecznych i zawiera katalog reguł rządzących obrotem towarami i usługami na linii od producenta do konsumenta. Tym samym do obrotu gospodarczego należą stosunki prywatnoprawne, zachodzące w toku prowadzonej działalności gospodarczej. Według innego, syntetycznego ujęcia, przez obrót gospodarczy należy rozumieć stosunki prywatnoprawne powstające w związku z prowadzeniem przedsiębiorstwa[453], a więc działalności o charakterze zorganizowanym, łączącej w sobie składniki materialne oraz niematerialne w uporządkowaną całość funkcjonalno-gospodarczą. W piśmiennictwie zwraca się również uwagę, że profesjonalna działalność to uczestniczenie w obrocie gospodarczym w sposób uzasadniający przekonanie, że ma się do czynienia z samodzielnym podmiotem zarobkowym trudniącym się świadczeniem

[452] P. Opitek, G. Ocieczek, *Analiza definicji walut wirtualnych*…, s. 129–130.

[453] A. Doliwa, *Ogólna charakterystyka prawa gospodarczego prywatnego*, [w:] *Zasady prawa gospodarczego prywatnego*, red. T. Mróz, M. Stec, Warszawa 2007, s. 80.

dla innych[454]. Podobnie w orzecznictwie sądowym wykrystalizował się pogląd, że obrót gospodarczy jest miejscem, gdzie przedsiębiorcy prowadzą działalność gospodarczą; obok zawodowego charakteru działalności, powtarzalności podejmowanych czynności, czy podporządkowania regułom zysku i opłacalności, „obrót" stanowi jedną ze specyficznych cech prowadzenia takiej działalności[455]. Widać zatem, że zarówno doktryna, jak i sądy uznały sferę obrotu gospodarczego za miejsce, gdzie przedsiębiorca prowadzi swoją działalność gospodarczą.

Wynika z tego, że kryptoaktywo stanowi walutę wirtualną, gdy jest wymienialne na prawne środki płatnicze przez przedsiębiorców w ramach prowadzonej przez nich działalności gospodarczej. Chodzi przede wszystkim o giełdy i kantory kryptowalutowe, ale także platformy crowdfundingowe, rynek zdecentralizowanych finansów (DeFi), czy strony internetowe do tradingu, a więc przez podmioty posiadające pewną zorganizowaną strukturę, których działalność jest widoczna i rozpoznawalna dla otoczenia poprzez np. otwarcie kantoru lub prowadzenie platformy cyfrowej w sieci. Inna wskazówka mówiąca o tym, czy akceptant tokena jest profesjonalnym uczestnikiem rynku, to wypełnienie przez niego prawnego obowiązku rejestracji lub zgłoszenia. W Polsce chodzi o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej albo do rejestru przedsiębiorców Krajowego Rejestru Sądowego lub innego rejestru wskazanego w ustawie szczególnej. Funkcjonuje także rejestr działalności w zakresie walut wirtualnych (art. 129m u.p.p.p.) oferowany podmiotom, o których mowa w przepisie art. 2 ust. 1 pkt 12 u.p.p.p. *A contrario*, „wartość" znajdująca się w użytkowaniu wyłącznie przez konsumentów nie może być uznana za walutę wirtualną, chociaż w praktyce taka sytuacja jest mało prawdopodobna, bowiem każde dobro atrakcyjne dla większej liczby osób od razu wzbudza zainteresowanie profesjonalnych „graczy" na rynku, którzy chcą zarobić i pośredniczyć w obrocie tym dobrem[456].

Owi profesjonalni uczestnicy rynku „krypto" często pochodzą spoza Europy i działają transgranicznie, a więc sprawdzenie, czy posiadają status przedsiębiorcy, jest trudne. Nie ma to jednak decydującego znaczenia dla określenia, czy uczestniczą oni w obrocie gospodarczym, gdyż miarodajny jest faktyczny obraz ich działalności: platforma cyfrowa, która posiada tysiące użytkowników, jest ogólnodostępna, oferuje profesjonalne usługi w zakresie obrotu tokenami cyfrowymi – uczestnicy w obrocie gospodarczym w takim znaczeniu, o jakim mowa w art. 2 ust. 2 pkt 26 u.p.p.p. Jeśli określone wartości są notowane na platformach internetowych, a osoby indywidualne i prawne mogą je sprzedać lub kupić za pieniądz fiducjarny, to spełniają definicję walut wirtualnych.

[454] J. Grykiel, *Pojęcie działalności gospodarczej i zawodowej w rozumieniu art. 43(1) k.c.*, „Studia Prawnicze" 2005, nr 4, s. 31.

[455] Uchwała Sądu Najwyższego z dnia 23 lutego 2005 r., III CZP 88/04, OSNC 2006/1, poz. 5, uchwała Sądu Najwyższego z dnia 6 grudnia 1991 r., III CZP 117/91, OSNC 1992/5, poz. 65, postanowienie Sądu Najwyższego z dnia 1 lipca 2021 r., III USK 223/21, LEX nr 3380183, wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z dnia 8 kwietnia 2021 r., I SA/Po 229/21, LEX nr 3172268.

[456] P. Opitek, G. Ocieczek, *Analiza definicji walut wirtualnych*…, s. 131–133.

Obrót gospodarczy bowiem ma charakter mieszany, gdyż stosunki prawne kreowane są na podstawie czynności dokonywanych przez strony, z których jedna może być przedsiębiorcą, a druga konsumentem. „Wymienialność" oznacza natomiast, że token („wartość") na podstawie różnorodnych zdarzeń prawnych pomiędzy uczestnikami obrotu gospodarczego (umowa sprzedaży, zastawu, zamiany, pożyczki itd.) może zostać wymieniony na prawny środek płatniczy[457].

Zgodnie z przepisem zamieszczonym w art. 2 ust. 2 pkt 26 u.p.p.p., „waluta wirtualna" to aktywo, które jest wymienialne w obrocie gospodarczym na prawne środki płatnicze, a ponadto „akceptowane jako środek wymiany". Akceptować, zgodnie z językowym znaczeniem tego słowa, oznacza tyle, co „aprobować", „wyrażać formalną zgodę na coś"[458]. Spójnik łączny pomiędzy dwiema cechami użytkowymi walut wirtualnych, tj. wymienialność i akceptowalność, oznacza, że muszą być one spełnione jednocześnie, aby można było mówić o takiej walucie. Warto jednak zadać pytanie: Jaka jest różnica pomiędzy sytuacją, że „coś" jest wymienialne w obrocie gospodarczym i zarazem akceptowane jako środek wymiany?

Logicznie rzecz biorąc, w obu wyrażeniach chodzi o identyczną sytuację: jeśli coś można wymienić, to oznacza, że ktoś (druga strona umowy) akceptuje taką wymianę. Założenie „racjonalnego ustawodawcy", a więc takiego, który nie dodaje do przepisów ustawy treści zbędnych, nakazuje jednak poszukiwać sensownego wytłumaczenia dla komentowanej konstrukcji. Zapis „akceptowane jako środek wymiany" należy odczytywać w ten sposób, że pewna część rynku, pod względem ilości podmiotów lub wolumenu transakcji, akceptuje daną „wartość" i dlatego spełnia ona definicję „waluty wirtualnej".

Teoretycznie można wyobrazić sobie sytuację, że niektóre rodzaje kryptoaktywów są akceptowane jako środek wymiany, ale tylko przez osoby indywidualne nie prowadzące działalności gospodarczej, a co za tym idzie – nie są „wymienialne w obrocie gospodarczym na prawne środki płatnicze". Jednak w praktyce, jeśli większa grupa osób interesuje się danymi tokenami, a ponadto jest gotowa za nie zapłacić, to zaczynają one „funkcjonować własnym życiem" w cyberprzestrzeni, są listowane na giełdach kryptowalutowych i uzyskują konkretną cenę. Ich emisja przyjmuje postać ICO (ang. *Initial Coin Offering*) lub IPO (ang. *Initial Public Offering*) i prowadzona jest pod nadzorem profesjonalnych programistów, prawników i managerów. Tak więc posiadanie przez określony rodzaj waluty wirtualnej przymiotu „akceptowalnego środka wymiany" może być wynikiem celowego działania osób, które powołały do życia dany projekt, ale także niezamierzonym skutkiem rozwoju „wartości". J. Ryfa podaje przykład tzw. złota używanego przez uczestników gry komputerowej World of Warcraft. Wydawca gry, firma Blizzard Entertainment, zaplanowała jej system monetarny w ten sposób, aby „złoto" nie miało zastosowania poza światem gry, i zrezygnowała z mechanizmu

[457] Tamże, s. 133–134.

[458] https://sjp.pwn.pl/slowniki/akceptowa%C4%87.html [dostęp: 30.10.2022].

umożliwiającego jego bezpośrednią wymianę na pieniądze lub inne cyfrowe artefakty. Nie przeszkodziło to graczom nadać „złotu" realną wartość i znaleźć metodę na jego dystrybucję poza systemem World of Warcraft. Obecnie duża liczba graczy uczestniczy w wymianie cyfrowego „złota" na pieniądze w sposób nieoficjalny, tj. za pośrednictwem aukcji internetowych[459]. Zdaniem autora, „złoto" pochodzące z World of Warcraft spełnia tym samym definicję waluty wirtualnej, o której mowa w art. 2 ust. 2 pkt 26 u.p.p.p.

Ostatni z czterech składników definicji legalnej „waluty wirtualne"; „odwzorowanie wartość" może być dodatkowo:

1. elektronicznie przechowywany lub przeniesiony albo
2. stanowić przedmiot handlu elektronicznego.

W pierwszym przypadku chodzi o sytuację, gdy cechy techniczne systemu podtrzymującego funkcjonowanie „wartości" pozwalają na jej „istnienie" *in se* w postaci cyfrowej. Typowym przykładem są bitcoiny, których cyfrowe odzwierciedlenie znajduje się w księdze rozrachunkowej nazywanej protokołem Bitcoina, a instrumenty do zarządzania nimi, tzw. klucze, przesyłane są w Internecie pomiędzy użytkownikami systemu (nawet jeśli klucz zapisany jest „na papierze", to wykonanie transferu BTC z jednego adresu na drugi wymaga przetworzenia klucza w programie komputerowym). Z kolei „handel elektroniczny", określany mianem e-commerce, nie został zdefiniowany w przepisach prawa, ale oznacza on „transakcje przeprowadzane przez sieci, oparte na protokole IP i przez inne sieci komputerowe"[460]. Chodzi o działalność polegającą na kupowaniu oraz sprzedawaniu towarów i usług w sieci za pomocą komputerów (laptopa, smartfona itd.). Wymóg ten spełniają: „złoto" pochodzące z gry World of Warcraft i skiny w grze Counter Strike. Ostatnimi z wymienionych artefaktów można handlować na popularnych platformach cyfrowych, takich jak Allegro, dmarket.com lub csgo.fandom.com, a ceny skinów dochodzą nawet do kilku tysięcy dolarów. Skiny przesyłane są na specjalne wirtualne konta Steam zakładane indywidualnie przez graczy, chociaż cały system transferów i zarządzania nimi funkcjonuje na podstawie innej technologii, aniżeli blockchain[461].

Przykład kreacji waluty wirtualnej na rynku krajowym stanowiła działalność spółki, którą zajmował się Wojewódzki Sąd Administracyjny w Gdańsku. Zamierzała ona zebrać środki na finansowanie działalności poprzez przeprowadzenie crowdfundingu kryptowalutowego w formie tzw. ICO. W tym celu wyemitowała token użytkowy pod nazwą X wydawany osobom, które wspierały projekt, dokonując wpłat pieniężnych lub kryptowalutowych na rzecz spółki. Za otrzymane środki emitent budował platformę internetową, przeznaczoną do udzielania odpłatnych porad online z zakresu prawa, realizacji zleceń dotyczących przygotowania pism procesowych i reprezentowania

[459] J. Ryfa, *Waluty wirtualne – problem zdefiniowania i klasyfikacji nowego środka płatniczego*, „Nauka o Finansach" 2014, nr 2, s. 143.

[460] Handel elektroniczny, https://stat.gov.pl/metainformacje/slownik – pojec/pojecia – stosowane – w – statystyce – publicznej/1778,pojecie.html [dostęp: 30.09.2022].

[461] P. Opitek, G. Ocieczek, *Analiza definicji walut wirtualnych*…, s. 134–136.

przed sądem. Planowano, że cena usługi uiszczana będzie tokenami X funkcjonującymi w oparciu o technologię blockchain. System posiadał dwie grupy użytkowników: doradzających prawników oraz ich klientów. Spółka zakładała ponadto, że wyemitowane tokeny będą notowane i sprzedawane na zewnętrznych giełdach kryptowalutowych, a więc staną się autonomicznym prawem majątkowym niezależnym od emitenta. Tokeny X miały uzyskać status środka płatniczego użytkowanego przez osoby indywidualne i podmioty gospodarcze, niepowiązane ze spółką, gdyż posiadacz tokenów nie nabywał żadnych uprawnień korporacyjnych w spółce, a ona sama nie była zobowiązana do wykupu wyemitowanych przez siebie artefaktów[462].

Jest kilka zasadniczych powodów, dla których prokurator powinien znać definicję walut wirtualnych i potrafić dokonać wykładni jej części składowych. Otóż, podstawą efektywnego prowadzenia śledztwa dotyczącego kryptoaktywów jest ustalenie, z jakimi cyfrowymi wartościami majątkowymi ma się do czynienia, a w szczególności, czy są to waluty wirtualne. Potwierdzenie, że rzeczywiście tak jest, otwiera przed organami ścigania nowe źródła dowodowe. Wykorzystanie takich źródeł uzależnione jest od znajomości mechanizmów, którymi rządzi się system AML w stosunku do instytucji obowiązanych prowadzących działalność gospodarczą polegającą na świadczeniu usług w zakresie walut wirtualnych (art. 2 ust. 1 pkt 12 u.p.p.p.). Podmioty takie mają obowiązek m.in. sporządzenia i stosowania wewnętrznej procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Przepis art. 50 u.p.p.p. enumeratywnie wymienia, co zawiera procedura AML, z uwzględnieniem charakteru, rodzaju i rozmiaru działalności prowadzonej przez przedsiębiorcę, a całe podejście do bezpieczeństwa finansowego opiera się na szacowaniu ryzyka. Tym ryzykiem jest potencjalna możliwość zaktualizowania się zagrożenia, łącznie z popełnieniem przestępstwa, w stosunku do konkretnego klienta instytucji obowiązanej w ramach świadczonych przez nią usług. Ryzyko może być określone jako minimalne i wtedy nie wymaga się stosowania szczególnych środków ostrożności; jednak w momencie, gdy stwierdzi się wysoki poziom ryzyka, to zostają wdrożone wzmożone środki bezpieczeństwa finansowego, wnikliwie są badane źródła pochodzenia środków, ustalany jest beneficjent rzeczywisty itd., co skutkować może decyzją o zaprzestaniu współpracy z klientem. Na samym początku nawiązania stosunków gospodarczych instytucja obowiązana dokonuje identyfikacji przyszłego kontrahenta, która polega przede wszystkim na zebraniu podstawowych informacji o nim, określonych w art. 34 u.p.p.p., oraz poznaniu jego tożsamości, o czym mowa w art. 37 u.p.p.p. W czasie trwania współpracy z określoną osobą dostarczyciel produktów i usług w zakresie walut wirtualnych prowadzi monitoring transakcji dokonywanych przez klientów, a więc rejestruje i przechowuje informacje o wpłatach środków na rachunek bankowy operatora, czasie i wysokości przelewów,

[462] Uzasadnienie do wyroku Wojewódzkiego Sądu Administracyjnego w Gdańsku z dnia 28 kwietnia 2020 r., I SA/Gd 275/20, Legalis, nr 2393242.

danych identyfikujących rachunek i osobę, od której pochodzą aktywa, oraz aktualnym saldzie na rachunku[463].

W metodyce realizacji czynności procesowych w sprawach dotyczących walut wirtualnych, której autor był merytorycznym konsultantem, wskazano, że prokurator może wystąpić z następującymi pytaniami do podmiotu gospodarczego zajmującego się walutami wirtualnymi:

1. Czy w zachowaniu klienta pojawiły się symptomy mogące świadczyć o prowadzeniu przez niego nielegalnej działalności z wykorzystaniem zasobów i bazy logistycznej instytucji obowiązanej (np. giełdy kryptowalutowej) poprzez:
   a. posługiwanie się wieloma rachunkami bankowymi i adresami walut wirtualnych zarejestrowanymi na inne osoby;
   b. wielokrotne przewalutowanie środków zgromadzonych na rachunkach lub konwersji pomiędzy pieniądzem, a walutami wirtualnymi bez sprecyzowanego celu biznesowego;
   c. korzystanie przez klienta z bankomatów, wpłatomatów, kryptobankomatów lub innych urządzeń umożliwiających anonimowe wpłaty/wypłaty gotówki i walut wirtualnych (szczególnie jeśli nie miało to racjonalnego uzasadnienia w profilu transakcyjnym klienta lub wykonywanej przez niego działalności zawodowej);
   d. wykorzystywanie do transakcji („wejścia" lub/i „wyjścia") niestandardowych metod płatności, takich jak Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram;
   e. anulowanie przez klienta zlecenia transakcji w momencie powzięcia przez niego wiadomości, że zaszły przesłanki do jej raportowania GIIF-owi lub wystosowania przez instytucję obowiązaną zawiadomienia do organów ścigania o podejrzeniu popełnienia przestępstwa.
2. Zapytanie, czy klient:
   a. w relacjach handlowych ukrywał prawdziwe dane osobowe?
   b. posługiwał się rachunkiem (np. płatniczym, bankowym, walut wirtualnych) założonym na inną osobę?
   c. podawał się za kogoś innego w kontaktach z pracownikami instytucji obowiązanej?
   d. przedkładał dokumenty wzbudzający zastrzeżenia, co do ich autentyczności lub rzetelności?
   e. podał numer telefonu należący do innej osoby?
   f. logował się na konta osób trzecich?
   g. odmawiał przedłożenia określonych dokumentów lub podania źródła pochodzenia środków?
   h. korzystał z wpłat lub wypłat bankomatowych z zaangażowaniem środków na giełdzie?
   i. w jeszcze inny sposób utrudniał działanie instytucji obowiązanej?

[463] J. Skała, *Uzyskiwanie przez prokuratora – na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – informacji i danych od instytucji obowiązanych*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2020, nr 3, s. 86, 90.

3. Prokurator ma prawo:
   a. zwrócić się do instytucji obowiązanej o przedstawienie informacji w formie analitycznej, czy w relacjach z klientem odnotowano anomalia transakcyjne w jego zachowaniu (np. zlecanie przelewów środków tylko w godzinach nocnych, logowanie się do systemu instytucji obowiązanej z adresów IP obsługiwanych przez sieć TOR, używanie przez klienta narzędzi typu VPN-y, PROXY); jeśli tak, to kiedy i czym były one spowodowane oraz jak obsłużono alert bezpieczeństwa dotyczący tych anomalii;
   b. zlecić wykonanie dodatkowych czynności weryfikacyjnych i sprawdzających w stosunku do klienta na potrzeby toczącego się śledztwa (np. czy przelewał środki do rajów podatkowych lub krajów objętych sankcjami);
   c. zażądać udzielenia informacji, z jakich usług i produktów finansowych/kryptowalutowych (szczególnie nietypowych) korzystał klient;
   d. zażądać przedłożenia indywidualnej (obowiązującej oraz historycznej, jeśli ulegała zmianie) oceny ryzyka przypisanego dla klienta, który jest objęty prowadzonym śledztwem.
4. Zgodnie z art. 129m u.p.p.p. podmioty zawiadujące działalnością w zakresie walut wirtualnych mają obowiązek uzyskania wpisu do rejestru działalności prowadzonej w tym zakresie. Prokurator powinien sprawdzić, czy podmiot pozostający w jego zainteresowaniu uzyskał taki wpis; jeśli tak, to należy zwrócić się do Dyrektora Izby Administracji Skarbowej w Katowicach o przedłożenie wszelkich informacji i danych, w tym kserokopii lub oryginałów dokumentów, związanych z wpisem oraz zgromadzonych w stosunku do konkretnego podmiotu[464].

Przykładowy, jak podaje J. Skała, ogólny schemat wykorzystania informacji uzyskanych od instytucji obowiązanej mógłby wyglądać następująco: w dostarczonej prokuratorowi opinii biegły wskazał, że w zbadanej przez niego pamięci dowodowego komputera ujawnił ślady połączeń nawiązywanych z internetową giełdą kryptowalutową, tj. podmiotem, o którym mowa w art. 2 ust. 1 pkt 12 u.p.p.p. W złożonych zeznaniach świadek zaprzeczył jednak, aby posiadał wiedzę o funkcjonowaniu tokenów cyfrowych i korzystał z nich. W celu zweryfikowania treści zeznań prokurator może zwrócić się do giełdy o udzielenie informacji na temat połączeń realizowanych z adresu IP dedykowanego zabezpieczonemu komputerowi z giełdą w ciągu ostatnich 5 lat oraz przedstawienie aktywności transakcyjnej osoby, która za pomocą ustalonego IP dokonywała połączeń. W konkretnym śledztwie, na podstawie informacji zwrotnej od instytucji obowiązanej, być może potwierdzi się, że świadek jednak łączył się z giełdą, posługując się danymi osobowymi tzw. słupa, zlecał liczne wymiany bezgotówkowego pieniądza bankowego na bitcoiny, które następnie przesyłał na ustalony adres portfela. Analiza rachunku bankowego, który użytkowała na giełdzie osoba pozostająca w zainteresowaniu

[464] E. Przewłoka, *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Wydział do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Bydgoszczy, Bydgoszcz 2023 (zbiory własne autora).

prokuratora, może doprowadzić do konkretnego banku i udowodnić, że wpływające na rachunek środki pochodziły z ataków hakerskich[465]. Warto dodać, że w bazach instytucji obowiązanych da się weryfikować wszelkie informacje i dane powiązane z konkretną osobą: jej dane osobowe, numer telefonu, adresy mailowe itd.

W pojęciu „waluty wirtualne" mieszczą się „kryptowaluty" na czele z bitcoinem jako tokeny, które najczęściej pojawiają się w *modus operandi* sprawców przestępstw teleinformatycznych. Jednak odmiennie, jak w przypadku wartości opisanych w art. 2 ust. 2 pkt 26 u.p.p.p., zwrot „kryptowaluty" nie posiada definicji ustawowej, chociaż za jej wprowadzeniem do prawa karnego, a nawet uchwaleniem specjalnej „ustawy komplementarnie regulującej materię kryptowalut w polskim porządku prawnym"[466], opowiadali się niektórzy przedstawiciele doktryny. Jednak sformułowanie uniwersalnej definicji dla kilkudziesięciu tysięcy artefaktów jest niemożliwe, gdyż ich właściwości techniczne, a przede wszystkim status prawny, mogą się różnić. Nie wnoszą wiele do praktycznych działań z kryptowalutami ich definicje formułowane w doktrynie, takie jak chociażby J. Liberackiego. Twierdzi on, że kryptowaluta to pewien nie fizyczny, ale cybernetyczny twór pozanormatywny, a jednocześnie nadaje on kryptowalutom status „środków płatniczych"[467]. Mało konkretne jest określenie „cybernetyczny twór pozanormatywny", ale przede wszystkim kryptowaluty nie są środkiem płatniczym, o jakim mowa w art. 310 k.k.

Na podstawie przeprowadzonych badań J. Charatynowicz twierdzi, że kryptowaluty to rodzaj waluty cyfrowej, cyfrowa reprezentacja wartości, oparta na publicznym kodzie źródłowym, z rozproszonym i zdecentralizowanym charakterem emisji, używającej kryptografii do weryfikacji i realizacji konwersji, która w pewnych okolicznościach może pełnić funkcje płatnicze i inwestycyjne[468]. Pobieżna analiza przytoczonej definicji pokazuje już, że występują w niej pojęcia nieostre i problematyczne. Nie każdy kod źródłowy protokołów ma charakter open source; prywatne kryptowaluty to np. Monero i Verge. Zwrot „pewne okoliczności" nie spełnia wymogu określoności, który obowiązuje w prawie karnym, i zasady techniki legislacyjnej zabraniają umieszczania takich pojęć w przepisach prawa. W końcu, duża część kryptowalut działa na mniej lub bardziej scentralizowanych rejestrach.

W orzecznictwie można spotkać różne wypowiedzi na temat tego, czym jest bitcoin lub szerzej ‑ kryptowaluta, chociaż nie nadają się one do bezpośredniego stosowania w prawie

[465] J. Skała, *Uzyskiwanie przez prokuratora*…, s. 93.

[466] A. Petrys, *Bitcoin – współczesna alternatywa wobec pieniądza fiducjarnego w perspektywie postępowania karnego*, „Palestra" 2022, nr 5, wydanie internetowe: https://palestra.pl/pl/czasopismo/wydanie/5 – 2022/artykul/bitcoin – wspolczesna – alternatywa – wobec – pieniadza – fiducjarnego – w – perspektywie – postepowania – karnego [dostęp: 12.07.2022].

[467] J. Liberacki, *Karnoprawne aspekty walut kryptograficznych (bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2019, r. XXIII, nr 3, s. 167.

[468] J. Charatynowicz, *Kryptowaluty jako zagrożenia i wyzwania dla bezpieczeństwa finansowego państwa,* rozprawa doktorska, Akademia Sztuki Wojennej, Wydział Bezpieczeństwa Narodowego, praca niepublikowana, (w zbiorach autora), s. 44, 59.

karnym. Trybunał Sprawiedliwości UE w wyroku z dnia 22 października 2015 r.[469] określił bitcoina jako rodzaj nieobjętych regulacjami pieniędzy cyfrowych, emitowanych i kontrolowanych przez osoby, które je tworzą, oraz używanych i akceptowanych przez członków danej społeczności wirtualnej. Waluta taka charakteryzuje się dwukierunkowym przepływem, umożliwiającym dokonywanie sprzedaży i zakupu bitcoina zgodnie z obowiązującym kursem. Różni się od pieniądza elektronicznego, ponieważ jej kapitał wyraża się w cyfrowej (abstrakcyjnej) jednostce rozliczeniowej, a nie pieniądzu[470]. Jeśli chodzi o administrację publiczną, to na temat charakteru prawnego kryptowalut, a szczególnie BTC, wypowiadały się organy podatkowe, sądy administracyjne i Ministerstwo Finansów. W piśmie z 2015 r. ministerstwo stwierdziło, iż zasady posługiwania się walutami wirtualnymi nie zostały skodyfikowane w przepisach prawa i w konsekwencji ocena prawna dotycząca charakteru cywilnoprawnego i prawnopodatkowego transakcji zawieranych przy użyciu walut wirtualnych może zostać dokonana wyłącznie w odniesieniu do konkretnej operacji, po zapoznaniu się ze stanem faktycznym oraz poszczegółowej analizie treści kontraktu[471]. Jednak dla ustalenia natury bitcoina w prawie karnym decydujące znaczenie będzie miało odwołanie się do prawa cywilnego, ponieważ decyzje administracyjne, wydawane zazwyczaj na potrzeby podatkowe, zbytnio utożsamiają kryptowaluty z prawnymi środkami płatniczymi. Przepisy Kodeksu karnego operują natomiast cywilistycznymi terminami: „rzecz ruchoma" i „prawo majątkowe", chociaż ich znaczenie zostało nieco zmodyfikowane.

W prawie cywilnym dominuje stanowisko, że bitcoin stanowi prawo podmiotowe; dotyczy ono mienia, o którym mowa w art. 44 k.c.: „Mieniem jest własność i inne prawa majątkowe"[472]. W Kodeksie cywilnym zakres pojęcia „prawo majątkowe" należy rozumieć bardzo szeroko i obejmuje ono także pewne stany faktyczne, z których wynikają konkretne uprawnienia lub roszczenia mające wartość majątkową. Odpowiada to naturze kryptowalut, których znaczenie w stosunkach międzyludzkich opiera się tylko i wyłączne na woli stron, nadającej tokenom wartość majątkową, a nie bezwzględnie obowiązujących przepisach prawa[473]. BTC nie jest natomiast rzeczą opisaną w art. 45 k.c., ale konglomeratem elementów prawnorzeczowych i prawnoobligacyjnych, gdyż stanowi zbywalne prawo majątkowe. Biorąc pod uwagę techniczne aspekty jego funkcjonowania, to bitcoin nie może być przedmiotem własności, ale zawiera się w majątku osoby uprawnionej jako prawo podmiotowe względne, czyli wierzytelność. Nad bitcoinem nie sposób roztoczyć władztwa faktycznego, ale można objąć klucze prywatne, do których prawo podmiotowe osoby utytułowanej ma charakter wyłączny, co wiąże się

[469] C – 264/14 przeciwko D. H. (opublikowano: ZOTSiS 2015/10/I – 718).
[470] Wyrok Naczelnego Sądu Administracyjnego z dnia 11 marca 2021 r., II FSK 3296/18, LEX nr 3229870.
[471] Pismo Ministerstwa Finansów z dnia 28 maja 2015 r. prezentujące wyjaśnienia Ministerstwa Finansów w przedmiocie funkcjonowania walut wirtualnych, sygn. FN7.054.9.2015, Regulacje dotyczące wirtualnej waluty Bitcoin, LEX, dalej jako: Pismo z 28 maja 2015 r.
[472] Zob. A. Zacharzewski, *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21.
[473] P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia...*, s. 46.

z powszechnym (*erga omnes*) zakazem naruszania klucza prywatnego przez osoby trzecie[474]. Charakter kryptowaluty jako niematerialnego prawa majątkowego wielokrotnie potwierdził w swoich wyrokach Naczelny Sąd Administracyjny, pisząc m.in., że chociaż brak jest ustawowej definicji kryptowaluty, to w doktrynie i judykaturze panuje zgoda, że stanowi ona zbywalne, niematerialne prawo majątkowe. Kryterium uznania prawa za majątkowe stanowi bowiem „typowy interes" majątkowy, jaki realizuje posiadanie i obrót bitcoinami. BTC ma zdolność generowania wartości majątkowej, co powoduje, że może być i jest przedmiotem obrotu, w tym czynności prawnych *inter vivos* i *mortis causa*[475].

Przechodząc do konkretnych przestępstw popełnianych z użyciem waluty wirtualnej, stwierdzić należy, że tokeny cyfrowe są coraz powszechniej wykorzystywane przez przestępców, a więc siłą rzeczy stanowią ważne zagadnienie w pracy sędziów, prokuratorów, funkcjonariuszy policji oraz przedstawicieli innych służb i agencji ochrony prawa. Notuje się nieustanny wzrost liczby przestępstw dokonywanych z udziałem takich tokenów, co potwierdziły m.in. badania spraw karnych z lat 2014–2019 przeprowadzone przez autora we wszystkich jednostkach powszechnych prokuratury[476]. Ze względu na system monetarny i potencjał inwestycyjny interesują się nimi także Narodowy Bank Polski, Ministerstwo Finansów, Komisja Nadzoru Finansowego i Urząd Ochrony Konkurencji i Konsumentów.

Status kryptowaluty w ujęciu karno-kryminalistycznym	Stan faktyczny
Informacja	**W toku czynności operacyjno-rozpoznawczych dotyczących przestępstwa prania pieniędzy uzyskano informację z giełdy kryptowalutowej, że ustalona osoba założyła na giełdzie konto i na przypisany do konta adres wpłynęły bitcoiny pochodzące z włamania na serwer innej wirtualnej giełdy. Determinuje to podjęcie szeregu czynności, łącznie z udostępnieniem materiałów do śledztwa w celu dokonania zabezpieczenia majątkowego na BTC pochodzących z przestępstwa.**

[474] Drugie stanowisko, reprezentowane przez J. Szewczyka, głosi, że bitcoin jest dobrem cyfrowym, a także dobrem ekonomicznym, ale nie może stanowić składnika mienia w rozumieniu art. 44 k.c. Uzasadnieniem tego poglądu jest twierdzenie, że kryptowaluta stanowi element sfery faktów, a nie rzeczywistości normatywnej, a zatem w świetle prawa cywilnego nie może być zaliczany jako składnik mienia. Uzyskanie klucza publicznego, na którym znajduje się określony bitcoin, oraz klucza prywatnego do niego jest kwestią faktów i w taki sposób powinno być określane przez system prawny. Bitcoin nie jest ani przedmiotem materialnym, ani rzeczą. Może on być jednak przedmiotem pewnych praw, ale sam w sobie nie jest żadnym prawem. Natomiast dysponowanie określonym adresem publicznym, jak również kluczem prywatnym, pozwalającym na posługiwanie się bitcoinem, stanowi korzystną sytuację faktyczną (dysponenta właściwych kluczy) o wymiernej wartości majątkowej i może być uznane za składnik mienia.

[475] Wyrok Naczelnego Sądu Administracyjnego z dnia 10 lutego 2021 r., II FSK 2870/18, LEX nr 3212191; podobnie: wyrok Naczelnego Sądu Administracyjnego z dnia 11 marca 2021 r., II FSK 3296/18, LEX nr 3229870.

[476] Szczegółowe wyniki badań zob.: P. Opitek, K. Góral, *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, „Prokuratura i Prawo" 2020, nr 5–6, s. 75.

Status kryptowaluty w ujęciu karno-kryminalistycznym	Stan faktyczny
Ślad	**W trakcie realizacji ekspertyzy zleconej na podstawie postanowienia prokuratora biegły z zakresu informatyki śledczej ujawnił na dysku twardym dowodowego komputera ślady cyfrowe świadczące o tym, że użytkownik komputera miał zainstalowany elektroniczny portfel kryptowalutowy i dokonywał szeregu transferów jednostek kryptowaluty na adres publiczny, na którym, jak wynika z przekazanych biegłemu materiałów śledztwa, były deponowane bitcoiny pochodzące z ataków ransomware.**
Dowód	**Na podstawie ekspertyzy dysku twardego dowodowego komputera biegły we wnioskach końcowych opinii stwierdził, że użytkownik laptopa miał zainstalowany portfel elektroniczny, na który wpływały transfery kryptowalutowe z podanych w opinii adresów, a bitcoiny były przesyłane z portfela na adres oznaczony w aktach sprawy jako służący do przyjmowania środków pochodzących z ataków ransomware.**
Przedmiot ochrony	**Integralność danych informatycznych, prawo majątkowe.**
Przedmiot czynności wykonawczej	**Jednostki kryptowaluty jako część systemu informatycznego, do którego sprawca uzyskuje dostęp bez uprawnienia (art. 267 § 2 k.k.), zapis na informatycznym nośniku danych (art. 268 § 2 k.k.), dane informatyczne (art. 268a § 1 k.k., art. 287 § 1 k.k.) i prawo majątkowe (art. 284 § 1 k.k.).**
Przedmiot zabezpieczenia majątkowego	**Ustanowienie zabezpieczenia majątkowego na kryptowalucie (art. 291 k.p.k. i nast.).**
Przedmiot poręczenia majątkowego	**Ustanowienie poręczenia na kryptowalucie (art. 266 k.p.k.).**

Tabela nr 1. Rola kryptowalut w postępowaniu karnym: ujęcie prawno-kryminalistyczne

Kryptowaluty stanowią przedmiot czynności wykonawczej w strukturze przestępstwa, na którym sprawca dokonuje czynu zabronionego, a innym razem wykorzystuje tokeny do realizacji *modus operandi,* żądając okupu w BTC. W pierwszym przypadku naruszone zostaje prawo własności lub posiadania bitmonet poprzez ich „kradzież", przywłaszczenie lub różnego rodzaju oszustwa. Jeszcze więcej sytuacji dotyczy zapłaty bitcoinami za nielegalne towary i usługi. W „pochodzie" instytucji kryminalistycznych, kryptowaluta pełni dodatkowo rolę informacji, gdyż na etapie czynności operacyjno-rozpoznawczych sam „sygnał" o tym, że ktoś interesuje się walutą wirtualną, może dać impuls do sprawdzenia „figuranta" pod kątem rozpracowywanej sprawy. Skutkuje to niejednokrotnie zabezpieczeniem sprzętu elektronicznego ze śladami cyfrowymi dotyczącymi transferów wykonanych tokenami, które mogą finalnie stać się dowodami

elektronicznymi. W podobnych sprawach stosuje się tymczasowe zajęcie mienia i zabezpieczenie majątkowe na walutach wirtualnych. Możliwe jest także poręczenie majątkowe przy użyciu BTC, chociaż w Polsce nie odnotowano jeszcze takiego przypadku. Jeśli dodać do tego skomplikowaną naturę prawną walut wirtualnych, to prowadzenie postępowania karnego z ich udziałem wymaga nie tylko wiedzy prawniczej, ale także wykorzystania wiadomości specjalnych, którymi dysponują biegli z zakresu informatyki śledczej. W takich sprawach udział biegłych w śledztwie jest konieczny szczególnie w sytuacji, gdy postępowanie ma charakter rozwojowy, a zatrzymanie sprawcy czynu zabronionego realnie możliwe. Niestety, w znacznej liczbie przypadków, dotyczących np. ataków ransomware i phishingu, ustalenie osób naruszających prawo jest trudne, czynności dowodowe ograniczają się do przesłuchania pokrzywdzonego i pozostaje tylko wydanie postanowienia o umorzeniu śledztwa na podstawie art. 322 § 1 k.p.k.[477]

5.3. „Kradzież" bitcoina

Ustalić należy, czy bitcoin/Bitcoin może stać się przedmiotem kradzieży z art. 278 k.k., a treść odpowiedzi zależy od tego, czy mowa jest o bitcoinie, a więc jednostce kryptowaluty, czy też o programie komputerowym Bitcoin. Aby Bitcoin stał się przedmiotem kradzieży, musiałby stanowić element cudzego mienia, a tymczasem jest on oprogramowaniem typu open source, a więc ogólnodostępną bazą danych otwartą dla każdego, kto chce się z nią zapoznać, przechowywać na swoim komputerze i użytkować łańcuch bloków. Co więcej, przyjmuje się, że im większa liczba osób tworzy nowe węzły Bitcoina, tym bardziej umacnia się cyberbezpieczeństwo całej sieci. Wynika z tego, że osoba, która „ukradłaby" jedną z równorzędnych kopii bitcoinowego blockchaina poprzez fizyczne przejęcie nośnika danych lub zdalnie ściągnęła taką kopię z innego komputera, nie wypełniłaby znamion przestępstwa opisanego w art. 278 § 2 k.k., chociaż w pierwszym przypadku przedmiotem zamachu byłoby mienie w postaci nośnika danych, a w drugim nieuprawniona manipulacja danymi w systemie informatycznym osoby trzeciej. Bitcoin nie posiada centralnego administratora nadającego uprawnienia do przechowywania lub użytkowania programu. Podobnie sprawa ma się z innymi blockchainami publicznymi typu: Ethereum, Litecoin, Bitcoin Gold, czy Ethereum Classic. Niemniej, są to rozważania czysto teoretyczne, ponieważ podstawą funkcjonowania Bitcoina jest ogólnoświatowe rozproszenie jego identycznej bazy danych (*nodów*) liczonych w tysiącach egzemplarzy. Na chwilę obecną wydaje się zadaniem niewykonalnym, aby przejąć fizycznie wszystkie komputery podtrzymujące pracę systemu lub w sposób zdalny „ściągnąć" z nich historię transakcji, wykasowując zapisy na pierwotnych nośnikach danych. Gdyby tak się stało, to sprawca mógłby ponieść odpowiedzialność za zakłócenie pracy systemu teleinformatycznego i sieci teleinformatycznej (art. 269a k.k.). Jeśli

[477] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*, [w:] *Wokół kryminalistyki. Nauka i praktyka, Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, red. D. Zienkiewicz, Toruń 2021, s. 245.

destrukcyjne działania dotyczyłyby danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej czy jednostki państwowej lub samorządowej, to wchodzi w grę odpowiedzialność karna z art. 269 k.k., gdyż niektóre blockchainowe projekty związane są z działalnością organów publicznych.

Na świecie funkcjonują jednak kryptowaluty, czy szerzej – kryptoaktywa, których działanie opiera się na mniej rozbudowanych, prywatnych protokołach typu Ripple i Hyperledger. Oprogramowanie closed source to zastrzeżony i zamknięty dla osób postronnych kod źródłowy, który nie jest rozpowszechniany publicznie. Prawo do jego kopiowania, modyfikowania, aktualizowania i edytowania posiadają tylko twórcy/właściciele oprogramowania i osoby przez nich upoważnione. Funkcjonowanie blockchaina prywatnego może opierać się zaledwie na kilku komputerach, które zawierają historię transakcji i pracują dla podtrzymania całego systemu. W takim przypadkach osoba, która ściągnęłaby podobny program bez zgody twórcy lub zarekwirowała urządzenia systemu z jego kodem źródłowym, mogłaby wypełnić znamiona przestępstwa z art. 278 § 2 k.k. Rozważania takie mają charakter teoretyczny, gdyż w działalności organów ścigania praktyczne znaczenie ma „kradzież" bitcoina pisanego małą literą, a więc wycinka kodu programistycznego nazwanego tokenem. Najprostsza postać owej „kradzieży" polega na przetransferowaniu środków z portfela pokrzywdzonego na adres przestępcy.

Jeśli program komputerowy o nazwie Bitcoin stanowi zamknięty algorytm łączący w sobie różnego rodzaju dane informatyczne, to klucze publiczne i prywatne są wycinkiem takich danych. To cyfrowe hasła umożliwiające elektroniczne podpisywanie transakcji kryptowalutowych; jako fragment kodu informatycznego, klucze dają dostęp do bitcoinowego protokołu, a więc pozwalają na identyfikację konkretnego tokena i zarządzanie artefaktem. Nie sposób zatem zakwalifikować bitcoina jako programu komputerowego, tak samo nie jest on „rzeczą ruchomą [478]. Definicja karnoprawna rzeczy ruchomej, chociaż o bardzo ekstensywnym charakterze, jest zasadniczo zbieżna z rozumieniem tego pojęcia na gruncie art. 44 k.c.[479] Zgodnie z art. 115 § 9 k.k. „Rzeczą ruchomą lub przedmiotem jest także polski albo obcy pieniądz lub inny środek płatniczy, środek pieniężny zapisany na rachunku oraz dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce". Bitcoina jako jednostkę rozliczeniową zapisaną w blockchainie nie sposób podnieść, przesunąć czy organoleptycznie zmierzyć. Nie posiada on żadnych cech „rzeczy" w rozumieniu prawa cywilnego tak samo, jak nie posiada statusu pieniądza, środka płatniczego albo dokumentu. Nie stanowi zatem przedmiotu czynności wykonawczej opisanego w art. 278 § 1 k.k. i art. 279 § 1 k.k. Pomimo

[478] Por. A. Petrys, *Bitcoin – współczesna alternatywa*..., [za:] P. Czaplicki, *Wybrane przestępstwa gospodarcze związane z obrotem walutą Bitcoin w prawie polskim, Unii Europejskiej oraz Stanów Zjednoczonych*, „Studenckie Zeszyty Naukowe" 2017, nr 20, s. 42.

[479] A. Błachnio, *Res extra commercium jako przedmiot czynności wykonawczej przestępstwa przeciwko mieniu*, „Wojskowy Przegląd Prawniczy" 2017, nr 2, s. 54–55.

tego zbyt wiele decyzji procesowych zawiera błędną kwalifikację prawną czynu, tak jak gdyby bitcoin mieścił się w legalnej definicji art. 115 § 9 k.k.; poniżej opisano przykłady postanowień o umorzeniu dochodzenia wydanych przez Prokuraturę Rejonową Warszawa-Śródmieście w Warszawie, Prokuraturę Okręgową w Krośnie, Prokuraturę Rejonową dla Wrocławia-Krzyki Wschód we Wrocławiu, Prokuraturę Rejonową dla Wrocławia-Stare Miasto we Wrocławiu oraz Prokuraturę Okręgową w Olsztynie. Dokonano w nich nieprawidłowego opisu i kwalifikacji prawnej „kradzieży" BTC.

> w sprawie dokonanego w dn. 23 grudnia 2017 r. w sieci internet ominięcia w nieustalony sposób hasła do konta poczty elektronicznej o adresie /…/ i uzyskania w ten sposób bezprawnego dostępu do informacji na koncie, a następnie za pomocą uzyskanych informacji nieuprawnionego zalogowania się do serwisu /…/ i kradzież z konta Macieja S. kryptowaluty o wartości 3500 zł tj. o przestępstwo z art. 267 § 1 kk w zb. z art. 278 § 1 kk w zw. z art. 11 § 2 kk[480]

> w sprawie przełamania w dniu 3 stycznia 2018 r., w nieustalonym miejscu, elektronicznych zabezpieczeń konta prowadzonego w serwisie /…/ przez spółkę /…/ z siedzibą w Katowicach na rzecz T. W., a następnie zmiany zapisu danych informatycznych na tym koncie poprzez zlecenie operacji na kryptowalutach, w wyniku czego doszło do zaboru w celu przywłaszczenia 14,76 jednostki kryptowaluty BitCoin (BTC) na szkodę T. W. o wartości około 793 000 zł, co stanowi mienie znacznej wartości, tj. o przestępstwo z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 294 § 1 k.k. w zw. z art. 11 § 2 k.k.[481]

> w sprawie dokonanego w dniu 30 czerwca 2017r. w sieci internet przez nn sprawcę włamania się za pośrednictwem Wirtualnej Poczty /…/ na konto znajdujące się na portalu www./.../ i kradzieży znajdującej się tam kryptowaluty Etherum 1,37446989 jednostek o wartości 1500zł na szkodę /…/ tj. o czyn z art. 267 § 1 k.k. i art. 278 § 1 k.k. w zw. z art. 11 § 2 k.k.[482]

> w sprawie włamania w dniu 25 września 2018 roku w nieustalony miejscu, do systemu spółki /…/ poprzez uzyskanie nieuprawnionego dostępu do infrastruktury informatyczną i utworzenie zlecenia wypłat kryptowalut należących do firm /…/ w ilości 36.000 jednostek waluty LISK, co stanowi kwotę ok. 300.000 zł, waluty FURURCOIN w ilości 80.000 jednostek , co stanowi kwotę ok. 2.400.000 zł oraz

[480] Akta Prokuratury Rejonowej Warszawa-Śródmieście w Warszawie o sygn. PR 3 Ds. 106.2018.II.
[481] Akta Prokuratury Okręgowej w Krośnie o sygn. PO I Ds. 3.2018.
[482] Akta Prokuratury Rejonowej dla Wrocławia-Krzyki Wschód we Wrocławiu o sygn. PR 1 Ds. 1511.2017.

waluty BITCOIN w ilości 108 jednostek, co stanowi kwotę ok. 2.265.000 zł działając na szkodę w/w tj. o czyn z art. 279 § 1 k.k. w zw. z art. 267 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 k.k.[483]

w sprawie dokonanego w czasie od 31 stycznia do 4 lutego 2016 r. za pośrednictwem sieci internet w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru, uzyskania przez pokonanie zabezpieczeń serwisu i nieuprawnionego dostępu do kont użytkowników giełdy elektronicznej kryptowalut oraz konta technicznego serwisu /…/, a następnie kradzieży wirtualnych walut bitcoin oraz litecoin o łącznej szacunkowej wartości 622.500 zł na szkodę /…/ tj. o przestępstwo określone w art. 267 § 3 kk w zw. z art. 279 § 1 kk w zw. z art. 294 kk w zw. z art. 11 § 2 kk w zw. z art. 12 kk[484].

Oprócz podstawowego, wspomnianego już błędu czynionego przez prokuratorów, tj. kwalifikowania nieuprawnionego przejęcia kryptowaluty jako kradzieży lub kradzieży z włamaniem, przytoczone decyzje procesowe zawierają jeszcze inne nieprawidłowości. Chodzi o przyjmowanie zbiegu realnego pomiędzy art. 267 § 1 k.k. (267 § 3 k.k.) i art. 279 § 1 k.k., podczas gdy przełamanie zabezpieczenia należy do znamion kradzieży z włamaniem (postanowienia Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu i Prokuratury Okręgowej w Olsztynie). Gdyby jednak, zakładając teoretycznie, bitcoin był „rzeczą ruchomą", to w wyjątkowych okolicznościach doszłoby do popełnienia dwóch odrębnych czynów w przypadku włamania do portfela i kradzieży BTC. Można sobie wyobrazić sytuację, że sprawca najpierw przygotowuje się do ataku hakerskiego, używa wyrafinowanego programu w celu uzyskania informacji, do której nie jest uprawniony, i posługując się malware'em, otrzymuje dostęp do informacji zgromadzonych w komputerze pokrzywdzonego, a „przy okazji" otwiera portfel kryptowalutowy i po kilku dniach od ataku przetransferowuje z niego bitcoiny na specjalnie założony adres. W takiej sytuacji podlega rozważeniu zakwalifikowanie opisanego zachowania jako dwóch odrębnych czynów z art. 267 § 1 i 3 k.k. oraz art. 278 § 1 k.k. Jednak należy powtórzyć, że zapis na blockchainie – w przeciwieństwie do zapisu na rachunku bankowym – nie jest normatywnie rzeczą ruchomą, a więc nie może być przedmiotem czynności wykonawczej przestępstwa kradzieży.

W analizowanych postanowieniach nie wskazano, chociażby ogólnie, w jaki sposób doszło do przełamania albo ominięcia zabezpieczenia lub jak działało oprogramowanie lub urządzenie hakerskie; mowa jest tylko o „ominięciu w nieustalony sposób hasła", „przełamaniu (…) elektronicznych zabezpieczeń konta", „włamaniu się za pośrednictwem Wirtualnej Poczty", „włamaniu", czy „uzyskaniu [dostępu do kont giełdy

[483] Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 818.2019.
[484] Akta Prokuratury Okręgowej w Olsztynie o sygn. PO II Ds. 18.2017.

elektronicznej – przyp. autora] przez pokonanie zabezpieczeń serwisu". Taki zdawkowy opis *modus operandi* sprawców budzi wątpliwości co do właściwego rozpoznania przez organy ścigania sposobu działania przestępców i stosowanych przez nich narzędzi i metod omijania lub przełamywania zabezpieczeń. Dochodzi do tego kwestia stosowanej terminologii na określenie cyfrowych tokenów; widać bowiem całkowitą dowolność w tym zakresie, a język prawniczy powinien dążyć do ujednolicenia słownictwa opisującego identyczny rodzaj przedmiotu czynności wykonawczej. W decyzjach napisano o „kryptowalucie", „jednostkach kryptowaluty BitCoin", „wirtualnej walucie bitcoin", a nawet tokeny cyfrowe określono mianem „waluty", chociaż pod tą nazwą kryje się jednostka monetarna będąca podstawą systemu pieniężnego w Polsce, podczas gdy krytpowaluty nie stanowią znaków pieniężnych będących prawnym środkiem płatniczym.

Przechodząc do sedna problemu, a więc udzielenia odpowiedzi na pytanie o kwalifikację prawną „kradzieży" kryptowaluty, to wskazać należy na art. 287 § 1 k.k. jako właściwy do zastosowania. Autor w 2017 r. pisał o tym, że kryptowaluta to zapis cyfrowy i przestępstwa mające za przedmiot czynności wykonawczej bitcoiny powinny być penalizowane z przepisów zamieszczonych w rozdziale XXXIII k.k.; ewentualnie z przepisu łączącego w sobie ochronę dóbr prawnych, którymi są mienie i dane informatyczne. W opracowaniu pt. *Przegląd polskiego prawa w kontekście zastosowania technologii rozproszonych rejestrów oraz walut cyfrowych* z 19 stycznia 2017 r. napisano, że:

> przestępstwa godzące w dobro prawne, jakim jest prawo majątkowe w postaci jednostek walut cyfrowych, można podzielić na trzy grupy:
> 1. manipulowanie danymi teleinformatycznymi w środowisku wirtualnym bez bezpośredniego oddziaływania na psychikę ludzką i przedmioty materialne,
> 2. oddziaływanie na świadomość i wolę osoby celem doprowadzenia jej do niekorzystnego rozporządzenia mieniem,
> 3. przestępstwa realizowane w „realnym" świecie i noszące znamiona zamachu na mienie.
>
> Czyny zabronione mieszczące się w kategorii 2 i 3 mają „klasyczną" postać i ich kwalifikacja prawna nie powinna budzić wątpliwości. W pierwszej kolejności są to różnego rodzaju oszustwa w sieci celem wyłudzenia jednostek walut cyfrowych (art. 286 § 1 k.k.), często przy zastosowaniu zabiegów socjotechnicznych. Rzadziej może chodzić o kradzieże i przywłaszczenia nośników danych (rzeczy) z cyfrowym zapisem jednostek waluty cyfrowej (art. 278 § 1 k.k., art. 284 § 1 i 2 k.k.), rozbój i wymuszenie rozbójnicze mające na celu zabór mienia w postaci jednostek waluty cyfrowej (art. 280 k.k., art. 282 k.k.)[485].

Skomplikowany i doniosły praktycznie jest problem kwalifikacji przestępstw mających bezpośrednio za cel cyfrowe prawa majątkowe. Realizowane są one poprzez bezprawne manipulowanie danymi informatycznymi na różnym etapie ich przetwarzania,

[485] P. Opitek, *Kodeksowe prawo materialne oraz procesowe...*, s. 15–16.

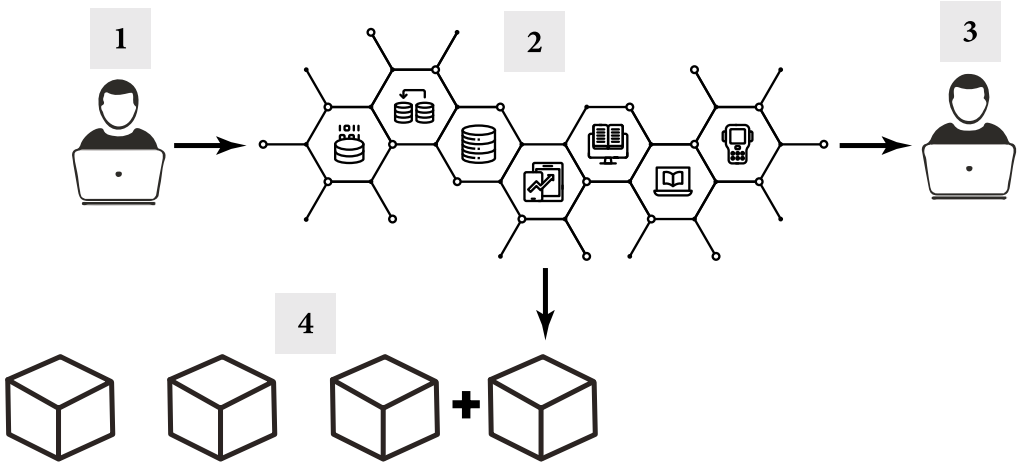
przybierając postać zmiany sekwencji znaków kodowych, usunięcia części z nich lub dodawania pewnych elementów niewystępujących w pierwotnej wersji zapisu, najczęściej w celu osiągnięcia przez sprawcę korzyści majątkowej. Może dochodzić do „włamań" do portfeli wirtualnych i wyprowadzenia z aplikacji jednostek kryptowaluty, ataków na giełdy i kantory sieciowe, zakłócania prawidłowej transmisji danych, fałszerstwa komputerowego zapisu informacji stanowiącego dokument. W tym zakresie zastosowanie znajdą przepisy art. 267 § 1–3 k.k., art. 268 § 2 k.k., art. 268a § 1 k.k. i art. 287 § 1 k.k. Handel na „czarnym rynku" w Internecie programami, narzędziami i hasłami umożliwiającymi popełnienie omawianych czynów zabronionych jest objęty penalizacją z art. 269b § 1 k.k. W przypadku ataku na łańcuch bloków o szczególnym znaczeniu dla funkcjonowania administracji państwowej i samorządowej lub organów państwa w grę wchodzi art. 269 § 1 i 2 k.k.[486] Mimo że od publikacji *Przeglądu polskiego prawa w kontekście zastosowania technologii rozproszonych rejestrów oraz walut cyfrowych* minęło już ponad sześć lat, to zawarte w raporcie ustalenia co do kwalifikacji prawnej przestępstw ukierunkowanych na kryptowaluty są nadal aktualne.

Przystępując do szczegółowego omówienia zastosowania art. 287 § 1 k.k. do „kradzieży" BTC, warto rozpocząć od stwierdzenia, że byt fizyczny bitcoina jest nierozerwalnie związany z funkcjonowaniem protokołu Bitcoina. Nie da się „oderwać" tokena od sieci i przekazywać go z pominięciem łańcucha bloków. System kryptowalut to rejestr przeprowadzonych transakcji, a faktyczne władztwo nad bitcoinem związane jest z posiadaniem tzw. klucza prywatnego. To ważne ustalenie w świetle realizacji znamion przestępstwa z art. 287 § 1 k.k., gdyż przepis ten mówi o „danych informatycznych": „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych". Pojęcie „danych informatycznych" oznacza zespół znaków (liter lub cyfr), ale bez określonej treści, który odgrywa funkcję związaną z przetwarzaniem danych w systemie informatyczny, łącznie z odpowiednim programem powodującym wykonanie tej funkcji przez system. Jakie zatem czynności na „danych informatycznych" realizowane są w każdym, także noszącym znamiona przestępstwa, bitcoinowym transferze? Aby przesłać jednostkę kryptowaluty z jednego adresu na drugi:

1. sprawca najpierw wprowadza w portfelu pokrzywdzonego odpowiednie ustawienia, które określają parametry planowanej operacji (wysokość transferowanych środków, opłaty transakcyjnej, adres docelowy); chodzi zazwyczaj o oznaczenie wszystkich jednostek znajdujących się w posiadaniu pokrzywdzonego, bowiem przestępca zamierza osiągnąć jak największy zysk z nielegalnego procederu. Już w momencie zarządzenia transakcji zmianie ulega zapis danych informatycznych

[486] Tamże.

w portfelu, a wraz z jej realizacją „znikną" klucze do zarządzania jednostkami kryptowaluty (punkt 1);
2. po zastosowaniu funkcji „wyślij" transakcja rozgłaszana jest w sieci i walidowana przez górników – pomiędzy węzłami następuje automatyczne przetwarzanie, gromadzenie i przekazywanie danych (punkt 2);
3. po „uzgodnieniu" transakcji operacja zostaje zaakceptowana przez węzły i zapisana w nowym bloku, a więc wprowadzony zostaje nieistniejący dotychczas zapis w protokole Bitcoina znajdującym się na tysiącach komputerów na świecie (punkt 4);
4. na końcu w portfelu odbiorcy transakcji pojawia się nowa wartość przesłanych do niego BTC, zatem ulega zmianie zapis danych informatycznych w drugim portfelu (punkt 3). W przypadku blockchaina Bitcoina w rzeczywistości transakcja jest jeszcze bardziej skomplikowana: podczas gdy większość kryptowalut działa podobnie do przelewów bankowych, przesyłając monety z jednego adresu na inny pojedynczy adres, to przelew BTC ma wiele wejść (In) i wyjść (Out)[487].



Grafika nr 19. Realizacja transakcji przesłania waluty wirtualnej bitcoin pomiędzy dwoma adresami

Realizacja transakcji określana mianem „kradzieży bitcoinów" powoduje zatem automatyczne przetwarzanie, gromadzenie i przekazywanie danych informatycznych w różnych miejscach systemu Bitcoina. Chodzi o zmianę wartości w co najmniej dwóch portfelach oraz wprowadzanie nowego zapisu takich danych w blockchainowym protokole, tj. w ostatnim bloku cyfrowej księgi rozrachunkowej. W praktyce działanie sprawcy może powodować nieuprawnioną modyfikację danych informatycznych w jeszcze innych miejscach, np. na serwerze giełdy kryptowalutowej, jeśli ona przechowywała klucze prywatne osoby pokrzywdzonej. Wynika z tego, że czynność sprawcza

[487] Odnośnie do szczegółów technicznych realizacji transakcji kryptowalutą bitcoin, ether, bitcoin cash, ripple, liecoin i monero patrz: P. Opitek, K. Góral, *Analiza kryminalna transferów kryptowalutowych*…, s. 14–21.

„kradzieży" kryptowaluty niesie ze sobą wiele jednostkowych modyfikacji danych informatycznych w różnych miejscach cyberprzestrzeni, ale ich szczegółowe wymienianie w opisie czynu jest niecelowe. Po pierwsze, czyniłoby to treść zarzutu zbyt obszerną, a w konsekwencji niezrozumiałą dla adresatów decyzji procesowych. Ponadto trudno wymagać od organu procesowego (sądu lub prokuratora), aby znał w szczegółach zawiłości technologiczne każdego protokołu statuującego kryptowaluty i kazuistycznie opisywał w zarzucie kolejne skutki oszukańczej transakcji. Teoretycznie sprawca może wykonać przelew w celu „wyrządzenia innej osobie szkody" i przesłać BTC na zupełnie przypadkowy adres publiczny, ale w praktyce działa on „w celu osiągnięcia korzyści majątkowej" i opis czynu oraz kwalifikacja prawna przestępstwa „kradzieży" 0,5 BTC może wyglądać następująco:

> J. K. jest oskarżony o to, że w dniu 1 stycznia 2023 r. w Krakowie działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia, wpłynął na automatyczne przetwarzanie i przekazywanie danych informatycznych w ten sposób, że wywołał transakcję przesłania danych informatycznych statuujących 0,5 bitcoina z portfela należącego do /…/ do swojego portfela i w ten sposób zmienił zapis w cyfrowej księdze rozrachunkowej Bitcoin oraz portfelu pokrzywdzonego działając na szkodę J. K. /…/ w wysokości 7 280 zł, co stanowiło równowartość 0,5 bitcoina w dniu 1 stycznia 2023 r., tj. o przestępstwo z art. 287 § 1 k.k.

> J. K. jest oskarżony o to, że w dniu 1 stycznia 2023 r. w Krakowie działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia, wpłynął na automatyczne przetwarzanie i przekazywanie danych informatycznych w ten sposób, że wywołał transakcję przesłania danych informatycznych reprezentujących 0,5 bitcoina z adresu pokrzywdzonego o nazwie /…/ na własny adres o nazwie /…/ i w ten sposób zmienił zapis w cyfrowej księdze rozrachunkowej Bitcoin oraz portfelu pokrzywdzonego działając na szkodę J. K. /…/ w wysokości 7 280 zł, co stanowiło równowartość 0,5 bitcoina w dniu 1 stycznia 2023 r., tj. o przestępstwo z art. 287 § 1 k.k.

„Kradzież" kryptowaluty nierzadko połączona jest z ominięciem lub przełamaniem zabezpieczenia elektronicznego i uzyskaniem dostępu do portfela kryptowalutowego osoby pokrzywdzonej, a następnie wykonaniem nieuprawnionej transakcji przelewu zgromadzonych w nim środków. Jeśli *modus operandi* sprawcy polegałby wpierw na włamaniu do portfela „przechowującego" bitcoiny, a następnie ich „kradzieży", to opis i kwalifikację prawną przestępstwa należałoby zmodyfikować w następujący sposób:

J. K. jest oskarżony o to, że w dniu 1 stycznia 2023 r. w Krakowie bez uprawnienia uzyskał dostęp do informacji dla niego nieprzeznaczonych zapisanych w portfelu do zarządzania kryptowalutami o nazwie /…/ poprzez ominięcie informatycznego zabezpieczenia portfela w postaci procedury uwierzytelniającej i wpisanie loginu i kodu należącego do J. K., a następnie działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia, wpłynął na automatyczne przetwarzanie i przekazywanie danych informatycznych w ten sposób, że wywołał transakcję przesłania danych informatycznych reprezentujących 0,5 bitcoina z adresu pokrzywdzonego o nazwie /…/ na własny adres o nazwie /…/ i w ten sposób zmienił zapis w cyfrowej księdze rozrachunkowej Bitcoin oraz portfelu pokrzywdzonego działając na szkodę J. K. /…/ w wysokości 7 280 zł, co stanowiło równowartość 0,5 bitcoina w dniu 1 stycznia 2023 r., tj. o przestępstwo z art. 267 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

J. K. jest oskarżony o to, że w dniu 1 stycznia 2023 r. w Krakowie działając w celu uzyskania informacji, do których nie był uprawniony, posłużył się oprogramowaniem typu „brute force", którego algorytm odszukał kombinację nazwy hasła dla przełamania elektronicznego zabezpieczenia aplikacji i uzyskania nieautoryzowanego dostępu do portfela kryptowalutowego o nazwie /…/ należącego do J. K., a następnie działając w celu osiągnięcia korzyści majątkowej, bez upoważnienia, wpłynął na automatyczne przetwarzanie i przekazywanie danych informatycznych w ten sposób, że wywołał transakcję przesłania danych informatycznych reprezentujących 0,5 bitcoina z adresu pokrzywdzonego o nazwie /…/ na własny adres o nazwie /…/ zmieniając zapis w cyfrowej księdze rozrachunkowej Bitcoin oraz portfelu pokrzywdzonego działając na szkodę J. K. /…/ w wysokości 7 280 zł, co stanowiło równowartość 0,5 bitcoina w dniu 1 stycznia 2023 r., tj. o przestępstwo z art. 267 § 1 i 3 k.k. oraz art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

Użyty w opisie czynu zwrot „zmienił zapis w cyfrowej księdze rozrachunkowej Bitcoina oraz portfelu pokrzywdzonego" może być także zastąpiony określeniem „zmienił zapis w systemie Bitcoin". Ów system definiowany jest przez A. Behana jako cały ekosystem, na który składają się urządzenia wraz z oprogramowaniem nim sterującym.

> Przez ekosystem – pisze A. Behan – należy rozumieć nie tylko dziesiątki tysięcy komputerów uczestniczących w sieci i walidujących transakcje, ale również każde z indywidualnych urządzeń wchodzących w jego skład – każdy komputer stacjonarny/przenośny, smartphone, tablet na którym zainstalowany mamy portfel w formie aplikacji desktopowej, czy mobilnej[488].

[488] A. Behan, *Waluty wirtualne jako*…, s. 603.

W tym znaczeniu system Bitcoin jako system informatyczny, a nawet teleinformatyczny, wyposażony będzie w różne urządzenia, na których dokonuje się transfer lub weryfikacja środków, komputery ASIC górników, komputery pełnego węzła przechowujące blockchainowy protokół oraz wszystkie inne części infrastruktury informatycznej np. routery, switche. W ujęciu takim system jest połączeniem warstwy sprzętowej (ang. *hardware*) i programowej (ang. *software*)[489].

Wśród decyzji o umorzeniu dochodzenia/śledztwa zdarzały się postanowienia, gdzie prawidłowo zastosowano art. 287 § 1 k.k.; prokurator Prokuratury Rejonowej w Chorzowie zatwierdził postanowienie o umorzeniu postępowania w sprawie:

> oszustwa komputerowego mającego miejsce w dniu 03 listopada 2017 roku w dotąd nieustalonym miejscu, gdzie sprawca w celu osiągnięcia korzyści majątkowej bez uprawnienia wprowadził nowy zapis danych informatycznych poprzez przełamanie zabezpieczeń do portalu /…/, a następnie dokonał przelewu wirtualnej waluty w ilości /…/ BTC powodując straty na szkodę /…/ w dotąd nieustalonej kwocie, tj. o przestępstwo określone w art. 287 § 1 k.k.[490]

Art. 287 § 1 k.k. nie zawiera zwrotu „oszustwo komputerowe" i błędem jest posługiwanie się w opisie czynu takimi nazwami. W momencie sporządzania postanowienia nie ustalono miejsca popełnienia przestępstwa, więc zwrot „w dotąd" jest zbędny. Znamię czynu z art. 287 § 1 k.k. zawiera się w zwrocie „bez upoważnienia", a napisano „bez uprawnienia". W analizowanym postanowieniu zawarto znamiona przestępstwa z art. 267 § 1 k.k. („poprzez przełamanie zabezpieczeń do portalu"), bez przywołania tego przepisu w kwalifikacji prawnej czynu. Pisząc o „wprowadzeniu nowego zapisu danych informatycznych", powinno się chociaż ogólnie wskazać, na czym działanie takie polegało i gdzie wprowadzono ów „nowy zapis".

Dane informatyczne do zarządzania kryptowalutami najczęściej są „przejmowane" przez sprawców poprzez manipulacje w portfelach indywidualnych uczestników rynku „krypto". Druga grupa ataków ukierunkowana jest na profesjonalne podmioty działające na rynku i dotyczy w pierwszej kolejności giełd kryptowalutowych, gdyż one przechowują klucze prywatne swoich klientów. Przedmiot nielegalnych działań na giełdzie będzie dotyczył bądź konta klienta, ale niekiedy może być ukierunkowany na serwer giełdy i potencjalny skutek ataku spowoduje utratę wszystkich jednostek kryptowaluty, którymi zarządza administrator platformy cyfrowej. Przykład stanowi czyn opisany w aktach Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu, gdzie toczyło się postępowanie w sprawie:

[489] Tamże, s. 602.

[490] Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 1 Ds. 1448.2017.

> wpływania w dniu 20 czerwca 2018 roku w nieustalonym miejscu za pomocą złośliwego oprogramowania na gromadzenie danych informatycznych zgromadzonych na serwerze spółki /…/ w celu osiągniecia korzyści majątkowej w kwocie 2000 dolarów liczonych w bitcoinach, tj. o czyn z art. 287 § 1 k.k.[491]

Z treści postanowienia wynika, że ustalono miejsce skutku w postaci „wpływania", a należało przyjąć, że skutek miał miejsce tam, gdzie ulokowany był serwer spółki, gdyż to on był przedmiotem działania sprawcy; nie ustalono natomiast miejsca jego pobytu. Kwalifikację prawną z art. 287 § 1 k.k. przywołano także w postanowieniu Prokuratury Rejonowej Katowice-Południe w Katowicach:

> w sprawie uzyskania w dniu 27 stycznia 2018 r. przez nieustaloną osobę w celu osiągnięcia korzyści majątkowej nieuprawnionego dostępu do konta użytkownika giełdy kryptowalutowej /…/ a następnie wykonania transakcji zakupu kryptowaluty BitCoin oraz przelewu wychodzącego zgromadzonych na tym koncie środków waluty BitCoin w ilości /…/ o łącznej wartości na dzień przelewu ok. 4000 zł na szkodę /…/, tj. o czyn z art. 287 § 1 kk[492].

Skoro z opisu czynu wynika, że sprawca, po uzyskaniu nieuprawnionego dostępu na konto użytkownika giełdy kryptowalutowej, zakupił bitcoiny za środki pieniężne zgromadzone na rachunku bankowym posiadacza konta, to doszło do popełnienia przestępstwa z art. 279 § 1 k.k., a nie z art. 287 § 1 k.k. Bitcoiny stanowiły w tym przypadku „owoc przestępstwa" tak samo, jak nie karze się sprawcy kradzieży z włamaniem za to, że wszedł w posiadanie rzeczy uzyskanej za pomocą czynu zabronionego (art. 291 § 1 k.k.). W tak doniosłej decyzji procesowej, jak postanowienie kończące postępowanie karne, nie powinno się pisać „ok.". Chociaż skróty przyjęte są na mocy pewnej konwencji i można skrócić prawie każdy wyraz, to należy postępować tak tylko wtedy, kiedy jest to naprawdę niezbędne. Podobna sytuacja nie występuje w momencie sporządzania wyroku lub decyzji kończącej postępowanie przygotowawcze, które można przygotować bez pośpiechu i budować wypowiedź organu procesowego w taki sposób, aby odznaczała się „dostojną" formą i wzbudzała u jej adresatów szacunek oraz respekt dla wymiaru sprawiedliwości[493]. Nieprawidłowe zastosowanie zwrotu „ok." miało także konotacje procesowe: zasada określoności treści zarzutu oraz rozstrzygania niedających się usunąć wątpliwości na korzyść podejrzanego nakazywały opisać liczbę „skradzionych" BTC w ilości „co najmniej".

[491] Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 2354.2018.
[492] Akta Prokuratury Rejonowej Katowice-Południe w Katowicach o sygn. PR 3 Ds. 778.2018.
[493] P. Opitek, *Kwalifikacja prawna i opis czynów zabronionych*…, s. 170.

Kryptowaluta nie jest „rzeczą ruchomą", a bezprawne rozporządzanie nią nie może być kwalifikowane z art. 279 § 1 k.k. W postanowieniu Prokuratury Rejonowej Katowice-Południe w Katowicach znamionom art. 287 § 1 k.k. nie nadano konkretnej treści wynikającej z ustalonego stanu faktycznego; decyzja o umorzeniu postępowania brzmiała:

> w dniu 14 stycznia 2018 r. nieustalony sprawca w celu osiągnięcia korzyści majątkowej bez upoważnienia wpłynął na automatyczne przetwarzanie, gromadzenie lub przesyłanie danych informatycznych, przełamując jednocześnie zabezpieczenie systemu informatycznego i w ten sposób za pomocą giełdy kryptowaluty /…/ przelał z konta /…/ kryptowalutę o łącznej wartości około 2600 zł, tj. o czyn z w art. 287 § 1 kk i art. 279 § 1 kk w zw. z art. 11 § 2 kk[494].

Z opisu czynu i jego kwalifikacji prawnej wybrzmiewa chaos, gdyż kryptowaluta została potraktowana zarówno jako rzecz (art. 279 § 1 k.k.), jak i dane informatyczne (art. 287 § 1 k.k.). Nie wskazano, które ze znamion czynności czasownikowej zrealizował sprawca, ale znamiona takie zostały połączone alternatywą „lub", a więc kierując się logiką, przynajmniej jedno ze znamion musiało zostać faktycznie dokonane. Trudno zaaprobować sformułowanie „za pomocą giełdy kryptowaluty" sugerujące, że giełda była narzędziem służącym do popełnienia przestępstwa; można było napisać, że sprawca „bez upoważnienia wprowadził nowy zapis danych informatycznych w systemie giełdy (…) i przetransferował z konta (…)". W opisie czynu zabrakło podania liczby i rodzaju jednostek kryptowaluty, które stały się przedmiotem czynności wykonawczej, a w kwalifikacji prawnej nie wskazano, który przepis Kodeksu kanego wyczerpał działanie polegające na przełamaniu zabezpieczenia systemu informatycznego giełdy.

5.4. Pozostałe przestępstwa dokonywane z wykorzystaniem walut wirtualnych

Zostało już powiedziane, że przestępcy chcą się wzbogacić kosztem innych osób, dlatego swoją aktywność kierują na „kradzież" tokenów. Chociaż w takich przypadkach bezpośrednim przedmiotem czynności wykonawczej są dane informatyczne, to słusznie zauważa A. Behan, że szerokie spektrum nielegalnych działań, które można zaobserwować w związku z kryptowalutami, wymusza prawnokarną ochronę nie tylko dobra prawnego, będącego danymi informatycznymi lub informacją, ale także wartości majątkowych reprezentowanych przez tokeny cyfrowe[495]. Charakterystyczną rzeczą jest, że omawiana przestępczość ma uniwersalny charakter, o czym autor się przekonał, biorąc udział w konferencjach i szkoleniach międzynarodowych poświęconych nadużyciom na

[494] Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 3 Ds. 171.2018.
[495] A. Behan, *Waluty wirtualne jako*…, s. 584.

rynku „krypto". Oznacza to, że rodzaj oraz sposób popełniania takich przestępstw wygląda podobnie na całym świecie i wszystkie służby ochrony prawa borykają się z identycznymi problemami[496]. Działania przestępcze, godzące w cyfrowe prawa majątkowe, skierowane są w pierwszej kolejności na dane oraz informacje przechowywane w formie binarnej bez bezpośredniego oddziaływania na psychikę ludzką i przedmioty materialne. *Modus operandi* sprawców powiązany jest z omijaniem lub przełamywaniem zabezpieczeń informatycznych, a w najbardziej wyrafinowanej formie ataku dochodzi do „zainfekowania" systemu bazowego użytkownika kryptowaluty złośliwym oprogramowaniem, takim jak trojany, backdoory czy spyware i modyfikacji zawartości jego portfela, skopiowania danych lub zablokowania dostępu. Niekiedy łączy się to z pishingiem, tj. podstawieniem użytkownikowi sieci fałszywej strony autoryzującej i w konsekwencji przejęciem hasła i loginu do aplikacji przechowującej klucze prywatne[497].

Scharakteryzowano już oszustwa związane z działaniem platform inwestycyjnych, w tym tradingowych, oraz ataki typu ransomware, ale warto jeszcze przeanalizować najprostsze formy przestępczości teleinformatycznej ukierunkowane na kryptoaktywa. W dochodzeniu nadzorowanym przez Prokuraturę Rejonową Warszawa-Śródmieście Północ w Warszawie, prokurator zatwierdził postanowienia o umorzeniu dochodzenia na podstawie art. 322 § 1 k.p.k. w sprawie:

> uzyskania w dniu 19 stycznia 2018 roku w nieustalonym miejscu bez uprawnienia dostępu do portfela kryptowalutowego przez osobę nieuprawnioną na szkodę A. D., tj. o czyn z art. 267 § 1 k.k.[498]

W treści decyzji zabrakło wskazania, jak doszło do popełnienia czynu: czy poprzez ominięcie albo przełamanie zabezpieczeń portfela, ponadto umknęło znamię „informacja dla sprawcy nieprzeznaczona". Treść postanowienia i zastosowana podstawa prawna, jeszcze bardziej rozmijają się w postanowieniu Prokuratury Rejonowej Warszawa-Wola w Warszawie wydanym w sprawie:

> zainfekowania laptopa i baz danych firmy /…/ Sp. z o.o. w okresie od 21 do 22 kwietnia 2019 r. i skierowanie żądania przelania kryptowaluty Bitcoins przez użytkownika posługującego się adresem e-mail sprt@kwwmail.com, suport@cock.li, tj. o przest. z art. 267 § 1 k.k.[499]

[496] Zob. P. Opitek, *Sprawozdanie z konferencji naukowej pt. Kryptowaluty w cyberprzestępczości. Międzynarodowa wymiana doświadczeń*, „Wojskowy Przegląd Prawniczy" 2019, nr 10–12, s. 113–119.
[497] P. Opitek, *Aspekty kryminalistyczne, techniczne i prawne*…, s. 158.
[498] Akta Prokuratury Rejonowej Warszawa-Śródmieście Północ w Warszawie o sygn. PR 4 Ds. 396.2018.
[499] Akta Prokuratury Rejonowej Warszawa-Wola w Warszawie o sygn. PR 4 Ds. 1848.2019.

W opisie podano znamiona czynności czasownikowej należącej do konstrukcji czynu zabronionego innego, aniżeli art. 267 § 1 k.k.; chodzi o zwrot: „żądanie przelania kryptowaluty" wskazujący na art. 287 § 1 k.k., ewentualnie w zbiegu realnym z którymś z przepisów penalizujących ataki typu ransomware w zależności od tego, jak poważny był skutek działania sprawcy.

Omawiając nadużycia w bankowości elektronicznej, stwierdzono już, że działanie hakera może być ukierunkowane nie tylko na urządzenie końcowe indywidualnego użytkownika każdego systemu, ale także dotyczyć infrastruktury zlokalizowanej po stronie profesjonalnego dostawcy usług sieciowych. Przypadek taki miał miejsce w sprawie prowadzonej przez Prokuraturę Rejonową w Staszowie, gdzie prokurator, bez uzupełnienia kwalifikacji prawnej o czyn z art. 287 § 1 k.k., zatwierdził postanowienie o umorzeniu dochodzenia z powodu niewykrycia sprawcy przestępstwa dotyczącego:

> uzyskania w dniu 17 stycznia 2018 roku w nieustalonym miejscu w sposób bezprawny dostępu do konta na giełdzie BitBay poprzez przełamanie hasła dostępu i kradzieży środków w kwocie 1239,35 zł na szkodę M. P., tj. o przestępstwo z art. 267 § 1 k.k.[500]

W Prokuraturze Okręgowej w Tarnobrzegu umorzono na podstawie art. 322 § 1 k.p.k. śledztwo w sprawie:

> przełamania w dniu 3 stycznia 2018 r. w nieustalonym miejscu, elektronicznych zabezpieczeń konta prowadzonego w serwisie BitBay.net przez Spółkę BitBay z siedzibą w K. na rzecz T. W., a następnie zmiany zapisu danych informatycznych na tym koncie poprzez zlecenie operacji na kryptowalutach, w wyniku czego doszło do zaboru w celu przywłaszczenia 14,76 jednostek kryptowaluty BitCoin (BTC) na szkodę T. W. o wartości około 793 000 zł, co stanowi mienie znacznej wartości, tj. o przest. z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 294 § 1 k.k. w zw. z art. 11 § 2 k.k.[501]

Włamanie na konto było powiązane z ustalonym adresem mailowym oraz adresami IP logującymi się z Europy, Ameryki Północnej i Azji, a więc można przypuszczać, że sprawca anonimizował ruch sieciowy poprzez korzystanie z sieci TOR i narzędzi typu VPN-y i PROXY. Następnie przełamał elektroniczne zabezpieczenia sieci teleinformatycznej, a realizowana przez niego wypłata kryptowaluty następowała na różne portfele. W sprawie tej zaistniał notorycznie pojawiający się błąd w analizowanych decyzjach procesowych, tj. traktowanie kryptowaluty jako „rzeczy ruchomej" lub „innego środka płatniczego".

[500] Akta Prokuratury Rejonowej w Staszowie o sygn. PR Ds. 256.2018.
[501] Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO I Ds. 3.2018.

Najbardziej lukratywne dla przestępców, bo generujące wysokie straty finansowe i dotyczące setek, a nawet tysięcy pokrzywdzonych osób, są ataki na profesjonalne podmioty działające na kryptowalutowym rynku, przede wszystkim giełdy i kantory internetowe, powiązane z przejęciem kluczy prywatnych depozytariuszy giełdy, kantoru lub platformy inwestycyjnej. W kodzie źródłowym statuującym blockchainowe środowisko (inteligentne umowy, tokeny cyfrowe, portfele i powiązane z nimi aplikacje itp.) mogą znajdować się luki pozwalające na dokonywanie nadużyć. Jeśli twórca oprogramowania zamieścił w nim backdoora, to w każdym momencie może zmienić algorytm działania kodu źródłowego i przelać do swojego portfela tokeny stanowiące własność innych osób. Innym razem wystarczy drobna zmiana jednej sekwencji kodu w obszernym protokole statuującym program komputerowy, aby cały algorytm zaczął działać inaczej, niż planowano lub zapewniano inwestorów[502]. Atak na infrastrukturę teleinformatyczną może mieć charakter jednorazowy lub być prowadzony permanentnie za pomocą botnetów, które skanują systemy zabezpieczenia platformy cyfrowej, szukając luk dostępu. W Polsce najpoważniejsze włamanie dotyczyło giełdy Bitcurex w październiku 2016 r. i „kradzieży" w ciągu 2 sekund BTC na kwotę 5,5 mln złotych (wg ceny kryptowaluty w dniu popełnienia przestępstwa) wraz z danymi osobowymi ich użytkowników. Giełda zaprzestała działalności, a pokrzywdzeni atakiem nie odzyskali utraconych środków[503]. Inne śledztwo w 2016 r. obejmowało atak hakerski na jedną z największych giełd i wytransferowania znajdujących się na niej jednostek kryptowaluty o wartości 622 500 zł. Sprawa Prokuratury Rejonowej Olsztyn-Południe w Olsztynie dotyczyła:

> dokonanego w czasie od 31 stycznia do 4 lutego 2016 r. za pośrednictwem sieci Internet w krótkich odstępach czasu, w wykonaniu z góry powziętego zamiaru, uzyskanie poprzez pokonanie zabezpieczeń serwisu i nieuprawnionego dostępu do konta technicznego serwisu /…/, a następnie dokonanie kradzieży wirtualnych walut bitcoin i litecoin o łącznej szacunkowej wartości 622.500 zł na szkodę /…/ Ltd. w /…/, tj. o przestępstwo określone w art. 267 § 3 kk w zw. z art. 279 § 1 kk w zw. z art. 294 kk w zw. z art. 11 § 2 kk w zw. z art. 12 kk[504].

W kwalifikacji prawnej czynu kolejny raz pojawił się błąd traktowania jednostki kryptowalut, jak rzeczy i kwalifikowania jej zaboru z art. 279 § 1 k.k., podczas gdy należało przywołać art. 287 § 1 k.k. Sprawca miał wyczerpać znamiona przestępstwa opisanego w art. 267 § 3 k.k., ale z treści decyzji wynika co innego, tj. popełnił on czyn stypizowany w § 1 tego przepisu. W uzasadnieniu postanowienia o umorzeniu śledztwa napisano, że:

[502] P. Opitek, *Aspekty kryminalistyczne, techniczne i prawne*…, s. 197–198.
[503] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*…, s. 146.
[504] Akta Prokuratury Rejonowej Olsztyn-Południe w Olsztynie o sygn. PR 2 Ds. 242.2016.

> w ramach postępowania uzyskano m.in. kluczowe dla ustalenia sprawcy wykazy logowań typowanych jako działania sprawcy przestępstwa oraz adresy portfeli wirtualnych na które przetransferowano skradzione pieniądze. Analiza logów wskazuje, iż logowań dokonano w krótkich odstępach czasu za pośrednictwem serwerów znacznie oddalonych od siebie, których administratorzy usytuowani są na Seszelach, w Niemczech, Szwecji oraz Irlandii, co wskazuje, iż sprawca działał używając oprogramowania maskującego prawdziwy adres IP.

Przeprowadzona w śledztwie analiza wirtualnych portfeli, na które przetransferowano kryptowalutę, nie wniosła nic nowego do sprawy i nie ustalono „gdzie ostatecznie trafiły środki pozyskane w wyniku przestępstwa", a na podstawie obowiązujących przepisów prawa brak było, zdaniem referenta sprawy, możliwości skutecznej realizacji pomocy międzynarodowej[505].

Oprócz czynów wyczerpujących znamiona przestępstw z Rozdziału XXXIII k.k. lub art. 287 § 1 k.k. działania sprawców ukierunkowane na nielegalne przejęcie tokenów opierają się także na socjotechnice i oddziaływaniu bezpośrednio na psychikę ludzką po to, aby pokrzywdzonego wprowadzić w błąd i uzyskać od niego nienależną korzyść majątkową. W akcie oskarżenia skierowanym do sądu przez Prokuraturę Rejonową Warszawa-Mokotów w Warszawie M. S. został oskarżony o to, że:

> w dniu 3 marca 2016 r. w /…/ działając w celu osiągnięcia korzyści majątkowej doprowadził A. S. do niekorzystnego rozporządzenia mieniem w postaci pieniędzy w łącznej kwocie 54 000 zł w ten sposób, że wprowadził pokrzywdzonego w błąd zarówno, co do osoby sprzedającego, jak i zamiaru dostarczenia kryptowaluty przedstawiając mu Ł. K. jako sprzedającego, a także przekazując za jego pośrednictwem nośnik w postaci pendrive zawierającego nie mające charakteru kodu dostępowego rząd cyfr mający uprawniać do dostępu do stu siedemnastu i stu czternastu tysięcznych (117.114) elektronicznych jednostek kryptowaluty bitcoin, tj. o czyn z art. 286 § 1 kk[506]

W sprawie ustalono, że pokrzywdzony spotkał się w jednym z warszawskich hoteli z Ł. B. i A. S. i z pierwszym z nich zawarł umowę sprzedaży bitcoinów, a A. S. zorganizował i pośredniczył w transakcji. Techniczna operacja przelewu kryptowaluty była realizowana w obecności kupującego, który nie zauważył jakichkolwiek nieprawidłowości, ale finalnie okazało się, że na wręczonym mu portfelu sprzętowym nie ma żadnych kluczy prywatnych do bitcoinów. W dochodzeniu ustalono, że Ł. B. i A. S., działając wspólnie i w porozumieniu, sfingowali całą transakcję rzekomego przelewu BTC po to, aby uzyskać od pokrzywdzonego 54 000 zł.

Popularne wśród przestępców są kampanie mailowe, w których podszywają się pod inne osoby i próbują wyłudzić od potencjalnych ofiar środki w kryptowalucie tytułem

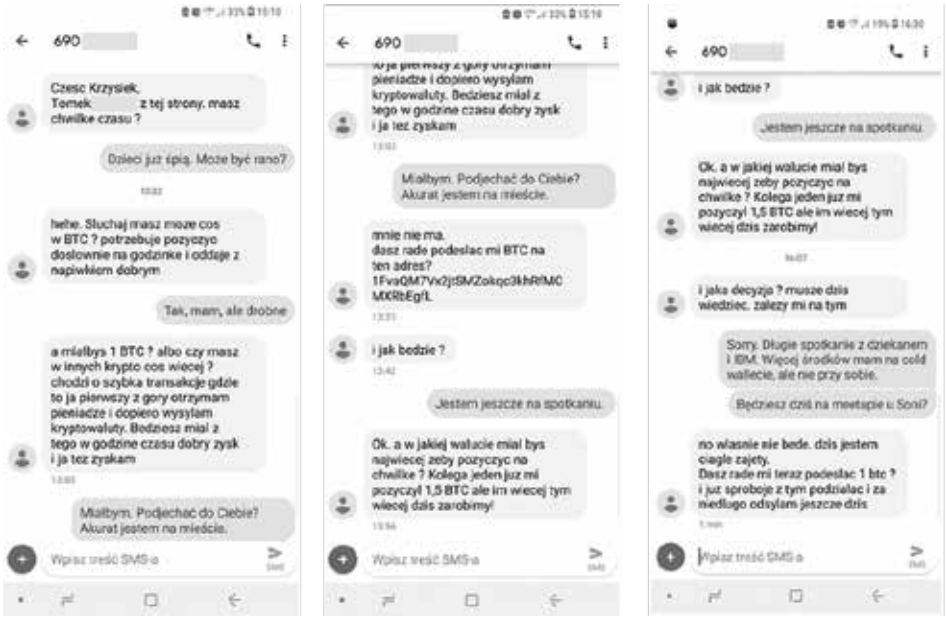
[505] Tamże.

[506] Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 5 Ds. 412.2017.

pożyczki, pomocy w ciężkiej sytuacji życiowej czy intratnej inwestycji. Dochodzenie prowadzone przez Prokuraturę Rejonową Warszawa-Śródmieście Północ w Warszawie, umorzone na podstawie art. 322 § 1 k.p.k., dotyczyło:

> usiłowania doprowadzenia w dniu 28 września 2018 r. w /…/ przy ul. /…/ do niekorzystnego rozporządzenia mieniem K. P. w celu osiągnięcia korzyści majątkowej w kwocie 24 500,00 (odpowiadającej wartości prawa majątkowego do zapisu informatycznego w postaci 1 Bitcoina) poprzez wprowadzenie w błąd ww. pokrzywdzonego co do tożsamości osoby proszącej go o udzielenie pożyczki środków zgromadzonych w tej kryptowalucie oraz zamiaru zwrotu tych środków, tj. o czyn z art. 13 § 1 k.k. w zw. z art. 286 § 1 k.k.[507]

27 września 2018 r. pokrzywdzony otrzymał wiadomość SMS z nieznanego numeru telefonu z prośbą o kontakt od osoby podpisującej się imieniem i nazwiskiem jego znajomego. Następnego dnia nadeszła wiadomość o podobnej treści, zawierająca także prośbę o pożyczenie kryptowaluty i deklarację zwrotu środków w ciągu godziny wraz z nawiązką. K. P. skontaktował się telefonicznie ze swoim kolegą i ustalił, że to nie on wysyłał podejrzane komunikaty, a zaraz potem kontakt z przestępcą się urwał. Kwalifikacja prawna czynu i jego opis były prawidłowe, gdyż sprawca nie oddziaływał na proces przetwarzania danych informatycznych, ale na akt wolnej woli człowieka, chcąc od niego wyłudzić prawo majątkowe.



Grafika nr 20. Rozmowa SMS-owa z 28 września 2018 r. między pokrzywdzonym (Krzyśkiem) a oszustem próbującym wyłudzić kryptowalutę

[507] Akta Prokuratury Rejonowej Warszawa-Śródmieście Północ w Warszawie o sygn. PR 4 Ds. 1544.2018.

Zastosowanie socjotechniki okazało się skuteczne i sprawca osiągnął korzyść z oszustwa w sprawie nadzorowanej przez Prokuraturę Okręgową w Tarnobrzegu, dotyczącej tego, że nieustalona osoba najpierw włamała się na Facebookowe konto i stamtąd, podszywając się pod znajomego mężczyzny, poprosiła go o udzielenie krótkoterminowej pożyczki w kwocie 980 zł. Sprawca wskazał numer rachunku bankowego do wpłaty oraz tytuł przelewu „zasilenie-bitmarket24-Mrass". Pokrzywdzony przekonany, że koresponduje z kolegą, wykonał przelew i aplikacją Messenger wysłał jego potwierdzenie do odbiorcy środków. Potem okazało się, że na skutek przeprowadzonej tego dnia kampanii mailingowej, osób pokrzywdzonych przestępstwem było o wiele więcej, a do masowego rozsyłania fałszywych wiadomości z przejętych kont na platformie społecznościowej sprawca wykorzystał najprawdopodobniej sieć zainfekowanych komputerów (botnet). Ostatecznie dochodzenie zostało umorzone w sprawie:

> doprowadzenia w dniu 5 lutego 2018 r. ze skutkiem w S. woj. podkarpackiego w celu osiągnięcia korzyści majątkowej S. P., który przelał pieniądze w kwocie 980 zł na ustalony rachunek bankowy giełdy kryptowalutowej /…/ do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie w błąd co do tożsamości osoby z którą rozmawiał za pośrednictwem komunikatora Messenger, tj. o przest. z art. 286 § 1 k.k.[508]

W innym *modus operandi*, nazywanym sextortion, przestępca groził pokrzywdzonemu opublikowaniem w Internecie kompromitujących go materiałów: jego nagich zdjęć, prowadzonych na komunikatorze rozmów o zabarwieniu erotycznym, wiadomości o intymnej treści lub filmów z jego udziałem, o charakterze seksualnym. Sprawca oświadczył przy tym, że zdobył takie materiały, instalując w telefonie lub komputerze ofiary oprogramowanie szpiegujące albo włamując się do skrzynki mailowej. Zazwyczaj są to groźby bez pokrycia, ale zmanipulowane i przestraszone osoby płacą niekiedy okup w kryptowalucie. Postępowanie w takiej sprawie prowadziła Prokuratura Rejonowa w Lidzbarku Warmińskim. Dotyczyło ono:

> zaistniałego w dn. 24 kwietnia 2019 r. w bliżej nieustalonym miejscu za pośrednictwem internetu, w celu osiągnięcia korzyści majątkowej – usiłowania doprowadzenia M. S. do niekorzystnego rozporządzania własnym mieniem w postaci pieniędzy w łącznej kwocie 2.900,00 zł za pomocą wprowadzenia w błąd co do potrzeby zasilenia wskazaną kwotą pieniędzy portfela Bitcoin o nr /…/, celem uniknięcia rozpowszechniania za pośrednictwem portali społecznościowych kompromitujących informacji, i nie osiągnięcia zamierzonego celu z uwagi na postawę pokrzywdzonej,

[508] Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO IV Ds. 19.2018.D.

która nie przekazała rzeczonej kwoty pieniędzy, na szkodę M. S., tj. o czyn z art. 13 § 1 k.k. w zw. z art. 286 § 1 k.k.[509]

W takich sprawach należy rozważyć zastosowanie art. 191a § 1 k.k., zgodnie z którym odpowiedzialności karnej podlega „Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia", jeśli sprawca rzeczywiście utrwaliłby sceny intymne z udziałem osoby trzeciej i bez jej zgody albo treści takie rozpowszechniał.

Kryptowaluty wykorzystywane są jako środek zapłaty za nielegalne towary i usługi oferowane w Internecie; w pierwszej kolejności chodzi o narkotyki. W sieci rozwija się handel substancjami psychotropowymi i środkami odurzającymi, a oprócz tradycyjnych narkotyków cyfrowe platformy oferują swoim klientom *research chemicals*, bardziej znane jako „dopalacze", a więc różnego rodzaju mieszaniny ziół i kanabinoidów powodujące upośledzenie funkcji mózgu. Jeszcze kilka lat temu handel narkotykami był domeną tzw. darkmarketów, ale obecnie platformy sprzedażowe działają również w otwartej sieci pod przykrywką dystrybucji dozwolonych produktów (środków chemicznych, suplementów diety). Obserwuje się ponadto funkcjonowanie zamkniętych forów na komunikatorach, gdzie spotykają się sprzedawcy i osoby szukające metaamfetaminy lub marihuany, mieszkający w tym samym mieście lub powiecie.

Internetowe sklepy, oferujące zakazane substancje, prowadzone są w bardzo fachowy oraz bezpieczny dla przestępców sposób i posiadają określone cechy wspólne: profesjonalną i łatwą w obsłudze zamówienia stronę internetową, płatności w kryptowalutach, ustalone metody dostawy „towaru", specjalne, bezpieczne dla przestępców kanały komunikowania się. Można tam znaleźć szczegółowe informacje o rodzaju oferowanych substancji: ich nazwę, skład chemiczny, niekiedy opis sposobu użytkowania i działania proszków lub kryształów. Witryny sprzedażowe są dobrze zarządzane marketingowo: mają atrakcyjny wygląd oraz podają treści w sposób syntetyczny i zrozumiały. Sprzedaż odbywa się w określonych godzinach, a procedura transakcyjna przewiduje nawet możliwość złożenia reklamacji[510]. Opłatę za narkotyki uiszcza się z reguły w najpopularniejszych kryptowalutach, takich jak bitcoin, ethereum, litecoin; coraz rzadziej zdarzają się pieniężne formy płatności. System uiszczania ceny za towar, opierający się na kryptowalucie, wykorzystuje usługę escrow. Polega ona na tym, że w momencie zakupu cena za produkt oddawana jest w depozyt podmiotowi trzeciemu (arbitrowi), a BTC trafiają do sprzedającego dopiero w momencie, gdy kupujący potwierdzi otrzymanie zamówionych substancji[511].

[509] Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 1 Ds. 340.2019.

[510] P. Opitek, *Międzynarodowa przestępczość narkotykowa w ujęciu kryminalistycznym i kryminologicznym*, „Kwartalnik Prawa Międzynarodowego", 2023, nr 2, s. 251.

[511] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*..., s. 433.

Podstawową formą komunikacji pomiędzy sprzedawcą i nabywcą jest adres mailowy chroniony przez kilka warstw bezpieczeństwa m.in. w postaci szyfrowania end-to--end i mechanizmu zero-access. Szyfrowanie przesyłanych treści odbywa się automatycznie na urządzeniu klienta, zanim maile zostaną wysłane na zewnętrzne serwery, ale nie wymaga się instalacji specjalnego oprogramowania ani umiejętności technicznych do obsługi poczty. W rezultacie jej administrator (dostawca usługi) nie ma dostępu do treści wiadomości mailowej, gdyż są one natychmiast szyfrowane na jego serwerach przy użyciu klucza publicznego nadawcy. Specjalne systemy poczty wprowadzają jeszcze inne mechanizmy zabezpieczające, m.in. blokowanie reklam wyświetlanych na podstawie aktywności konsumenta w usłudze pocztowej, automatyczną blokadę śledzenia pikseli lub ukrycie adresu IP użytkownika, co pozwala na odczytywanie wiadomości bez ujawniania jakichkolwiek danych osobowych i metadanych. Znane są także systemy przesyłania wiadomości, które po jej odczytaniu automatycznie kasują treść przekazu. Nielegalne fora deklarują, że nie przechowują historii logowania się (adresów IP), a konta ich użytkowników są anonimowe poprzez szyfrowanie danych oraz systemy „przeciwbotowe". Podstawowe znaczenie dla funkcjonowania internetowych sklepów narkotykowych ma skuteczny mechanizm wysyłki i dostawy zamówionego towaru[512]. Wykorzystywane są do tego firmy kurierskie lub tradycyjna instytucja poczty. Nielegalne strony internetowe zawierają szczegółowy opis, jak należy zamówić i odebrać narkotyki. Jeśli chodzi o ich niewielkie partie, to najlepszym rozwiązaniem może okazać się zwykły list z zapakowaną niewielką, kilkugramową porcją narkotyku. Do ekspedycji większej ilości środków odurzających lub substancji psychotropowych, wykorzystuje się firmy kurierskie, a towar pakuje bezpośrednio w paczkach i maskuje w taki sposób, aby nie został wykryty w trakcie ewentualnej kontroli. Zamówiony „towar" konsument lub diler pobiera w paczkomacie, biurze firmy kurierskiej lub pod przypadkowym adresem, niemającym żadnego związku z jego miejscem pobytu lub zamieszkania[513].

Sprzedaż narkotyków syntetycznych za pośrednictwem internetowych platform handlowych, zwłaszcza w darknecie, stanowi poważne utrudnienie w skutecznym prowadzeniu śledztwa i dlatego organy krajowe zaangażowane w przypadki transgranicznego handlu narkotykami powinny skontaktować się z przedstawicielami partnerskich służb w Eurojuscie i uzyskać wsparcie na różnych etapach postępowania karnego. Postuluje się budowę wspólnych zespołów dochodzeniowo-śledczych oraz organizację centrów koordynacyjnych przez Eurojust, co zapewni kompleksowe podejście do

[512] Nieprzypadkowo Unia Europejska wzywa do rozwoju, stosowania i wymiany najlepszych praktyk i sprzętu między państwami członkowskimi w zakresie monitorowania podejrzanych przesyłek pocztowych poprzez stosowanie takich rozwiązań, jak psy wyszkolone do wykrywania narkotyków lub urządzenia rentgenowskie, [w:] Plan działań UE w zakresie narkotyków na lata 2021–2025, https://eur – lex.europa.eu/legal – content/PL/TXT/HTML/?uri=CELEX:52021XG0708(01) [dostęp: 15.06.2023].

[513] P. Opitek, *Międzynarodowa przestępczość narkotykowa…*, s. 252–254. Więcej na temat handlu narkotykami w Internecie patrz: P. Opitek, K. Lenczowska-Soboń, G. Ocieczek, *Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w świecie „realnym" i cyberprzestrzeni*, materiał szkoleniowy, „Prokuratura i Prawo" 2022, nr 7–8, s. 237–268.

zwalczania grup przestępczych. Ponadto dystrybucja narkotyków w Internecie wymaga zredefiniowania metodyki prowadzenia czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych. Jeśli chodzi o pierwszą sferę działań, to przydatne okazuje się zastosowanie instytucji zakupu kontrolowanego i przesyłki niejawnie nadzorowanej w cyberprzestrzeni, aby nabyć substancję dystrybuowaną przez administratora platformy i potwierdzić, że rzeczywiście ma się do czynienia z narkotykami oraz ustalić ich rodzaj i skład fizykochemiczny. W działaniach ukierunkowanych na rozpracowanie grupy konieczne jest odtworzenie kanału dystrybucji podejrzanych substancji, sposobu ich wysyłki oraz miejsc docelowego przeznaczenia. Ponieważ omawiana przestępczość ma charakter transgraniczny, to wykorzystuje się procedury międzynarodowej pomocy prawnej do realizacji czynności obserwacji, wywiadu środowiskowego, zatrzymania osób i przeszukania pomieszczeń, czy wdraża kontrolę operacyjną na podstawie europejskiego nakazu dochodzeniowego[514].

W tym miejscu należy jeszcze wspomnieć o praniu pieniędzy z wykorzystaniem walut wirtualnych, które stało się nieodłącznym elementem współczesnego obrazu już nie tylko cyberprzestępczości, ale dotyczy także korzyści uzyskanych poprzez „tradycyjne" formy nielegalnych działań. Opracowania naukowe, raporty i analizy, ale przede wszystkim praktyka dochodzeniowo-śledcza pokazują, że waluty wirtualne i pranie pieniędzy to zagadnienia ściśle ze sobą powiązane. Obecnie wysiłki organów ścigania skupiają się na dwóch podstawowych kwestiach: wdrożeniu skutecznych narzędzi analizy kryminalnej transferów opartych na blockchainie i metodyce zabezpieczenia majątkowego na kryptowalutach. W 2022 i 2023 r. autor przeprowadził w całym kraju dziesiątki różnego rodzaju szkoleń dla sędziów, prokuratorów, ale przede wszystkim funkcjonariuszy służb ochrony prawa, dotyczących praktycznych aspektów technicznych, ekonomicznych i prawnych funkcjonowania cyfrowych praw majątkowych także w aspekcie odzyskiwania mienia pochodzącego z przestępstwa.

Umownie, na potrzeby niniejszego opracowania, można wyróżnić dwie metody prania pieniędzy przy wykorzystaniu kryptowalut: podstawową i zaawansowaną. Pierwsza polega na tym, że skradzione środki pieniężne są automatycznie konwertowane na kryptowalutę z wykorzystaniem tzw. szybkich płatności. W akcjach marketingowych często jest mowa o tym, że niektóre sklepy internetowe lub firmy przyjmują płatności w „walucie wirtualnej BTC", ale w rzeczywistości okazuje się, że wpierw kryptowaluta jest wymieniana na pieniądz fiducjarny przez podmiot pośredniczący w transakcji i w takiej formie trafia do tradycyjnego usługodawcy[515]. Podobnie oszukańcze płatności w złotówkach na popularnych platformach sprzedażowych są konwertowane przez przestępców na tokeny cyfrowe, co pozwala im ukryć nielegalne źródło pochodzenia

[514] Szczegółowa procedura wdrożenia kontroli operacyjnej na podstawie END-u została opisana w artykule: P. Opitek, *Wdrożenie kontroli operacyjnej na terytorium innego państwa członkowskiego Unii Europejskiej w ramach europejskiego nakazu dochodzeniowego*, „Kwartalnik Prawa Międzynarodowego" 2022, nr 1, s. 143–161.

[515] Pismo z 28 maja 2015 r.

wartości finansowych. W Prokuraturze Okręgowej w Tarnobrzegu umorzono, na podstawie art. 322 § 2 k.p.k., śledztwo w sprawie:

1. dokonanego w dniu 11 lipca 2017 r. w Tarnobrzegu woj. podkarpackiego w celu osiągnięcia korzyści majątkowej, bez upoważnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez Bank /…/ rachunku bankowego P. S. o ustalonym numerze zmiany zapisu danych informatycznych w elektronicznym systemie bankowym w ten sposób, że utworzono i wysłano do realizacji przelew w kwocie 63.099,00 zł, a następnie z rachunku pokrzywdzonego na rachunek T. K., prowadzony w Banku /…/ pod ustalonym numerem wykonano przelew w kwocie 63.099,00 zł na szkodę P. S., tj. o czyn z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. – wobec nie wykrycia sprawcy przestępstwa,
2. dokonanego w dniu 9 sierpnia 2017 r. w Tarnobrzegu woj. podkarpackiego w celu osiągnięcia korzyści majątkowej, bez upoważnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez Bank /…/ rachunku bankowego P. S. o ustalonym numerze zmiany zapisu danych informatycznych w elektronicznym systemie bankowym w ten sposób, że utworzono i wysłano do realizacji przelew w kwocie 9.000,00 zł, a następnie z rachunku pokrzywdzonego na rachunek spółki /…/ Sp. z o.o. (właściciela platformy zajmującej się obrotem kryptowalutami), prowadzony w Banku /…/ pod ustalonym numerem wykonano przelew w kwocie 9.000,00 zł na szkodę P. S., tj. o czyn z art. 279 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. – wobec nie wykrycia sprawcy przestępstwa[516].

Ustalono, że 11 lipca 2017 r. kiedy pokrzywdzony próbował zalogować się do swojej aplikacji bankowości elektronicznej, zauważył: „jakby strona się zawiesiła i nie przeszła dalej". Mimo ponawianych prób, P. S. nie udało się zalogować do aplikacji, a zaraz potem zadzwonił pracownik banku, który poinformował go, że nastąpiło włamanie do systemu i ma zgłosić się osobiście w siedzibie banku. Po przeprowadzeniu procedury sprawdzającej właściciel rachunku zwrócił P. S. utracone w wyniku ataku środki, tj. 63099 zł. Z zapisów zawartych w systemie banku wynikało, że pieniądze zostały przelane na giełdę BitMarket24. Mężczyzna, aby uniknąć podobnych ataków, kupił nowy komputer i za jego pomocą logował się do aplikacji bankowej. Zakupiony laptop podłączył do drukarki, która współpracowała z „zainfekowanym" komputerem 11 lipca 2017 r. Najprawdopodobniej spowodował tym, że złośliwe oprogramowanie mogło implementować się na nowym komputerze i 9 sierpnia 2017 r. historia się powtórzyła: gdy mężczyzna podjął próbę zalogowania się do bankowości elektronicznej, strona banku znowu „jakby się zawiesiła", a saldo jego rachunku pomniejszyło się o kwotę 9000 zł przelaną na konto

[516] Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO IV Ds. 38.2017.D.

giełdy kryptowalutowej. W toku śledztwa ustalono, że na komputerze pokrzywdzonego najprawdopodobniej działało złośliwe oprogramowanie, które wyświetlało fałszywą stronę logowania się do banku, na której P. S. wpisywał login oraz hasło, i w ten sposób przestępca mógł przejąć dane uwierzytelniające dostęp do pieniędzy. W konsekwencji, zanim P. S. zalogował się do serwisu, kilka sekund wcześniej atakujący, korzystający z adresów IP pochodzących ze Stanów Zjednoczonych i Rumunii, zlecał w jego imieniu transfery środków na fałszywe konto ulokowane na giełdzie kryptowalutowej, gdzie zamieniał pieniądze na bitcoiny i wyprowadzał tokeny na anonimowe konta.

Przykładem skomplikowanej sprawy dotyczącej wykorzystania bitcoinów do „prania" stanowiło śledztwo Prokuratury Regionalnej w Gdańsku[517], zakończone sporządzeniem 27 grudnia 2018 r. aktu oskarżenia. Dotyczyło ono tzw. tajemniczego listonosza: K. Z. został oskarżony o popełnienie 470 przestępstw polegających na tym, że działając w celu osiągnięcia korzyści majątkowej, doprowadził lub usiłował doprowadzić firmy pożyczkowe (m.in. Payday Loans, Vivus Finance, Cream Finance, VIA SMS PL, Regita, Szybka Gotówka, Wonga) do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie ich pracowników w błąd, co do zamiaru wywiązania się z umowy pożyczki zawieranej za pośrednictwem Internetu oraz posługując się wcześniej wyłudzonymi danymi osobowymi, czym wyrządził szkodę majątkową w łącznej wysokości kilkudziesięciu tysięcy złotych, czyniąc sobie z popełniania przestępstw stałe źródło dochodu, tj. o czyn z art. 286 § 1 k.k. (art. 13 § 1 k.k. w zw. z art. 286 § 1 k.k.) w zw. z art. 65 § 1 k.k. K. Z. postawiono ponadto zarzut prania pieniędzy; miało ono polegać na tym, że:

> w okresie od 27 lipca 2017 roku do 9 marca 2018 roku w Gdyni, Nadolu i innych nieustalonych miejscach, działając w krótkich odstępach czasu, z góry powziętym zamiarem, dokonał transferów środków w łącznej wysokości 50 600 zł, pochodzących z korzyści związanych z popełnieniem czynów zabronionych z art. 286 § 1 k.k., polegających na działania w celu osiągnięcia korzyści majątkowej i doprowadzeniu w okresie od 27 lipca 2017 roku do 9 marca 2018 roku ustalonych firm pożyczkowych do niekorzystnego rozporządzenia mieniem w łącznej wysokości 50 600 zł wprowadzając w błąd pracowników ustalonych spółek, co do tożsamości pożyczkobiorców poprzez posłużenie się danymi osobowymi wymienionych w akcie oskarżenia osób, nie mając zamiaru wywiązania się z zawartych umów w ten sposób, w okresie od 27 lipca 2017 roku do 9 marca 2018 roku w Gdyni, Nadolu i innych nieustalonych miejscach, działając w krótkich odstępach czasu, z góry powziętym zamiarem, dokonał transferów środków w łącznej wysokości 50 600 zł, pochodzących z korzyści związanych z popełnieniem czynów zabronionych z art. 286 § 1 k.k.,

[517] Akta Prokuratury Regionalnej w Gdańsku o sygn. RP II Ds. 22.2017.

polegających na działania w celu osiągnięcia korzyści majątkowej i doprowadzeniu w okresie od 27 lipca 2017 roku do 9 marca 2018 roku ustalonych firm pożyczkowych do niekorzystnego rozporządzenia mieniem w łącznej wysokości 50 600 zł wprowadzając w błąd pracowników ustalonych spółek, co do tożsamości pożyczkobiorców poprzez posłużenie się danymi osobowymi wymienionych w akcie oskarżenia osób, nie mając zamiaru wywiązania się z zawartych umów w ten sposób, że wielokrotnie przelewał uzyskane środki pomiędzy 42 rachunkami bankowymi założonymi na „słupy", a następnie transferował pieniądze, częściowo za pośrednictwem usługi tzw. szybkich przelewów międzybankowych pozwalających anonimizować strony transakcji, na giełdy kryptowalutowe i kupował za nie bitcoiny, które to czynności mogły znacznie utrudnić stwierdzenie przestępczego pochodzenia środków, miejsca ich umieszczenia, jak również ich wykrycie i zajęcie w skutek czego osiągnął korzyść majątkową w kwocie 50 600 zł, tj. o przestępstwo z art. 299 § 1 k.k. w zw. z art. 12 k.k. w zw. z art. 65 1 k.k.

W sprawie ustalono, że K. Z., podszywając się pod fikcyjne firmy zamierzające rzekomo zatrudnić pracowników, zamieszczał w Internecie (trójmiasto.pl, gumtree.pl) atrakcyjne oferty pracy w charakterze „tajemniczego klienta", czyli audytora bankowego. Osoby odpowiadające na ogłoszenie przesyłały „pracodawcy" swoje dane osobowe, skany dowodów osobistych oraz przelewały na wskazane konta symboliczną złotówkę. W ten sposób, niczego nieświadome, autoryzowały założone przez przestępcę rachunki bankowe, które następnie posłużyły sprawcy do wyłudzenia pożyczek i prania pieniędzy. K. Z. zawierał bowiem drogą elektroniczną umowy na tzw. chwilówki, wykorzystując dane osobowe pokrzywdzonych. Wyłudzone środki wpływały na rachunki bankowe, a następnie sprawca, stosując bramki płatności typu Dotpay S.A. lub Krajowy Integrator Płatności S.A., przelewał je na giełdy kryptowalutowe (m.in. BitBay, BTC Coin, Coinroom, Beatcoin.pl, 4Coins), gdzie pieniądze wymieniane były na kryptowaluty lub kolejny raz realizowano nimi tzw. szybkie płatności (DialCom24 Sp. z o.o.). Podjęte przez sprawcę działania znacznie utrudniły stwierdzenie przestępczego pochodzenia środków oraz ich lokalizację (art. 299 § 1 k.k.).

Grafika nr 21. Schemat działania przestępcy (sprawa „tajemniczego listonosza")

W sprawie „tajemniczego listonosza", podobnie jak w dziesiątkach innych śledztw dotyczących „prania", prokurator uznał, że altcoiny stanowią prawa majątkowe, o których mowa w art. 299 k.k. Przepis mówi, że przedmiotem bezpośredniego działania mogą być środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe oraz mienie ruchome lub nieruchome pochodzące z korzyści związanych z popełnieniem czynu zabronionego przez samego sprawcę lub przez inne osoby. Jeśli chodzi o bitcoina oraz podobnie funkcjonujące altcoiny, to stanowią one prawa majątkowe w takim znaczeniu, o jakim mowa w art. 44 k.c. W orzecznictwie i doktrynie podkreśla się, że pojęcie „prawa majątkowe" ma szeroki zakres znaczeniowy. Zdaniem M. Balwickiej-Szczyrby, instytucję „innych praw majątkowych" należy bezpośrednio wiązać z ekonomicznym interesem uprawnionego, a w skład mienia wchodzi posiadanie jako stan faktyczny, oraz ekspektatywa, za czym przemawia wykładnia funkcjonalna art. 44 k.c.[518]. Podobnego zdania jest P. Nazaruk, pisząc, że „inne prawa majątkowe" pozostają „w ścisłym związku z ekonomicznym interesem uprawnionego niezależnie od tego, czy w konkretnej sytuacji za prawo takie można uzyskać pewną sumę pieniężną lub inne dobro"[519]. Zatem cywilistyczna wykładnia art. 44 k.c. uprawnia do twierdzenia, że waluty wirtualne mają charakter praw majątkowych. Stanowią one dającą się określić kwotowo w pieniądzu, realną wartość ekonomiczną i dlatego cieszą się dużą popularnością i funkcjonuje cały ekosystem do inwestowania w kryptowaluty. Bitcoiny są przedmiotem obrotu, a ponadto kreują różnego rodzaju stosunki zobowiązaniowe: przesłanie bitmonety z jednego adresu na inny adres może rodzić obowiązek zapłaty ceny lub spełnienia innego świadczenia (np. dostarczenia towaru lub realizacji usługi, jeśli chodzi o *utility tokens*). Obrót kryptowalutami rodzi skutki w sferze prawa publicznego, przede wszystkim podatkowego. Dlatego K. Zacharzewski wprost określa bitcoina jako „konglomerat elementów prawnorzeczowych i prawno-obligacyjnych", a więc zbywalne prawo majątkowe[520].

Waluty wirtualne stanowią zatem prawa majątkowe, o jakich mowa w art. 299 k.k., bowiem „brudnymi pieniędzmi są nie tylko środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, mienie ruchome lub nieruchomości, ale również prawa majątkowe, a zatem prawa bezpośrednio uwarunkowane interesem ekonomicznym podmiotu"[521]. Nie można udawać, że jednostki kryptowaluty stanowią jedynie „jakieś byty abstrakcyjne" niepowiązane ze „światem realnym", podobnie jak błędem jest proste przenoszenie na grunt prawa karnego dyskusji cywilistów o skomplikowanej naturze bitcoina. W tym kontekście jakże trafne i aktualne są wypowiedziane sto lat temu słowa W. Makowskiego:

[518] M. Balwicka-Szczyrba, *Komentarz do art. 44 kodeksu cywilnego, teza 1*, [w:] *Komentarz do kodeksu cywilnego*, red. A. Sylwestrzak, LEX/el. 2022, stan prawny: 1 stycznia 2022 r.
[519] P. Nazaruk, *Komentarz do art. 44 kodeksu cywilnego, teza 2*, [w:] *Komentarz do kodeksu cywilnego*, red. J. Ciszewski, LEX/el. 2022, stan prawny: 1 stycznia 2022 r.
[520] K. Zacharzewski, *Bitcoin jako przedmiot...*, s. 1333.
[521] Wyrok Sądu Apelacyjnego w Warszawie z dnia 25 lutego 2021 r., II AKa 72/20, LEX nr 3189608.

> próżnobyśmy zatem szukali ścisłej analogii i starali się oprzeć konstrukcje i klasyfikacje przestępstw przeciwko mieniu i prawom majątkowym na koncepcjach i rozgraniczeniach prawa cywilnego, prawo cywilne będzie nam czasami służyło pomocą przy wyświetlania niektórych zagadnień, ale będziemy musieli przedewszystkiem posługiwać się odrębnemi pojęciami karnoprawnemi w zakresie stosunków i praw majątkowych człowieka. W prawie karnem mianowicie rzeczy i stosunki faktyczne wysuwają się na plan pierwszy, komplikacje stosunków i pretensji prawnych odegrywać mogą tylko role pomocniczą[522].

Skoro wiele osób, również przestępcy, czerpią korzyści finansowe z posiadania bitcoinów, to zarządzanie nimi musi kreować prawa majątkowe.

Niektórzy przedstawiciele doktryny prawa karnego prezentują tymczasem zachowawcze podejście co do uznania, że kryptowaluty stanowią przedmiot czynności wykonawczej w rozumieniu art. 299 § 1 k.k., a nawet odmawiają im przymiotu prawa majątkowego. Błędne jest stanowisko A. Behana, który twierdzi, że:

> w prawie cywilnym znane są różne dobra niematerialne, jak na przykład utwór audio czy wideo, który może mieć postać cyfrową. Jednakże film zapisany na dysku komputera będzie składał się z zestawu zer i jedynek stanowiących ów utwór. Tego w istocie nie ma w przypadku Bitcoina, gdyż zakup waluty wirtualnej jest – od strony informatycznej – „zakupem" matematycznego uprawnienia do podpisania transakcji. O ile w przypadku zakupu utworu można go odtworzyć czy choćby nawet zapisać na kartce papieru w postaci samych zer czy jedynek, o tyle w przypadku bitcoina nie jest to możliwe, ponieważ taki obiekt po prostu nie istnieje[523].

A. Behan formułowane wnioski opiera tylko i wyłącznie na technicznej naturze bitcoina, tracąc z pola widzenia fakt, że jego status uzależniony jest nie tylko od „zero-jedynkowej" budowy komputerowego kodu, ale także faktycznego znaczenia i roli kryptowalut w sferze prawa prywatnego i publicznego, tj. zdolności do kreowania stosunków obligacyjnych, zobowiązań publicznoprawnych i faktycznej wartości ekonomicznej związanej z posiadaniem BTC. Zresztą można wyobrazić sobie, że sam utwór, o którym pisze A. Behan, zostanie stokenizowany do postaci danych umieszczonych w blockchainowym protokole i wówczas nie straci on przymiotu prawa majątkowego, podobnie jak nie traci go token nazywany bitcoinem.

W. Wróbel, przełamując własne wątpliwości co do możliwości zakwalifikowania waluty wirtualnej jako prawa majątkowego, ostatecznie stwierdza, że władanie nią

> łączy się z posiadaniem pewnych uprawnień. Może to prowadzić do wniosku, że uznanie waluty wirtualnej za prawo majątkowe nie wykracza poza rezultat wykład-

[522] W. Makowski, *Prawo karne. O przestępstwach w szczególności. Wykład porównawczy prawa karnego austryackiego, niemieckiego i rosyjskiego obowiązującego w Polsce*, Warszawa 1924, s. 384, [w:] T. Tyburcy, *Mienie jako przedmiot ochrony w prawie karnym (na wybranych przykładach)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2018, r. XXII, z. 3, k. 71.

[523] A. Behan, *Waluty wirtualne jako*…, s. 533–534.

> niczy wynikający z zastosowania wykładni językowej art. 299 § 1 k.k." [524]. Taki punkt widzenia – pisze dalej W. Wróbel – korespondowałby również z dobrem prawnym chronionym przez art. 299 § 1 k.k. Nie ulega bowiem wątpliwości, że lokowanie korzyści pochodzących z przestępstwa w walutę wirtualną i jej dalsza zamiana na inną walutę wirtualną godzi w obrót gospodarczy i interesy majątkowe w obrocie cywilnoprawnym[525].

Część autorów jednoznacznie akceptuje pogląd, że kryptowaluty stanowią nie tylko „inne prawa majątkowe", ale nawet zawężają je do pojęcia „mienie". M. Sawicki postuluje za szerokim ujęciem „mienia" w prawie karnym. Komentując art. 287 k.k., twierdzi on, że mienie „należy rozumieć jako zbiorczą nazwę dla wszystkich praw majątkowych, których potwierdzeniem (dowodem istnienia) jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym związany jest taki zapis"[526]. P. Chmielarz wskazuje, że chociaż „nadal brakuje odpowiedzi na pytanie o cywilnoprawny charakter kryptowalut", to jednak w przypadku podziału majątku wspólnego jest możliwy „podział" bitcoinów[527]. Za uznaniem kryptowaluty jako prawa majątkowego opowiada się także A. Petrys[528]. J. Liberacki, analizując charakter karnistyczny bitcoina, dochodzi do wniosku, że choć BTC nie jest prawem majątkowym i trudno uznać, że pozostaje składnikiem mienia (majątku), to może pośrednio stanowić przedmiot przestępstw, które w swoich znamionach zawierają terminy „mienie" lub „majątek". Potencjalne działanie sprawcy należy jednak badać z perspektywy nie samego bitcoina, ale całej sytuacji faktycznej związanej z możliwością dysponowania nim, tj. zarejestrowaniem danego bitcoina i dysponowaniem kluczem prywatnym, który jest do niego przypisany, a to ze względu na fakt, że z bitcoinem jest związana pewna wartość ekonomiczna i istnieją w obrocie podmioty, które płacą za BTC[529]. Nie wdając się w szczegóły wywodu J. Liberackiego, bez analizy takich kontrowersyjnych stwierdzeń, jak „zarejestrowanie bitcoina" oraz zrównanie pojęcia „mienia" z „majątkiem", najistotniejsze jest to, że ww. autor uznaje kryptowaluty za przedmiot czynności wykonawczej opisany w art. 299 § 1 k.k. J. Budziński ma rację, twierdząc, że dobra wirtualne jako dobra przedstawiające wartość materialną (ekonomiczną) mogą być przedmiotem innych praw majątkowych, a co za tym idzie, można przypisać im status mienia. Autor odwołuje się w tym zakresie do poglądów P. Nazaruka[530] piszącego, że prawo majątkowe pozostaje w ścisłym związku z ekonomicznym interesem uprawnionego niezależnie od tego, czy w konkretnej sytuacji za prawo takie

[524] W. Wróbel, S. Tarapata, *Komentarz do art. 299 k.k.*, *teza 29*, [w:] *Komentarz do Kodeksu karnego*, red. A. Zoll, W. Wróbel, LEX, stan prawny: 1 września 2021 r.
[525] Tamże.
[526] M. Siwicki, *Prawo karne wobec oszustw i innych związanych z nimi przestępstw…*, s. 174.
[527] P. Chmielarz, *Bitcoin a podział majątku wspólnego*, „Homo Politicus" 2019, nr 14 s. 23.
[528] A. Petrys, *Bitcoin – współczesna alternatywa…*
[529] J. Liberacki, *Karnoprawne aspekty walut kryptograficznych...*
[530] P. Nazaruk, *Komentarz do art. 44 kodeksu cywilnego teza 2...*

można uzyskać pewną sumę pieniężną lub inne dobro. Oznacza to, że o ile dane dobro posiada wartość majątkową, to może w stosunku do niego przysługiwać prawo majątkowe nawet wtedy, gdyby jego sprzedaż była w danym momencie zabroniona lub niemożliwa. W przeciwieństwie do własności, przedmiotem innych praw majątkowych mogą być zarówno rzeczy, jak i przedmioty niebędące rzeczami, np. wierzytelności czy energia gazowa[531], a więc także waluty wirtualne.

Praktyka funkcjonowania organów ścigania pokazuje, że wielokrotnie uznawały one altcoiny za przedmiot czynności wykonawczej „prania pieniędzy", a poniżej przedstawiono przykładową treść ogłoszonego przestępcy zarzutu potwierdzającą, że kryptowaluty to przedmiot czynności wykonawczej, należący do znamion przestępstwa prania pieniędzy; prokurator Prokuratury Okręgowej w Zielonej Górze oskarżył mężczyznę o to, że:

> w okresie od 21 maja 2014 r. do 14 października 2014 r. w Warszawie w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru wspólnie i w porozumieniu z innymi nieustalonymi osobami w celu osiągnięcia korzyści majątkowej czyniąc sobie stałe źródło dochodu, podejmował czynności zmierzające do udaremnienia stwierdzenie przestępnego pochodzenia oraz miejsca przechowywania środków pieniężnych w ten sposób, że wykorzystując będący w jego dyspozycji uprzednio założony przez D. H. rachunek bankowy w /…/ Bank o numerze /…/ oraz zakładane na jego podstawie kolejne rachunki bankowe na dane osobowe D. H. przyjął na w/w rachunek środki pieniężne
> - na konto nr /…/ w okresie od 20 czerwca do 2 lipca 2014 r. w kwocie 15 331,00 zł oraz przyjął na kolejne rachunki bankowe, które założył poprzez bankowość elektroniczną na dane osobowe D. H. poprzez ich weryfikację za pośrednictwem konta założonego przez D. H. w /…/ Bank
> - na konto w /…/ o nr /…/ w okresie od 6 czerwca 2014 r. do 3 lipca 2014 r. w kwocie 5683,00 zł
> – na konto /…/ Bank o nr /…/ w okresie od 30 maja 2014 r. do 20 czerwca 2014 r. w kwocie 9 139,00 zł
> - na konto w /…/ Bank o nr /…/ w okresie od 21 maja 2014 r. do 2 czerwca 2014 r. w kwocie 4488,04 zł
> - na konto w /…/ o nr /…/ w okresie od 9 czerwca 2014 r. do 8 lipca 2014 r. w kwocie 7 760,00 zł
> - na konto w /…/ o nr /…/ w okresie od 5 czerwca 2014 r. do 12 czerwca 2014 r. w kwocie 1705,00 zł

[531] J. Budziński, *Luka prawna w zakresie karnoprawnych kwalifikacji dla zaboru przedmiotów wirtualnych w internetowych grach komputerowych*, „Probacja" 2020, nr 3, s. 156–157.

- na konto w /…/ o nr /…/ w okresie od 13-14 października 2014 r. w kwocie 5240,80 zł wiedząc iż wpłaty te pochodzą z korzyści związanych z popełnieniem czynów zabronionych – przez inne osoby – oszustw dokonanych na portalu aukcyjnym allegro.pl polegających na wprowadzeniu w błąd za pośrednictwem sieci informatycznej, co do faktycznych danych osobowych sprzedającego towar na portalu aukcyjnym allegro.pl oraz zamiaru wywiązania się z umowy sprzedaży wystawionego do sprzedaży towaru i doprowadzeniu w ten sposób innych osób do niekorzystnego rozporządzania mieniem przez inne nieustalone osoby, a następnie zgodnie z dyspozycją tych osób dokonywał dalszego przekazania przedmiotowych środków, w ten sposób, że z konta /…/ Bank przekazał pieniądze na konto założone na dane osobowe K. S., a z pozostałych w/w kont przekazał pieniądze za pośrednictwem systemu płatności „dotpay" celem zakupu kryptowaluty na adresach w Bitmarket.pl, które założył na dane osobowe D. H. pod nazwami /…/, /…/ przypisując im określony login i hasła, do których miał dostęp, oraz na adres /…/, z których to adresów przekazywał dalej na kolejne adresy w Bitmarket.pl udaremniając w ten sposób lub znaczenie utrudniając stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia uzyskując w zamian korzyść majątkową w kryptowalucie w wysokości, co najmniej 10% wartości wytransferowanych środków z konta bankowego na Bitmarket.pl, tj. co najmniej 4935,00 zł. tj. o czyn z art. 299 § 1, 5 kk w zw. z art. 12 kk i art. 65 § 1 kk[532]

W sprawie nadzorowanej przez Prokuraturę Okręgową w Warszawie sprawca został oskarżony o to, że:

w okresie od 6 listopada 2017 roku do dnia 8 stycznia 2018 roku, w bliżej nieustalonych miejscach, a ujawnionych w Warszawie przyjął na założone przez siebie z wykorzystaniem konta mailowego /…/@t.pl anonimowe portfele Bitcoin prowadzone na giełdzie kryptowalut BitBay Sp. z o.o., z.s. w Katowicach prawa majątkowe w postaci kryptowaluty bitcoin,
Na adres portfela 3BMBhk/…/ – w dniu 2017-11-06 – 0,0143082 BTC (tj.100,42 USD), oraz w dniu 2018-01-06 – 0,00979018 BTC (tj. 163,21 USD)
Na adres portfela 3BRHHb/…/ – w dniu 2017-11-07 – 0,02324423 BTC (tj.165,04 USD)
Na adres portfela 3M44Au/…/ - w dniu 2017-11-22 0,01373533 BTC (t.j.112,04 USD), 2017-11-22 w dniu 0,0149031 BTC (t.j.121,63 USD),
Na adres portfela 3Jb52a/…/ – w dniu 2017-11-29 – 0,01270176 BTC (t.j. 138,52 USD)

[532] Akta Prokuratury Okręgowej w Zielonej Górze o sygn. PO I Ds. 43.2016.

Na adres portfela 39YMB2/…/ – w dniu 2017-12-07 – 0,01414318 BTC (tj. 219,52 USD), w dniu 2017-11-29 – 0,01349856 BTC (131,81 USD)
Na adres portfela 3B3Vyj/…/ – w dniu 2017-11-29 – 0,01323393 BTC (t.j. 132,45 USD)
Na adres portfela 3E5f81/…/ w dniu 2018-01-08 – 0,00809819 BTC (t.j.124,14 USD)
co łącznie odpowiada kwocie 1408,78 USD stanowiących równowartość 5 071, 6 złotych, pochodzące z korzyści związanych z popełnieniem czynów zabronionych w postaci oszustw internetowych polegających na podszywaniu się pod inne podmioty, przesyłaniu złośliwego oprogramowania ransomware, a po zaszyfrowaniu danych informatycznych znajdujących się na komputerze pokrzywdzonego, żądaniu opłaty za przekazanie klucza deszyfrującego dane,
a następnie za pośrednictwem giełdy kryptowalut BitBay Sp. z o.o., dokonał ich konwersji z kryptowaluty bitcoin na Euro i przekazał na prowadzony w Belgii rachunek bankowy o numerze BE61 0016 /…/, przy czym działał w celu udaremnienia lub znacznego utrudnienia stwierdzenia przestępnego pochodzenia lub miejsca umieszczenia, wykrycia lub zajęcia przekazanych mu przez pokrzywdzonych za odszyfrowanie komputerów środków, czyniąc sobie z popełnienia przestępstwa stałe źródło dochodu
- tj. o czyn z art. 299 § 1 kk w zw. z art. 65 §1 k.k.[533]

Mając powyższe na uwadze, jako prawidłową należy ocenić praktykę stosowania art. 299 k.k. do walut wirtualnych, a ponadto odnosi się do nich art. 291 k.p.k. Zgodnie z tytułem rozdziału 32 k.p.k. przedmiotem zabezpieczenia majątkowego może być mienie podejrzanego/oskarżonego, a pogląd wyrażający się w stwierdzeniu, iż na gruncie prawa karnego kryptowaluta stanowi mienie, nie budził wątpliwości u prokuratorów wielokrotne stosujących zabezpieczenie majątkowe na bitcoinie i altcoinach[534].

5.5. Zabezpieczenie majątkowe na kryptowalutach

Temat zabezpieczenia majątkowego na kryptowalutach od pewnego czasu jest intensywnie eksploatowany przez organy ścigania, bowiem coraz częściej ujawnia się takie wartości majątkowe, które podlegają zajęciu. Wbrew pozorom, metodyka postępowania w takim przypadku jest stosunkowo prosta w porównaniu z trudnością zadania polegającego na ustaleniu, gdzie znajdują się tokeny oraz jak uzyskać do nich dostęp. Patrząc na statystyki dotyczące wszystkich powszechnych jednostek prokuratury w Pol-

[533] Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.
[534] Zabezpieczenie majątkowe, którego przedmiot stanowiły kryptowaluty, ustanowiono m.in. w następujących sprawach: Prokuratury Regionalnej w Katowicach o sygn. akt RP. I Ds. 16.2018, Prokuratury Okręgowej w Gliwicach o sygn. akt PO I Ds. 37.2018, Prokuratury Okręgowej w Nowym Sączu o sygn. akt PO IX Ds. 7.2017.Sp, Prokuratury Okręgowej w Jeleniej Górze o sygn. akt PO IV Ds. 37.2017.

sce, to w czerwcu 2023 r. łączna liczba pozostających na biegu spraw, w których wydano postanowienie o zabezpieczeniu majątkowym na kryptowalucie lub zajęto takie jednostki w charakterze dowodów rzeczowych, wyniosła 125, a wartość zajętych kryptowalut stanowiła ponad 23 mln zł. Jeśli chodzi o liczbę takich postanowień wydanych w minionych latach, to kształtowała się ona następująco: 2019 r. – 29, 2020 r. – 43, 2021 r. – 75, 2022 r. – 39, do połowy 2023 r. – 75 postanowień. Co ważne, większość spraw, gdzie zabezpieczono kryptowaluty, zakończyła się skierowaniem do sądu aktu oskarżenia, chociaż liczba umorzeń z powodu niewykrycia sprawcy uplasowała się na drugim miejscu[535].

Jednego z pierwszych quasi-zabezpieczeń majątkowych na kryptowalucie dokonano w sprawie prowadzonej w 2015 r. przez Prokuraturę Okręgową w Katowicach, dotyczącej grupy hakerów. Trzej mężczyźni przeprowadzili wyrafinowane cyberataki na urzędy gminne w całej Polsce z wykorzystaniem zaawansowanych narzędzi teleinformatycznych oraz socjotechniki[536], a skradzione z rachunków bankowych pieniądze zamienili na bitcoiny, wykorzystując do tego nieistniejącą już giełdę Bitcurex, a następnie przelali BTC do własnych portfeli. W trakcie śledztwa dwóch podejrzanych przyznało się do popełnienia zarzucanych im czynów i ujawnili posiadane bitcoiny. Procedura ich przejęcia przez organy ścigania przebiegała w specyficzny sposób: podczas przesłuchania mężczyzna, korzystając z pomocy osoby obeznanej w kryptowalutach i działając pod ścisłym nadzorem funkcjonariuszy policji, zalogował się na platformę hakerską w darknecie, nawiązał kontakt ze współsprawcami przestępstwa i nakłonił ich do przelania jego części bitcoinów na podany adres portfela. Potem zalogował się do konta ze służbowego komputera policjantów i wystawił do sprzedaży ponad 59 BTC na jednej z polskich giełd kryptowalutowych. Aktywa upłynniono po najkorzystniejszym kursie, a otrzymane złotówki przelano na rachunek bankowy znajdujący się w posiadaniu przestępcy i wcześniej zablokowany przez prokuratora. Wszystkie czynności opisano szczegółowo w protokole wyjaśnień złożonych przez hakera, a na końcu referent sprawy wydał postanowienie o zabezpieczeniu majątkowym przekonwertowanych środków[537].

Kolejny etap kształtowania się omawianej praktyki należał do instytucji eksperymentu procesowego, w trakcie którego ujawnione, pochodzące z przestępstwa bitcoiny zamieniano na giełdzie kryptowalutowej na bezgotówkowy pieniądz bankowy i stamtąd przelewano na rachunek będący w dyspozycji organów ścigania. Korzystano jednocześnie z pomocy biegłego; w jednej z prokuratur białostockich powołano go „w celu udziału w eksperymentach procesowych w toku których dokonane zostanie zajęcie środków waluty wirtualnej".

[535] Dane z systemu elektronicznego prokuratury PROK – SYS [dostęp: 12.07.2023].

[536] Okoliczności popełnienia tego przestępstwa i *modus operandi* jego sprawców zostały dokładnie opisane w: P. Opitek, *Przestępczość z wykorzystaniem kryptowalut oraz ich status w postępowaniu karnym*, [w:] *Przestępczość teleinformatyczna 2017. Rozdział 12*, red. J. Kosiński, Szczytno 2018, s. 23.

[537] Akta Prokuratury Okręgowej w Katowicach o sygn. V Ds. 103/15.

Wspomniana metodyka była obarczona błędami procesowymi, bo zgodnie z art. 211 k.p.k. „w celu sprawdzenia okoliczności mających istotne znaczenie dla sprawy można przeprowadzić w ramach eksperymentu procesowego doświadczenie lub odtworzenie przebiegu stanowiących przedmiot rozpoznania zdarzeń lub ich fragmentów". Eksperyment procesowy może przybrać dwie formy:

1. doświadczenia: chodzi o sprawdzenie możliwości wystąpienia faktów lub zjawiska oraz spostrzegania ich w określonych warunkach. Doświadczenie nie musi być realizowane na miejscu zdarzenia ani być ściśle powiązane z jego przebiegiem;
2. odtworzenia: jest ono rekonstrukcją polegającą na sprawdzeniu, czy zdarzenie lub jego fragment mogło zajść w określonych okolicznościach, dlatego czynność taka powinna być przeprowadzona w warunkach niemalże identycznych do tych, w jakich przebiegał czyn stanowiący przedmiot śledztwa.

Charakter prawny eksperymentu procesowego pokazuje, że brak jest podstaw do jego stosowania w celu realizacji zabezpieczenia majątkowego na walutach wirtualnych, a tym bardziej ich sprzedaży. W takich przypadkach nie sposób mówić o eksperymencie jako doświadczeniu, bowiem z góry wiadome jest, że transfer kryptowaluty między portfelami i wymiana BTC na złotówki są wykonalne. Także nie wchodzi w grę odtworzenie, gdyż taki eksperyment nie polega na powtórzeniu krok po kroku zachowania sprawcy przestępstwa, a chodzi jedynie o konwersję bitmonet na pieniądze. Teoretycznie możliwa jest sytuacja, kiedy w toku postępowania przygotowawczego rzeczywiście zajdą okoliczności do zastosowania art. 211 k.p.k., np. linia obrony podejrzanego będzie polegała na wyjaśnieniach, że z powodów technicznych nie mógł użyć do transferu BTC aplikacji sprzętowej zainstalowanej na dysku twardym dowodowego komputera. Wtedy organ procesowy może zweryfikować jego alibi w formie eksperymentu, z wykorzystaniem zabezpieczonego komputera i podjąć próbę przelania symbolicznej kwoty kryptowaluty. W podobnych, wyjątkowych sytuacjach chodzić będzie o rekonstrukcję i sprawdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy[538].

Realizacja zabezpieczenia poprzez zamianę kryptowaluty na pieniądz fiducjarny już na samym początku śledztwa miała praktyczne zalety: nie wymagała posiadania własnego portfela przez organy ścigania i przetrzymywania w nim „ulotnych" środków, a ponadto likwidowała problem znacznych wahań kursów bitmonet. Takie postępowanie nie znajdowało jednak oparcia w przepisach prawa. Modelowy sposób realizacji zabezpieczenia na kryptowalutach zastosowano dopiero w śledztwie prowadzonym w 2017 r. przez Prokuraturę Okręgową w Jeleniej Górze. Sprawa dotyczyła internetowych oszustów, którzy na portalach aukcyjnych wystawiali fałszywe oferty sprzedaży maszyn rolniczych i budowlanych. Sprawcy byli oskarżeni o to, że:

[538] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*…, s. 425–426.

w okresie od 4 do 22 kwietnia 2016 r. w /…/, działając w krótkich odstępach czasu, w wyniku z góry powziętego zamiaru, w celu osiągnięcia korzyści majątkowej, doprowadzili do niekorzystnego rozporządzenia mieniem obywatela Holandii M. J. w kwocie 21.500 EURO, co stanowi równowartość 92.220,60 zł oraz rumuńską Spółkę o nazwie /…/ w kwocie 60.000 EURO, co stanowi równowartość 257.310,00 zł, a w łącznej kwocie 81.500 EURO o równowartości 349.530,60 zł stanowiące mienie znacznej wartości w ten sposób, że po uprzednim założeniu rachunku bankowego w oddziale /…/ Banku o nr /…/ na nazwisko /…/ i wprowadzeniu w błąd M. J., co do zamiaru wywiązania się z umowy sprzedaży buldożera marki Komatsu oraz C.-V. B. i C.-M. B. działających w imieniu /…/, co do zamiaru wywiązania się z umowy sprzedaży autokaru marki Setra doprowadzili do zawarcia umów sprzedaży wyżej wymienionych pojazdów, a po przyjęciu pieniędzy od pokrzywdzonych na rachunek umówionych pojazdów nie dostarczyli zaś za pieniądze uzyskane w wyniku umów zakupili tzw. kryptowalutę BitCoin, czym działali na szkodę M. J. oraz /…/, tj. o czyn z w art. 286 § 1 kk w zw. z art. 294 § 1 kk w zw. z art. 12 kk[539].

Pokrzywdzeni wpłacili zaliczki tytułem zawarcia przyszłej umowy, ale do finalizacji transakcji nigdy nie doszło. Otrzymane od pokrzywdzonych pieniądze przestępcy zamieniali na BTC i składowali na giełdzie kryptowalutowej. Po ich zatrzymaniu prokurator wykonał wobec ujawnionej kryptowaluty następujące czynności procesowe:

1. wydał postanowienie o zabezpieczeniu majątkowym w bitcoinach tytułem grożącego podejrzanym obowiązku naprawienia szkody wyrządzonej przestępstwem w kwocie 350 000 zł oraz przepadku osiągniętej w ten sposób korzyści majątkowej. Zabezpieczenia wykonano poprzez zajęcie tokenów znajdujących się na wirtualnym koncie sprawcy „podpiętym" do giełdy kryptowalutowej (wcześniej konto zablokowano);
2. zmienił następnie postanowienie w ten sposób, że bitmonety zostały przelane na inne konto giełdy utworzone specjalnie na potrzeby prowadzonego śledztwa;
3. wystosował do sądu wniosek o nadanie klauzuli wykonalności postanowieniu o zarządzeniu sprzedaży zabezpieczonych środków;
4. wydał postanowienie o sprzedaży z wolnej ręki 8 BTC,
5. organ egzekucyjny, tj. naczelnik właściwego urzędu skarbowego, na podstawie art. 154 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji[540] dokonał zabezpieczenia należności pieniężnych (formularzu ZZ-1) i sprzedał bitcoiny;
6. uzyskane złotówki, stanowiące zabezpieczenie majątkowe, organ egzekucyjny przekazał na rachunek sum depozytowych prowadzony przez Sąd Okręgowy w Jeleniej Górze.

[539] Akta Prokuratury Okręgowej w Jeleniej Górze o sygn. PO IV Ds. 37.2017.
[540] Dz. U. z 1966 r. Nr 24, poz. 151 z późn. zm.

Odrzucić należy błędną praktykę polegającą na wydawaniu postanowień o uznaniu za dowód rzeczowy kryptowalut. Kodeks postępowania karnego nie zna takiej instytucji, tj. uznania śladów za dowód rzeczowy, gdyż formą ich procesowego zabezpieczenia są czynności procesowe dokumentowane protokołem oględzin lub przeszukania. Problematykę postępowania z dowodami rzeczowymi normują przepisy rozdziału 25 k.p.k. i żaden z nich, oraz innych rozdziałów k.p.k., nie stanowi podstawy do podejmowania przez organ procesowy dodatkowej czynności nadającej zatrzymanej do sprawy rzeczy statusu dowodu rzeczowego, a tym bardziej nie uzależnia takiego statusu rzeczy od wydania postanowienia o uznaniu jej za dowód rzeczowy. Pojęcie „uznania za dowód rzeczowy" nie występuje w Kodeksie postępowania karnego. Natomiast „postanowienie w przedmiocie dowodów rzeczowych", którego zaskarżalność przewiduje art. 236 § 1 k.p.k., to rodzajowe określenie każdego postanowienia zawierającego rozstrzygnięcie odnoszące się do rzeczy stanowiącej dowód w sprawie. Zawarte we wspomnianym przepisie pojęcie „postanowienie w przedmiocie dowodów rzeczowych", jak tożsame zakresowe z określeniem „postanowienie co do dowodów rzeczowych" (art. 323 § 1 k.p.k.), choć są one kategoriami zbiorczymi, to jednak obejmują swoim zakresem wyłącznie takie decyzje, dla których podjęcia istnieje ustawowa podstawa prawna, a ustawa karnoprocesowa nie przewiduje takiej czynności, jak „uznanie za dowód rzeczowy". Co więcej, podstawy prawnej dla wydania takiego postanowienia, nawet tytułując go jako „postanowienie w przedmiocie dowodów rzeczowych", nie stwarza przywoływany już art. 236 § 1 k.p.k. Przepis ten posługuje się wprawdzie pojęciem „postanowienie w przedmiocie dowodów rzeczowych", jednak stanowi on jedynie normę legitymizującą zaskarżalność wskazanych w nim decyzji oraz normę kompetencyjną – w zakresie, w jakim wskazuje organ właściwy do ich rozpoznania. Stąd też, odwołując się również do ugruntowanych poglądów nauki prawa i dotyczących zakresu zażalenia (art. 236 § 1 k.p.k.), uznać należy, że w odniesieniu do orzeczeń w przedmiocie dowodów rzeczowych, to decyzje takie dotyczą np. postanowień o zwrocie rzeczy (art. 230 § 1 i 2 k.p.k.) czy przekazaniu rzeczy właściwemu urzędowi lub instytucji (art. 230 § 3 k.p.k.) [541].

Argumentowanie, że nadawanie rzeczy statusu dowodu rzeczowego w drodze postanowienia jest konieczne dla zagwarantowania osobom, których odnoszące się do rzeczy prawa zostały naruszone, dostatecznej ochrony prawnej przez wprowadzenie możliwości zaskarżenia takiego orzeczenia, jest nieprzekonujące. Prawa tych osób dostatecznie zagwarantowane są poprzez możliwość zaskarżenia czynności, w wyniku których rzeczy zostały zajęte przez organ procesowy (np. art. 217 § 3 zdanie pierwsze k.p.k. i art. 228 § 3 k.p.k.). Co więcej, przyjęcie poglądu, że zaskarżalnym postanowieniem w przedmiocie dowodów rzeczowych, o którym mowa w art. 236 § 3 k.p.k., objęte są również inne rozstrzygnięcia niż określone w art. 230–233 k.p.k., do których odwołuje się tożsamy zakresowo przepis art. 323 § 1 k.p.k., prowadziłoby do wniosku o nieracjonalności ustawodawcy, stwarzającego podstawy do dwukrotnego

[541] Tamże.

zaskarżania tych samych czynności przez te same osoby, co jednocześnie pozostawałoby w sprzeczności z zasadą ekonomiki procesowej[542].

Powracając do realizacji zabezpieczenia majątkowego na kryptowalutach, to kolejnym etapem kształtowania się metodyki postępowania w tym zakresie stanowiła wydana w 2018 r. przez Prokuraturę Krajową książka pt. *Metodyka zabezpieczeń majątkowych*, której jeden rozdział dotyczył kryptowalut[543]. Natomiast w lipcu 2023 r. Departament do Spraw Cyberprzestępczości i Informatyzacji w Prokuraturze Krajowej wystosował pismo instruktażowe dla prokuratorów, na temat procesowego zabezpieczenia kryptowalut w formie zabezpieczenia majątkowego lub dowodów rzeczowych[544]. Nie wdając się w szczegóły instrukcji, warto jedynie zwrócić uwagę na przyjęte rozwiązania w kwestiach kluczowych.

W piśmie podkreślono, że waluta wirtualna może być uznana za dowód, a zatem również za dowód rzeczowy, a jednocześnie jest cyfrowym odzwierciedleniem wartości, o którym mowa w art. 2 ust. 2 pkt 26 u.p.p.p., gdyż posiada określoną wartość majątkową. Wobec powyższego, w toku prowadzonych postępowań karnych zasadne jest procedowanie w stosunku do waluty wirtualnej, w zależności od ustalonego stanu faktycznego, w dwojaki sposób:

1. dokonując zabezpieczenia majątkowego na kryptowalucie lub
2. postępując z nią tak, jak z każdym innym dowodem rzeczowym, jeżeli ujawnione jednostki cyfrowe mają w danej sprawie znaczenie dowodowe. Wówczas zastosowanie znajdą wszystkie uregulowania rozdziału 25 k.p.k.

Nie zmienia to faktu, zaznaczono w instrukcji, że tak pozyskane dowody rzeczowe, z uwagi na swoją wartość materialną, na dalszym etapie również mogą stanowić przedmiot zabezpieczenia majątkowego. Po przetransferowaniu środków na adres zarządzany przez prokuratora należy, w zależności od dokonanych ustaleń, wydać postanowienie o zabezpieczeniu majątkowym bądź dokonać rejestracji dowodów rzeczowych.

Zdaniem autora, przyjęcie alternatywnego sposobu postępowania w stosunku do ujawnionego prawa majątkowego, tj. uznanie go za przedmiot zabezpieczenia majątkowego lub dowód rzeczowy, jest dyskusyjne. Otóż, charakter pierwotny podstawy zabezpieczonych kryptowalut oraz ich status prawny, wynikający z okoliczności śledztwa, decyduje o tym, czy mają one charakter dowodu, czy też są „owocami przestępstwa" i podlegają zabezpieczeniu majątkowemu. Wynika z tego, że decyzja w tym zakresie nie ma charakteru arbitralnej woli organu procesowego. Przepis art. 236b § 1 i 2 k.p.k. stanowi, że rzeczą lub przedmiotem w rozumieniu przepisów niniejszego rozdziału są również środki na rachunku, a postanowienie w przedmiocie dowodów rzeczowych

[542] Tamże.

[543] P. Opitek (współautor opracowania), *Metodyka zabezpieczeń majątkowych*, Prokuratura Krajowa 2018 (zbiory własne autora).

[544] Pismo instruktażowe Zastępcy Dyrektora Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z lipca 2023 r. dotyczące zabezpieczenia majątkowego na kryptowalutach, znak: 1001 – 12.024.4.2023 (zbiory własne autora), dalej jako: Pismo instruktażowe z lipca 2023 r.

może dotyczyć takich środków, jeżeli zostały zatrzymane jako dowód w sprawie. Pomijając już wątpliwości, czy adres kryptowalutowy można określić mianem „rachunku", to art. 236b k.p.k. nie przyznaje prokuratorowi kompetencji uznania czegoś za dowód rzeczowy na podstawie „postanowienia o uznaniu rzeczy (kryptowaluty) za dowód rzeczowy", ale upoważnia do postępowania ze „środkami na rachunku", tak jak stanowią o tym przepisy Rozdziału 25 k.p.k., tj. mogą one zostać np. sprzedane, jeśli zachodzą przesłanki z art. 232 k.p.k. Podsumowując, jeśli ujawnione jednostki kryptowaluty spełniają przesłanki, o których mowa w art. 291 k.p.k. i nast., to można, a w praktyce trzeba, ustanowić na nich zabezpieczenie majątkowe.

Powracając do pisma instruktażowego Prokuratury Krajowej, to wskazano w nim ponadto, że „zatrzymanie waluty cyfrowej" następuje w drodze jej dobrowolnego wydania przez właściciela portfela; inny sposób stanowi wydanie tokenów przez giełdę na podstawie postanowienia prokuratora o żądaniu wydania rzeczy. Niekiedy konieczne będzie zastosowanie właściwych przepisów międzynarodowych, regulujących procedurę zabezpieczenia mienia/dowodów rzeczowych od podmiotów zagranicznych, aby dokonać realizacji art. 291 k.p.k. W przypadku przeszukania miejsc lub osób związanych z kryptowalutami, czynności należy przeprowadzić z udziałem biegłego z zakresu informatyki bądź specjalisty od kryptowalut. W trakcie czynności zwraca się uwagę na ślady mogące stanowić adres klucza publicznego bądź prywatnego, hasła, loginy, PIN-y, kody uwierzytelniające do portfeli, informacje o transakcjach, a ponadto zabezpiecza się ujawnione karty płatnicze, nośniki danych informatycznych itp. Dążyć trzeba, jeśli to możliwe, do ujawnienia portfeli papierowych i sprzętowych, urządzeń do uwierzytelniania dwuskładnikowego oraz zabezpieczyć wszelkie nośniki elektroniczne, na których mogą być zainstalowane portfele desktopowe czy webowe, bądź znajdować się wiadomości SMS z kodami autoryzacyjnymi, wiadomości mailowe dotyczące kryptowalut lub tzw. seed. W przypadku ujawnienia tokenów cyfrowych zachodzi konieczność niezwłocznego objęcia ich w samoistne posiadanie przez organy ścigania, a po przetransferowaniu jednostek na portfel prokuratury dokonuje się zabezpieczenia majątkowego lub rejestracji jednostek. W zależności od ustalonego stanu faktycznego, konieczne może okazać się zablokowanie tokenów zdeponowanych na giełdzie, kierując się art. 86 ust. 10 u.p.p.p. W zakresie postępowania z kryptowalutami po ich zabezpieczeniu należy rozstrzygnąć, czy tokeny przechowywać w pierwotnej postaci, czy może sprzedać. Praktyczniejsza jest sprzedaż waluty wirtualnej na podstawie art. 232 § 1 k.p.k. według trybu określonego dla właściwych organów postępowania wykonawczego, tj. komornika lub naczelnika urzędu skarbowego, przy czym sprzedaży dokonuje organ egzekucyjny, nie prokurator. W pierwszej kolejności wydaje się postanowienie o zarządzeniu sprzedaży zabezpieczonych środków, którego przedmiot stanowią tokeny zabezpieczone na podstawie art. 292 k.p.k. (ich wartość zostanie pomniejszona o koszt opłaty transakcyjnej). W przypadku zbycia dokonywanego według Kodeksu postępowania cywilnego, należy wystąpić do właściwego sądu o nadanie klauzuli wykonalności

postanowieniu o sprzedaży, które doręcza się właściwemu organowi egzekucyjnemu. Nie zachodzi jednak konieczność transferu kryptowaluty, podlegającej sprzedaży, na portfel organu egzekucyjnego, gdyż przedmiot czynności widoczny jest na publicznie dostępnym „prokuratorskim" adresie. W piśmie instruktażowym nakazano przechowywać zabezpieczone kryptowaluty na portfelach zewnętrznych, papierowych lub sprzętowych, a decyzja o wyborze rodzaju portfela należy do referenta sprawy i podyktowana jest rodzajem i charakterem zabezpieczenia. Administratorem portfela skonfigurowanego na potrzeby konkretnego śledztwa jest wówczas prokurator. W piśmie polecono założenie na potrzeby prowadzonych postępowań portfeli zewnętrznych w każdej prokuraturze regionalnej oraz okręgowej, które służyć powinny tylko do czasowego przechowywania kryptowalut, zabezpieczonych w nagłych sytuacjach procesowych. W przypadku planowanego pozyskiwania waluty wirtualnej w toku śledztwa należy utworzyć indywidualny portfel zewnętrzny, administrowany przez prokuratora, w zależności od potrzeb papierowy bądź sprzętowy, służący do przetransferowania skonkretyzowanych środków[545].

Obecnie w prokuraturach w całej Polsce skutecznie i profesjonalnie realizuje się zabezpieczenia majątkowe na kryptowalutach, tak jak miało to miejsce w sprawie Prokuratury Okręgowej w Gliwicach. Podejrzani stali pod zarzutem popełnienia przestępstw z ustawy o przeciwdziałaniu narkomanii[546], a prokurator ujawnił stanowiące ich własność i pochodzące z przestępstwa jednostki kryptowaluty. Na podstawie art. 291 § 1 pkt 3 k.p.k., art. 292 § 2 k.p.k. oraz art. 293 § 1 i 2 k.p.k. w dniu 3 czerwca 2022 r. wydano postanowienie o zabezpieczeniu majątkowym; w decyzji napisano:

> zabezpieczyć na mieniu podejrzanego /…/ grożący mu przepadek równowartości korzyści majątkowej pochodzącej z przestępstwa w kwocie co najmniej /…/ zł poprzez dokonanie zajęcia praw majątkowych do jednostek waluty cyfrowej, a mianowicie praw do:
> - /…/ BTC, co na dzień 3 czerwca 2022 roku stanowi równowartość kwoty /…/ złotych, które to jednostki zapisane są aktualnie na portfelu publicznym o adresie /…/
> - /…/ ETH, co na dzień 3 czerwca 2022 roku stanowi równowartość kwoty /…/ złotych, które to jednostki zapisane są aktualnie na portfelu publicznym o adresie /…/
> do których klucze prywatne znajdują się wyłącznie w posiadaniu Prokuratury Okręgowej w Gliwicach, a które to jednostki zostały ujawnione przez biegłego z zakresu blockchain i kryptowalut[547]

W uzasadnieniu do postanowienia prokurator wskazał m.in., że kryptowalutę ujawniono w trakcie czynności przeszukania i została ona przetransferowana na adresy

[545] Pismo instruktażowe z lipca 2023 r.
[546] Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2023 r. poz. 1939).
[547] Akta Prokuratury Okręgowej w Gliwicach o sygn. PO I Ds. 26.2021.

wskazane w sentencji postanowienia, należące do portfela administrowanego przez Prokuraturę Okręgową w Gliwicach. Następnie 18 czerwca 2022 r. prokurator wydał postanowienie „o sprzedaży praw majątkowych do waluty cyfrowej będącej przedmiotem zabezpieczenia majątkowego" na podstawie art. 293 § 3 k.p.k. w zw. z art. 232 § 1 k.p.k., które brzmiało:

> sprzedać, według trybu określonego dla właściwych organów postępowania wykonawczego, z uwagi na nadmierne trudności w przechowywaniu, a także znaczne ryzyko obniżenia wartości, prawa majątkowe do jednostek waluty cyfrowej, a mianowicie prawa do:
> - /…/ BTC, które to jednostki zapisane są aktualnie na portfelu publicznym o adresie /…/
> - /…/ ETH, które to jednostki zapisane są aktualnie na portfelu publicznym o adresie /…/
> zabezpieczone na mieniu podejrzanego /…/ będące przedmiotem wydanego w dniu 3 czerwca 2022 r. postanowienia o wykonania grożącego podejrzanemu przepadku równowartości korzyści majątkowej pochodzącej z przestępstwa w kwocie /…/ zł

W uzasadnieniu podjętej decyzji prokurator wskazał, że przechowywanie zabezpieczonych tokenów generuje trudności ze względu na potencjalne ataki hakerskie na portfel kryptowalutowy, duże wahania kursów cen bitcoinów i ethereum, „problemy z zachowaniem poufności" danych, co skutkuje obawą zapoznania się z kluczami prywatnymi przez osoby trzecie; brak ponadto precyzyjnych regulacji prawnych dotyczących walut wirtualnych. Zwieńczenie całej procedury stanowił wystosowany przez prokuratora wniosek do właściwego naczelnika urzędu skarbowego o wszczęcie postępowania na podstawie art. 292 § 3 k.p.k. w zw. z art. 232 § 1 k.p.k., art. 27 k.k.w., art. 27 § 2 k.k.w. oraz art. 188 § 5 k.k.w., a także art. 26 ust. 1, art. 104 ust. 1 i art. 105 ust. 1 pkt 1 ustawy o postępowaniu egzekucyjnym[548] w administracji o sprzedaż, według trybu określonego dla właściwych organów postępowania wykonawczego, jednostek waluty cyfrowej, a mianowicie zabezpieczonych na mieniu podejrzanego.

5.6. Cyfrowe artefakty w grach komputerowych

Gry komputerowe istniały niemal od samego początku pojawienia się komputerów, a ich popularność znacznie wzrosła wraz z rozwojem Internetu, który stwarza możliwości jednoczesnej rywalizacji wielu osób online w jednej grze. To właśnie funkcja integracyjna gier sprawia, że tworzą się internetowe społeczności liczone nawet w milionach

[548] Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2022 r. poz. 479 z późn. zm.).

osób, które uczestniczą w wirtualnej rozrywce. Szeroki zakres gier i wielość funkcji, które oferują, są przyczyną niezwykłej ich atrakcyjności do tego stopnia, że obecnie gry nie stanowią jedynie formy spędzania wolnego czasu w postaci indywidualnego grania. Użytkownicy często uczestniczą w transmisjach na żywo, czerpiąc radość ze wspólnego „przeżywania" historii opowiedzianej w grze z innymi widzami zainteresowanymi daną tematyką, np. fantastyką. W ten sposób platformy streamingowe stały się przestrzenią budowania więzi między ludźmi w oparciu o wspólne zainteresowania[549]. Jednak owe platformy stanowią także miejsce różnego rodzaju nadużyć wypełniających niekiedy znamiona przestępstw i coraz częściej sądy skazują sprawców popełniających czyny zabronione ma omawianym polu. W literaturze przedmiotu opisano przypadek, kiedy już w lipcu 2010 r. zorganizowane grupy przestępcze wykorzystały gry funkcjonujące w trybie online w procesie prania pieniędzy: za nielegalnie uzyskane środki pieniężne kupowano jednostki wirtualnej waluty do gier i płacono nimi za cyfrowe „przedmioty" potrzebne graczom. Następnie przedmioty takie odsprzedawano, a zebrane pieniądze przetransferowano na zagraniczne konta. Tym sposobem środki finansowe, „skradzione" pierwotnie w wyniku cardingu, wyprowadzono poza Stany Zjednoczone, co bez opisanego *modus operandi* byłoby niemożliwe[550]. Inne formy przestępczości ukierunkowanej na artefakty w grach komputerowych dotyczą m.in. „kradzieży" awatara (cyfrowej postaci utożsamiającej gracza) lub innego artefaktu wykorzystywanego w grze, reprezentującego broń (miecze, kusze, pistolety, karabiny, broń białą itp.), amunicję, części zbroi, czy tzw. lootboxy. Wartości takie najczęściej ulokowane są na internetowym koncie zarządzanym przez gracza, zakładanym w momencie rejestracji i chronionym poprzez login i hasło.

Charakter taki miała sprawa rozpatrywana przez Sąd Rejonowy dla Krakowa-Krowodrzy w Krakowie[551]. Ustalono w niej, że sprawca przestępstwa D. H., działając wspólnie i w porozumieniu z osobą nieletnią, stworzył stronę internetową www.metin2-bany.c0.pl i wykorzystał ją do uzyskiwania danych innych graczy Metina2 w postaci loginów i haseł dostępu do kont osób trzecich. Następnie, wykorzystując te informacje, logował się na konto konkretnego użytkownika, gdzie uzyskiwał adres jego skrzynki mailowej; potem logował się do niej i zmieniał hasła autoryzacyjne do poczty elektronicznej. Dostęp do kont pokrzywdzonych umożliwiał sprawcy przejmowanie danych do zarządzania cudzymi awatarami. W taki sposób D. H. zalogował się bez zgody i wiedzy T. K. na jego konto skrzynki poczty elektronicznej i zmienił hasło dostępu do poczty, a następnie przejął postać w grze. Zawarta w akcie oskarżenia treść zarzutu sformułowana wobec D. H. brzmiała następująco:

[549] M. Majorek, *Kod YouTube. Od kultury partycypacji do kultury kreatywności*, Kraków 2015, s. 135.

[550] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*…, s. 150, [za:] *Bitcoin Virtual Currency: Intelligence Unique Features: Present Distinct, Challenges for Deterring Illicit Activity, Prepared by FBI Directorate of Intelligence*, 24 April 2012, s. 5 (zbiory własne autora).

[551] Wyrok Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie z dnia 3 sierpnia 2012 r., II Ka 776/11/K.

> w dniu 6 lutego 2011 r. w K. w celu osiągnięcia korzyści majątkowej, bez upoważnienia wpłynął na przesyłanie informacji poprzez przełamanie elektronicznego zabezpieczenia w ten sposób, że zmienił hasło dostępowe do skrzynki poczty elektronicznej o nazwie …@poczta.onet.pl należącej do T. K. po czym przejął jego postać w grze Metin 2 o nazwie Joker 78 czym doprowadził T. K. do niekorzystnego rozporządzenia mieniem w kwocie nie mniejszej niż 500 zł, tj. o czyn z art. 287 § 1 k.k.

W wyroku z dnia 3 sierpnia 2012 r. sąd uznał oskarżonego winnym popełnienia zarzucanego mu czynu, ale zmodyfikował jego treść w następujący sposób:

> w dniu 6 lutego 2011 r. w Krakowie uzyskał bez uprawnienia dostęp do informacji dla niego nieprzeznaczonej, to jest danych zawartych w skrzynce poczty elektronicznej o adresie '/.../@poczta.onet.pl' należącej do T. K., przełamując jej elektroniczne zabezpieczenie w postaci hasła dostępowego, co stanowi występek z art. 267 § 1 k.k.

Sąd warunkowo umorzył postępowanie „ustalając okres próby na 1 'jeden' rok", orzekł wobec oskarżonego świadczenie pieniężne w wysokości 500 zł oraz zasądził od niego na rzecz Skarbu Państwa koszty sądowe. W uzasadnieniu wyroku sąd stwierdził brak znamienia „działania w celu uzyskania korzyści majątkowej", gdyż D. H. nie chciał nielegalnie wzbogacić siebie lub też osoby trzeciej, ale odzyskać utracony ekwipunek wykreowanej przez siebie postaci gry komputerowej. Nie zaszło także drugie z przewidzianych w art. 287 § 1 k.k. znamion podmiotowych w postaci działania w celu wyrządzenia innej osobie szkody, gdyż oskarżony działał z zamiarem rewindykacji utraconego wcześniej mienia, a nie kierował się zamiarem uczynienia jakiejkolwiek szkody T. K.

Przechodząc do oceny prawnokarnej wyroku, stwierdzić należy, że przedmioty wirtualne, takie jak postać w grze Metin 2, nie mogą być uznane za znaki pieniężne, pieniądz elektroniczny czy środki zapisane na rachunku, dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach czy stwierdzającego uczestnictwo w spółce, a więc nie spełniają definicji „rzeczy ruchomej" z art. 115 § 9 k.k. Nie są także środkiem płatniczym, gdyż definicja środka płatniczego zalicza do niego banknoty i monety nominowane w określonej walucie, które są używane i powszechnie akceptowane przy dokonywaniu płatności na terenie danego państwa. Zatem, aby uznać jakiś przedmiot za środek płatniczy, musi być on powszechnie akceptowalną formą płatności na terenie określonego kraju, a przedmiot wirtualny takich przymiotów nie posiada[552].

Podsumowując, artefakty wykorzystywane w grach komputerowych nie mogą być przedmiotem kradzieży (art. 278 § 1 k.k.) lub kradzieży z włamaniem (art. 279

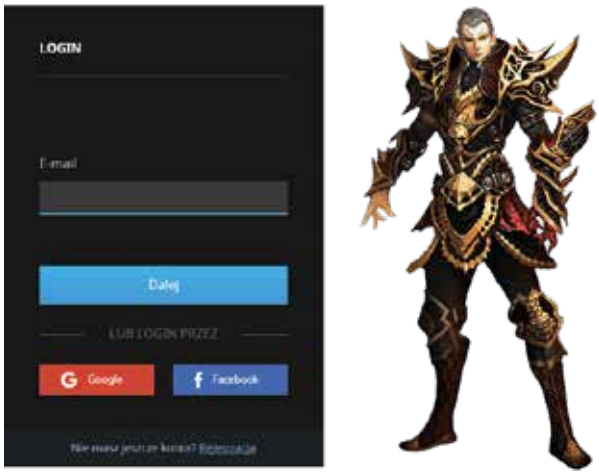
[552] J. Budziński, *Luka prawna w zakresie karnoprawnych kwalifikacji*…, s. 156–157.

§ 1 k.k.)[553]. Nie spełniają również cech programu komputerowego (art. 278 § 2 k.k.), gdyż zbudowane są tylko z określonej „linijki" źródłowej, która istnieje dzięki głównemu programowi komputerowemu obsługującemu funkcjonowanie cyfrowego artefaktu w grze. Sam kod określający dany przedmiot nie będzie miał żadnego zastosowania bez połączenia z obsługującym go kompatybilnym programem. Zapis informatyczny tworzący dany przedmiot wirtualny nie stanowi żadnej samoistnej całości, albowiem w przypadku usunięcia danej gry komputerowej zniknie także ów zapis[554]. Pod względem technicznym bowiem gra jest definiowana jako program, czyli kod, niedostrzegalny „gołym okiem". Można go traktować jako fundament, na którym budowana jest warstwa graficzna, muzyka i odgłosy towarzyszące wzajemnej rywalizacji, interfejs do wykonywania funkcji w grze itd. Program komputerowy stanowi zatem kod źródłowy warunkujący istnienie gry i regulujący jej przebieg.

Krótka analiza „technicznego" sposobu funkcjonowania artefaktów w grach komputerowych pozwala stwierdzić, że w sprawie kradzieży postaci w grze Metin 2 kwalifikacja prawna czynu przyjęta przez prokuratora, jak również subsumpcja ustalonych przez sąd okoliczności faktycznych, były nieprawidłowe. Jeśli chodzi o zarzut zawarty w akcie oskarżenia, to słusznie dotyczył on wpływania przez sprawcę na automatyczne przetwarzania danych informatycznych bez upoważnienia, co skutkowało „kradzieżą" cyfrowej postaci. Jednak prokurator, wskazując w opisie czynu, że sprawca „przełamał elektroniczne zabezpieczenie w ten sposób, że zmienił hasło dostępowe do skrzynki poczty elektronicznej", powinien dać temu wyraz w kwalifikacji prawnej czynu, bo ww. działanie nie należy do znamion art. 287 § 1 k.k., ale stanowi typową czynność sprawczą z art. 267 § 1 k.k. Pogląd, że oba przestępstwa mogą pozostawać w realnym zbiegu, został już wcześniej szczegółowo omówiony. Sąd z kolei uznał, że oskarżony dopuścił się tylko nielegalnego hakingu, przy czym podana na tę okoliczność argumentacja, jakoby nie chciał on „nielegalnie wzbogacić siebie lub też osoby trzeciej, ale odzyskać utracony ekwipunek wykreowanej przez siebie postaci gry komputerowej", budzi poważne wątpliwości, gdyż dochodzenie roszczeń cywilnych odbywa się na drodze sądowej, a nie poprzez ich samodzielną „egzekucję" i hakowanie konta osoby trzeciej.

[553] Podobnie: tamże, s. 159.

[554] Podobnie: tamże, s. 160; także O. Winkiel, *„Kradzież" dóbr wirtualnych w grach sieciowych – wprowadzenie do zagadnienia*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, nr 2, LEX, *teza 1*.



Grafika nr 22. Panel logowania do konta uczestnika gry oraz awatar z gry Metin 2. Ważnym elementem gier komputerowych jest interfejs, z poziomu którego następuje m.in. logowanie się do konta w grze przechowującego „klucze" do zarządzania cyfrowymi postaciami. Haking artefaktów w grach komputerowych ukierunkowany jest najczęściej poprzez przełamanie takiego zabezpieczenia i zalogowanie się na konto pokrzywdzonego

Powracając do kumulatywnej kwalifikacji prawnej art. 267 § 1 k.k. i art. 287 § 1 k.k., to w podobnej sprawie jak rozpatrywana przez Sąd Rejonowy dla Krakowa-Krowodrzy w Krakowie, prokurator Prokuratury Rejonowej w Złotowie przyjął zbieg realny przepisów i R. N. został oskarżony o to, że:

> w dniu 27 października 2013 r. w Ł. /…/, za pomocą sieci internetowej bez uprawnienia przełamał elektroniczne zabezpieczenie adresu e-mail o nazwie venzon83@o2.pl należącego do P. B. użytkownika gry online stworzonej na specjalnie przygotowanej stronie internetowej o nazwie http:/metin2.pl, a następnie w osiągnięcia korzyści majątkowej bez upoważnienia zmienił na nim zapis danych informatycznych uniemożliwiając prawidłowe zalogowanie się wyżej wymienionego użytkownika gry, po czym wszedł w nieuprawnione posiadanie jego loginu i hasła do konta gry /…/ i logując się na koncie tego gracza przejął akcesoria stworzonej przez niego postaci o łącznej wartości ponad 2 000 złotych, czym działał na szkodę P. B., tj. o przestępstwo z art. 267 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.[555]

Sąd Rejonowy w Złotowie w wyroku z dnia 10 listopada 2016 r. (II K 371/16) uznał, iż w zgromadzonym materiale dowodowym brak było obiektywnych dowodów

[555] Wyrok Sądu Okręgowego w Poznaniu z dnia 7 marca 2017 r., IV Ka 111/17, LEX nr 2280584.

świadczących o tym, że oskarżony R. N. wypełnił znamiona przestępstwa. Na sprawstwo oskarżonego wskazywał jedynie fakt logowania się do poczty elektronicznej pokrzywdzonego z numeru IP przydzielonego jego matce oraz wcześniejsze jego prawomocne skazanie za podobny czyn. Sąd Okręgowy w Poznaniu, rozpoznając apelację złożoną przez prokuratora od wyroku uniewinniającego, podzielił pogląd sądu I instancji, iż ustalone okoliczności nie przesądzały w sposób jednoznaczny o sprawstwie i winie oskarżonego. Żaden z ww. sądów nie zakwestionował natomiast przyjętego w akcie oskarżenia opisu czynu i jego kwalifikacji prawnej.

W większości przypadków subsumpcja stanu faktycznego jedynie pod kątem art. 287 § 1 k.k., ewentualnie w zbiegu z art. 267 § 1 k.k. gdy doszło do przełamania zabezpieczenia, nie budzi wątpliwości. Dochodzi wtedy do manipulacji danymi i „kradzieży" wartości majątkowych w formie cyfrowej, które nie mają statusu rzeczy ruchomej. Po przeprowadzeniu takiego „ataku" zarówno konto gracza, pamięć i system operacyjny jego laptopa, a także serwer firmy przechowującej program komputerowy (grę) – nadal działają poprawnie, podobnie jak wspomniany „incydent" nie przeszkadza innym osobom w korzystaniu z gry. Jeśli jednak sprawca, oprócz „kradzieży" cyfrowych artefaktów, umyślnie zakłóciłby pracę całego systemu informatycznego gracza lub systemu teleinformatycznego gry, to skutek jego działania znacznie wykraczałby poza znamiona „oszustwa komputerowego"; naruszałby nie tylko prawo własności lub posiadania mienia oraz prawo do poufności informacji, ale także bezpośrednio godziłby w przedmiot ochrony, jakim jest na gruncie art. 269a k.k. bezpieczeństwo funkcjonowania systemów informatycznych i teleinformatycznych oraz sieci teleinformatycznych. Potraktowanie skutku w postaci istotnego naruszenia pracy ww. systemów lub sieci jako okoliczności wpływającej na dyrektywy wymiaru kary i zaostrzenie odpowiedzialności karnej, bez dodania do podstawy skazania art. 269a k.k., to stanowczo za mało, aby oddać całość kryminalnego bezprawia czynu.

5.7. Nielegalny hazard z wykorzystaniem walut wirtualnych

Zgodnie z orzecznictwem sądów administracyjnych, urządzanie gier na automatach to ogół czynności i działań stanowiących zaplecze logistyczne dla umożliwienia realizowania w praktyce działalności w zakresie gier hazardowych, w szczególności: zorganizowanie i pozyskanie odpowiedniego miejsca na zamontowanie urządzeń, przystosowanie go do danego rodzaju działalności, umożliwienie dostępu do takiego miejsca nieograniczonej ilości graczy, utrzymywanie automatów w stanie stałej aktywności, umożliwiającym ich sprawne funkcjonowanie, wypłacanie wygranych, obsługa urządzeń, zatrudnienie i odpowiednie przeszkolenie personelu, zapewniające graczom możliwość uczestniczenia w grze. Dzisiaj, jeśli chodzi o nielegalny hazard, to działania takie zyskują zupełnie nowy wymiar pod wieloma względami. W ostatnich latach zmienił się obraz przestępczości hazardowej w Polsce; chociaż już wcześniej działalność nielegalnych grup odznaczała się dużym zorganizowaniem i rozmachem, to teraz są one jeszcze bardziej profesjonalne, korzystają z rozwiązań nowych technologii i dotykają

sfery cyberprzestępczości. Kiedyś lokale do gier były wyposażone w automaty, przypominające duże i ciężkie skrzynie, zasilane bezpośrednio przez gracza pieniędzmi dla uzyskania kredytu do prowadzenia gry. Maszyny stały w ogólnodostępnych miejscach, np. barach, dyskotekach, a nawet wstawiano je na powierzchni osiedlowych „warzywniaków". Dzisiaj są to niewielkich gabarytów komputery, np. laptopy z dotykowym ekranem, podłączone zdalnie przez sieć Internet do centralnego serwera. Pozwala to przestępcom momentalnie „odciąć" maszyny od źródła, z którego pobierają oprogramowanie w postaci gier hazardowych, a więc maksymalnie utrudnić organom ścigania zabezpieczenie śladów cyfrowych pozwalających na sporządzenie opinii przez biegłego i ustalenie, jaki charakter miały prowadzone w lokalu gry. W całej Polsce funkcjonują setki nielegalnych „kasyn" w lokalach położonych w środku miasta lub usytuowanych w przydrożnych kontenerach; zajmują one stosunkowo niewielkie powierzchnie, na zewnątrz oznaczone są wyrazistymi, kolorowymi reklamami często nawiązującymi swą grafiką do kryptowalut, z zamontowanymi, świecącymi neonami.

Struktura grupy zajmującej się nielegalnym hazardem ma charakter piramidalny, tj. na samym jej szczycie usytuowany jest szef lub niewielka grupa osób, czerpiąca największe zyski z popełnianych przestępstw i wydająca decyzje w najważniejszych sprawach organizacji nielegalnego procederu. Polecenia (gdzie otworzyć nowy punkt, jak nim zarządzać, kogo dokooptować do grupy itp.) wydawane i przekazywane są na coraz niższe szczeble funkcjonowania osób organizujących hazard, przy czym przestępcy prowadzący salony do gier są tylko ich wykonawcami bez jakiejkolwiek samodzielności w działaniu. Im niżej piramidy, tym liczba przestępców się zwiększa odwrotnie proporcjonalnie do ich pozycji (znaczenia). Inaczej sprawa ma się z przepływem „owoców przestępstwa": w punktach gier pozostaje tylko pewna część nielegalnie zarobionych środków, a największe „profity" otrzymują szefowie grupy. Chodzi o ogromne kwoty pieniędzy, które następnie trzeba wyprać, aby zgubić ślad ich pochodzenia. Postuluje się zatem, aby grupy przestępcze rozpracowywać „od góry", tj. czynności operacyjne i procesowe powinny być ukierunkowane w pierwszej kolejności na zebranie materiału dowodowego i udowodnienie winy organizatorom nielegalnego hazardu, gdyż tylko tak można zlikwidować opisywany proceder (samo zatrzymanie właściciela „kasyna" lub osób zajmujących się jego administrowaniem spowoduje, że na jego miejsce momentalnie pojawi się inny przestępca chcący zarobić na nielegalnym hazardzie). Organy ścigania, w tym przede wszystkim Krajowa Administracja Skarbowa, mają wypracowaną szczegółową metodykę postępowania w opisywanych sprawach, która z oczywistych względów nie może być upubliczniona.

W skład profesjonalnie działającej, obejmującej swym zasięgiem terytorialnym nawet kilka województw, grupy przestępczej wchodzą także serwisanci, producenci automatów i osoby je przechowujące, informatycy i „obsługa IT" lokali, „księgowi" zajmujący się zarządzaniem pieniędzmi pochodzącymi z przestępstwa oraz kancelarie prawne. Jeśli mowa o tych ostatnich, to profesjonalni prawnicy m.in. przygotowują lub uzyskują

opinie prawne sporządzone pod kątem jak najkorzystniejszej wykładni przepisów karnych, karnoskarbowych i podatkowych dla realizacji nielegalnego procederu. Opinię taką wykorzystano w sprawie toczącej się przed Wojewódzkim Sądem Administracyjnym w Łodzi, która dotyczyła zaskarżonej przez stronę decyzji Dyrektor Izby Administracji Skarbowej w przedmiocie wymierzenia kary pieniężnej z tytuł urządzania gier na automatach, poza kasynem gry. Pomimo że w wydanej opinii biegły jednoznacznie stwierdził, iż zabezpieczone urządzenia były automatami do gry w rozumieniu ustawy o grach hazardowych, to strona przedstawiła jako dowód, dokument – „opinię" w sprawie urządzenia CSANI sporządzoną przez firmę posiadającą upoważnienie jednostki badającej, wydane przez Ministra Finansów, która to opinia zawiera konkluzję, iż platforma CSANI jest legalna. Sąd uznał, że taki dokument prywatny nie ma znaczenia dla rozstrzygnięcia sprawy. Z treści opinii wynikało bowiem, że dotyczy ona oceny Binarnego Systemu Spekulacji Giełdowych Csani.com, na którą złożyła się weryfikacja niezawodności i przewidywalności wyświetlanych w czasie rzeczywistym przez stronę internetową Csani.com danych dotyczących różnych opcji finansowych (oceny kursów wymiany walut, wartości waluty wirtualnej, tzw. kryptowaluty – bitcoin). W opinii wskazano, że manipulowano kursem walut wirtualnych w ten sposób, że stworzona przez przestępców strona podawała kurs z minimalnym opóźnieniem do rzeczywistych notowań po to, aby można nim było manipulować i wstawiać wartości gwarantujące przestępcom zysk z nielegalnego procederu. W ocenie sądu badaniu podlegało tylko działanie samej platformy Csani, wyświetlanej na stronie internetowej, z jaką może się łączyć sporne urządzenie. W opinii nie było także mowy o działaniu urządzeń, a jedynie o funkcjonowaniu platformy. Sąd podzielił stanowisko organu celno-skarbowego, że wiarygodnym dowodem w niniejszej sprawie mogła być wyłącznie opinia sporządzona po zbadaniu urządzenia, którego postępowanie dotyczy. Dokumenty prywatne przedłożone przez stronę nie mogą stanowić „konkurencji" dla opinii i ustaleń poczynionych podczas eksperymentów przeprowadzonych przez funkcjonariuszy celnych w ramach czynności kontrolnych potwierdzonych protokołem. Wynikający z protokołu kontroli opis obserwacji działania dwóch urządzeń oraz przebieg rozgrywanych na nich gier, a także ostateczne wnioski, nie budziły, w ocenie sądu, żadnych zastrzeżeń co do ich poprawności, odpowiadały także regułom doświadczenia życiowego i logiki[556].

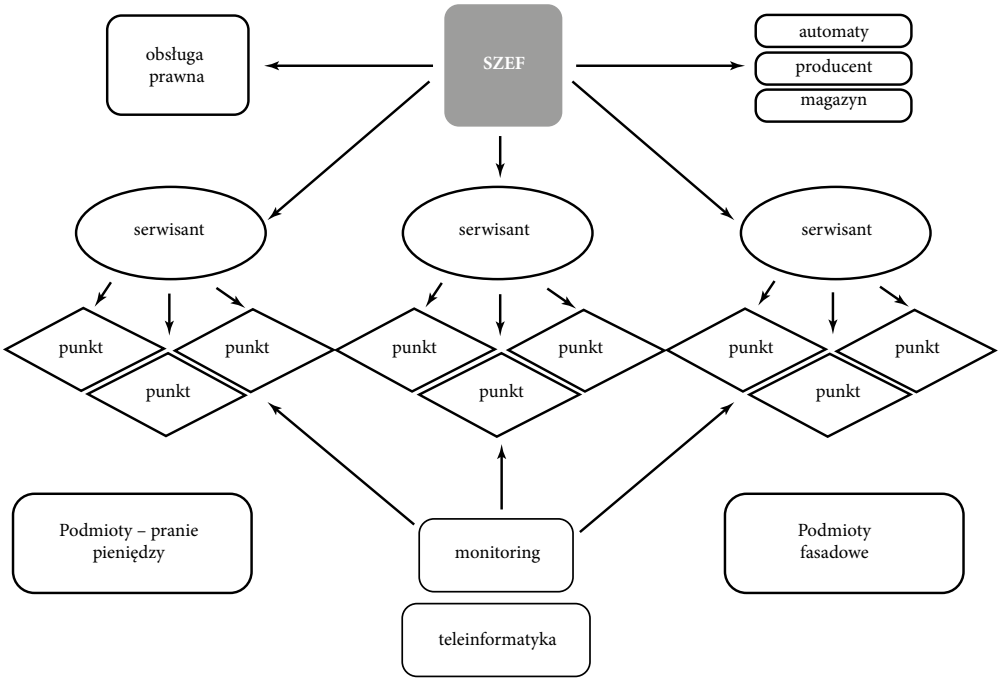
Sędziowie i prokuratorzy traktują zazwyczaj „opinie prywatne" jako niepożądane w procesie, zaburzające i przedłużające przebieg dowodzenia, a nawet stanowiące wyraz „pieniactwa" strony przedstawiającej taką opinię. Faktem jest, że za odpowiednią gratyfikację finansową można znaleźć „specjalistę" z każdej dziedziny, gotowego „udowodnić" każdą tezę. Z drugiej strony nowe źródło dowodowe może (potencjalnie) przyczynić się do wyjaśnienia okoliczności faktycznych sprawy. Wynika z tego, że błędem jest negacja *a priori* wartości opinii „prywatnej" dla procesu, chociaż wyniesione przez

[556] Wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 16 października 2018 r., III SA/Łd 537/18, LEX nr 2582970.

autora kilkunastoletnie doświadczenie z sali sądowej wskazuje, że dokumenty takie charakteryzują się z reguły małą wartością informacyjną dla sądu, a raczej „nachalnie" promują tezy korzystne dla obrony. W jednej ze spraw Sąd Okręgowy we Wrocławiu stwierdził, że „już sam fakt powołania się na wnioski opinii prywatnej wydanej na zlecenie strony (oskarżonego) w sposób zasadniczy podważał wartość argumentacji obrony"[557]. Podobnie było w przypadku opisanej wyżej „opinii" w sprawie urządzenia CSANI, która formalnie polegała na prawdziwych ustaleniach, ale dokonywanych na podstawie przetwarzanych przez urządzenie informacjach dotyczących kursów walut wirtualnych, podczas, gdy w rzeczywistości stosowano je do urządzania gier[558].

Powracając jeszcze do prawników wynajętych przez przestępców, to oczywiście pełnią oni także funkcję obrońcy podejrzanych/oskarżonych, gdy zostaną zatrzymani lub tymczasowo aresztowani przez organy ścigania. Inna ważna podgrupa członków grupy przestępczej trudniącej się organizowaniem nielegalnego hazardu, to informatycy i serwisanci, którzy bezpośrednio na miejscu lub zdalnie zajmują się obsługą sprzętu informatycznego i teleinformatycznego wykorzystywanego do prowadzenia nielegalnych gier, a także nadzorują lokale w trybie audio-wideo. Zabezpieczenie salonów odpowiednim nadzorem elektronicznym z monitoringiem na czele ma za zadanie kontrolować, co się dzieje w ich wnętrzu, ale także selekcjonować osoby chętne do wejścia do kasyna i wpuszczać tylko sprawdzonych już lub rokujących nadzieję graczy. Można powiedzieć, że lokal taki stanowi nierzadko „punkt towarzyski" dla hermetycznego grona osób: bywalcy „kasyna" nie tylko grają w nim na automatach, ale spędzają towarzysko czas, spożywają alkohol, a niekiedy także narkotyki. W większości salonów na miejscu znajduje się administrator lokalu, ale zdarza się, że kontrola nad jego funkcjonowaniem prowadzona jest zdalnie i oprócz „klientów" salonu nie ma w jego środku nikogo z organizatorów nielegalnego procederu. Ważna rola przypada „księgowym", którzy zajmują się gromadzeniem i inwestowaniem nielegalnie zarobionych pieniędzy, a więc ich „praniem" w taki sposób, aby prokuratura i sądy nie mogły stosować skutecznie zabezpieczenia majątkowego na środkach pochodzących z przestępstwa. Sposobów jest wiele, a jeden z nich opiera się na tworzeniu fasadowych podmiotów gospodarczych w formie spółek, które dokumentując fikcyjny obrót gospodarczy, transferują pomiędzy sobą pieniądze z nielegalnego hazardu, prowadzą fałszywą dokumentację księgowo-podatkową w tym wystawiają podrobione faktury VAT. Są też producenci maszyn do gier, osoby, które opracowują ich działanie, a także takie, które zajmują się magazynowaniem tego sprzętu i dostarczaniem go we wskazane miejsce.

[557] Wyrok Sądu Okręgowego we Wrocławiu z dnia 23 września 2014 r., IV Ka 1222/13, LEX nr 1882442.
[558] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*…, s. 444–445.



Grafika nr 23. Struktura zorganizowanych grup przestępczych trudniących się nielegalnym hazardem

Z uwagi na temat rozdziału ważny oraz interesujący jest fakt, że organizatorzy nielegalnego hazardu coraz pewniej sięgają po kryptoaktywa jako wartości majątkowo kupowane przez graczy w celu uzyskania „kredytu" (punktów) do prowadzenia gry. Z punktu widzenia bezpiecznego (dla przestępców) prowadzenia salonów, kryptoaktywa posiadają wiele zalet: dzięki ich zastosowaniu unika się obrotu gotówkowego, który wiąże się z koniecznością przetrzymywania pieniędzy w „kasynie", ich odbioru, transportu i dalszego składowania aż do momentu ukrycia lub zamiany na bezgotówkowy pieniądz bankowy. Każdy z ww. etapów „obsługi" pieniędzy wymaga zaangażowania ludzi i środków logistycznych, a poza tym zachodzi możliwość ich utraty (kradzieży, przywłaszczenia pieniędzy przez właścicieli punków, ich zajęcia przez organy ścigania itp.). Powoduje to, że najlepszy mechanizm funkcjonowania salonu gier opiera się na możliwości zapłaty przez graczy kartą płatniczą za tokeny cyfrowe do gry i w ten sposób nie angażuje się gotówki do rozliczeń. Z kolei po stronie organów ścigania generuje to konieczność ustalenia, w jaki sposób działa przyjęty przez przestępców mechanizm płatności jako jedna z podstawowych okoliczności faktycznych mających znaczenie dla sprawy. Oprócz ustalenia roli poszczególnych osób w grupie, ich wzajemnych powiązań, przepływów finansowych i metody prania pieniędzy, kolejne źródło dowodowe stanowi opinia biegłego o specjalności badania automatów do gier wydana na podstawie

przeprowadzonej ekspertyzy funkcjonowania zabezpieczonych w czasie tzw. realizacji urządzeń.

Istotny jest charakter gier na automacie, a więc de facto sposób działania obsługującego go programu komputerowego, a nie tylko samo urządzenie, tj. czy program oferuje klientom „kasyna" jedną z kategorii gier hazardowych wymienioną w ustawie z dnia 19 listopada 2009 r. o grach hazardowych[559]. Przepisy ustawy ewaluowały przez ostatnie lata po to, aby dostosować je do form hazardu związanego z cyberprzestrzenią. Wyrazem tego była ustawa z dnia 15 grudnia 2016 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw[560], której najważniejszym z założonych celów było dostosowanie obowiązujących przepisów do zjawiska migracji gier hazardowych do Internetu i zmniejszenie skali występowania tzw. szarej strefy w zakresie gier na automatach oraz w sieci Internet[561]. Realizacja tego celu nastąpiła m.in. poprzez skreślenie zapisu ustawowego, zamieszczonego na końcu art. 2 ust. 1 ustawy o grach hazardowych o treści „a podmiot urządzający loterię oferuje wygrane pieniężne lub rzeczowe", gdyż nie pozwalał on na ściganie wygranych w postaci walut wirtualnych. Po nowelizacji przepisów nadano takie brzmienie, że odwołują się one do hazardu internetowego; np. treść art. 2 ust. 2 pkt 5 stanowi: „Grami na automatach są także gry na urządzeniach mechanicznych, elektromechanicznych lub elektronicznych, w tym komputerowych, oraz gry odpowiadające zasadom gier na automatach urządzane przez sieć Internet organizowane w celach komercyjnych, w których grający nie ma możliwości uzyskania wygranej pieniężnej lub rzeczowej, ale gra ma charakter losowy".

W sprawach o hazard, pytania skierowane do biegłego, badającego zabezpieczone automaty, dotyczą ustalenia, czy gry prowadzone na urządzeniu teleinformatycznym, którego budowa i zastosowane w nim oprogramowanie pozwala na uzyskanie wygranej (rzeczowej, pieniężnej, w formie kryptoaktywów), mają charakter losowy zawierający jednocześnie element losowości, a uzyskiwane wyniki gier są nieprzewidywalne i niezależne od woli grającego. Kluczowe pytania dotyczą także ustalenia oprogramowania, które steruje grą, w jaki sposób można zarządzać takim urządzeniem, gdzie znajduje się serwer obsługujący „kasyno", jaka jest forma płatności za grę i wygrana, jak wygląda mechanizm wypłaty wygranej przez urządzenie, jakie gry dostępne są na urządzeniu, czy maszyna do gier jest wyposażone w moduł zdalnej łączności, a w szczególności, czy urządzeniem można sterować „na odległość". W badanych sprawach, aby odpowiedzieć na tak postawione pytania, urzędy celno-skarbowe powoływały biegłych o specjalności: „badania technicznego automatów i urządzeń do gier" oraz „z informatyki, telekomunikacji i automatów do gier"[562]. W jednej ze spraw zabezpieczono jako dowody rzeczowe wiele egzemplarzy sprzętu elektronicznego, takiego jak automaty do gier hazardowych

[559] T.j. Dz. U. z 2023 r. poz. 227.
[560] Dz. U. z 2017 r. poz. 88.
[561] Uzasadnienie projektu ustawy. VIII. 795, Zmiana ustawy o grach hazardowych oraz niektórych innych ustaw. Wersja: Ustawa po rozpatrzeniu stanowiska Senatu, Senat nie wniósł poprawek, LEX.
[562] Akta Świętokrzyskiego Urzędu Celno-Skarbowego o sygn. RKS 5/2019/348000/DB i RKS 228/2019/348000.

(zestawy komputerowe do gier hazardowych), laptopy, komputery stacjonarne z monitorami, drukarki, routery. Biegły ustalił, że prowadzenie gier hazardowych nie byłoby możliwe, gdyby automaty nie były podłączone do sieci Internet, bo na tej podstawie działa m.in. mechanizm kredytowania. „Sieć Internet należy postrzegać jako medium, za pośrednictwem którego mogą być rozgrywane gry hazardowe" – stwierdził biegły.

Już w 2012 r. Generalny Inspektor Informacji Finansowej alarmował, że zorganizowane grupy przestępcze wykorzystują „wirtualną walutę cyfrową" w celu ukrycia faktycznego źródła pochodzenia środków finansowych. Z waluty tej korzystają m.in. podmioty zajmujące się działalnością związaną z grami hazardowymi – szacuje się, że już pod koniec 2012 r. przechowywano w obszarze internetowych gier hazardowych na wirtualnych rachunkach BTC ok. 300 mln USD i kwota ta systematycznie wzrastała, pisał w swoim raporcie GIIF[563]. Z punktu widzenia niniejszego opracowania szczególnie interesujące okazały się jednak okoliczności sprawy, gdzie przestępcy zastosowali do płatności tzw. BitKonika. Osoba, zamierzająca grać na automatach, musiała wpierw uiścić cenę punktów do gry w formie pieniężnej płatności kartą płatniczą, a następnie osoby obsługujące „kasyno" drukowały na pustych kartonikach z symbolem Bitkonika unikatowy kod QR przechowujący zakupioną wartość w kryptowalucie VSC. Tokeny służyły do „zakredytowania" urządzeń, tj. zasilenia w punkty do prowadzenia gry: gracz przykładał kartonik do skanera (kamery) automatu do gry i zakredytowana kwota wprowadzana była do systemu teleinformatycznego maszyny. Po naciśnięciu na ekranie laptopa ikony portfela z symbolem bitcoina wyświetlało się polecenie: „zeskanuj portfel" i należało przyłożyć kartonik z kodem BitKonika do czytnika kodu QR; dochodziło do synchronizacji portfela i po wybraniu opcji „doładuj" do przypisania punktów kredytowych do licznika gry. Punkty, wyświetlane na dotykowym monitorze, były przeznaczone do obstawiania zakładów w grze losowej, np. za 20 VSC gracz otrzymywał 200 pkt[564]. Po „zakredytowaniu" urządzenia wyświetlała się liczba dostępnych dla gracza jednostek kredytowych, która zależała od wartości znajdującej się na zeskanowanym kodzie QR. Następnie gracz wybierał rodzaj gry oraz ustawiał stawkę, tj. liczbę punktów kredytowych, którą program pobierał za rozpoczęcie losowania. Gra uruchamiła się w momencie wyboru opcji „start", na ekranie ruszał bęben losujący z symbolami, a kończyła się wraz z samoczynnym zatrzymaniem się tego bębna. Gracz mógł prowadzić grę do momentu wyczerpania punktów kredytowych[565].

W sprawie Świętokrzyskiego Urzędu Celno-Skarbowego akt oskarżenia wystosowano wobec trzech sprawców. Zawierał on łącznie 22 zarzuty o popełnienie przestępstwa skarbowego z art. 107 k.k.s. w zw. z art. 9 k.k.s.; przykładowo, zarzucane im czyny brzmiały następująco:

[563] M. Mazur, *Penalizacja prania pieniędzy*, Warszawa 2014, https://bip.brpo.gov.pl/sites/default/files/Penalizacja_prania_pieniedzy.pdf, s. 48 [dostęp: 19.07.2023].
[564] Akta Świętokrzyskiego Urzędu Celno-Skarbowego o sygn. RKS 228/2019/348000.
[565] Akta Świętokrzyskiego Urzędu Celno-Skarbowego o sygn. RKS 5/2019/348000/DB.

w okresie od nieustalonego dnia po dniu 30 listopada 2018 r. do dnia 4 grudnia 2018 r. w lokalu o nazwie /…/ mieszczącym się przy ul. /…/ w Kielcach urządzał gry hazardowe na czterech urządzeniach o nazwie „Inter Cafe"

w okresie od nieustalonego dnia po dniu 12 grudnia 2018 r. do dnia 4 grudnia 2018 r. w lokalu o nazwie /…/ mieszczącym się przy ul. /…/ w Sandomierzu urządzał gry hazardowe na urządzeniach do gier o nazwie „Inter Cafe nr /…/", „Inter Cafe nr /…/", „Inter Cafe nr /…/" i „Inter Cafe nr /…/"

w okresie od nieustalonego dnia po dniu 7 lipca 2019 r. do dnia 19 października 2019 r. w lokalu o nazwie /…/ mieszczącym się przy ul. /…/ w Kielcach urządzał gry hazardowe na dwóch zestawach komputerowych marki Lenovo o numerach /…/ i /…/ oraz zestawie komputerowym marki HP ELLITE DESK /…/[566]

W sprawie ustalono, że jeden z oskarżonych jako pełnomocnik spółki, w sposób bezpośredni urządzał gry hazardowe w ten sposób, że wynajmował lokale, gdzie następnie prowadzone były takie gry z wykorzystaniem „internetowej kryptowaluty BitKonik". Dwóch pozostałych oskarżonych serwisowało urządzenia do gry znajdujące się w lokalach, odbierało pieniądze z „utargu", zatrudniało osoby do bieżącego prowadzenia „kasyn", a wcześniej przeprowadzało ich szkolenia, a także dowoziło nowe automaty, gdy służba celno-skarbowa zatrzymała maszyny. W opisie czynu i jego kwalifikacji prawnej należało zatem wskazać, które znamiona przepisów ustawy szczególnej wypełniły swoim zachowaniem ww. osoby. Wyrażenie „wbrew przepisom ustawy", użyte w art. 107 § 1 k.k.s., wymaga bowiem konkretyzacji w wyroku skazującym, a wcześniej w akcie oskarżenia, także przez wskazanie w opisie czynu i podstawie skazania przepisu, z którego wynika norma naruszona przez oskarżonego (art. 413 § 2 pkt 1 k.p.k.)[567]. Konstrukcja przepisu art. 107 k.k.s. określa typ czynu zabronionego, którego odczytanie ściśle wiąże się z koniecznością zestawienia z przepisami ustawy związkowej. Przepis ten oparty jest zatem na blankiecie, a wypełniają go przepisy ustawy o grach hazardowych z 2009 r.[568]

Powracając jeszcze do tokenów wykorzystywanych w zakresie organizacji nielegalnego hazardu elektronicznego, takich jak wskazany w opinii biegłego VSC (w opinii zaznaczono, że chodzi o „kryptowalutę", ale podany skrót nie wskazuje jednoznacznie, jaki konkretnie token biegły miał na uwadze), to system rozliczeń w nielegalnych kasynach posiada przymiot „szczelnego". Oznacza to, że zarówno kupno tokenów umożliwiających grę oraz ich wypłaty (realizacja wygranej) są dokonywane przez jeden podmiot, tj. organizatora hazardu.

[566] Akta Prokuratury Rejonowej Kielce-Wschód w Kielcach o sygn. 4 Ds. 297.2021.

[567] Postanowienie Sądu Najwyższego z dnia 30 września 2015 r., I KZP 6/15, OSNKW 2015, nr 12, poz. 99; podobnie: postanowienie Sądu Najwyższego z dnia 22 grudnia 2021 r., V KK 396/21, LEX nr 3527395.

[568] Wyrok Sądu Rejonowego w Golubiu-Dobrzyniu z dnia 7 maja 2018 r., II K 372/17, LEX nr 2609309.

Ogólnie rzecz biorąc, system jednostek cyfrowych do obsługi gry na automatach można uzyskać na dwa sposoby, wykorzystując:

1. łańcuch bloków lub
2. zcentralizowaną, tradycyjną bazę danych.

W pierwszym przypadku najlepszym rozwiązaniem będzie prywatny blockchain z zerowymi opłatami (brak opłaty transakcyjnej, a zatem „cena gazu = 0"), niskim czasem bloku (np. 3 sekundy) i dogodnym rodzajem PoA[569] (wyznaczony serwer lub serwery „produkują" kolejne bloki). W takim układzie operator hazardu wykonuje transakcję zakupu tokenów za pieniądz fiducjarny przekazany przez gracza, a gracz musi zrealizować transakcję zapłaty tokenami, aby uruchomić maszynę. W systemie zamkniętym osoby przychodzące do salonu nie muszą nawet posiadać własnego portfela ani kluczy prywatnych, gdyż wystarczy im tylko adres/identyfikator. System transakcyjny sprzedaży i wgrywania tokenów może być obsługiwany automatycznie przez odpowiednie oprogramowanie.

Drugie rozwiązanie, tj. „zwykła" baza danych, polega na rejestracji przez operatora zakupu przez gracza tokenów, a oprogramowanie dedykowane prowadzeniu hazardu jedynie zmniejsza saldo w trakcie doładowywania „kredytów" w grze i zwiększa przy wygranej. Przy wypłacie wygranej operator ponownie zeruje saldo. W tym rozwiązaniu użytkownik także posługuje się indywidualnym identyfikatorem/adresem, a całość transferów system przetwarza automatycznie.

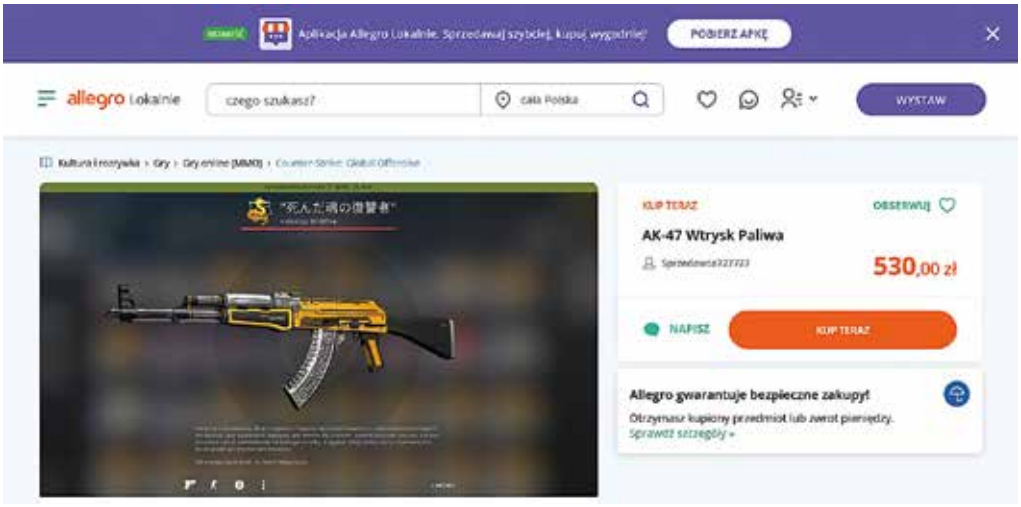
Z punktu widzenia osób korzystających z nielegalnego kasyna trudno jest zauważyć, które z przedstawionych rozwiązań zastosował organizator gier, chyba że operator udostępni oprócz „konto-balans" również historię transakcji z ich haszami, to wówczas użycie „zwykłej bazy" staje się technicznie trudniejsze niż prywatnego blockchaina. Taki prywatny „coin" nie musi być publicznie „listowany", a jego zakup i sprzedaż odbywa się wyłącznie w punktach hazardu. Nie jest on więc dostępny w Internecie na portalach typu coinmarketcap czy coinpaprika. Jeżeli nielegalne kasyna posiadałyby wspólną bazę lub wspólny łańcuch bloków emitujące tokeny do gry, to wzajemne rozliczenia/balansowanie również mogłoby się odbywać z użyciem wspólnego systemu dla grupy kasyn. W przypadku gdy obsługa klientów nie jest prowadzona „24/7", a salda muszą być rozliczane przy wyjściu klienta z gry, można taki łańcuch codziennie zerować i restartować, nie zostawiając nigdzie śladów po wykonanych transakcjach sprzedaży tokenów[570], co utrudniałoby czynności procesowe zmierzające do ustalenia sposobu funkcjonowania nielegalnych gier hazardowych.

[569] *Proof of Authority* polega na ograniczonej liczbie walidatorów bloków, dzięki czemu jest on w stanie osiągnąć wysoki stopień skalowalności. Bloki i transakcje w PoA weryfikowane są przez tzw. wstępnie zatwierdzonych uczestników, którzy działają jako moderatorzy systemu.

[570] R. Kiełbus, programista i advisor, w blockchainowych projektach; programista smartkontraktów, członek Zarządu Izby Gospodarczej Blockchain i Nowych Technologii, Arbiter Sądu Polubownego przy Izbie. Informacja otrzymana w wiadomości mailowej 30.07.2023 r. (zbiory własne autora).

5.8. Skiny (analiza przypadku)

Niekiedy hazard internetowy może być prowadzony przy wykorzystaniu bardziej abstrakcyjnych kryptoaktywów, aniżeli kryptowaluty. Dotyczy to skinów („skórek") wykorzystywanych w grze Counter-Strike: Global Offensive. Stanowią one, jak podaje producent i właściciel gry[571], rodzaj funkcji używanej w grze w postaci różnego rodzaju broni, którą można dozbroić gracza: zmieniają one wygląd stosowanych w Counter-Strike artefaktów, chociaż ich cechy użytkowe są niezmienne, tj. siły rażenia karabinu czy sposobu użytkowania wirtualnego noża doposażonego w skina, nadal jest taka sama. „Skórkę" uzyskuje się na różne sposoby: poprzez losowanie tzw. nagrody, grając w społeczności online lub handlując z innymi graczami na rynku Steam. Oferty sprzedaży skinów zamieszczone są na wielu portalach internetowych, najczęściej o charakterze aukcyjnym, zarówno specjalistycznych, związanych z grami komputerowymi, jak i ogólnodostępnych, jak np. Allegro. Ich ceny oscylują w granicach kilkuset złotych, ale rzadkie „skórki" są warte dużo więcej, np. w 2021 r. doszło do rekordowej transakcji w historii Counter-Strike: chińscy kolekcjonerzy kupili dwie „skórki" AWP Dragon Lore (Factory New) oraz StatTrak AK-47 Case Hardened (Minimal Wear) za kwotę prawie na 3 mln zł. Są to niezwykle rzadkie skiny, a ich wartość dodatkowo wzrosła przez fakt naklejenia na każdą skórkę czterech naklejek Titan Holo z ESL Major Series One Katowice 2014. Takie połączenie tworzy prawdopodobnie jedyną w swoim rodzaju postać cyfrowego aktywa na całym świecie[572].



Grafika nr 24. Oferta sprzedaży skina wystawiona na portalu Allegro

[571] https://counterstrike.fandom.com/wiki/Skins [dostęp: 17.02.2022].

[572] D. Jaroszewski, *Kolekcjoner zapłacił prawie 3 mln zł za dwa skiny do CS:GO*, portal Telepolis, https://www.telepolis.pl/rozrywka/gry/csgo – rekordowa – transakcja – skiny [dostęp: 10.02.2022].

Chociaż handel artefaktami konkretnej gry może być zakazany przez wewnętrzny regulamin uczestnictwa w rywalizacji, to nie posiadają one charakteru przepisów powszechnie obowiązujących i czyny takie są relewantne z punktu widzenia prawa karnego. Jednak skiny, jako przedmiot czynności wykonawczej, mogą potencjalnie stać się przedmiotem innego przestępstwa. Dotyczyła tego sprawa zawisła przed Sądem Rejonowym w Przasnyszu, w której R. W. został oskarżony o to, że:

> w bliżej nieustalonym czasie – nie wcześniej niż od dnia 1 września 2016 roku do 23 kwietnia 2017 roku w miejscowości K., zajmując się własną działalnością gospodarczą figurującą pod nazwami 'Skins Project R. W.' oraz 'Dream Project R. W.' wykorzystując siec Internet poprzez posiadane i administrowane osobiście strony internetowe o adresach: https://coinsell.pl/ oraz https://skinproject.pl/, urządzał gry hazardowe o charakterze losowym w których ryzyku poddawane są tzw. skiny – wirtualne klucze posiadające w świecie rzeczywistym realna wartość pieniężną i umożliwiające dostęp do wirtualnej broni o różnej sile rażenia i osprzętów wykorzystywanych w walkach gry zręcznościowej 3D o nazwie Counter-Strike Global Offensive (w skrócie CS: GO) oferowane w ramach platformy społecznościowej STEAM należącej do Valve Corporation z siedzibą w Bellevue, Waszyngton, USA – naruszając w ten sposób przepisy art. 29a ust. 1 w zw. z art. 2 ust. 1 ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz. U. z 2009, Nr 201, poz. 1540 ze zm.) a także art. 5 ust. 1b w zw. z art. 2 ust. 1 ustawy z dnia 19 listopada 2009 r. o grach hazardowych[573]

Postępowanie przygotowawcze prowadzili funkcjonariusze jednego z urzędów celno-skarbowych pod nadzorem prokuratora, posiłkując się stanowiskiem Izby Celnej w Szczecinie z sierpnia 2016 r. Stwierdzono w nim, że w Internecie funkcjonują platformy odpowiedzialne za działanie witryn, na których odbywają się – według regulaminu konkretnego serwisu – losowania skinów o określonej wartości wyrażonej w złotówkach i należących do graczy platformy społecznościowej Steam. Po losowaniu od 85% do 90% „skórek" z puli trafia do zwycięzcy, a reszta stanowi prowizję dla administratora organizującego loterię. Dochodzi więc do urządzania gier hazardowych przez Internet, co było – zdaniem autor pisma – penalizowane z art. 2 ust. 1 ustawy z dnia 19 listopada 2009 r. o grach hazardowych w ówczesnym brzmieniu tego przepisu; przed 1 kwietnia 2017 r., przepisy podane w kwalifikacji prawnej czynu zarzucanego oskarżonemu brzmiały następująco:

[573] Akta Sądu Rejonowego w Przasnyszu II Wydział Karny o sygn. II K 608/18.

Art. 2 ust. 1. Grami losowymi są gry, w tym urządzane przez sieć Internet, o wygrane pieniężne lub rzeczowe, których wynika zależy w szczególności od przypadku. Są to /…/
Art. 5 ust. 1b. Urządzanie gier hazardowych przez sieć Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych, jest objęte monopolem państwa.
Art. 29a. Zakazane jest urządzanie gier hazardowych przez Internet.

Sąd podzielił stanowisko oskarżyciela publicznego i wyrokiem nakazowym z dnia 18 października 2019 r. uznał R. W. „za winnego popełnienia zarzucanego mu czynu wypełniającego dyspozycję art. 107 § 1 k.k.s." oraz na podstawie tego przepisu skazał R. W. na karę grzywny.

Na tym etapie postępowania doszło do naruszenia prawa materialnego, tj. art. 107 § 1 k.k.s.[574], ponieważ nie został on wskazany w kwalifikacji prawnej czynu; w momencie kierowania do sądu aktu oskarżenia przepis ten brzmiał: „Kto wbrew przepisom ustawy lub warunkom koncesji lub zezwolenia urządza lub prowadzi grę losową, grę na automacie lub zakład wzajemny podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności do lat 3 albo obu tym karom łącznie". Komentowany przepis ma charakter blankietowy, a regulacje ustawy o grach hazardowych stanowią jego „wypełnienie". Ponadto w akcie oskarżenia przywołano art. 2 ust. 1 ustawy o grach hazardowych, ale nie wskazano, jaką „grę hazardową o charakterze losowym" urządzał oskarżony, co czyniło postawiony mu zarzut niekompletnym w zakresie określenia znamion przestępstwa. Sąd, pomijając poczynione przez niego błędne ustalenia faktyczne, popełnił rażący błąd w sferze orzekania i zasad budowania wyroku, tj. odmiennie aniżeli prokurator przywołał przepis blankietowy (art. 107 § 1 k.k.s.) bez wskazania, które konkretnie normy ustawy szczególnej (o grach hazardowych) wypełniły jego treść.

Jednak obrońcy oskarżonego, którzy wnieśli apelację od wyroku skazującego, zarzuty środka odwoławczego sformułowali na jeszcze innych podstawach, tj. błędu w ustaleniach faktycznych dokonanych przez sąd I instancji. Zasadniczą kwestią do rozstrzygnięcia stało się, pod kątem wypełnienia przez oskarżonego znamion przestępstwa, czym jest skin na gruncie prawa karnego. Jeden z obrońców podniósł, że skin stanowi

> z technicznego punktu widzenia jedynie fragment kodu programistycznego, a w grze CS: GO służy tylko zmianie wyglądu broni gracza (wyświetla się na ekranie monitora jako obrazek przedstawiający określony rodzaj broni, przy czym rodzajów broni w CS: GO jest kilkadziesiąt, a ich wygląd za pomocą skinów może zostać zmieniony na setki sposobów). Skin z całą pewnością nie jest przedmiotem materialnym, a zatem nie jest rzeczą w rozumieniu art. 45 k.c. Nie można zatem twierdzić, że osoby korzystające ze strony skinproject.pl uzyskały nagrody rzeczowe. Ustawa o grach ha-

[574] Ustawa z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2023 r. poz. 654, 818).

> zardowych bez wątpienia przez pojęcie wygranej rzeczowej rozumie wygraną w postaci rzeczy jako przedmiotu materialnego, spełniającego definicję z art. 45 k.c.[575]

Obrońca w apelacji podniósł ponadto, że:

> Wbrew temu, co twierdzi się w uzasadnieniu zaskarżonego wyroku, skiny nie dają graczowi żadnej przewagi nad innymi graczami (dodatkowych żyć, lepszych parametrów wykorzystywanej broni), nie przedłużają także gry. Z używania skina gracz nie ma żadnych, obiektywnych korzyści. Z tego względu nie można uznać skina (prawa do korzystania ze skina) za ekwiwalent prawnego środka płatniczego. Skoro skin (prawa do korzystania ze skina) nie jest prawnym środkiem płatniczym, ani nawet ekwiwalentem prawnego środka płatniczego, ani też nie można obiektywnie ustalić wartości skina (prawa do korzystania z niego) to z całą pewnością nie może stanowić wygranej pieniężnej w rozumieniu ustawy o grach hazardowych, a w szczególności w rozumieniu art. 2 ust. 1 tej ustawy[576].

Sąd Okręgowy w Ostrołęce II Wydział Karny całkowicie podzielił zawartą w apelacji argumentację obrony i wyrokiem z dnia 27 sierpnia 2020 r. uniewinnił oskarżonego od popełnienia zarzucanego mu czynu. W uzasadnieniu do wyroku sąd wskazał, że przepisów art. 2 ust. 1 pkt 1 ustawy o grach hazardowych nie można interpretować rozszerzająco i przez analogię zrównywać skina z rzeczą ruchomą lub pieniądzem. Oczywiste jest, napisał sąd, że skiny nie mają statusu rzeczy lub przedmiotu, ale ma się do czynienia z wartościami cyfrowymi[577].

Obecnie przepis art. 29a ustawy o grach hazardowych, ustanawiający zakaz urządzania takich gier przez Internet, został uchylony, a nowe brzmienie art. 2 ust. 3 i 5 tej ustawy wskazuje, że kryptoaktywa mogą być przedmiotem wygranej w grach hazardowych określonego rodzaju. Chodzi o gry na automatach, tj. na urządzeniach mechanicznych, elektromechanicznych lub elektronicznych, w tym komputerowych oraz gry odpowiadające zasadom gier na automatach urządzane przez sieć Internet o wygrane pieniężne lub rzeczowe, w których gra zawiera element losowości (art. 2 ust. 3). Przepis art. 2 ust. 5 ustawy o grach hazardowych poszerza rodzaj wygranej, stanowiąc: „Grami na automatach są także gry na urządzeniach mechanicznych, elektromechanicznych lub elektronicznych, w tym komputerowych, oraz gry odpowiadające zasadom gier na automatach urządzane przez sieć Internet organizowane w celach komercyjnych, w których grający nie ma możliwości uzyskania wygranej pieniężnej lub rzeczowej, ale gra ma charakter losowy" (art. 2 ust. 5). Wynika z tego, że formułując zarzut o taki czyn, jaki był przedmiotem rozpoznania Sądu Rejonowego w Przasnyszu, należałoby zdecydować, czy ma się do czynienia z „grami na automatach". W piśmie instruktażowym Ministerstwa Finansów z 2019 r. przyjęto natomiast, że „skiny to rodzaj stawki o określonej

[575] Akta Sądu Rejonowego w Przasnyszu o sygn. II K 608/18.
[576] Tamże.
[577] Wyrok Sądu Okręgowego w Ostrołęce z dnia 27 sierpnia 2020 r., II Ka 40/20.

wartości, stawianej przez graczy w danej grze, od której zależy zarówno wygrana, jak i wysokość tej wygranej. Dlatego możliwe jest uznanie takiej gry za grę hazardową". Wskazano ponadto, że

> Istnieje wiele stron internetowych, na które gracze, mający konto na steamie, wysyłają swoje skiny, uzyskane w trakcie gry Counter Strike (również poprzez wylosowanie ze skrzynek otwieranych przy pomocy kluczy). Wstawianie skinów do gier organizowanych przez inne podmioty następuje na zasadzie wymiany z właścicielem danej strony, za pośrednictwem platformy steam. W jednym z wariantów gier, gracze posiadają skiny o konkretnej wartości materialnej i mogą wchodzić do gry obstawiając te skiny, a w wyniku przeprowadzonej gry/losowania gracz może wygrać określone rzeczy (skiny), pobierając np. całą pulę, która była dostępna w grze[578].

Z pisma wprost nie wynika, który rodzaj gry lub zakładu za grę losową, zakładu wzajemnego albo gry na automacie, opisanych w art. 2 ustawy o grach hazardowych, miałby stanowić opisany w piśmie instruktażowym proceder, a mylące może okazać się ponowne przyrównywania skinów do „konkretnej wartości materialnej", skoro jest to artefakt cyfrowy.

Problem cyfrowych artefaktów wykorzystywanych w hazardzie internetowym nie dotyczy tylko skinów, ale też innych kryptoaktywów, takich jak chociażby lootboxy. Mechanizm działania lootboxa polega na tym, że w zamian za określoną cenę, wyrażoną w pieniądzu lub różnego rodzaju punktach, kupujący nabywa wirtualną „skrzynię", w której znajdują się losowo dobrane, za pomocą komputerowego algorytmu, przedmioty. Gracz poznaje zawartość lootboxa dopiero po jego otwarciu i wtedy okazuje się, że pomnożył zainwestowane środki lub stracił na losowaniu, gdyż skrzynia jest pusta albo umieszczono w niej przedmioty o małej wartości. W niektórych przypadkach mechanizm losowania podlega pewnym modyfikacjom: użytkownik może stworzyć własną skrzynię, tj. wybiera, jakie przedmioty mają się w niej znaleźć, i sam ustala mechanizm losowania na zasadzie: czym wyższa opłata, tym zwiększa się szansa zdobycia atrakcyjnego przedmiotu, chociaż nigdy nie można być pewnym ostatecznego wyniku rozgrywki. Wykorzystanie „skrzyń" w różnego rodzaju wirtualnych losowaniach także pozostaje w zainteresowaniu służby celno-skarbowej, ale określenie ich ostatecznego statusu prawnego na gruncie ustawy o grach hazardowych nie jest łatwe i budzi kontrowersje.

Na koniec warto zwrócić uwagę na ważny problem prawny, o charakterze procesowym, który pojawił się w sprawie dotyczącej skinów, a dostrzec go można w innych postępowaniach karnych związanych z przestępstwami teleinformatycznymi. W apelacji złożonej od wyroku Sądu Rejonowego w Przasnyszu obrońca wskazał na „nieprzydatność dowodu" w postaci „papierowych wydruków" stron internetowych, na których

[578] Pismo instruktażowe Departamentu Nadzoru nad Kontrolami w Ministerstwie Finansów z dnia 7 marca 2019 r. w sprawie „skinów" (zbiory własne autora).

znajdowały się informacje stanowiące, zdaniem oskarżyciela publicznego, dowód popełnienia przestępstwa. Obrońca oskarżonego wskazał, że

> W analizowanym stanie faktycznym ewidentnie ma miejsce sytuacja, polegająca na tym, że przeprowadzenie dowodu wskazanego we wniosku dowodowym nie może doprowadzić do stwierdzenia okoliczności w nim wskazanej. Strona internetowa ma charakter interaktywny i sam tylko „zrzut ekranu", do tego wydrukowany na kartce, nie oddaje jej istoty i sposobu funkcjonowania.

Zdaniem obrońcy, dowód na okoliczności, których dotyczyły zakwestionowane wydruki, powinien zostać przeprowadzony w ten sposób, że oskarżyciel, podczas postępowania dowodowego, odtworzy funkcjonowanie witryn https://coinsell.pl, https://skinproject.pl, https://skins.pl, Allegro.pl, https://sklep-skiny.pl, https://skinmarket.pl. Jest to technicznie możliwe, chociażby poprzez zapisanie stron na trwały nośnik, ale wymagało od oskarżyciela większego wysiłku – wskazał obrońca. Rzeczywiście jest tak, że zapoznanie się przez organ procesowy ze stroną internetową, której działanie ma być związane z *modus operandi* sprawcy przestępstwa i stanowić dowód w sprawie, organ procesowy realizuje w ramach czynności procesowych oględzin i dokumentuje protokołem (art. 143 § 1 pkt 3 k.p.k.). Najlepsza praktyka realizacji takich działań, oprócz protokołowanie obserwacji i wniosków poczynionych przez organ procesowy, wskazuje także na konieczność nagrywania obrazu monitora, tj. treści, z którymi zapoznaje się prokurator, a nośnik danych z nagraniem stanowi załącznik do protokołu. Nagranie powinno być zabezpieczone kluczem kryptograficznym potwierdzającym datę i czas jego realizacji, a ponadto gwarantującym, że materiał od momentu jego rejestracji nie został zmodyfikowany. Konieczność stosowania opisanej praktyki potwierdza pismo instruktażowe Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej w Prokuraturze Krajowej z dnia 19 października 2021 r., które co prawda odnosi się do funkcjonowania platform inwestycyjnych na rynku Forex, ale zawarte w nim zalecenia mają charakter ogólny i odnoszą się do prowadzenia postępowania dowodowego. W piśmie wskazano, że po ustaleniu strony internetowej, pozostającej w zainteresowaniu organów ścigania, należy dokonać jej oględzin przy udziale biegłego informatyka z laboratorium kryminalistycznego policji, biegłego z zakresu informatyki śledczej lub specjalisty z wydziałów „cyberpolicji". Z przeprowadzonych oględzin sporządza się protokół do którego, jako załącznik, należy dołączyć nośnik (płytę CD/DVD/pendrive'a) z zapisanym obrazem strony internetowej wraz ze wszystkimi podstronami obejmującymi jej funkcjonalności, dokumentującymi w szczególności strukturę witryny oraz znajdujące się na niej pliki tekstowe, dźwiękowe i filmy[579].

[579] Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej w Prokuraturze Krajowej z dnia 19 października 2021 r. w sprawie funkcjonowania platform inwestycyjnych na rynku Forex, znak: 1001 – 7.024.4.2021.

Podsumowanie

Podstawowym zamysłem projektu badawczego w postaci monografii była odpowiedź na pytanie:

— Czy prokuratorzy i sędziowie popełniają błędy w kwalifikacji prawnej i opisie znamion przestępstw teleinformatycznych?

Chcąc kompleksowo naświetlić główny problem badawczy, odpowiedziano także na pytania poboczne, dotyczące aspektów procesowo-kryminalistycznych przestępczości teleinformatycznej. Stanowią one fundament do eksploracji głównego wątku monografii dlatego warto zająć się nimi w pierwszej kolejności.

Przeprowadzone badania pokazały, że obraz przestępczości teleinformatycznej jest niejednorodny. Prokuratorzy i sędziowie, obok poważnych naruszeń prawa dokonanych z zastosowaniem wyrafinowanego *modus operandi* i skutkujących znaczną szkodą w mieniu lub poważnymi zakłóceniami pracy systemów informatycznych, mają do czynienia ze stosunkowo drobnymi występkami polegającymi na użyciu skradzionej karty płatniczej, uzyskaniu nieuprawnionego dostępu do konta na platformie społecznościowej, czy zalogowaniu się do cudzej aplikacji bankowej i kradzieży pieniędzy. Określenie „drobna przestępczość" oznacza, że sposób popełnienia czynu jest nieskomplikowany, np. w przypadku transakcji zbliżeniowych wyczerpujących znamiona art. 279 § 1 k.k. wystarczyło przyłożyć do czytnika przywłaszczony lub skradziony „plastik" i zapłacić kartą za towar. Ale zdarzają się sprawy poważniejsze, jak chociażby wielokierunkowa, nielegalna działalność w cyberprzestrzeni Armaged0na, któremu prokurator postawił trzydzieści dziewięć zarzutów dotyczących m.in. sprzedaży nielegalnego oprogramowania w darknecie, ataków DDoS, ransomware, phishingu, oszustw ukierunkowanych na posiadaczy bankowości elektronicznej oraz prania pieniędzy. Negatywne skutki działalności Tomasza T. spowodowały u kilkuset osób straty majątkowe oraz dezintegrację danych informatycznych w ich urządzeniach, a instytucje finansowe musiały przez lata angażować swoje zasoby logistyczne w neutralizację „ataków" prowadzonych przez Armaged0na.

Interesującym zjawiskiem, pod względem kryminalistycznym i kryminologicznym, jest wkraczanie narzędzi i metod typowych dla przestępczości teleinformatycznej w obszary dotąd zarezerwowane dla „tradycyjnej" przestępczości. Mowa chociażby o nielegalnym hazardzie: kiedyś lokale do gier były wyposażone w automaty przypominające duże i ciężkie skrzynie, zasilane bezpośrednio przez gracza pieniędzmi w gotówce. Dzisiaj są to niewielkich gabarytów komputery podłączone zdalnie przez Internet do centralnego serwera znajdującego się poza kasynem, a organizatorzy nielegalnego hazardu coraz częściej sięgają po kryptoaktywa, które świetnie nadają się do bezpiecznego obrotu przez przestępców wartościami majątkowymi zarobionymi na nielegalnym hazardzie. Podobnie rzecz się ma z handlem narkotykami, który, można powiedzieć, z ulicy przeniósł się do Internetu. Analiza spraw pod kątem zabezpieczenia majątkowego na

kryptowalutach dowiodła, że w sieci rozwija się handel narkotykami oraz podobnymi substancjami psychoaktywnymi znanymi jako „dopalacze". Nielegalne, wirtualne sklepy prowadzone są w profesjonalny oraz bezpieczny dla przestępców sposób: stosuje się szyfrowanie komunikacji, płatności dokonuje się w bitcoinie lub monero, obowiązują ustalone metody dostawy „towaru" oraz specjalne kanały komunikowania się. Platformy dystrybuujące narkotyki są profesjonalnie zarządzane i zawierają szczegółowe informacje o rodzaju oferowanych substancji: ich nazwę, skład chemiczny, opis sposobu użytkowania i działania proszków lub kryształów. Sprzedaż odbywa się w określonych godzinach, a procedura transakcyjna przewiduje możliwość złożenia reklamacji. Wszystko to sprawia, że nawet osoby bez doświadczenia w korzystaniu z tego rodzaju produktów i usług szybko się uczą i bez problemu mogą zamówić wybrane przez siebie substancje. Transgraniczna sprzedaż narkotyków syntetycznych za pośrednictwem internetowych platform handlowych, zwłaszcza w darknecie, stanowi poważne utrudnienie w skutecznym prowadzeniu śledztwa.

Sprawy znajdujące się w referatach sędziów i prokuratorów dotyczyły w dużej liczbie „ataków" ukierunkowanych na bankowość elektroniczną, bowiem podstawowym celem cyberprzestępców jest chęć wzbogacenia się. Wspomniano już o nieautoryzowanych transakcjach kartami płatniczymi, włamaniach do elektronicznych aplikacji bankowych i kradzież pieniędzy oraz wypłatach bankomatowych noszących znamiona przestępstwa. Wiele postępowań skupiało się na bezprawnym manipulowaniu cyfrowymi artefaktami: zmianą, usunięciem, odmową dostępu oraz „kradzieżą" informacji i/lub danych informatycznych zapisanych w bazach elektronicznych. Odnotowano także dość nietypowe formy przestępstw, jak chociażby zakłócenie przez sprawcę automatycznego przekazywania danych informatycznych w systemie kontrolującym skrzynie załadunkowe cysterny, masowe składanie fałszywych zamówień w celu uniemożliwienia funkcjonowania wirtualnego sklepu, czy umieszczenie na stronie internetowej złośliwego oprogramowania, które propagowało się w urządzeniach osób odwiedzających tę stronę. Kilka czynów karalnych, znajdujących się w badanym materiale aktowym, polegało na zakładaniu nielegalnych urządzeń podsłuchowych. Szczególnie „popularne" było przestępstwo nieuprawnionego uzyskiwania w wyniku przełamania lub ominięcia zabezpieczeń elektronicznych, dostępu do kont osób trzecich na platformach społecznościowych typu Facebook lub do skrzynek poczty elektronicznej. Analiza akt potwierdziła ponadto, że działania sprawców coraz intensywniej ukierunkowane są na waluty wirtualne; służą one do zapłaty za nielegalne towary i usługi, do uiszczenia okupu za odszyfrowanie plików lub prania pieniędzy z wykorzystaniem systemu blockchain; chodziło także o „kradzież" bitcoinów z portfela osoby fizycznej lub giełdy. Zdarzały się sprawy dotyczące bezprawnego przejęcia awatarów w grach komputerowych. Dochodzą do tego różnego rodzaju oszustwa oparte na socjotechnice, które łączą w sobie elementy świata „realnego" z działaniami w cyberprzestrzeni, jak chociażby malwersacje inwestycyjne na platformach tradingowych czy budowanie z wykorzystaniem środków

oraz naiwności pokrzywdzonych piramid finansowych oraz telesprzedaż nosząca znamiona przestępstwa.

Jeśli weźmie się pod uwagę profil przestępców, to zdiagnozowany obraz przestępczości teleinformatycznej pozwala wyodrębnić dwie grupy osób popełniających omawiane czyny karalne, tj. sprawców „z przypadku" oraz takich, którzy działali w sposób wyrafinowany i szczegółowo planowali łamanie prawa.

Mianem przestępcy „przypadkowego" zwykło się określać osobę niemającą wcześniej problemów z prawem, o ustabilizowanym trybie życia, która czynu zabronionego dopuściła się pod wpływem impulsu: zazdrości, zdrady, chęci zemsty. Monografia opisuje przypadki, gdy oskarżeni włamywali się do kont osób im bliskich na platformach społecznościowych, bo czuli się w jakiś sposób zranieni i chcieli w ten sposób zamanifestować swoją złość ukarać pokrzywdzonych lub dowiedzieć się czegoś więcej o nich. W innym przypadku kobieta bez uprawnienia zmieniła informacje (menu, godziny otwarcia lokalu) zamieszczone na stronie internetowej restauracji, bo chciała zemścić się na pracodawcy za zwolnienie jej matki. Po drugiej stronie plasują się „przestępcy zawodowi", których motywowała do działania chęć wzbogacenia się; niekiedy potwierdzała to sama kwalifikacja prawna zarzucanych im czynów w postaci art. 65 § 1 k.k. Tak było w przypadku Tobiasza O., który oszukał kilkadziesiąt osób w ramach nielegalnej działalności związanej z firmą Crypto Academy, zbudował schemat Ponziego i prał „zarobione" pieniądze z wykorzystaniem kryptowalut. Analiza spraw karnych potwierdziła jeszcze jedną regułę: sprawcy omawianych przestępstw to ludzie młodzi lub bardzo młodzi i chociaż w badaniach nie zastosowano metod statystycznych do dokładnego oszacowania ich wieku, to rzadko przekraczał on 40 lat. Armaged0n zaczął popełniać cyberprzestępstwa, mając 18 lat, jego wspólnik Kamil C. – 28, twórcy sklepów internetowych oferujących narkotyki za bitcoiny Kamil R. i Adam G. mieli 34 lata, Tobiasz O., twórca piramidy kryptowalutowej, 32 lata. Zaobserwowano ponadto pewną regułę: im stosowane przez przestępców narzędzia teleinformatyczne miały bardziej zaawansowany charakter, tym byli oni młodsi.

W kilkuset analizowanych sprawach, które dotyczyły „ataków" przeprowadzonych spoza terytorium Polski, organom ścigania tylko raz udało się ustalić tożsamość hakera, tj. Tomasza T. Na terenie kraju zostały natomiast zatrzymane osoby popełniające skimming (Bułgarzy i Rumuni) oraz twórcy internetowych sklepów sprzedających narkotyki z terenu Holandii. Wynika z tego, że cyberprzestępcy działający zdalnie z często nieustalonego geograficznie miejsca, pozostają zazwyczaj całkowicie anonimowi dla organów ścigania. Wiąże się to m.in. z kwestią archaicznych procedur realizacji międzynarodowej pomocy prawnej oraz szerzej, problemami, jakie generuje transgraniczna przestępczość komputerowa. Dlatego akty oskarżenia i wyroki sądowe dotyczyły Polaków. Ich status majątkowy i sytuacja osobista były różne, ale charakterystyczne było to, że wśród oskarżonych ponadprzeciętnie reprezentatywna była grupa osób zajmujących się zawodowo informatyką lub chociażby posiadających wykształcenie związane

z komputerami. Osoby takie miały wiedzę, jak wykorzystać systemy informatyczne i teleinformatyczne do popełniania przestępstw, a poza tym niejednokrotnie same były zatrudnione w charakterze administratorów systemów komputerowych, co czyniło dla niech naturalną okazję do nadużyć.

Jeśli chodzi o *modus operandi* sprawców, to warto ponownie odwołać się do podziału na przestępców „z przypadku" i „zawodowych". Przestępcy okazjonalni to osoby, które znalazły się w szczególnym „splocie sytuacyjnym" i przy nadarzającej się okazji, bez przygotowanego planu, popełniły przestępstwo. Mowa tu o prostych środkach działania, np. uzyskaniu dostępu do cudzego rachunku bankowego, gdy sprawca podglądnął hasło i login lub wykorzystał funkcję automatycznego logowania do konta, kiedy dane autoryzacyjne zapisały się w pamięci komputera albo znalazł zapisek z takimi danymi. W monografii ustalono, że zdecydowanie największa liczba spraw o haking dotyczyła zdobycia hasła w prosty sposób, a nie przy użyciu specjalistycznych programów lub wyrafinowanych technik hakerskich. W zdecydowanej większości przypadków sprawcy oskarżeni o czyn z art. 267 § 1 k.k. posiadali jedynie podstawową wiedzę o technologiach informatycznych i nie potrafili przeprowadzać jakichkolwiek „ataków hakerskich" lub przełamywać skomplikowanych zabezpieczeń komputerowych. Zdarzały się też sytuacje, kiedy przestępca z tytułu sprawowanej funkcji lub wykonywanej pracy posiadał akces do elektronicznej bazy danych i dzięki temu mógł manipulować znajdującymi się tam zapisami księgowymi (pracownik banku) lub odmówić dostępu do informacji osobom uprawnionym (administrator systemu informatycznego szkoły). Napisano już o nieuprawnionych transakcjach bankomatowych, które są proste w realizacji, jeśli sprawca wszedł w posiadanie karty płatniczej.

Ale zdarzały się przypadki, kiedy przestępcy stosowali na odległość wyrafinowane narzędzia teleinformatyczne do przełamywania zabezpieczeń i atakowania komputerów pokrzywdzonych osób. W książce opisano sytuacje, gdy złośliwe oprogramowanie: „ransomware w postaci wirusa określanego jako Polski Ransomware, Vortex lub Flotera szyfrowało dane", „wpływało na automatyczne przetwarzanie danych teleinformatycznych na serwerze", „automatycznie oraz bez wiedzy i zgody użytkowników Internetu instalowało się i zmieniało dane", czy też „służyło do zmiany rachunków bankowych". Cyberprzestępcy używali także narzędzia IT do maskowania adresu IP za pomocą sieci TOR oraz VPN-ów, szyfrowania komunikacji, podszywali się pod inne osoby lub tworzyli całkowicie fikcyjne profile w celu ukrycia swojej prawdziwej tożsamości. Powszechne okazało się użytkowanie przez nich numerów telefonów, rachunków bankowych, adresów kryptowalutowych oraz kont internetowych założonych „na słupa", czyli osoby niemające nic wspólnego z popełnianiem przestępstw. Nieodłączny element *modus operandi* „zawodowych" cyberprzestępców stanowiło także pranie pieniędzy z wykorzystaniem kryptowalut, co opisano m.in. w sprawie „tajemniczego listonosza".

Bardo częstym elementem *modus operandi* sprawców jest socjotechnika. Nawet stosując wyrafinowane narzędzie hakerskie, przestępca niejednokrotnie musi podstępnie

„zachęcić" potencjalną ofiarę, aby uruchomiła działanie malware'a; przykładowo w jednej ze spraw kobieta otrzymała mail z adresu przypominającego pocztę jej banku, a treść wiadomości wzywała ją do kliknięcia w hiperłącze, które przekierowało ją na fałszywą stronę instytucji finansowej, stanowiącą element phishingu. Opisano także „marketing sprzedażowy", którego przynajmniej pewien etap realizacji opiera się na środkach łączności elektronicznej, zazwyczaj telefonach, oraz oszustwa inwestycyjne, kiedy sprawca omamiony wizją ogromnego zysku przekazuje przestępcy nie tylko pieniądze, ale także umożliwia mu zdalny dostęp do zasobów własnego komputera. W innych sprawach napastnicy stosowali metody socjotechniczne typu mail boombing lub SPAM po to, aby „manipulować" ludźmi, którzy dobrowolnie przekazywali im hasła do aplikacji bankowych, wpłacali środki na zarządzane przez cyberprzestępców rachunki bankowe lub przekazywali im szczegółowe dane osobowe.

Powracając jeszcze do *modus operandi*, to „zawodowi" cyberprzestępcy dysponowali wyrafinowanymi narzędziami informatycznymi służącymi do nielegalnych działań; chodzi m.in. o złośliwe oprogramowanie (wirusy, robaki) do „kradzieży" danych lub informacji z pamięci zainfekowanego systemu informatycznego, a nawet jego niszczenia. Inną grupę stanowiły programy szpiegujące, które w tajemnicy przed użytkownikiem komputera rejestrowały poświadczenia logowania i aktywność przeglądarki oraz kopiowały dane tak, aby wykorzystać je do kradzieży tożsamości lub włamań. Hakerzy stosowali często ataki siłowe, kiedy specjalne algorytmy obliczeniowe metodą prób i błędów próbowały uzyskać nieuprawniony dostęp do określonej bazy elektronicznej. Najbardziej zaawansowane były ataki określane mianem man in the middle, polegające na niejawnym podsłuchu transmisji danych i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami prowadzonej komunikacji.

Jednak obraz cyberprzestępczości w przeważającej liczbie przeanalizowanych spraw był stosunkowo prosty, a *modus operandi*, jeśli chodzi o zastosowane środki, nieskomplikowany. Taki stan rzeczy utrzymuje się od kilku lat, bowiem autor monografii już w 2017 r. pisał, że większość informacji medialnych skupia się na spektakularnej cyberprzestępczości w skali makro (państwa, regionu, całego świata), gdyż są to tematy nośne, cechuje je znaczna ogólnikowość i łatwiej wzbudzić nimi zainteresowanie odbiorców. I chociaż „modne" są kwestie związane z Internetem, bezpieczeństwem infrastruktury krytycznej czy obrazem wojny cybernetycznej, to jednak codzienna twarz cyberprzestępczości, która dotyka „przeciętnego" obywatela, jest o wiele bardziej banalna. Skłania to do wniosku, że jej obraz medialny odbiega od tego, czym na co dzień zajmują się organy ścigania. Chociaż istnieje pilna potrzeba budowania ogólnopolskich strategii bezpieczeństwa cybernetycznego przed atakami dużego kalibru, to niezbędne jest także

wypracowanie skutecznych mechanizmów walki z oszustwami i innymi nadużyciami w skali mikro[580].

Jakie zatem podejmowano czynności kryminalistyczno-procesowe w sprawach dotyczących przestępczości teleinformatycznej, aby ścigać ich sprawców? Przyjęło się twierdzenie, że w śledztwie dotyczącym cyberprzestępczości konieczne jest powołanie biegłego (instytucji specjalistycznej lub naukowej) z zakresu informatyki śledczej w celu przeprowadzenia ekspertyzy, której przedmiotem są ślady cyfrowe znajdujące się w zabezpieczonych urządzeniach końcowych (laptopach, telefonach), a niekiedy także w sieciach informatycznych oraz systemach teleinformatycznych. Analiza spraw karnych dowiodła, że chodzi zarówno o komputery ofiar przestępstwa, ale też sprawców nielegalnych działań. Zadaniem biegłego było ustalenie np., czy dostarczony do badań komputer łączył się z innym urządzeniem, stanowiącym cel ataku, czy w jego pamięci znajdowało się złośliwe oprogramowanie służące do popełnienia przestępstwa; biegłemu zlecono także ujawnienie słów i haseł, które mogły mieć związek z *modus operandi* sprawcy.

Opiniowanie było efektywne w tym znaczeniu, że prokuratorzy otrzymywali wyczerpujące odpowiedzi na stawiane biegłym pytania, pozwalające na dokonywanie węzłowych ustaleń faktycznych w śledztwie. W analizowanych sprawach biegły „jednoznacznie stwierdził, iż zabezpieczone urządzenia były automatami do gry w rozumieniu ustawy o grach hazardowych", „badane urządzenie umożliwiało m.in. lokalizowanie położenia osób/obiektów przy użyciu sygnału GPS, monitorowanie aktualnej pozycji w czasie rzeczywistym", „oskarżony dzięki oprogramowaniu miał dostęp do wiadomości wychodzących i przychodzących na dowodowy numer telefonu /…/ aparat był wykorzystywany jako telefon sterujący podsłuchem typu SpyPhone i odbierał on wszystkie wiadomości SMS od telefonu podsłuchiwanego". Zdarzały się sytuacje, gdy ekspertyza nie dostarczyła śladów lub dowodów pozwalających na ustalenie sprawcy przestępstwa, a główną tego przyczynę stanowiło użycie przez sprawców zaawansowanych algorytmów do szyfrowania danych. Dotyczyło to przede wszystkim ataków typu ransomware, kiedy w opinii wskazywano, iż system serwera zainfekował programem TrueCrypt i „zaszyfrowanie obejmuje całą powierzchnię dysku wraz z sektorem startowym MBR". Biegły, posługując się specjalistycznym oprogramowaniem i sprzętem o określonej mocy obliczeniowej, nie posiadał możliwości technicznych do odszyfrowania dysku.

Badania dostarczyły podstaw do sformułowania jeszcze innego, ważnego wniosku; otóż tylko w niektórych sprawach dotyczących szeroko rozumianej cyberprzestępczości powoływano biegłego z zakresu informatyki śledczej. Wynikało to z następujących powodów:

[580] P. Opitek, *Zwyczajny obraz cyberprzestępczości – jak problem ten dotyka „przeciętnego" obywatela?*, https://cyberdefence24.pl/instytut-kosciuszki-zwyczajny-obraz-cyberprzestepczosci-jak-problem-ten-dotyka-przecietnego-obywatela [dostęp: 23.05.2023].

1. sposób popełnienia przestępstwa był oczywisty, a więc nie zachodziły przesłanki do korzystania z „wiadomości specjalnych" (w sprawach nielegalnych transakcji kartami płatniczymi można by potwierdzić, „badając" terminal POS, że użyto w nim do zapłaty określonego „plastiku", ale fakt ten jednoznacznie ustalono wykorzystując inne źródła dowodowe);
2. zabezpieczenie sprzętu do badań okazało się niemożliwe (np. nie ustalono sprawcy i miejsca jego działania);
3. organ procesowy, ze względu na ekonomikę procesową, zaniechał badania komputera.

Postawa organu procesowego, opisana w ostatnim punkcie, może budzić kontrowersje. Dotyczyła ona często ataków ransomware, gdy prokuratorzy nie zlecali biegłym badania zaszyfrowanych maszyn, zakładając, że haker i tak pozostanie nieustalony, a więc koszty i czas poświęcony na opiniowanie są zbędne. Inne, podobne przypadki odnosiły się do spraw kwalifikowanych z art. 267 § 1 k.k., kiedy sprawca przyznał się do popełnienia zarzucanego mu czynu i organ procesowy rezygnował z badania sprzętu komputerowego zaangażowanego w popełnienie przestępstwa. Skutkowało to sytuacjami, że w dużej liczbie decyzji procesowych „nie wskazano, chociażby ogólnie, w jaki sposób doszło do przełamania albo ominięcia zabezpieczenia lub jak działało oprogramowanie lub urządzenie hakerskie"; organ procesowy poprzestawał tylko na ogólnym stwierdzeniu, że miało miejsce „ominięcie w nieustalony sposób hasła", „przełamanie elektronicznych zabezpieczeń konta", „włamanie się za pośrednictwem Wirtualnej Poczty", czy „uzyskanie dostępu do kont giełdy elektronicznej przez pokonanie zabezpieczeń serwisu". Taki zdawkowy opis *modus operandi* i „luki" w ustaleniach faktycznych mogą implikować wątpliwości, co do realizacji przez organ procesowy obowiązków wynikających z art. 2 § 2 k.p.k., art. 7 k.p.k. i art. 193 § 1 k.p.k.

Opisana sytuacja, oceniana pod kątem najlepszych standardów prowadzenia postępowania karnego, nie zasługuje na aprobatę, gdyż od sądu i prokuratora wymaga się poczynienia wszystkich możliwych ustaleń co do okoliczności popełnienia przestępstwa, nawet jeśli (prawdopodobnie) nie doprowadzi to do ujęcia sprawcy czynu zabronionego albo sprawca przyznał się do popełnienia przestępstwa i dobrowolnie poddał karze. Nie zmienia tego fakt, że opinie biegłych są drogie i płacone z pieniędzy podatników. Zaniechania sądu czy prokuratora na omawianym polu mogą bowiem skutkować brakami w ustaleniach faktycznych, co zauważył w jednej sprawie Sąd Najwyższy. Wskazał on, że błąd w procedowaniu stanowił brak kluczowych ustaleń, na podstawie wiedzy specjalnej dotyczącej szczegółów techniczno-informatycznych, jak doszło do zarzucanego skazanemu przełamania zabezpieczeń i wysyłania wiadomości przez nieuprawnioną osobę. Przełamanie takiego zabezpieczenia jest trudne, a w materiale dowodowym zabrakło opinii biegłego na temat owego przełamania, co zdaniem Sądu Najwyższego dyskwalifikowało rozumowanie sądów niższych instancji, jako spekulatywne, a więc dowolne, i stanowiło rażące naruszenie normy art. 7 k.p.k.

Powracając do typowych czynności realizowanych w sprawach dotyczących przestępstw teleinformatycznych, to podstawowe źródło dowodowe stanowiły zeznania świadków, a czasami wyjaśnienia podejrzanego (oskarżonego). Sprawę inicjowało najczęściej złożone przez pokrzywdzonego lub jego pełnomocnika zawiadomienie o podejrzeniu popełnienia przestępstwa, w którym stosunkowo często wskazywano potencjalnego sprawcę czynu zabronionego. W śledztwach dotyczących poważnych cyberprzestępstw gromadzono ponadto informacje pochodzące od dostarczycieli usług sieciowych: wykazy połączeń telekomunikacyjnych (tzw. bilingi), dane logowania do nadajników BTS, logi opisujące pracę systemów komputerowych, aktywność cyfrową posiadaczy kont założonych na portalach społecznościowych, giełdach kryptowalutowych czy platformach sprzedażowych, zapis monitoringu, dane od operatora bankomatów itd.

W trakcie badań napotkano także specyficzne źródła dowodowe, charakterystyczne dla spraw nazywanych „przestępczością teleinformatyczną". Akta dotyczące walut wirtualnych zawierały analizy kryminalne przepływów kryptowalutowych po to, aby ustalić adres zdeponowania środków „skradzionych" pokrzywdzonemu lub źródło ich pochodzenia. Inny, specyficzny dowód stanowiła „analiza psychiatryczna dotycząca portretu psychologicznego nieznanego autora anonimu" w sprawie, gdzie przestępca od firmy produkującej żywność zażądał okupu w bitcoinach za odstąpienie od wprowadzenia na rynek zatrutych produktów spożywczych. W innej, wspomnianej sprawie Tobiasza O. materiały śledztwa zawierały „Raport z czynności" przeprowadzonych przez firmę detektywistyczną wynajętą przez jednego z pokrzywdzonych w celu „prowadzenia poszukiwań Tobiasza O." oraz „windykacji wartości materialnych w postaci 183 bitcoinów, które przywłaszczył sobie Tobiasz O.". Pokazuje to, że czynności kryminalistyczno-procesowe w sprawach dotyczących przestępczości teleinformatycznej to materia niezwykle „żywa", gdzie tradycyjne środki i źródła dowodowe mieszają się z nowymi technikami i metodami wykrywczymi.

Pozostaje jeszcze odpowiedzieć na pytanie, czy ściganie sprawców przestępstw teleinformatycznych jest efektywne. Jeśli chodzi o efektywność, rozumianą jako ustalenie wykonawców czynów zabronionych oraz pociągnięcie ich do odpowiedzialności karnej, to dzieje się to odnośnie do sprawców działających na terytorium Polski. Sporo takich osób udaje się ująć, zazwyczaj przyznają się one do popełniania występku, składają obszerne wyjaśnienia na okoliczności sprawy i korzystają z instytucji konsensualnego zakończenia postępowania karnego. Jeśli sprawa trafiła do sądu z aktem oskarżenia, to charakterystyczną rzeczą jest to, iż sąd najczęściej warunkowo umarzał postępowanie karne lub skazywał oskarżonych na karę grzywny w symbolicznej wysokości. Surowsze wyroki zapadały jedynie co do sprawców stosujących wyrafinowane *modus operandi* i osiągających znaczne zyski, najczęściej finansowe, z realizacji zakazanych działań. Widoczna jest ponadto reguła, że o wiele efektywniejsze jest ściganie przestępstw niewielkiego kalibru popełnionych „z przypadku", aniżeli profesjonalnych cyberprzestępców.

Dobitnie pokazała to analiza ataków typu ransomware: spośród kilkudziesięciu analizowanych spraw, tylko haker Armaged0n został zatrzymany i sąd skazał go na karę pozbawienia wolności. W przytłaczającej liczbie podobnych spraw, ale także phishingu, ataków na portfele i giełdy kryptowalutowe, ustalenie osób naruszających prawo jest praktycznie niemożliwe, czynności dowodowe ograniczają się do przesłuchania pokrzywdzonego i procedowanie kończy wydanie postanowienia o umorzeniu śledztwa/dochodzenia bez dodatkowych badań specjalistycznych.

Niemniej organy ścigania wytrwale uczą się walki z poważnymi naruszeniami prawa w cyberprzestrzeni, realizowanymi także przez „aktorów" działających z zagranicy i stosujących wyrafinowaną technologię informatyczną. Przykładem są aresztowania administratorów wspomnianych już sklepów internetowych sprzedających narkotyki i dopalacze. Zmiana koncepcji handlowej wśród przestępców spowodowała nowe podejście do walki z nimi, zastosowane przez Centralne Biuro Śledcze Policji: niezbędne okazały się zaawansowane czynności operacyjno-rozpoznawcze w cyberprzestrzeni w postaci zakupu kontrolowanego, przesyłki niejawnie nadzorowanej i funkcjonariusza działającego pod przykryciem po to, aby zinfiltrować działalność cyfrowej platformy, poznać mechanizm realizacji przesyłek z zakazanymi substancjami oraz ustalić ich odbiorców. Dochodziła do tego możliwość realizacji kontroli operacyjnej na terenie innego kraju Unii Europejskiej w ramach europejskiego nakazu dochodzeniowego. Rezultatem działań CBŚP były zatrzymania twórców darkmarketów, zamknięcie stron internetowych służących do popełniania przestępstw oraz konfiskata znacznych ilości narkotyków, a ponadto pieniędzy pochodzących z przestępstwa.

Przechodząc do meritum monografii, to przeprowadzone badania nie tylko potwierdziły tezę, że opis i kwalifikacja prawna przestępstw teleinformatycznych sprawiają kłopoty sędziom i prokuratorom, co znajduje odzwierciedlenie w błędach dotyczących wydawanych przez nich decyzji procesowych, ale udowodniły ponadto, że owych nieprawidłowości jest zbyt wiele. Nawet jeśli przyjąć, że działalność orzecznicza, jako przejaw aktywności ludzkiej, musi być obarczona jakimś błędem i stąd wynika prawo złożenia apelacji od rozstrzygnięcia pierwszoinstancyjnego, to jednak ustalony stan rzeczy przekracza dopuszczalną granicę „błądzenia" organów procesowych.

Stwierdzone w analizowanych sprawach błędy miały kilka postaci, a nierzadko w jednym orzeczeniu nakładały się na siebie. Pierwsza grupa „omyłek" dotyczyła, można by rzec, „okoliczności obiektywnych", gdy niepoprawności wynikały z subsumpcji abstrakcyjnych znamion czynu do skomplikowanych okoliczności faktycznych sprawy. Faktem jest, że owe znamiona sprawiają trudności wykładnicze, gdyż odnoszą się do kwestii specjalistycznych z zakresu techniki czy informatyki, a więc dziedzin wiedzy z reguły obcych prawnikom – humanistom. Oczywiste jest, że sędzia i prokurator powinien zgłębić temat rozpoznawanej kwestii, ale nie sposób być specjalistą we wszystkim, szczególnie że sprawy karne przydzielane są losowo, a więc każdy sędzia może otrzymać do swojego referatu akta dotyczące hakingu, malware'a, czy jeszcze innego

cyberprzestępstwa. Poza tym, czyny stypizowane w art. 267 k.k. – art. 269b k.k. to stosunkowo „młode" przepisy, których wykładnia nie jest tak ugruntowana, jak ma to miejsce chociażby w przypadku czynów karalnych godzących w życie i zdrowie człowieka, procedowanych i komentowanych od dziesiątek lat przez prawników. Stąd pojawiają się dyskusje oraz kontrowersje dotyczące prawidłowego odczytania znamion przestępstw teleinformatycznych, którymi judykatura i piśmiennictwo zajęły się niekiedy tylko powierzchownie; w jeszcze innych przypadkach funkcjonują odmienne, konkurujące ze sobą linie orzecznicze. Oczywiście, nie stanowi to usprawiedliwienia dla popełnianych błędów w orzekaniu, ale fakty pozostają faktami i rzeczywiście istnieją „okoliczności obiektywne" rzutujące na stwierdzone w trakcie badań nieprawidłowości. Widoczne to było m.in. odnośnie do przestępstwa stypizowanego w art. 269b § 1 k.k. Przepisowi temu zarzuca się zbyt daleko idącą kryminalizację zachowań leżących na przedpolu wymienionych w nim czynów zabronionych, niedookreśloność znamion czasownikowych w kontekście specyfiki komunikowania się w sieci oraz karalność przekazania narzędzi i urządzeń „innym osobom", podczas gdy taki sam czyn w stosunku do „jednej osoby" pozostaje bezkarny. Inny dylemat to praktyczne rozróżnienie pomiędzy znamionami: „system informatyczny", „system teleinformatyczny" i „sieć teleinformatyczna", bo dzisiaj trudno jest wytyczyć ścisłe ramy pojęciowe i znaki graniczne pomiędzy zakresem pojęciowym każdej z trzech opisanych wyżej kategorii.

Nawiązując do „okoliczności obiektywnych" prokurujących błędy wykładnicze, to zdaniem autora problemy orzecznicze wynikają w dużej mierze z niewłaściwego ukształtowanie niektórych znamion przestępstw stypizowanych w rozdziale XXXIII k.k. Niekiedy wygląda to tak, jakby ustawodawca „na siłę" chciał implementować na grunt krajowy zapisy konwencji o cyberprzestępczości. Oczywiście, Polska była zobowiązana do przyjęcia ustanowionych w umowie międzynarodowej rozwiązań, ale należało to poprzedzić gruntowną analizą systemową treści przestępstw zapisanych w konwencji budapesztańskiej w świetle obowiązujących już rozwiązań krajowych. Tymczasem ustawodawca poszedł „na skróty" i momentami literalnie przetłumaczył zapisy w języka angielskiego na język polski, zamiast rozważyć, czy treści konkretnych zwrotów funkcjonujących za granicą nie należałoby oddać w inny sposób, bardziej adekwatny na gruncie ustawy karnej. W rezultacie nie sposób wytłumaczyć logicznie, dlaczego przestępstwo nieuprawnionego dostępu do informacji wymaga przełamania albo ominięcia zabezpieczeń (art. 267 § 1 k.k.), a nieuprawniony dostęp do danych informatycznych (art. 267 § 2 k.k.) nie jest limitowany takim szczególnym zachowaniem sprawcy. Zresztą część doktryny, co znajduje odzwierciedlenie w decyzjach sądów, twierdzi, że już samo podglądnięcie „cudzych" haseł do konta jest równoznaczne z uzyskaniem dostępu do informacji. Zdaniem autora, jest to zbyt rygorystyczne podejście, prowadzące do nadmiernej penalizacji zachowań, które powinny być prawnie relewantne. Taki czyn, dokonany z zamiarem zalogowania się do cudzego konta, mógłby wypełnić znamiona usiłowania popełnienia przestępstwa z art. 267 § 1 k.k. przy założeniu, że treść owego

przepisu zostałaby zmieniona i karałaby nieuprawnione zapoznanie się z informacją poprzez ominięcie lub przełamanie jej szczególnego zabezpieczenia.

Powracając do przyczyn odnotowanych błędów, to należy krytycznie ocenić wcale nierzadkie sytuacje, gdy nieprawidłowości w opisie czynu i/lub jego kwalifikacji prawnej leżały całkowicie po stronie organu orzekającego, wynikały z jego niefrasobliwości, a niekiedy wręcz nonszalancji i działania „na skróty". Polegały one np. na niezamieszczeniu w opisie czynu znamion przestępstwa, które wynikały z przyjętej kwalifikacji prawnej; oto niektóre przykłady: brak w sądowym opisie czynu z art. 267 § 3 k.k. znamienia „w celu uzyskania informacji, do której nie był uprawniony", niezamieszczenie w opisie czynu znamienia skutku, o którym mowa w art. 268 § 2 k.k. („udaremnienie osobie uprawnionej zapoznania się z informacją"), brak znamienia przestępstwa o treści „nie będąc do tego uprawnionym", czy znamienia „działania w celu uzyskania korzyści majątkowej"; w jeszcze innym przypadku w opisie czynu z art. 267 § 2 k.k. zabrakło słów „uzyskania bez uprawnień dostępu do części systemu informatycznego".

Zdarzały się całkowite rozbieżności pomiędzy przyjętą kwalifikacją prawną czynu a jego opisem. W jednej ze spraw z treści prokuratorskiego postanowienia wynikało, że przestępca nie oddziaływał na psychikę pokrzywdzonego lub osoby reprezentującej pokrzywdzoną instytucję (bank) i w dacie orzekania należało przyjąć kwalifikację z art. 287 § 1 k.k., a nie art. 286 § 1 k.k. Innym razem zachodziła konieczność uzupełnienia kwalifikacji prawnej przestępstwa lub sformułowania odrębnego czynu z art. 267 § 1 k.k. lub art. 267 § 2 k.k. (ewentualnie z art. 267 § 3 k.k.), ale prokurator i sąd zapominał, że samo manipulowanie danymi lub informacją musiało poprzedzić przełamanie zabezpieczeń elektronicznych i dostanie się do zasobów cyfrowych bez uprawnienia. Takie poważne błędy mogłyby stanowić podstawę skutecznej apelacji lub nawet uniewinnienia oskarżonego.

W analizowanym materiale badawczym zdarzało się, że popełnione przez sąd błędy w wykładni, stanowiące niekiedy poważne naruszenie prawa materialnego, pozostawały niezauważone przez uczestników postępowania i przeniknęły do prawomocnych wyroków. Były także przypadki, gdy oskarżony został skazany przez sąd I instancji, ale na skutek apelacji wniesionej przez jego obrońcę w postępowaniu odwoławczym doszło do jego uniewinnienia. Takie procedowanie sądu budziło poważne zastrzeżenia szczególnie, że rozpatrywane sprawy nie były zbyt skomplikowane, ale zabrakło wnikliwości organu orzekającego dla właściwej subsumpcji stanu faktycznego do właściwej normy prawnej. Dotyczyło to m.in. podsłuchu częstotliwości radiowej użytkowanej przez policję: do wydania prawidłowego wyroku przez sąd pierwszoinstancyjny wystarczyła znajomość orzecznictwa Sądu Najwyższego, w którym stwierdza się, że urządzenie nadawczo-odbiorcze, którym posługiwał się oskarżony, nie jest urządzeniem specjalnym w rozumieniu art. 267 § 3 k.k. W innej sprawie, obejmującej skiny, wystarczyłaby nieco pogłębiona analiza zapisów ustawy o grach hazardowych oraz odszyfrowanie pojęć „rzecz" i „pieniądz" na gruncie prawa karnego, aby prokurator i sąd mieli jasny

obraz, że „skórki" takich definicji nie spełniały i oskarżony nie popełnił przestępstwa. Zatem przytoczone błędy orzecznicze nie powinny się zdarzyć.

Kolejny przykład błędów wykładniczych stanowił częsty brak rozróżnienia pomiędzy „danymi informatycznymi" a „informacją", a przecież na rozdzielności tych dwóch znamion czynu zabronionego osadza się cała logika determinująca konstrukcję przestępstw opisanych w rozdziale XXXIII k.k. Skutkowało to wieloma opisanymi w monografii omyłkami, jak choćby tą, kiedy prokurator uznał, że system informatyczny operatora sieci komórkowej, do którego sprawca w sposób nieuprawniony uzyskał dostęp za pośrednictwem aplikacji, stanowi zarówno „informacje", jak i „dane informatyczne", co skutkowało błędnym przyjęciem realnego zbiegu przestępstw z art. 267 § 1 k.k. i art. 267 § 2 k.k., podczas gdy wyświetlona na ekranie zawartość bazy klientów firmy była „informacją". Dochodziło do sytuacji, gdy w podobnych stanach faktycznych sprawy sądy skazywały oskarżonych na podstawie różnych przepisów karnych, tj. z § 1 lub 2 lub 3 art. 267 k.k., a niekiedy przyjmowały zbieg realny art. 267 § 1 i 2 k.k. Inny przykład „dowolności wykładniczej" stanowiły opisane w monografii postanowienia prokuratora o umorzeniu śledztwa w sprawach o ransomware. Braku dociekliwości sądu w postaci nierozróżnienia pomiędzy treścią znamion „ominąć" i „przełamać" informatyczne zabezpieczenie, to kolejny punkt generujących błędy orzecznicze w ocenie przestępstwa hakingu.

Odnotowano ponadto błędy językowe i chociaż odznaczają się one mniejszym ciężarem gatunkowym aniżeli uchybienia prawa materialnego, to także rzutują na zaniżoną ocenę pracy sędziego czy prokuratora. W jednym z wyroków napisano „formy" zamiast „firmy", wskazano na „ceny potraw dań", a przecież „potrawy" i „dania" to synonimy. W orzeczeniu nie powinno stosować się takich zwrotów z mowy potocznej, jak „zainfekować", „przelewać" (kryptowalutę). Ponadto w Kodeksie cywilnym jest mowa o „umowie sprzedaży", a nie „kupna-sprzedaży".

Czy warto wypominać sądowi takie „nieścisłości"? Autor uważa, że tak, bo wyrok decydujący o podstawowych interesach uczestników postępowania powinien odznaczać się „krystaliczną nieskazitelnością", zwłaszcza że jego treść jest krótka i można sformułować ją ze szczególną starannością. Orzekanie wymaga ponadto dyscypliny terminologiczno-pojęciowej oraz nieustającego poszukiwania odpowiedniego balansu między kazuistyką a elastycznością wypowiedzi. I chociaż polski proces karny nie ma charakteru „formułkowego", ale jest procesem, w którym przepisy określają jedynie sposób postępowania sądu przy redagowaniu opisu czynu tak, aby odzwierciedlał on zdarzenie przestępne ze wskazaniem znamion, to jednak da się zauważyć zbyt dużą dowolność, a nawet niefrasobliwość, w posługiwaniu się językiem przez sądy i prokuratorów w formułowaniu decyzji procesowych. Słuszny jest postulat, aby sąd posługiwał się językiem prawniczym, odzwierciedlającym znamiona przestępstwa zawarte w jednostce redakcyjnej przepisu, a nie używał zwrotów: „kradzież" zamiast „zabór w celu przywłaszczenia", „strata" zamiast „szkoda". Wynika z tego, że juryslingwistyka stanowi

niezwykle istotny element przy wykładni przepisów. Jednak przeprowadzone badania potwierdziły, że organy procesowe nie zawsze wykazują świadomość, jak ważną rolę odgrywa terminologiczno-pojęciowa precyzja języka prawniczego w zakresie nowych technologii.

Na koniec pozostaje odpowiedzieć na najważniejsze pytanie, jakie należy postawić w świetle wyników przeprowadzonych badań: Jak „naprawić" zdiagnozowaną sytuację w której sędziowie i prokuratorzy popełniają zbyt wiele błędów w opisie czynów i kwalifikacji prawnej przestępstw teleinformatycznych?

Zdaniem autora są trzy ścieżki „sanacji": chęć i wola „lepszego orzekania" wśród wymienionych osób, ich edukacja i na końcu zmiany legislacyjne.

Przede wszystkim to sędziowie i prokuratorzy muszą chcieć doskonalić swój warsztat pracy w zakresie znajomości przestępczości teleinformatycznej i dociekliwego podejścia do rozpoznawanych spraw karnych. O ile w prokuraturze można „naprawiać" pewne rzeczy, stosując wytyczne przełożonych co do metodyki prowadzenia śledztwa, to w przypadku sędziów wchodzi w grę jedynie soft power, tj. dyskutowanie na temat zastałych problemów i pojawiających się błędów oraz zachęcanie Temidy do większego zainteresowania omawianą przestępczością oraz bardziej wnikliwego pochylenia się nad sprawami tam, gdzie dotychczas zabrakło, być może, skrupulatności. Stosowanie takich regulacji, jak art. 269b § 1 k.k., art. 269b § 1a k.k. czy art. 269c k.k. rodzi bowiem dodatkowe obowiązki po stronie sędziego, ale też rozszerza zakres jego władzy wprowadzając nowe treści do zasad niezawisłości oraz niezależności. Warto samodzielnie podejmować wysiłek odczytania znaczenia stosowanej normy prawnej, gdyż zbyt często organy procesowe bezrefleksyjnie kierują się utartymi poglądami, które niekoniecznie muszą pasować do realiów rozpoznawanej sprawy.

Należy ponadto lepiej i intensywniej edukować kadry wymiaru sprawiedliwości w zakresie przestępczości teleinformatycznej, szczególnie odnośnie do wykładni znamion takich przestępstw. Zadanie to najlepiej może zrealizować Krajowa Szkoła Sądownictwa i Prokuratury zarówno w ramach kształcenia aplikantów, jak i szkoleń organizowanych dla sędziów i prokuratorów.

Po stronie ustawodawcy zachodzi konieczność ponownego przenalizowania treści przepisów rozdziału XXXIII k.k. pod kątem zbadania, czy ich konstrukcja jest prawidłowa. Zastrzeżenia budzi obecna sytuacja, kiedy dla wykładni niektórych znamion przestępstw teleinformatycznych trzeba dokonywać „wygibasów" logicznych po to, aby odnaleźć ich sens i zaproponować racjonalne stosowanie norm prawnych. Zdaniem autora, implementacja do polskiej ustawy karnej postanowień konwencji budapesztańskiej mogła zostać wykonana lepiej. Dotyczy to m.in. treści art. 269b § 1 k.k., która de facto zawiera się w tradycyjnej instytucji prawa karnego materialnego, tj. pomocnictwa (art. 18 § 3 k.k.). Jednak ów problem „niedoskonałości" przepisów wykracza poza rozdział XXXIII ustawy karnej i obejmuje m.in. szczególną ochronę przyznaną w art. 278 § 1a k.k. „karcie uprawniającej do podjęcia pieniędzy z automatu bankowego".

Stwierdzono problemy wykładnicze związane z takim przedmiotem czynności wykonawczej, a sytuację konwalidowałby usunięcie z Kodeksu karnego indywidualnej penalizacji kradzieży karty bankomatowej.

To tylko część z postulatów *de lege ferenda* zaproponowanych w monografii, gdyż przeprowadzone badania pozwoliły autorowi na rozwiązanie jawiących się problemów naukowych w doktrynie i orzecznictwie odnośnie do kwestii związanych z kwalifikacją prawną i opisem niektórych stanów faktycznych charakteryzujących przestępczość teleinformatyczną. Niekiedy autor przychylał się do jednego z reprezentowanych stanowisk, ale najbardziej nowatorski charakter mają te wyniki badań, które pozwoliły zaproponować nowe podejście do opisu i kwalifikacji prawnej czynu. Dotyczy tego m.in. postulat o zbiegu pomijalnym art. 279 § 1 k.k. i art. 287 § 1 k.k. w przypadku włamania do elektronicznej aplikacji oraz kradzieży środków pieniężnych z rachunku bankowego.

Wypracowanie najlepszych standardów orzeczniczych leży bowiem w interesie całego wymiaru sprawiedliwości. Autor wierzy, że monografia przyczyni się do pogłębienia wiedzy prawników w tym zakresie, a zaproponowane w niej rozwiązania staną się pomocne w codziennej pracy sędziów i prokuratorów oraz nakłonią do refleksji prawnej nad przestępczością teleinformatyczną.

Bibliografia

Akty prawne:

1. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).
2. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dziennik Urzędowy Unii Europejskiej. https://european-union.europa.eu/select-language?destination=/node/1.
3. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.).
4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
5. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124, 1285).
6. Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. 2017 poz. 768).
7. Ustawa z dnia 15 grudnia 2016 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw (Dz. U. z 2017 r. poz. 88).
8. Ustawa z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. z 2013 r., Nr 1036).
9. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2021 r. poz. 1907, 1814, 2140).
10. Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim (t.j. Dz. U. z 2023 r. poz. 1028).
11. Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (t.j. Dz. U. z 2023 r. poz. 227).
12. Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2008 r. Nr 214, poz. 1344).
13. Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. z 2008 r. Nr 171, poz. 1056).
14. Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (t.j. Dz. U. z 2023 r. poz. 845).
15. Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2023 r. poz. 646, 825).
16. Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2023 r. poz. 172).
17. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568, 695).
18. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2023 r. poz. 57 z późn. zm.).
19. Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz. U. z 2023 r. poz. 659).

20. Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. z 2004 r. Nr 69, poz. 626).
21. Ustawa z dnia z dnia 27 lipca 2002 r. – Prawo dewizowe (t.j. Dz. U. z 2022 r. poz. 309).
22. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2022 r. poz. 1648, 1933, 2581).
23. Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych (t.j. Dz. U. z 2020 r. poz. 129).
24. Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz. U. z 2022 r. poz. 492, 655).
25. Ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439, 2447).
26. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138 z późn. zm.).
27. Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (t.j. Dz. U. z 2022 r. poz. 1375 z późn. zm.).
28. Ustawa z dnia 13 października 1995 r. - Prawo łowieckie (t.j. Dz. U. z 2023 r. poz. 1082).
29. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2022 r. poz. 1233).
30. Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2023 r. poz. 171).
31. Ustawa z dnia 20 maja 1971 r. - Kodeks wykroczeń (t.j. Dz. U. z 2022 r. poz. 2151 z późn. zm.).
32. Ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 1966 Nr 24 poz. 151 z późn. zm.).
33. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz. U. z 2022 r. poz. 1360 z późn. zm.).
34. Ustawa z dnia 7 lipca 2022 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2022 r. poz. 2600).
35. Obwieszczenie Prezesa Rady Ministrów z dnia 29 lutego 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie „Zasad techniki prawodawczej" (Dz. U. z 2016 r. poz. 283).

Literatura - pozycje monograficzne i rozdziały w monografiach zbiorowych:

1. Adamski A., *Kryminalizacja narzędzi hakerskich w europejskim i polskim prawie karnym*, [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018.
2. Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
3. Bala S., Kopyściański T., Srokosz W., *Kryptowaluta jako elektroniczny instrument płatniczy bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wrocław 2016.
4. Behan A., *Waluty wirtualne jako przedmiot przestępstwa*, Kraków 2022.

5. Bensel P., *Systemy i sieci komputerowe. Podręcznik do nauki zawodu technik informatyk*, Gliwice 2010.
6. Biegański J., *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, [w:] *Przestępczość teleinformatyczna*, red. J. Kosiński, Szczytno 2012.
7. Bojarski T., *Odmiany podstawowych typów przestępstw w polskim prawie karnym*, Warszawa 1982.
8. Charatynowicz J., *Kryptowaluty jako zagrożenia i wyzwania dla bezpieczeństwa finansowego państwa*, rozprawa doktorska, Akademia Sztuki Wojennej, Wydział Bezpieczeństwa Narodowego, praca niepublikowana (zbiory własne autora).
9. Chell D., Erasmus T., Colley S., Withehouse O., *Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera*, Gliwice 2017.
10. Doliwa A., *Ogólna charakterystyka prawa gospodarczego prywatnego*, [w:] *Zasady prawa gospodarczego prywatnego*, red. T. Mróz, M. Stec, Warszawa 2007.
11. Forshaw J., *Atak na sieci okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci*, Gliwice 2019.
12. Jakimowicz W., *Aktualność pojęć prawa administracyjnego*, Wolters Kluwer Polska 2021, LEX.
13. Kabaciński W., Żal M., *Sieci telekomunikacyjne*, Warszawa 2008, 2019.
14. *Kodeks cywilny. Komentarz*, red. P. Nazaruk, J. Ciszewski, Warszawa 2019, LEX.
15. *Kodeks karny. Część szczególna, Komentarz do artykułów 222–316*, t. 2, red. A. Wąsek, R. Zawłocki, Duże Komentarze Becka 2010.
16. *Kodeks karny. Część szczególna*, t. 2, cz. 1, *Komentarz do art. 117–211a*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2017.
17. *Kodeks karny. Część szczególna,* t. 2, cz. 2, *Komentarz do art. art. 212–277d*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2017, LEX.
18. *Kodeks karny. Część szczególna*, t. 2, *Komentarz do art. art. 117–277 k.k.*, red. A. Zoll, Wolters Kluwer Polska 2017, LEX.
19. *Kodeks karny. Część szczególna*, t. 2, *Komentarz do art. art. 117–277 k.k*, red. A. Zoll, LEX 2013.
20. *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. W. Wróbel, A. Zoll, Wolters Kluwer Polska 2022, LEX.
21. *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. A. Zoll, W. Wróbel, LEX 2022.
22. *Kodeks karny. Część szczególna*. *Komentarz*, red. J. Giezek, LEX 2014.
23. *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Wolters Kluwer Polska 2021, LEX.
24. *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2023.
25. *Kodeks karny. Komentarz*, red. M. Filar, Wolters Kluwer 2016, LEX.
26. *Kodeks karny. Komentarz*, red. R. Stefański, Legalis 2021.
27. *Kodeks karny. Komentarz*, red. T. Bojarski, Wolters Kluwer 2009.
28. *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Wolters Kluwer Polska 2020.

29. *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Wolters Kluwer Polska 2022, LEX.
30. *Komentarz do kodeksu cywilnego*, red. A. Sylwestrzak, LEX/el. 2022.
31. *Komentarz do kodeksu cywilnego*, red. J. Ciszewski, LEX/el. 2022, stan prawny: 1 stycznia 2022 r.
32. *Komentarz do Kodeksu karnego*, red. A. Zoll, W. Wróbel, LEX, stan prawny: 1 września 2021.
33. M. Kulicki (red.), V. Kwiatkowska-Darul, L. Stępka, *Kryminalistyka: wybrane zagadnienia teorii i taktyki śledczo-sądowej*, Toruń 2005.
34. Machnikowska A., *Zasady niezawisłości sędziów a wykładnia prawa*, [w:] M. Herman, S. Sykuna, *Wykładnia prawa. Tradycja i perspektywy*, Monografie Prawnicze, Warszawa 2016.
35. Majorek M., *Kod YouTube. Od kultury partycypacji do kultury kreatywności*, Kraków 2015.
36. Makowski W., *Prawo karne. O przestępstwach w szczególności. Wykład porównawczy prawa karnego austryackiego, niemieckiego i rosyjskiego obowiązującego w Polsce*, Warszawa 1924.
37. Marek A., *Kodeks karny. Komentarz*, LEX 2010.
38. Mariański M., *Ryzyka związane z rozwojem obrotu wirtualnymi walutami. Analiza na gruncie obecnie obowiązujących przepisów*, [w:] *Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania*, red. W. Pływaczewski, LEX 2015.
39. Morawski L., *Wstęp do prawoznawstwa*, Toruń 2014.
40. Opitek P. (współautor), *Metodyka zabezpieczeń majątkowych*. Prokuratura Krajowa 2018 (zbiory własne autora).
41. Opitek P., *Aspekty kryminalistyczne, techniczne i prawne przestępczości kryptowalutowej*, [w:] *Kryptowaluty – szanse i zagrożenia. Funkcjonowanie niepieniężnych środków płatniczych jako strategiczne wyzwanie dla bezpieczeństwa systemu finansowego państwa, publikacja pokonferencyjna*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego 2020.
42. Opitek P., *Biegły z zakresu kryptowalut w sprawach karnych,* [w:] *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, red. D. Zienkiewicz, Toruń 2021.
43. Opitek P., C*yberprzestępczość w pracy prokuratora*, Prokuratura Krajowa 2018.
44. Opitek P., *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Łódź 2022. P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6.
45. Opitek P., *Legalny haking w Polsce – krytyczna ocena uregulowań Kodeksu karnego*, [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018.
46. Opitek P., Lenczowska-Soboń K., *Tokeny NFT jako dzieło sztuki wykorzystywane do popełniania przestępstw*, [w:] *Taktyka i technika kryminalistyczna w zmieniającym się świecie,* [w:] *Kryminalistyka w zmieniającym się świecie. Wybrane zagadnienia,* red. D. Wilk, Wydawnictwo Naukowe FNCE 2023.

47. Opitek P., *Przestępczość z wykorzystaniem kryptowalut oraz ich status w postępowaniu karnym*, [w:] Przestępczość teleinformatyczna 2017, red. J. Kosiński, Szczytno 2018.
48. Opitek P., *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Monografie Prawnicze C.H. Beck 2017.
49. A. Petrys, *Bitcoin – współczesna alternatywa wobec pieniądza fiducjarnego w perspektywie postępowania karnego*, „Palestra" 2022, nr 5, wydanie internetowe: https://palestra.pl/pl/czasopismo/wydanie/5 - 2022/artykul/bitcoin - wspolczesna - alternatywa - wobec - pieniadza - fiducjarnego - w - perspektywie - postepowania - karnego.
50. Pietras A., Kawecki M., *Ustawowe znamiona czynów zabronionych w części wojskowej kodeksu karnego w tabelach*, Gliwice 2017.
51. Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
52. Rodwald P., *Kryptowaluty z perspektywy informatyki śledczej*, Gdynia 2021.
53. Siwicki M., *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018.
54. Skowron D., *Bitcoin jako przedmiot zabezpieczenia w postępowaniu karnym*, „Prawo Karne i Kryminologia", Warszawa 2018, wydanie internetowe: https://iws.gov.pl/analizy-i-raporty/raporty/#prawokarne2018.
55. *System prawa karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, t. 8, red. L. Gardocki, Warszawa 2018.
56. *Ustawa o rachunkowości. Komentarz*, red. E. Walińska, Wolters Kluwer Polska 2023, LEX.
57. Więcław W., *Inwestycje krótkoterminowe – definicje, podstawowe pojęcia, komentarze praktyczne*, 2022 ABC, LEX.
58. Wojciechowski J., *Kodeks karny. Komentarz. Orzecznictwo*, Warszawa 2000.
59. Zieliński M., *Wykładnia prawa. Zasady – reguły – wskazówki*, Warszawa 2017.

Literatura - artykuły:

1. Błachnio A., *Res extra commercium jako przedmiot czynności wykonawczej przestępstwa przeciwko mieniu*, „Wojskowy Przegląd Prawniczy" 2017, nr 2.
2. Budziński J., *Luka prawna w zakresie karnoprawnych kwalifikacji dla zaboru przedmiotów wirtualnych w internetowych grach komputerowych*, „Probacja" 2020, nr 3.
3. Chmielarz P., *Bitcoin a podział majątku wspólnego*, „Homo Politicus" 2019, nr 4.
4. Czaplicki P., *Wybrane przestępstwa gospodarcze związane z obrotem walutą Bitcoin w prawie polskim, Unii Europejskiej oraz Stanów Zjednoczonych*, „Studenckie Zeszyty Naukowe" 2017, nr 20.
5. Czech T., *Wpis na rachunek płatniczy*, „Monitor Prawa Bankowego" 2019, nr 10, LEX.
6. Czesnowicka A., *Transakcja nieautoryzowana z perspektywy prawnokarnej – kwalifikacja prawna dokonania tzw. płatności zbliżeniowej za pomocą cudzej*

karty płatniczej, „Palestra" 2022, nr 7–8, wydanie internetowe: https://palestra.pl/pl/czasopismo/wydanie/7-8-2022.
7. Domagała M., *Prawnokarna ochrona prywatności użytkowników Internetu*, „Państwo i Prawo" 2010, nr 3.
8. Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie" 2009, nr 798.
9. Grykiel J., *Pojęcie działalności gospodarczej i zawodowej w rozumieniu art. 43(1) k.c.*, „Studia Prawnicze" 2005, nr 4.
10. Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1 (25), LEX.
11. Kmąk K., *Odstąpienie od rezultatów wykładni językowej w prawie karnym (na kanwie uchwały Sądu Najwyższego z dnia 26 marca 2009 r., sygn. I KZP 35/08)*, „Studenckie Zeszyty Naukowe" 2019, vol. XXII, nr 42.
12. Kmiecik R., *Osobliwości postmodernizmu a funkcja skargi „kontrkasatoryjnej" w procesie karnym (Rozdział 55a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 3.
13. Koszut R., *Kwestie sporne na tle wykładni przestępstwa hackingu*, „Nowa Kodyfikacja Prawa Karnego" 2001, nr 8.
14. Korczyński R., Koszut R., *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2022, nr 2.
15. Kotowski A., *Z problematyki metody interpretacji językowo-logicznej – uwagi na gruncie dekodowania znaczenia prawno-karnego*, „Prokuratura i Prawo" 2015, nr 6.
16. Kukuła Z., *Dokonanie płatności skradzioną kartą bankomatową. Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r., sygn. III KK 349/16,* „Przegląd Sądowy" 2018, nr 7–8.
17. Kunicka-Michalska B., *Oszustwo komputerowe. Regulacje prawa polskiego*, „Studia Prawnicze" 2006, nr 4.
18. Lach A., *Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r., III KK 349/16*, „Prokuratura i Prawo" 2018, nr 5.
19. Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3.
20. Liberacki J., *Karnoprawne aspekty walut kryptograficznych (bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2019, r. XXIII, nr 3.
21. Macior W., *Z problematyki zbiegu przestępstw i przepisów ustawy (w sprawie pozornego zbiegu realnego przestępstw)*, „Państwo i Prawo" 1965, nr 1.
22. Małecki M., Dudek P.M., *Uzyskanie cudzego bitcoina karane jak kradzież*, Karne-24com, 3 października 2018, https://karne24.com/uzyskanie-cudzego-bitcoina-karane-kradziez/.
23. Nowak P., *Wykładnia znamienia „włamanie" na gruncie art. 279 § 1 Kodeksu karnego*, „Palestra" 2013, nr 7–8, wydanie internetowe: https://palestra.pl/pl/czasopismo.
24. Opitek P., *Kontrola operacyjna urządzenia końcowego*, „Prokuratura i Prawo" 2023, nr 4.

25. Opitek P., *Kryptowaluta jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6.
26. Opitek P., *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2.
27. Opitek P., *Kwalifikacja prawna i opis czynów zabronionych dotyczących przestępczości teleinformatycznej (zagadnienia wybrane)*, „Consilium Iuridicum. Kwartalnik Naukowy Krajowej Rady Sądownictwa" 2022, nr 1–2.
28. Opitek P., *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017, nr 2.
29. Opitek P., *Międzynarodowa przestępczość narkotykowa w ujęciu kryminalistycznym i kryminologicznym*, „Kwartalnik Prawa Międzynarodowego" 2023, nr 2.
30. Opitek P., *Odpowiedzialność karna za kradzież karty płatniczej*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2017, nr 4.
31. Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12.
32. Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2020, nr 9.
33. Opitek P., *Sprawozdanie z konferencji naukowej pt. Kryptowaluty w cyberprzestępczości. Międzynarodowa wymiana doświadczeń*, „Wojskowy Przegląd Prawniczy" 2019, nr 10–12.
34. Opitek P., *Wdrożenie kontroli operacyjnej na terytorium innego państwa członkowskiego Unii Europejskiej w ramach europejskiego nakazu dochodzeniowego*, „Kwartalnik Prawa Międzynarodowego" 2022, nr 1.
35. Opitek P., *Wpływ standardu EMV na nielegalne działania z wykorzystaniem kart płatniczych w kontekście przestępstwa skimmingu*, „Bezpieczny Bank" 2016, nr 1.
36. Opitek P., Góral K., *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, „Prokuratura i Prawo" 2020, nr 5–6.
37. Opitek P., Lenczowska-Soboń K., Ocieczek G., *Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w świecie „realnym" i cyberprzestrzeni*, materiał szkoleniowy, „Prokuratura i Prawo" 2022, nr 7–8.
38. Opitek P., Ocieczek G., *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum. Kwartalnik Naukowy Krajowej Rady Sądownictwa" 2022, nr 3–4.
39. Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13.
40. Ryfa J., *Waluty wirtualne – problem zdefiniowania i klasyfikacji nowego środka płatniczego*, „Nauka o Finansach" 2014, nr 2.
41. Siemkowicz P., *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym – z uwzględnieniem aktualnych zmian nowelizacyjnych*, CBKE e-Biuletyn, http://www.bibliotekacyfrowa.pl/Content/34363/PDF/Przestepstwa_skierowane.pdf.

42. Skała J., *Uzyskiwanie przez prokuratora – na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – informacji i danych od instytucji obowiązanych*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2020, nr 3.
43. Sobieszewska M., *Juryslingwistyka: między językiem i prawem*, „Studia Iuridica Lublinensia" 2015, nr 4.
44. Sosik R., *Wykorzystanie skradzionej karty płatniczej do wykonania płatności zbliżeniowych. Glosa do wyroku Sądu Najwyższego z 22.03.2017 r., III K 349/16*, „Prokuratura i Prawo" 2017, nr 2.
45. Stolarski K., *Prawny i podatkowy status walut wirtualnych w kontekście wprowadzenia do prawa polskiego definicji legalnej waluty wirtualne*, „Monitor Podatkowy" 2018, nr 9.
46. Szajna P., *Transakcja zbliżeniowa zrealizowana cudzą kartą płatniczą do kwoty niewymagającej autoryzacji kodem PIN – kradzież (art. 278 § 1 k.k., art. 119 § 1 k.w.) czy kradzież z włamaniem (art. 279 § 1 k.k.)?*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1.
47. Tarapata S., *Wybrane prawnokarne zagadnienia związane z dokonywaniem płatności zbliżeniowej za pomocą cudzej karty płatniczej bez zgody osoby uprawnionej – uwagi na marginesie wyroku Sądu Najwyższego z 22.3.2017, sygn. III KK 349/16*, „Kwartalnik Prawa Publicznego" 2017, nr 4, LEX.
48. Tyburcy T., *Treść i zakres znamienia „włamanie" (art. 279 § 1 k.k.) – czy kradzież z włamaniem może nastąpić tylko z pomieszczenia zamkniętego?*, „Acta Iuris Stetinensis" 2019, nr 25.
49. Tyburcy T., *Mienie jako przedmiot ochrony w prawie karnym (na wybranych przykładach)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2018, r. XXII, nr 3.
50. Wąsek A., *Glosa do wyroku Sądu Najwyższego z dnia 11 września 2002 r.*, V KKN 9/01, OSP 2003, nr 7–8, poz. 103.
51. Wiatrowski P., *Dyrektywy interpretacyjne systemowej wykładni przepisów prawa karnego materialnego w orzecznictwie Sądu Najwyższego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2009, r. XIII, nr 2.
52. Winkiel O., *„Kradzież" dóbr wirtualnych w grach sieciowych – wprowadzenie do zagadnienia*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, nr 2, LEX.
53. Zacharzewski A., *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21.
54. Zachuta A., *Opis i kwalifikacja prawna czynu z uwzględnieniem sprawczych odmian przestępnego współdziałania*, „Prokuratura i Prawo" 2005, nr 1.
55. Zielinko I., *Bezpośredniość jako element definicji pokrzywdzonego w procesie karnym*, „Przegląd Sądowy" 2014, nr 3.

Orzeczenia trybunałów:

1. Wyrok Trybunału Sprawiedliwości UE z dnia 22 października 2015 r., C-264/14, Skatteverket przeciwko Davidowi Hedqvistowi, https://eur-lex.europa.eu/legal-content/pl/ALL/?uri=CELEX:62014CJ0264.

2. Wyrok Trybunału Sprawiedliwości UE z dnia 22 października 2015 r., C-264/14 przeciwko D. H., opublikowano ZOTSiS 2015/10/I-718.
3. Uchwała Trybunału Konstytucyjnego z dnia 29 stycznia 1992 r., W 14/91, OTK 1992, poz. 20.
4. Wyrok Trybunału Konstytucyjnego z dnia 21 marca 2001 r., K 24/00, OTK 2001, nr 3, poz. 51.
5. Wyrok Trybunału Konstytucyjnego z dnia 11 stycznia 2000 r., K. 7/99, OTK ZU 2000, nr 1, poz. 2.

Orzeczenia Sądu Najwyższego i sądów powszechnych:

1. Uchwała pełnego składu Izby Karnej Sądu Najwyższego z dnia 11 stycznia 1999 r., I KZP 15/98, OSNKW 1999, nr 1–2.
2. Uchwała Sądu Najwyższego z dnia 26 marca 2009 r., I KZP 35/08, OSNKW 2009, nr 5 poz. 33.
3. Uchwała Sądu Najwyższego z dnia 23 lutego 2005 r., III CZP 88/04, OSNC 2006, nr 1, poz. 5.
4. Uchwała Sądu Najwyższego z dnia 29 października 2004 r., I KZP 24/04, LEX nr 125547.
5. Uchwała Sądu Najwyższego z dnia 21 listopada 2001 r., I KZP 26/01, OSNKW 2000, 1–2, poz. 4.
6. Uchwała Sądu Najwyższego z dnia 20 czerwca 2000 r., I KZP 16/00, OSNKW 2000, nr 7–8, poz. 60.
7. Uchwała Sądu Najwyższego z dnia 6 grudnia 1991 r., III CZP 117/91, OSNC 1992, Nr 5, poz. 65.
8. Wyrok Sądu Najwyższego z dnia 10 lutego 2022 r., V KK 543/21, LEX nr 3348356.
9. Wyrok Sądu Najwyższego z dnia 22 marca 2017 r., akt III KK 349/16 OSNKW 2017, nr 9, poz. 50.
10. Wyrok Sądu Najwyższego z dnia 27 stycznia 2017 r., V KK 347/16, LEX nr 2269116.
11. Wyrok Sądu Najwyższego z dnia 27 października 2016 r., V CSK 48/16.
12. Wyrok Sądu Najwyższego z dnia 30 września 2015 r., II KK 115/15, LEX nr 1866883.
13. Wyrok Sądu Najwyższego z dnia 22 marca 2012 r., IV KK 375/11, OSNKW 2012, nr 7, poz. 78.
14. Postanowienie Sądu Najwyższego z dnia 27 listopada 2019 r., sygn. VKK 505/2018, LEX nr 2966120.
15. Wyrok Sądu Najwyższego z dnia 4 października 2017 r., II KK 162/17, LEX nr 2397594.
16. Postanowienie Sądu Najwyższego z dnia 22 grudnia 2021 r., V KK 396/21, LEX nr 3527395.
17. Wyrok Sądu Najwyższego z dnia 4 października 2007 r., V CSK 255/07, OSNC-ZD 2008, nr 3, poz. 79.
18. Wyrok Sądu Najwyższego z dnia 19 października 2006 r., V KK 221/06, LEX nr 198105.
19. Wyrok Sądu Najwyższego z dnia 18 lutego 2004 r., V CK 233/03, LEX nr 550934.

20. Wyrok Sądu Najwyższego z dnia 2 czerwca 2003 r., II KK 232/02, LEX nr 78373.
21. Postanowienie Sądu Najwyższego z dnia 1 lipca 2021 r., III USK 223/21, LEX nr 3380183.
22. Postanowienie Sądu Najwyższego z dnia 18 maja 2021 r., III KK 102/21, LEX nr 3177284
23. Postanowienie Sądu Najwyższego z dnia 2 grudnia 2020 r., III KK 358/20, LEX nr 3183271.
24. Postanowienie Sądu Najwyższego z dnia 5 marca 2019 r., II KK 208/18, LEX nr 2639897.
25. Postanowienie Sądu Najwyższego z dnia 28 kwietnia 2016 r., I KZP 3/16, OSNKW 2016, nr 6, poz. 37.
26. Postanowienie Sądu Najwyższego z dnia 30 września 2015 r., I KZP 6/15, OSNKW 2015, nr 12, poz. 99.
27. Postanowienie Sądu Najwyższego z dnia 29 września 2009 r., OSNwSK 2009, nr 1, poz. 1903. WK 15/09.
28. Wyrok Sądu Apelacyjnego w Warszawie z dnia 25 lutego 2021 r., II AKa 72/20, LEX nr 3189608.
29. Wyrok Sądu Apelacyjnego w Lublinie z dnia 20 grudnia 2019 r., II AKa 235/19, LEX nr 3077417.
30. Wyrok Sądu Apelacyjnego w Katowicach z dnia 4 lipca 2019 r., II AKa 70/19, LEX nr 2747930.
31. Wyrok Sądu Apelacyjnego w Krakowie z dnia 8 stycznia 2019 r., II AKa 194/17, LEX nr 2707539.
32. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 27 listopada 2018 r., II AKa 307/18, KSAG 2019/1/197.
33. Wyrok Sądu Apelacyjnego w Warszawie z dnia 29 października 2018 r., II AKa 400/18, LEX nr 2593608.
34. Wyrok Sądu Apelacyjnego w Katowicach z dnia 5 kwietnia 2018 r., II AKa 273/17, LEX nr 2490242.
35. Wyrok Sądu Apelacyjnego w Lublinie z dnia 14 marca 2018 r., II AKa 40/18, LEX nr 2469980.
36. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 28 września 2017 r., II AKa 192/16, LEX nr 2391897.
37. Wyrok Sądu Apelacyjnego w Katowicach z dnia 29 czerwca 2017 r., II AKa 151/17, LEX nr 2440808.
38. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 26 kwietnia 2017 r., II AKa 191/16, LEX nr 2295144.
39. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 28 września 2016 r., II AKa 111/16, LEX nr 2191573.
40. Wyrok Sądu Apelacyjnego w Warszawie z dnia 21 grudnia 2015 r., II AKa 409/15, LEX nr 2031083.
41. Wyrok Sądu Apelacyjnego w Warszawie z dnia 21 grudnia 2015 r., akt II AKa 409/15, LEX nr 2031083

42. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 28 października 2015 r., II AKa 138/15, LEX nr 2191591.
43. Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 września 2014 r., II AKa 242/14, LEX nr 1527320.
44. Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 9 lipca 2014 r., II AKa 180/14, LEX nr 1506771.
45. Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 stycznia 2014 r., II AKa 397/13, LEX nr 1428051.
46. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.
47. Wyrok Sądu Okręgowego w Olsztynie z dnia 25 kwietnia 2022 r., I C 536/21, LEX nr 3357331.
48. Wyrok Sądu Okręgowego w Siedlcach z dnia 30 listopada 2021 r., II Ka 561/21, LEX nr 3290107.
49. Wyrok Sądu Okręgowego w Białymstoku z dnia 28 maja 2021 r., III K 7/21, LEX nr 3354429.
50. Wyrok Sądu Okręgowego w Ostrołęce z dnia 27 sierpnia 2020 r., II Ka 40/20.
51. Wyrok Sądu Okręgowego w Świdnicy z dnia 10 kwietnia 2019 r., IV Ka 112/19, LEX nr 2728262.
52. Wyrok Sądu Okręgowego w Radomiu z dnia 8 marca 2019 roku, II K 82/18, LEX nr 3077417.
53. Wyrok Sądu Okręgowego w Piotrkowie Trybunalskim z dnia 21 lutego 2019 r., III K 73/18, LEX nr 2635086.
54. Wyrok Sądu Okręgowego w Łodzi z dnia 27 marca 2018 r., III Ca 51/18, LEX nr 2538475.
55. Wyrok Sądu Okręgowego w Świdnicy z dnia 9 stycznia 2018 r., IV Ka 720/17, LEX nr 2474562.
56. Wyrok Sądu Okręgowego w Gliwicach z dnia 11 lipca 2017 r., VI Ka 461/17, LEX nr 2351893.
57. Wyrok Sądu Okręgowego w Lublinie z dnia 28 czerwca 2017 r., IV K 65/13, LEX nr 2385636.
58. Wyrok Sądu Okręgowego Warszawa-Praga w Warszawie z dnia 21 marca 2017 r., VI Ka 1343/16, LEX nr 2278402.
59. Wyrok Sądu Okręgowego w Poznaniu z dnia 7 marca 2017 r., IV Ka 111/17, LEX nr 2280584.
60. Wyrok Sądu Okręgowego w Warszawie z dnia 29 grudnia 2016 r., XVIII K 5/16, LEX nr 2188993.
61. Wyrok Sądu Okręgowego w Gliwicach z dnia 29 grudnia 2016 r., V Ka 135/16, LEX nr 2206759.
62. Wyrok Sądu Okręgowego w Siedlcach z dnia 11 lipca 2016 r., II Ka 329/16, LEX nr 2074573.
63. Wyrok Sądu Okręgowego w Bielsku-Białej z dnia 8 czerwca 2016 r., I C 534/15, LEX nr 2302379.

64. Wyrok Sądu Okręgowego w Bydgoszczy z dnia 13 maja 2015 r., IV Ka 141/15, LEX nr 1829043.
65. Wyrok Sądu Okręgowego w Olsztynie z dnia 28 kwietnia 2015 r., II K 181/14, LEX nr 1835835.
66. Wyrok Sądu Okręgowego w Gliwicach z dnia 17 kwietnia 2015 r., VI Ka 51/15, LEX nr 1831810.
67. Wyrok Sądu Okręgowego we Wrocławiu z dnia 20 lutego 2015 r., III K 137/11, LEX nr 1841717.
68. Wyrok Sądu Okręgowego w Elblągu z dnia 12 lutego 2015 r. o VI Ka 11/15, LEX nr 1830133.
69. Wyrok Sądu Okręgowego w Olsztynie z dnia 4 lutego 2015 r., VII Ka 1181/14, LEX nr 1835967.
70. Wyrok Sądu Okręgowego we Wrocławiu z dnia 23 września 2014 r., IV Ka 1222/13, LEX nr 1882442.
71. Wyrok Sądu Okręgowego w Nowym Sączu z dnia 17 czerwca 2014 r., II Ka 188/14, LEX nr 1859693.
72. Wyrok Sądu Okręgowego we Wrocławiu z dnia 5 lutego 2014 r., IV Ka 1233/13, LEX nr 1882446.
73. Wyrok Wojskowego Sądu Okręgowego w Poznaniu z dnia 6 listopada 2008 r., So 30/07.
74. Wyrok Sądu Rejonowego w Łukowie z dnia 5 maja 2022 r., II K 793/20, LEX nr 3369999.
75. Wyrok Sądu Rejonowego w Toruniu z dnia 19 kwietnia 2022 r., II K 1517/21, LEX nr 3355925.
76. Wyrok Sądu Rejonowego w Kaliszu z dnia 15 marca 2022 r., II K 882/19, LEX nr 3500689.
77. Wyrok Sądu Rejonowego w Mikołowie z dnia 30 marca 2021 r., II K 1/21, LEX nr 3232310.
78. Wyrok Sądu Rejonowego w Jeleniej Górze z dnia 28 września 2020 r., II K 739/20, LEX nr 3102107.
79. Wyrok Sądu Rejonowego w Toruniu z dnia 26 sierpnia 2020 r., II K 777/20, LEX nr 3060595.
80. Wyrok Sądu Rejonowego w Legionowie z dnia 7 lutego 2020 r., II K 1247/18, LEX nr 3069347.
81. Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 30 lipca 2019 r., X K 146/19, LEX nr 2785597.
82. Wyrok Sądu Rejonowego w Kielcach z dnia 27 maja 2019 r., IX K 1680/18, LEX nr 2764110.
83. Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 11 października 2018 r., X K 499/18, LEX nr 2622492.
84. Wyrok Sądu Rejonowego w Golubiu-Dobrzyniu z dnia 7 maja 2018 r., II K 372/17, LEX nr 2609309.

85. Wyrok Sąd Rejonowy w Goleniowie z dnia 27 lutego 2018 r., II K 424/17, LEX nr 2730262.
86. Wyrok Sądu Rejonowego Gdańsk-Południe w Gdańsku z dnia 14 grudnia 2017 r., X K 806/16, LEX nr 2785661.
87. Wyrok Sądu Rejonowego Poznań-Nowe Miasto i Wilda w Poznaniu z dnia 8 grudnia 2017 r., VI K 358/17, LEX nr 2415381.
88. Wyrok Sądu Rejonowego w Wałbrzychu z dnia 11 października 2017 r., II K 1036/16, LEX nr 2421166.
89. Wyrok Sądu Rejonowego w Lesku z dnia 31 sierpnia 2017 r., VI K 46/17, LEX nr 2445511.
90. Wyroku Sądu Rejonowego w Kłodzku z dnia 21 sierpnia 2017 r., VI K 527/16, LEX nr 2474562.
91. Wyrok Sądu Rejonowego dla Łodzi-Śródmieścia w Łodzi z dnia 24 lipca 2017 r., XVIII C 4854/16, LEX nr 2538475.
92. Wyrok Sądu Rejonowego w Legionowie z dnia 7 czerwca 2017 r., II K 406/16, LEX nr 2340308.
93. Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 26 kwietnia 2017 r., XIV K 1204/12, LEX nr 2392142.
94. Wyrok Sądu Rejonowego w Rudzie Śląskiej Wydział II Karny z dnia 5 kwietnia 2017 r., II K 580/17.
95. Wyrok Sądu Rejonowego w Radomsku z dnia 17 listopada 2016 r., VI K 288/16, LEX nr 2342576.
96. Wyrok Sądu Rejonowego w Wałbrzychu z dnia 23 września 2016 r., III K 865/15, LEX nr 2146034.
97. Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 6 czerwca 2016 r., VIII K 654/11, LEX nr 2096681.
98. Wyrok Sądu Rejonowego dla Warszawy Pragi-Północ z dnia 17 maja 2016 r., III K 1013/13.
99. Wyrok Sąd Rejonowy w Lipnie z dnia 15 lutego 2016 r., II K 313/14, LEX nr 2243448.
100. Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 29 stycznia 2016 r., VIII K 232/15, LEX nr 2148091.
101. Wyrok Sądu Rejonowego w Jaworznie z dnia 7 grudnia 2015 r., II K 621/14, LEX nr 2155219.
102. Wyrok Sądu Rejonowego w Wałbrzychu z dnia 6 października 2015 r., III K 242/15, LEX nr 1931358.
103. Wyrok Sądu Rejonowego w Giżycku z dnia 3 sierpnia 2015 r., II K 84/14, LEX nr 2070430.
104. Wyrok Sądu Rejonowego w Jeleniej Górze z dnia 21 kwietnia 2015 r., II K 1177/14, LEX nr 1862061.
105. Wyrok Sądu Rejonowego w Bydgoszczy z dnia 1 grudnia 2014 r., IX K 126/14, LEX nr 1829043.
106. Wyrok Sądu Rejonowego w Iławie z dnia 30 września 2014 r., II K 59/14, LEX nr 1830133.

107. Wyrok Sądu Rejonowego w Nowym Sączu z dnia 28 stycznia 2014 r., II K 322/13, LEX nr 1859693.
108. Wyrok Sądu Rejonowego dla Wrocławia-Fabrycznej z dnia 29 sierpnia 2013 r., II K 1227/10, LEX nr 1882442.
109. Wyrok Sądu Rejonowego dla Wrocławia-Śródmieścia we Wrocławiu z dnia 14 sierpnia 2013 r., II K 87/12, LEX nr 1903395.
110. Postanowienie Sądu Rejonowego w Dzierżoniowie z dnia 27 czerwca 2016 r., II Kp 171/16, LEX nr 2080684.
111. Postanowienie Sądu Rejonowego w Siedlcach z dnia 23 września 2015 r., VII Kp 203/15, LEX nr 1922632.
112. Postanowienie Sądu Rejonowego w Dzierżoniowie z dnia 16 kwietnia 2014 r., II Kp 44/14, LEX nr 1906875.

Orzeczenia sądów administracyjnych:

1. Wyrok Naczelnego Sądu Administracyjnego z dnia 11 marca 2021 r., II FSK 3296/18, LEX nr 3229870.
2. Wyrok Naczelnego Sądu Administracyjnego z dnia 10 lutego 2021 r., II FSK 2870/18, LEX nr 3212191.
3. Wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z dnia 8 kwietnia 2021 r., I SA/Po 229/21, LEX nr 3172268.
4. Wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z dnia 28 kwietnia 2020 r., I SA/Gd 275/20, Legalis, nr 2393242
5. Wyrok Naczelnego Sądu Administracyjnego z dnia 11 marca 2021 r., II FSK 3296/18, LEX nr 3229870.
6. Wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 16 października 2018 r., III SA/Łd 537/18, LEX nr 2582970.

Akta zbadanych przez autora spraw sądowych:

1. Akta Sądu Okręgowego w Krakowie o sygn. III K 27/19.
2. Akta Sądu Okręgowego w Krakowie o sygn. III K 193/17.
3. Akta Sądu Okręgowego w Krakowie o sygn. III K 106/17.
4. Akta Sądu Okręgowego w Krakowie o sygn. IV Ka 1131/16.
5. Akta Sądu Okręgowego w Krakowie o sygn. III K 272/13.
6. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie, sygn. II K 130/22/P.
7. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 289/19/P.
8. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1369/19/P.
9. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1534/19/P.
10. Akta Sądu Rejonowego w Przasnyszu o sygn. II K 608/18.
11. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 418/18/P.
12. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 503/17/N.

13. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 1629/17/N.
14. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 1666/17/N.
15. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 724/17/N.
16. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 228/17/N.
17. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 822/16/K.
18. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 875/16/P.
19. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 469/16/P.
20. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 104/15/N.
21. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 559/15/P.
22. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 45/15/N.
23. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 723/15/K.
24. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 28/15/K.
25. Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 1706/15/S.
26. Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 628/15/S.
27. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 32/14/K.
28. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 679/14/N.
29. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1085/13/P.
30. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 911/13/N.
31. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. II K 1168/13/P.
32. Akta Sądu Rejonowego dla Krakowa-Podgórza w Krakowie o sygn. XI K 971/13/P.
33. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 406/12/N.
34. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II K 549/12/K.
35. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. II K 641/12/N.
36. Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 578/11/S.
37. Akta Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie o sygn. II Ka 776/11/K.
38. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 992/11/N.
39. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 787/10/N.
40. Akta Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie o sygn. VIII K 1094/10/N.
41. Akta Sądu Rejonowego dla Krakowa-Śródmieścia w Krakowie o sygn. II K 44/10/S.

Akta zbadanych przez autora spraw postępowania przygotowawczego:

1. Akta Prokuratury Regionalnej w Katowicach o sygn. PR I Ds. 16.2018.
2. Akta Prokuratury Regionalnej w Gdańsku o sygn. RP II Ds. 22.2017.
3. Akta Prokuratury Okręgowej w Gliwicach o sygn. PO I Ds. 26.2021.
4. Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO IV Ds. 19.2018.D.
5. Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO I Ds. 3.2018
6. Akta Prokuratury Okręgowej w Krośnie o sygn. PO I Ds. 3.2018.
7. Akta Prokuratury Okręgowej w Tarnobrzegu o sygn. PO IV Ds. 38.2017.D.
8. Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.
9. Akta Prokuratury Okręgowej w Jeleniej Górze o sygn. PO IV Ds. 37.2017.
10. Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.
11. Akta Prokuratury Okręgowej w Warszawie o sygn. PO II Ds 129.2017.
12. Akta Prokuratury Okręgowej w Olsztynie o sygn. PO II Ds. 18.2017.
13. Akta Prokuratury Okręgowej w Zielonej Górze o sygn. PO I Ds. 43.2016.
14. Akta Prokuratury Okręgowej w Katowicach o sygn. V Ds. 103/15.
15. Akta Prokuratury Rejonowej Kielce-Wschód w Kielcach o sygn. 4 Ds. 297.2021.
16. Akta Prokuratury Rejonowej Warszawa-Wola o sygn. PR 4 Ds. 1848.2019.
17. Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 1 Ds. 340.2019.
18. Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 2 Ds. 1843.2019.
19. Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 2 Ds. 1322.2019.
20. Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 818.2019.
21. Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 818.2019.
22. Akta Prokuratury Rejonowej Warszawa-Wola w Warszawie o sygn. PR 4 Ds. 1848.2019.
23. Akta Prokuratury Rejonowej Katowice-Północ w Katowicach o sygn. PR 1 Ds. 67.2019.
24. Akta Prokuratury Rejonowej dla Wrocławia-Stare Miasto we Wrocławiu o sygn. PR 1 Ds. 2354.2018.
25. Akta Prokuratury Rejonowej Gliwice-Zachód w Gliwicach o sygn. PR Ds. 339.2018.
26. Akta Prokuratury Rejonowej Gliwice-Zachód w Gliwicach o sygn. PR Ds. 579.2018
27. Akta Prokuratury Rejonowej w Tarnobrzegu o sygn. PR 1 Ds. 610.2018.D.
28. Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 2 Ds. 1614.2018.
29. Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 5 Ds. 297.2018.
30. Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 1 Ds. 460.2018.
31. Akta Prokuratury Rejonowej Warszawa-Śródmieście w Warszawie o sygn. PR 3 Ds. 106.2018.II.

32. Akta Prokuratury Rejonowej Katowice-Południe w Katowicach o sygn. PR 3 Ds. 778.2018.
33. Akta Prokuratury Rejonowej Warszawa-Śródmieście Północ w Warszawie o sygn. PR 4 Ds. 396.2018.
34. Akta Prokuratury Rejonowej Warszawa-Śródmieście Północ w Warszawie o sygn. PR 4 Ds. 1544.2018.
35. Akta Prokuratury Rejonowej w Staszowie o sygn. PR Ds. 256.2018
36. Akta Prokuratury Rejonowej w Lidzbarku Warmińskim o sygn. PR 2 Ds. 15.2018.
37. Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 3 Ds. 171.2018.
38. Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 1 Ds. 1448.2017.
39. Akta Prokuratury Rejonowej w Rybniku o sygn. PR 1 Ds. 1825.2017.
40. Akta Prokuratury Rejonowej Warszawa-Mokotów w Warszawie o sygn. PR 5 Ds. 412.2017.
41. Akta Prokuratury Rejonowej dla Wrocławia-Krzyki Wschód we Wrocławiu o sygn. PR 1 Ds. 1511.2017.
42. Akta Prokuratury Rejonowej w Olsztyn-Południe w Olsztywnie o sygn. PR 2 Ds. 242.2016.
43. Akta Prokuratury Rejonowej w Chorzowie o sygn. PR 2 Ds. 424.2016.
44. Akta Prokuratury Rejonowej Kraków-Podgórze w Krakowie o sygn. 2 Ds. 180/13.
45. Akta Prokuratury Rejonowej dla Krakowa-Podgórza w Krakowie o sygn. 2 Ds. 1880/12/D.
46. Akta Świętokrzyskiego Urzędu Celno-Skarbowego o sygn. RKS 228/2019/348000.
47. Akta Świętokrzyskiego Urzędu Celno-Skarbowego o sygn. RKS 5/2019/348000/DB.

Pisma instruktażowe:

1. Pismo Zastępcy Dyrektora Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z czerwca 2023 r. dotyczące zabezpieczenia majątkowego na kryptowalutach, znak: 1001 – 12.024.4.2023 (zbiory własne autora).
2. Zalecenia Prokuratora Krajowego z dnia 15 września 2022 r. w sprawie zasad prowadzenia postępowań przygotowawczych o przestępstwa prowadzone w drodze oszukańczych sprzedaży przedmiotów i usług, w szczególności w drodze sprzedaży bezpośredniej połączonej z ich prezentacją, sygn. 1001 – 1.024.18.2022 (zbiory własne autora).
3. Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 17 stycznia 2022 r. dotyczące przestępstw związanych z fałszywymi panelami płatności i stronami podszywającymi się pod strony bankowości elektronicznej, sygn. 1001 – 7.024.1.2022 (zbiory własne autora).
4. Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 10 stycznia 2022 r. dotyczące przestępstw spoofingu, sygn. 1001 – 7.024.1.2022 (zbiory własne autora).

5. Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 6 grudnia 2021 r. dotyczące ataków ransomware, sygn. 1001 – 7.024.5.2021 (zbiory własne autora).
6. Pismo Zastępcy Dyrektora Departamentu do Spraw Przestępczości Gospodarczej w Prokuraturze Krajowej z dnia 19 października 2021 r. w sprawie funkcjonowania platform inwestycyjnych na rynku Forex, znak: 1001 – 7.024.4.2021 (zbiory własne autora).
7. Zalecenia Dyrektora Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 10 sierpnia 2021 r. w sprawie ataków DDoS, znak: 1001 – 7.025.1.2021 (zbiory własne autora).
8. Pismo Dyrektora Biura Prezydialnego Prokuratury Krajowej z dnia 4 grudnia 2019 r. w sprawie sposobu wprowadzania do materiałów sprawy dowodów rzeczowych, znak pisma: PK I BP 029.45.2018 (zbiory własne autora).
9. Pismo instruktażowe Departamentu Nadzory nad Kontrolami w Ministerstwie Finansów z dnia 7 marca 2019 r. w sprawie „skinów" (zbiory własne autora).
10. Pismo Ministerstwa Finansów z dnia 28 maja 2015 r. prezentuje wyjaśnienia Ministerstwa Finansów w przedmiocie funkcjonowania walut wirtualnych, sygn. FN7.054.9.2015, Regulacje dotyczące wirtualnej waluty Bitcoin, LEX.

Inne materiały:

1. Chinowski B., *Elektroniczne metody płatności. Istota, rozwój, prognoza*, publikacja Komisji Nadzoru Finansowego, Warszawa 2019, https://www.knf.gov.pl/knf/pl/komponenty/.
2. Jarmakiewicz J., *Sieci teleinformatyczne*, http://mml.pl/TT/wp-content/uploads/2016/05/Skrypt-TELEINFORMATYKA-2002.pdf, s. 3–4.
3. Jaroszewski D., *Kolekcjoner zapłacił prawie 3 mln zł za dwa skiny do CS:GO*, portal Telepolis, https://www.telepolis.pl/rozrywka/gry/csgo-rekordowa-transakcja-skiny.
4. Przewłoka E., *Algorytm podstawowych czynności realizowanych przez funkcjonariuszy Policji związanych z oszustwami inwestycyjnymi z wykorzystaniem walut wirtualnych*, Wydział do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Bydgoszczy, Bydgoszcz 2023 (zbiory własne autora).
5. Przewłoka E., *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Wydział do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Bydgoszczy, Bydgoszcz 2023 (zbiory własne autora).
6. Kiełbus R., programista i advisor, w blockchainowych projektach; programista smartkontraktów, członek Zarządu Izby Gospodarczej Blockchain i Nowych Technologii, Arbiter Sądu Polubownego przy Izbie, informacja otrzymana w wiadomości mailowej w 23.07.2023 r. (zbiory własne autora).
7. Informacja otrzymana w wiadomości mailowej 30.07.2023 r., zbiory własne autora.
8. Kiełbus R., programista i advisor, w blockchainowych projektach; programista smartkontraktów, członek Zarządu Izby Gospodarczej Blockchain i Nowych

Technologii, Arbiter Sądu Polubownego przy Izbie, informacja otrzymana w wiadomości mailowej w 25.07.2022 r. (zbiory własne autora).
9. Mazur M., *Penalizacja prania pieniędzy*, Warszawa 2014, https://bip.brpo.gov.pl/sites/default/files/Penalizacja_prania_pieniedzy.pdf.
10. Opitek P., *Kodeksowe prawo materialne oraz procesowe*, [w:] *Przegląd polskiego prawa w kontekście zastosowania technologii rozproszonych rejestrów oraz walut cyfrowych*, 19 stycznia 2017 r., przygotowany przez Zespół Prawo i Regulacje „Strumienia Blockchain i kryptowaluty" przy Ministerstwie Cyfryzacji, red. K. Piech, www.mc.gov.pl.
11. Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Uniwersytet w Białymstoku Wydział Prawa, praca doktorska napisana w Katedrze Prawa Karnego pod kierunkiem dr hab. Ewy M. Guzik-Makaruk, prof. UwB, Białystok 2017 (zbiory własne autora).
12. *Guidelines for Digital Forensics First Responders – Best practices for search and seizure of electronic and digital evidence*, INTERPOL, marzec 2021, tłumaczenie na język polski: *Poradnik Cyber Ratownika, IV Konferencja Naukowa Przestępczość Teleinformatyczna XXI wieku*, Gdynia 2022 (zbiory własne autora).
13. Virtual Assets and Virtual Asset Service Providers. Updated guidance for a risk-based approach, October 2021 (zbiory własne autora).
14. Dane z systemu elektronicznego prokuratury PROK-SYS.
15. Plan działań UE w zakresie narkotyków na lata 2021–2025, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021XG0708(01).

Materiały legislacyjne:

1. Uzasadnienie do projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, wdrażającej dyrektywę Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.04.2014, str. 39), LEX.
2. Uzasadnienie projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, wersja: ustawa po rozpatrzeniu stanowiska Senatu, Sejm przyjął poprawki Senatu, LEX.
3. Uzasadnienie projektu ustawy wprowadzającej karalność za przest. z art. 267 § 2 k.k., druk sejmowy nr 458 Sejmu VI kadencji, LEX.
4. Uzasadnienie projektu ustawy. VIII. 795, Zmiana ustawy o grach hazardowych oraz niektórych innych ustaw. Wersja: Ustawa po rozpatrzeniu stanowiska Senatu, Senat nie wniósł poprawek, LEX.
5. Druk nr 2031. Rządowy projekt ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń, https://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/2031.

Źródła internetowe

1. Co to jest bezpieczeństwo logowania?, https://www.microsoft.com/pl-pl/security/business/security-101/what-is-login-security
2. Słownik Języka Polskiego PWN, https://sjp.pwn.pl/slowniki/
3. https://synonim.net/synonim/kod
4. https://allegrolokalnie.pl/oferta/ak47-wtrysk-paliwa-aln
5. https://www.istockphoto.com/pl.
6. Słownik Języka Polskiego PWN, https://sjp.pwn.pl/slowniki/
7. Słownik Języka Polskiego PWN, https://sjp.pwn.pl/slowniki/
8. http://www.sn.pl/sites/orzecznictwo
9. https://thenewlook.pl/bramki-platnosci-online/
10. https://szybkieprzelewy.online/bramka-platnosci-ktora-wybrac-w-2023-roku/
11. https://www.esma.europa.eu/sites/default/files/library/2015/11/investor_warning_-_cfds_-_esma_2013_00070000_pl_cor.pdf
12. https://mfiles.pl/pl/index.php/Opcje_binarne
13. https://bitnodes.io/
14. Handel elektroniczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1778,pojecie.html
15. https://www.coinlore.com/pl/all_coins
16. https://www.dobreprogramy.pl/
17. https://encyklopedia.pwn.pl/haslo/system-informatyczny;3982203.html
18. Stanowisko Urząd Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf, s. 5
19. https://sjp.pwn.pl/slowniki/akceptowa%C4%87.html
20. https://counterstrike.fandom.com/wiki/Skins
21. https://dailyweb.pl/wielki-slownik-inwestora-bitcoin-wszystkie-pojecia-w-jednym-miejscu/
22. https://sjp.pl/bitcoin
23. https://sjp.pwn.pl/szukaj/dane.html
24. www.encyklopedia.pwn.pl
25. https://gameforge.com/pl-PL/sign-in, https://www.anyrgb.com/en-clipart-2xvqr
26. https://sjp.pwn.pl/szukaj/warto%C5%9B%C4%87.html
27. https://sjp.pwn.pl/szukaj/istotny.html

Źródła grafik:

1. https://stock.adobe.com/pl/images/binary-numbers-texture/187479145
   https://stock.adobe.com/pl/images/white-flower-isolated-on-white/627655801?asset_id=627655801
2. https://stock.adobe.com/pl/images/binary-numbers-texture/187479145
3. https://www.gov.pl/web/prokuratura-krajowa
4. https://www.gov.pl/web/prokuratura-krajowa
5. https://www.gov.pl/web/prokuratura-krajowa

6. https://www.istockphoto.com/pl
7. P. Opitek, *Skimming-aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Monografie Prawnicze C.H. Beck 2017.
8. Grafika własna autora.
9. Grafika własna autora.
10. Materiał własny autora.
11. Grafika własna autora.
12. Materiał własny autora.
13. Demo własne autora zastosowania root@kali (zrzut ekranu).
14. https://szybkieprzelewy.online/bramka-platnosci-ktora-wybrac-w-2023-roku/
15. Demo własne autora zastosowania root@kali (zrzut ekranu).
16. Grafika własna autora.
17. P. Opitek, *Cyberprzestępczość w pracy prokuratora*, Prokuratura Krajowa 2018.
18. Grafika własna autora.
19. Grafika własna autora.
20. Grafika własna autora.
21. P. Opitek, *Cyberprzestępczość w pracy prokuratora*, Prokuratura Krajowa 2018.
22. Grafika własna autora.
23. https://gameforge.com/pl-PL/sign-in, https://www.anyrgb.com/en-clipart-2xvqr
24. Chwat, prezentacja pt. Strategia zwalczania przestępczości hazardowej, szkolenie zorganizowane dla funkcjonariuszy Krajowej Administracji Skarbowej, Szczecin, 26–27 września 2022 r. (prezentacja w zbiorach własnych autora).
25. https://allegrolokalnie.pl/oferta/ak47-wtrysk-paliwa-aln

Paweł Opitek

Doktor nauk prawnych, prokurator Prokuratury Regionalnej w Krakowie del. do Prokuratury Krajowej, adiunkt Akademii im. Jakuba z Paradyża w Gorzowie Wlkp., ekspert Instytutu Kościuszki, członek Polskiego Towarzystwa Kryminalistycznego oraz Rady Naukowej Stowarzyszenia Ekspertów Blockchain.

Wykładowca Krajowej Szkoły Sądownictwa i Prokuratury; od 2019 r. egzaminator na egzaminach prokuratorskich.

Autor ponad 70 artykułów naukowych, monografii i rozdziałów w monografiach zbiorowych z zakresu prawa i kryminalistyki.

Specjalista w projektach Giełdy Papierów Wartościowych w Warszawie oraz Instytutu Ekspertyz Ekonomicznych i Finansowych w Łodzi; ekspert w programie wdrożeniowym „Find an Expert II" realizowanym na zlecenie Komisji Europejskiej.

Książka jest publikacją niezwykle przydatną dla prokuratorów, sędziów oraz innych podmiotów prowadzących postępowanie przygotowawcze i sądowe, a także dla aplikantów wszystkich kategorii oraz studentów prawa. Dla wielu z nich będzie stanowiła swego rodzaju przewodnik, ułatwiający ocenę znamion przestępstw i kwalifikację prawną czynów, ale też pozwalający na ujednolicenie orzecznictwa.

Prof. dr hab. Tadeusz Tomaszewski
Uniwersytet Warszawski

Zasługą Autora jest dokonanie wszechstronnej oceny norm prawa dedykowanych przestępstwom teleinformatycznym, związanych z tym aspektem norm proceduralnych, zagadnień metodycznych oraz uporządkowanie zapatrywań doktryny, przy jednoczesnym dostrzeżeniu i analizie problemów praktycznych, często dotąd pomijanych lub ujmowanych wybiórczo. Godna uwagi jest konsekwentna dociekliwość naukowa i kompleksowość opisu, która charakteryzuje całokształt prowadzonych rozważań.

Dr hab. Igor Zgoliński
prof. Akademii Kujawsko-Pomorskiej w Bydgoszczy
sędzia Sądu Najwyższego

ISBN 978-83-952072-9-7

9 788395 207297