

Paweł Opitek¹

Kwalifikacja prawna i opis czynów zabronionych dotyczących przestępczości teleinformatycznej (zagadnienia wybrane)

Streszczenie

W artykule przedstawione zostały wybrane zagadnienia dotyczące przestępstw teleinformatycznych, a więc czynów karalnych dokonywanych przy wykorzystaniu systemów informatycznych i teleinformatycznych. Na wstępie omówiono zakres przeprowadzonych badań, które stały się podstawą do sformułowania określonych tez i wniosków. Pierwsze dwa rozdziały dotyczą błędów popełnianych przez organy procesowe w opisie przestępstwa i jego kwalifikacji prawnej. W kolejnej części artykułu wytyczono granicę pomiędzy znamionami art. 267 § 1 k.k. i art. 267 § 2 k.k. Kulturze języka prawniczego w ferrowanych decyzjach procesowych poświęcono piąty rozdział opracowania, a całość zamyka podsumowanie podjętego tematu.

Słowa kluczowe

Przestępstwa teleinformatyczne, cyberprzestępczość, opis czynu, kwalifikacja prawna czynu, wykładnia przepisów prawa, wyrokowanie.

1. Wstęp

Artykuł został przygotowany na podstawie przeprowadzonych przez autora badań dotyczących kwalifikacji prawnej i opisu czynów karalnych zaliczanych do tzw. przestępstw teleinformatycznych. Określenie „przestępstwa teleinformatyczne” nie doczekało się definicji legalnej; i słusznie, gdyż dotyczą one różnego rodzaju nielegalnych działań

¹ Dr Paweł Opitek, prokurator Prokuratury Okręgowej w Krakowie del. do Prokuratury Krajowej, ORCID ID 0000-0002-4015-5774.

ukierunkowane na systemy informatyczne i teleinformatyczne przetwarzające dane, których nie da się „zamknąć” w jeden definiowalny zbiór. Podobnie sprawa ma się z określeniem „cyberprzestępczość”: o ile kilkanaście lat temu sensowne wydawały się próby wytyczenia granicy pomiędzy cyberprzestępczością, a zastanymi formami przestępczości, i rzeczywiście powstały na ten temat liczne opracowania i definicje, to dzisiaj próby ich tworzenia mają tylko akademickie znaczenie i nie przekładają się w żaden sposób na praktykę stosowania prawa. Obecnie prawie wszystkie czyny karalne opisane w części szczególnej Kodeksu karnego mogą być popełnione „na odległość” z wykorzystaniem Internetu lub innych urządzeń przetwarzających dane informatyczne. W pierwszej kolejności chodzi jednak o przestępstwa stypizowane w art. 267–269b k.k.² oraz art. 278 k.k., 279 k.k. i 287 k.k. i na tych kwalifikacjach prawnych skupia się niniejsza analiza. Inną przesłanką do przyjęcia takiego spektrum badań był fakt, że stosowanie ww. przepisów przez sędziów, prokuratorów i funkcjonariuszy policji nastrocza niejednokrotnie wiele trudności, pojawiają się w tym zakresie błędy lub co najmniej rozbieżności.

Przeprowadzone przez autora badania przebiegały wielotorowo, ale ich najbardziej twórczy element stanowiła dokonana w pierwszej połowie 2022 r. kwerenda prawomocnie zakończonych postępowań karnych z lat 2010–2021 prowadzonych przez sądy okręgu krakowskiego, tj. wydziały karne Sądu Okręgowego w Krakowie, Sąd Rejonowy dla Krakowa-Podgórze w Krakowie, Sąd Rejonowy dla Krakowa-Krowodrzy w Krakowie, Sądu Rejonowy dla Krakowa-Śródmieścia w Krakowie oraz Sąd Rejonowy dla Krakowa-Nowej Huty w Krakowie. Autor osobiście zapoznał się w siedzibie sądów z uprzednio wyselekcjonowanymi aktami kilkuset spraw. Druga ścieżka badań dotyczyła przestępczości kryptowalutowej i bazowała na treści decyzji kończących postępowania w tego typu sprawach na etapie dochodzenia lub śledztwa wydanych w okresie od 1 stycznia 2016 r. do 30 czerwca 2019 r. Całość uzupełniła analiza wyroków zamieszczonych w elektronicznych bazach: programie LEX oraz na Portalu Orzeczeń Sądów Powszechnych skonfrontowana z poglądami doktryny oraz doświadczeniem i wiedzą autora nabytymi w trakcie wykonywania zawodu prokuratora.

W artykule, mając na względzie jego ograniczone ramy objętościowe, podjęto tylko kilka wybranych zagadnień prawnych związanych z opisem czynu i kwalifikacją prawną przestępstw teleinformatycznych. Komplek-

² Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz. U. z 2022 r., poz. 1138).

sowa analiza podjętego tematu znajdzie się w przygotowywanej przez autora, kilkusetstronicowej monografii umieszczonej w planie wydawniczym Krajowej Szkoły Sądownictwa i Prokuratury na rok 2022.

2. Błędy w opisie czynu

Ustawowe znamiona przestępstwa to zespół charakterystycznych, wspólnych, powtarzalnych cech czynu zabronionego właściwych dla pewnego rodzaju zdarzeń prawnych umożliwiających ich typizację³. Typizacja oznacza sformułowanie w ustawie karnej abstrakcyjnych opisów ludzkiego postępowania, które uznano za zabronione, gdyż godzą one w powszechnie respektowane dobra prawne. Polega to na podaniu przez ustawodawcę schematów postępowania zabronionego, w obrębie których mieszczą się poszczególne zachowania ludzkie, jeżeli mają odpowiadać warunkom określonych typów przestępstw. W takim ustawowym opisie „przedstawia się” zespół znamion czynu, eksponując te cechy, które najdokładniej oddają istotę tego zachowania. Znamiona te zwykło się określać, jako znamiona przestępstwa i wytyczają one granicę między tym, co karalne, a zachowaniami dozwolonymi⁴.

Wynika z tego, że podstawowym zadaniem organu procesowego, tj. prokuratora i sądu, jest ustalenie, czy podejrzany/oskarżony wypełnił swoim zachowaniem znamiona czynu zabronionego. Jeśli tak jest, to znajduje to odzwierciedlenie w opisie wycinka aktywności ludzkiej zamieszczonym w postanowieniu o przedstawieniu zarzutów, akcie oskarżenia i wyroku skazującym. Przepis art. 366 § 1 k.p.k.⁵ i art. 413 § 2 pkt 1 k.p.k. stanowi, że obowiązkiem sądu jest wyjaśnienie wszystkich istotnych okoliczności sprawy, a następnie dokładne określenie w wyroku przypisanego oskarżonemu czynu.

Skoro decyzjom procesowym należy nadać konkretną treść odpowiadającą ustalonym okolicznościom faktycznym, to powstaje pytanie: „Na czym polega ‘dokładne określenie przypisanego oskarżonemu czynu’, o którym mowa w art. 413 § 2 pkt 1 k.p.k.?” Wskazówkę odnaleźć można w art. 332 § 1 pkt 2 k.p.k., który stanowi, że akt oskar-

³ A. Pietras, M. Kawecki, Ustawowe znamiona czynów zabronionych w części wojskowej kodeksu karnego w tabelach, Wydawnictwo Difin 2017, s. 47–48.

⁴ T. Bojarski, Odmianny podstawowych typów przestępstw w polskim prawie karnym, Warszawa 1982, s. 11.

⁵ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (tekst jedn. Dz. U. z 2022 r., poz. 1375).

żenia powinien wskazywać czas, miejsce, sposób i okoliczności popełnienia czynu zabronionego oraz skutki, jakie spowodował, a zwłaszcza wysokość powstałej szkody. Jak zauważył Sąd Apelacyjny w Szczecinie, opis czynu przypisanego sprawcy zawiera wszystkie elementy czynu mające znaczenie dla prawidłowej jego kwalifikacji, nie pomijając żadnego aspektu zachowania należącego do ustawowych znamion danego typu przestępstwa. Zwrot „dokładne określenie” należy rozumieć, jako konieczność objęcia opisem elementów istotnych, które mają znaczenie dla indywidualizacji czynu, nie zaś wymóg szczegółowego opisywania każdej z czynności sprawczych czy każdego z zachowań, jakich podjął się sprawca⁶. Wynika z tego, że ów opis powinien odnosić się do wszystkich znamion przestępstwa, ale z drugiej strony nie można popadać w zbytnią kazuistykę i zamieszczać w nim każdej aktywności, która towarzyszyła sprawcy i formalnie rzecz biorąc, przyczyniła się do realizacji znamion. Jak słusznie ujął to Sąd Apelacyjny we Wrocławiu: „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”⁷.

Generalnie rzecz ujmując, stopień konkretności i szczegółowości opisu zależy od kilku czynników: techniki legislacyjnej ujęcia typu przestępstwa w przepisach prawa materialnego, sposobu działania sprawcy w konkretnym kazusie, a także od zgromadzonego materiału dowodowego⁸. W przypadku przestępstw teleinformatycznych, poprzeczka skali trudności związanej z prawidłowym ujęciem znamion zawieszona jest wyżej w porównaniu do innych typów nielegalnych działań z kilku powodów. Najistotniejszy z nich dotyczy technicznych aspektów przetwarzania danych. Za takimi znamionami czasownikowymi czynności sprawczej, jak „niszczenie, uszkodzenie, usuwanie lub zmienianie zapisu istotnej informacji” (art. 268 § 1 k.k.), „przetwarzanie, gromadzenie lub przekazywanie” danych informatycznych (art. 268a § 1 k.k.), czy „wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych” (art. 287 § 1 k.k.) – stoją zazwyczaj skomplikowane, wielopoziomowe procesy obli-

⁶ Wyrok Sądu Apelacyjnego w Szczecinie z dnia 28 września 2017 r., sygn. II AKa 192/16, LEX nr 2391897.

⁷ Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 września 2014 r., sygn. II AKa 242/14, LEX nr 1527320.

⁸ Wyrok Sądu Apelacyjnego w Szczecinie z dnia 28 września 2017 r., sygn. II AKa 192/16, LEX nr 2391897.

czenia wykonywane przez programy komputerowe. Zdawałoby się, że transakcja kartą płatniczą jest stosunkowo prosta pod względem technicznym, ale w rzeczywistości powoduje ona zmiany danych informatycznych zapisywanych na serwerach banków, centrów rozliczeniowych, Krajowego Systemu Rozliczeń, a także innych podmiotów, które uczestniczyły w transakcji (np. platform aukcyjnych). W wyniku popełnionego przestępstwa, zmiany danych dokonują się także w pamięci urządzenia bezpośrednio wykorzystanego przez sprawcę, tj. w chipie i pasku magnetycznym karty, terminalu POS lub bankomacie. Trudno, aby w zarzucie dotyczącym wypłaty lub zapłaty skradzioną kartą (art. 279 § 1 k.k.) dokładnie opisywać wszystkie wspomniane procesy, gdyż w rezultacie powstałby wielozdaniowy, niezrozumiały dla uczestników postępowania, tekst stanowiący karykaturę zarzutu.

Inny przykład odnoszący się do problemu stopnia precyzyjności przypisanego oskarżonemu czynu, to transakcja określana mianem „kradzież bitcoinów”, tj. przelania jednostek kryptowaluty z portfela pokrzywdzonego na adres przestępcy. Powoduje ona automatyczne przetwarzanie, gromadzenie i przekazywanie danych informatycznych w różnych miejscach systemu Bitcoin. Chodzi o zmianę wartości takich danych w co najmniej dwóch portfelach oraz wprowadzenie ich nowego zapisu w blockchainowym protokole, tj. w ostatnim bloku cyfrowej księgi rozrachunkowej przechowywanej na dziesiątkach tysięcy komputerów (tzw. nodów). Działanie sprawcy może powodować nieuprawnioną modyfikację cyfrowych artefaktów w jeszcze innych miejscach, np. na serwerze giełdy kryptowalutowej, jeśli przechowywała ona klucze prywatne osoby pokrzywdzonej. Wynika z tego, że czynność sprawcza takiej „kradzieży” niesie ze sobą wiele jednostkowych konwersji śladów cyfrowych w różnych punktach cyberprzestrzeni. Ich szczegółowe wymienianie w opisie czynu jest niecelowe, a nawet niemożliwe. Trudno też wymagać od organu procesowego, aby w każdym przypadku perfekcyjnie znał zasady działania nowoczesnych technologii, chociaż powinien dysponować podstawowymi informacjami na temat charakteru „technicznego” rozstrzyganej sprawy. Podsumowując, jeśli sprawca „kradnie” bitcoiny w celu wzbogacenia się kosztem pokrzywdzonego, to opis i kwalifikacja prawna przestępstwa „kradzieży” 0,5 BTC może brzmieć następująco: *„J. K. jest oskarżony o to, że w dniu 1 stycznia 2022 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 (tzw. kluczy*

prywatnych) statuujących 0,5 bitcoina z portfela należącego do /.../ do swojego portfela i w ten sposób zmienił zapis w cyfrowej księdze rozrachunkowej Bitcoin oraz portfela pokrzywdzonego działając na szkodę J. K. /.../ w wysokości /.../ zł, co stanowiło równowartość 0,5 bitcoina w dniu 1 stycznia 2022 r., tj. o przestępstwo z art. 287 § 1 k.k.”

Badania aktowe pokazały jednak, że zbyt często takiego rodzaju przestępstwa były opisywane ogólnie, a znamionom czynu z art. 287 § 1 k.k. nie nadano konkretnej treści; oto przykład postanowienia o umorzeniu dochodzenia wydanego w sprawie prowadzonej przez Prokuraturę Rejonową 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 k.k.”⁹. Chociaż referent sprawy przyjął kwalifikację prawną z art. 287 § 1 k.k., to w opisie czynu brak jakichkolwiek informacji o sposobie manipulowania danymi, co stanowi czynność wykonawczą „oszustwa komputerowego”. Nie wiadomo, w jaki sposób nastąpiło automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmiana, usunięcie albo wprowadzenie nowego zapisu takich danych. Można się tylko domyślać, że takim działaniem było „wykonanie transakcji zakupu kryptowaluty BitCoin oraz przelewu wychodzącego”, ale organ procesowy powinien doprecyzować, o jakie znamię czasownikowe, zamieszczone w art. 287 § 1 k.k., chodzi. Na marginesie można dodać, że ów opis zawiera znamiona z art. 267 § 1 lub § 2 k.k. („nieuprawniony dostęp do konta”), ale nie podano żadnego z tych przepisów w kwalifikacji prawnej.

Błędy zdarzają się na etapie wyrokowania, a jako przykład niech posłuży orzeczenie Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie w którym zabrakło znamienia „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

⁹ Akta Prokuratury Rejonowej Katowice-Południe w Katowicach o sygn. PR 3 Ds. 778.2018 (zbiory własne autora).

k.k.”¹⁰ Klauzula normatywna „bez uprawnienia” stanowi niezbędny komponent znamion przestępstwa tzw. hakingu i oddaje pełną dozę bezprawności i karygodności czynu. Zachowanie podejmowane bez upoważnienia, to czynność dokonana bez wiedzy i świadomości podmiotu dysponującego informacją, a nawet wbrew jego woli. W tym kształcie wyrok sądu mokotowskiego nie zawiera wszystkich znamion czynu zabronionego, a więc jego literalnie brzmienie nie wskazuje, aby dana osoba popełniła przestępstwo.

Zdarzały się sytuacje, że 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.”¹¹

Sąd Apelacyjny w Katowicach zajął stanowisko, że w opisie czynu dopuszczalne jest zarówno wierne przytoczenie słów ustawodawcy, 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 zabronionego¹². Chociaż posłużenie się sformułowaniami równoważnymi językowo samo w sobie nie stanowi błędu, to zdaniem autora najlepsze standardy konstruowania opisu czynu przemawiają za tym, aby stosować w nim ściśle ustawowe brzmienie znamion dodając do nich, gdy jest to konieczne, treść właściwą dla sposobu działania sprawcy w procedowanej sprawie (konkretyzacja znamienia). Sprzyja to unifikacji języka prawniczego poprzez posługiwanie się takimi samymi zwrotami przy opisywaniu przestępstw o identycznej kwalifikacji

¹⁰ Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie VIII Wydział karny z dnia 6 czerwca 2016 r., sygn. VIII K 654/11, LEX nr 2096681.

¹¹ Wyrok Sądu Okręgowego w Olsztynie z dnia 4 lutego 2015 r., sygn. VII Ka 1181/14, LEX nr 1835967.

¹² Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 stycznia 2014 r., sygn. II AKa 397/13, LEX nr 1428051.

prawnej. Nie znajduje przy tym żadnego logicznego wytłumaczenia, ani praktycznej przesłanki, dlaczego sformułowanie „bez uprawnienia” zastępować zwrotem „nie będąc osobą uprawnioną” – ani nie brzmi on lepiej, od swojego ustawowego odpowiednika, ani jego zastosowanie nie ułatwia konstruowania decyzji procesowej.

Inny przykład braku obligatoryjnego elementu opisywanego czynu stanowi wyrok Sądu Rejonowego w Jeleniej Górze o treści: „*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.*”¹³ Nie zamieszczono w nim znamion charakteryzujących kradzież z włamaniem, chociaż przepis art. 279 § 1 k.k. znajduje się w kwalifikacji prawnej. W opisie czynu zabrakło ponadto wskazania, czy sprawca działała w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, o czym stanowi art. 287 § 1 k.k. Inna sprawa, że ten ostatni przepis w ogóle nie powinien znaleźć zastosowania na zasadzie zbiegu pomijalnego z art. 279 § 1 k.k. W przypadku nieuprawnionych transakcji kartowych zamiarem kierunkowym sprawcy jest wejście w posiadanie mienia, zamiar ten znajduje odzwierciedlenie w jego świadomości, a ponadto kradzież z włamaniem charakteryzuje się o wiele większym stopniem społecznej szkodliwości, aniżeli sama manipulacja danymi. Stanowisko takie nie jest obce orzecznictwu i wiele wyroków w kwalifikacji prawnej omawianego rodzaju przestępczości uwzględnia tylko art. 279 § 1 k.k., np. „*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.*”¹⁴

Przełamanie zabezpieczenia i zabór rzeczy, gdy czynności te są zbieżne czasowo, stanowi jeden czyn w rozumieniu prawa karnego. W przytoczonym poniżej wyroku 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 sta-

¹³ Wyrok Sądu Rejonowego w Jeleniej Górze II Wydział Karny z dnia 28 września 2020 r., sygn. II K 739/20, LEX nr 3102107.

¹⁴ Wyrok Sąd Rejonowy w Goleniowie z dnia 27 lutego 2018 r., sygn. II K 424/17, LEX nr 2730262.

nowiło „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.”¹⁵ Wyrok wydany w niniejszej sprawie, zakładając, że sprawca nie był w ogóle uprawniony do otwarcia skrzynki, powinien brzmieć: „w dniu 23 grudnia 2015 roku w Krakowie, na os. Piastów 60a, dokonał kradzieży z włamaniem do paczkomatu oznaczonego numerem /.../ firmy InPost S.A. przełamując elektroniczne zabezpieczenie schowka za pomocą wcześniej uzyskanego kodu dostępu i zabrał w celu przywłaszczenia zegarek marki Casio działając na szkodę InPost S.A. w wysokości 531 zł, tj. o przestępstwo z art. 279 § 1 k.k.” Jeśli natomiast sprawca uzyskał kod do paczkomatu „wykorzystując swoje stanowisko służbowe”, tj. do jego obowiązków należała obsługa tej skrzynki, to doszło do przestępstwa oszustwa (art. 286 § 1 k.k.): mężczyzna poczyniła bowiem podstępne zabiegi (rozliczenie fikcyjnej opłaty w systemie informatycznym Spółki) po to, aby wprowadzić pracodawcę w błąd, co do osoby odbierającej przesyłkę z zegarkiem i w ten sposób uzyskał korzyść majątkową w postaci tego zegarka.

3. Błędy w kwalifikacji prawnej czynu

Pod pojęciem „kwalifikacja prawna” należy rozumieć zaliczenie czynu do określonej kategorii przestępstwa, po uprzednim ustaleniu stanu faktycznego oraz dokonaniu jego oceny pod kątem zgodności okoliczności faktycznych sprawy ze znamionami ustawowymi¹⁶. Chodzi więc o subsumcję, której w trakcie postępowania karnego dokonuje organ procesowy. Stanowi ona przedostatni etap stosowania prawa i służy wydaniu indywidualnego rozstrzygnięcia w stosunku do okre-

¹⁵ Wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie Wydział II Karny, sygn. II K 228/17/N (zbiory własne autora).

¹⁶ P. K. Sowiński, Znaczenie wskazania kwalifikacji prawnej czynu oraz jej zmiany w toku postępowania karnego dla realizacji przez oskarżonego prawa do obrony, *Roczniki Nauk Prawnych* 2018, Tom XXVIII, nr 3, s. 113.

ślonego z imienia i nazwiska oskarżonego, będącego stroną postępowania karnego. Poprzedza ten etap faza interpretacyjna, wymagająca zrozumienia przepisu i wyjaśnienia treści użytych w nim pojęć oraz wyprowadzenia z tego przepisu właściwej normy¹⁷. Dalsze rozważania należy poprzedzić uwagą, że dokonane w artykule rozgraniczenie, w postaci dwóch rozdziałów, pomiędzy zagadnieniami: nieprawidłowy opis znamion i błędna kwalifikacja prawna czynu - ma nieco sztuczny charakter, ponieważ w większości przypadków owe błędy zachodzą na siebie, jeden wynika z drugiego i wzajemnie oddziałują na ostateczny kształt całego wyroku. Niemniej, dla uporządkowania omawianych kwestii, zdecydowano się na wspomniany podział redakcyjny.

Ustalenie, że kwalifikacja prawna czynu jest nieprawidłowa może odnosić się do różnych sytuacji. Jedną z nich stanowi kasus, gdy podano przepis w ogóle nie znany ustawie. Dotyczyło to wyroku Sądu Rejonowego dla Krakowa-Podgórze w Krakowie o treści: „*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 internetowo 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.*”¹⁸ Prokurator podał błędną kwalifikację prawną czynu, tj. art. 267 § 1 i 2 k.k. – chodzi bowiem o dwa różne typy przestępstw, które alternatywnie wykluczają się. Skoro ustalono, że sprawca uzyskał dostęp do informacji, a nie danych informatycznych, to przyjąć należało § 1 wspomnianego artykułu. Data czynu, to rok 2012; według obecnie obowiązujących przepisów, po rozszerzeniu w 2017 r. słowniczkowej definicji „rzecz ruchoma”, takie zachowanie wypełniłoby znamiona przestępstwa kradzieży z włamaniem.

W przypadku nieuprawnionych transakcji kartowych pojawia się problem, jak kwalifikować zabór karty, jeśli poprzedza on wypłatę gotówki z bankomatu czy kupno towaru. W treści poniżej zacytowanego wyroku Sąd Rejonowy w Radomsku uznał, że wejście w bezprawne posiadanie karty, a następnie uzyskanie przy jej wykorzystaniu środków finansowych wypełnia znamiona dwóch przestępstw: art. 278 § 1 k.k. i art. 278 § 5 k.k.

¹⁷ T. Chauvin, T. Stanecki, P. Winczorek, Wstęp do prawoznawstwa, Warszawa: Wydawnictwo C.H. Beck 2009, s. 203.

¹⁸ Wyrok Sądu Rejonowego dla Krakowa-Podgórze w Krakowie II Wydział Karny, sygn. II K 1085/13/P (zbiory własne autora).

w zw. z art. 279 § 1 k.k.: „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.”¹⁹ Tymczasem kradzież karty stanowi zazwyczaj „preludium” do dokonania przestępstwa głównego, tj. nieuprawnionej transakcji płatniczej. Dlatego, na zasadzie instytucji czynu współukarane, Sąd powinien pominąć art. 278 § 5 k.k. w treści wyroku tak samo, jak nie karze się w formie wykroczenia za zabór karty magnetycznej, którą sprawca otwiera następnie drzwi do pokojowego hotelu.

W badanych sprawach niektóre postanowienia o umorzeniu śledztwa lub dochodzenia zawierały nieprawidłowe kwalifikacje prawne czynu polegającego na „kradzieży” jednostki kryptowaluty; oto przykład: „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.”²⁰ Bitcoin, podobnie jak inne kryptowaluty, nie jest „rzeczą ruchomą”. Definicja karnoprawna rzeczy jest zasadniczo zbieżna z jej rozumieniem na podstawie art. 45 k.c.²¹ 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 obo-

¹⁹ Wyrok Sądu Rejonowego w Radomsku VI Wydział Karny z dnia 17 listopada 2016 r., sygn. VI K 288/16, LEX nr 2342576.

²⁰ Akta Prokuratury Okręgowej w Krośnie o sygn. PO I Ds. 3.2018 (zbiory własne autora).

²¹ A. Błachnio, *Res extra commercium* jako przedmiot czynności wykonawczej przestępstwa przeciwko mieniu, *Wojskowy Przegląd Prawniczy* 2017, nr 2, s. 15.

wiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce”. Bitcoina, rozumianego jako jednostka rozliczeniowa zapisana w blockchainie, nie sposób podnieść, przesunąć, czy organoleptycznie zmierzyć. Nie posiada on żadnych cech „rzeczy” oraz statusu pieniądza, środka płatniczego albo dokumentu, o którym mowa w art. 115 § 9 k.k. Nie może zatem stanowić przedmiotu czynności wykonawczej opisanego w art. 278 § 1 k.k. lub art. 279 § 1 k.k.

4. Granica pomiędzy art. 267 § 1 k.k. i art. 267 § 2 k.k.

Analiza orzeczeń sądowych pokazuje, że nieuprawniony dostęp do archiwalnych zapisów rozmów, komentarzy, zdjęć, filmów lub podobnych treści umieszczonych na zabezpieczonym (zazwyczaj loginem i hasłem) koncie internetowym kwalifikowany jest 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 ostatni przypadek, to od razu należy go wykluczyć. W jednej ze spraw prokurator oskarżył sprawcę 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 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.”*²² Sąd Rejonowy dla Krakowa-Podgórze w Krakowie, który oceniał tak sformułowany zarzut, słusznie stwierdził, że oskarżyciel publiczny podał błędną kwalifikację prawną czynu, tj. art. 267 § 1 i 2 k.k. – chodzi bowiem o dwa różne typy przestępstw, które alternatywnie wykluczają się. Skoro ustalono, że sprawca uzyskał dostęp do informacji, a nie danych informatycznych, to przyjąć należało § 1 wspomnianego artykułu.

Z kolei w sprawie rozpoznawanej przez Sąd Rejonowy w Nowym Sączu²³, a następnie Sąd Okręgowy w Nowym Sączu, mężczyzna został uznany za winnego tego, 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*

²² Akta Sądu Rejonowego dla Krakowa-Podgórze w Krakowie II Wydział Karny, sygn. II K 1085/13/P (zbiory własne autora).

²³ Wyrok Sądu Rejonowego w Nowym Sączu II Wydział Karny z dnia 28 stycznia 2014 r., sygn. II 1 K 322/13 (zbiory własne autora).

dostęp do konta pokrzywdzonego /.../ na platformie U., tj. o przestępstwo z art. 267 § 2 k.k.”²⁴ Sądy uznały, że dostęp do „konta pokrzywdzonego (...) na platformie U.”, gdzie znajdowała się m.in. korespondencja i informacje handlowe, wyczerpuje znamiona przestępstwa z art. 267 § 2 k.k. Zbieżne stanowisko zajął Sąd Rejonowy dla Wrocławia-Śródmieścia we Wrocławiu²⁵: dwaj sprawcy zostali oskarżeni o to, że posługując się łączem internetowym bez uprawnienia uzyskali dostęp do konta o nazwie (...) w systemie informatycznym firmy. Konto zawierało informacje m.in. o rodzaju produktów, którymi handlowała Spółka. W wyroku zostali oni skazani za popełnienie przestępstwa z § 2 art. 267 k.k.

Druga grupa przypadków dotyczy sytuacji, kiedy sądy podobne stany faktyczne, jak wyżej opisane, kwalifikują z § 1 omawianego przepisu. Uczynił tak Sąd Rejonowy w Giżycku uznając oskarżonego za winnego tego, że: „w bliżej nie ustalonym 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 przeznaczonych 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.”²⁶ W sprawie ustalono, że sprawca, korzystając z nieustalonego oprogramowania szpiegowskiego, rozszyfrował hasło do skrzynki mailowej swojej żony i przełamując zabezpieczenie uzyskał dostęp do treści znajdującej się w poczcie. Następnie skopiował korespondencję i rozesłał ją do innych osób.

Poszukiwanie odpowiedzi na pytanie: „Która w rozpatrywanych przypadkach kwalifikacja prawna czynu jest prawidłowa: § 1 czy § 2 art. 267 k.k.?” należy rozpocząć od stwierdzenia, że jeśli ustawodawca zdecydował się na wprowadzenie odrębnych typów czynów zabronionych, to muszą one regulować różniące się od siebie kategorie zachowań²⁷. Zdaniem W. Wróbla działanie opisane w art. 267 § 2 k.k. może realizować

²⁴ Wyrok Sądu Okręgowego w Nowym Sączu z dnia 17 czerwca 2014 r., sygn. II Ka 188/14, LEX nr 1859693.

²⁵ Wyrok Sądu Rejonowego dla Wrocławia-Śródmieścia we Wrocławiu II Wydział karny z dnia 14 sierpnia 2013 r., sygn. II K 87/12, LEX nr 1903395.

²⁶ Wyrok Sądu Rejonowego w Giżycku II Wydział karny z dnia 3 sierpnia 2015 r., sygn. II K 84/14, LEX nr 2070430.

²⁷ Zob. wyrok Sądu Najwyższego z dnia 4 października 2017 r., sygn. II KK 162/17, LEX nr 2397594.

znamiona przestępstwa, „o ile informacja, do której uzyskuje się dostęp, ma postać danych informatycznych (komputerowych), co do których sprawca nie jest uprawniony”²⁸. Stwierdzenie takie nie rozwiązuje problemu, ponieważ każda informacja przetwarzana przez system komputerowy ma postać danych informatycznych, a dopiero po zastosowaniu odpowiednich algorytmów zyskują one dla człowieka sens w postaci obrazu, czy dźwięku. Jeśli w sposób bezprawny przełamie się zabezpieczenie konta internetowego, to uzyskuje się równocześnie dostęp do informacji zapisanych na tym koncie, ale także metadanych „budujących” te informacje w języku programistycznym. Każda informacja przetwarzana przez system informatyczny ma zatem postać „danych informatycznych” i informacji *sensu stricto* – zależy, od której strony będzie się ją analizować: czy od strony kodu źródłowego (dane) albo patrząc na monitor na którym wyświetlają się komunikaty (informacja).

Odszyfrowując zamiar ustawodawcy, który wprowadził komentowane przepisy, warto sięgnąć do treści uzasadnienia projektu ustawy wprowadzającej karalność za przestępstwo z art. 267 § 2 k.k.; napisano w nim, że przepis ten „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 umożliwi sprawcy przejęcie zdalnej kontroli nad komputerem w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe. 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”²⁹. Po lekturze uzasadnienia sprawa niby wydaje się prosta: chodzi o przestępstwa, gdy sprawca uzyskuje dostęp tylko do systemu operacyjnego komputera po to, aby zainstalować w nim złośliwe oprogramowanie i wykorzystać moc obliczeniową maszyny do własnych celów. To typowe działanie dla takich przestępstw, jak np. budowa *bootnet*'u lub *cryptojacking* (nielegalne „kopanie” kryptowalut). Jednak uzyskując dostęp do „czystych” danych, uzyskuje się także dostęp do

²⁸ W. Wróbel, Art. 267. Znamiona określające typ czynu zabronionego, (w:) W. Wróbel (red.), A. Zoł (red.), Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212–277d, opublikowano: LEX, teza 15.

²⁹ Uzasadnienie projektu ustawy wprowadzającej karalność za przest. z art. 267 § 2 k.k., druk sejmowy nr 458 Sejmu VI kadencji (zbiory własne autora).

informacji zgromadzonych na komputerze i zazwyczaj trzeba ominąć w tym celu „jakieś” zabezpieczenie. Nie wydaje się także, aby o realizacji któregoś ze znamion mógł decydować tylko zamiar sprawcy, tzn. czy chciał on uzyskać dostęp do informacji (§ 1), czy danych (§ 2), chociaż *de facto* uzyskał dostęp do obu z nich. Słusznie zatem twierdzi P. Siemkowicz, 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 informacji³⁰. Problem w tym, że jeśli nawet teoretycznie sytuacje takie mogą mieć miejsce, to trudno wyobrazić je sobie w praktyce.

Analiza treści art. 267 § 2 k.k. i orzecznictwa z jego zastosowaniem pokazuje, że wprowadza on dużo „zamieszania”, jego znamiona są niejasne, szczególnie w kontekście funkcjonowania § 1, a organy procesowe nierzadko błędnie stosują omawianą regulację. Stało się tak w sprawie Sądu Rejonowego dla Krakowa-Podgórze w Krakowie, która dotyczyła jednego z dwóch współsprawców przestępstwa; Sąd uznał oskarżoną za winną tego, że: „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 BRE Bank S.A. w część służącej do obsługi rachunku bankowego nr /.../ co stanowi występek z art. 267 § 2 k.k.”³¹ Z poczynionych przez Sąd ustaleń faktycznych jasno wynika, że czyn oskarżonej powinien zostać zakwalifikowany z § 1, a nie § 2 art. 267 k.k., gdyż uzyskała ona dostęp do informacji, a nie danych. Ustalono przecież, że „panel klienta systemu bankowości internetowej BE Bank S.A., służący do obsługi rachunku bankowego nr (...) stanowi część systemu informatycznego, zawierającego szereg istotnych informacji o rachunku bankowym nr (...), takich jak dane posiadacza, saldo czy szczegółowa historia operacji”.

Przywołując ponownie P. Siemkowicza, to zachowanie opisane w art. 267 § 2 k.k. ma bardzo ogólny charakter, co *de facto* oznacza, że krymi-

³⁰ P. Siemkowicz, Przesłanki 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/Przeslanki_skierowane.pdf, s. 4, data odczytu: 18 sierpnia 2022 r.

³¹ Wyrok Sądu Rejonowego dla Krakowa-Podgórze w Krakowie II Wydział Karny, sygn. II K 1085/13/P (zbiory własne autora).

nalizuje on wszelkie możliwe przypadki uzyskania nieuprawnionego (nie-autoryzowanego) dostępu do systemu informatycznego przy użyciu jakiegokolwiek metody, a także bez względu na to, czy system ten posiada jakieś zabezpieczenia, czy też zabezpieczeń takich wcale nie posiada. Sytuacja ta stwarza niebezpieczeństwo niedookreśloności omawianego przepisu, a tym samym zbyt dużej swobody jego interpretacji przez organy ścigania oraz organy procesowe³². W tym kontekście warto odnieść się do nakazu respektowania przez ustawodawcę zasad przyzwoitej legislacji, stanowiącej element funkcjonowania demokratycznego państwa prawnego. Trybunał Konstytucyjny stwierdził, że zasady te obejmują między innymi wymaganie określoności przepisów, które muszą być formułowane w sposób poprawny, precyzyjny i jasny³³. Wynika z tego, że treść art. 267 § 2 k.k. wymaga ponownej, pogłębionej refleksji legislatora, co do poprawności zarówno jego znamion, jak i kontekstu systemowego funkcjonowania w świetle § 1.

5. Kultura języka prawniczego

Innym elementem badanych spraw karnych było posługiwanie się przez organy procesowe językiem prawniczym w ferowanych decyzjach, czyli językiem judykatury i doktryny. Jak słusznie stwierdził W. Jakimowicz: „Terminologiczno-pojęciowa precyzja odgrywa szczególnie ważną rolę w języku prawnym, stawiając podobne wymagania językowi prawniczemu. Należy dążyć do synergii terminologiczno-pojęciowej między językiem prawnym i prawniczym”³⁴. W. Grzeszczyk dodaje, że wyrokowanie powinno stanowić przykład wysokiej kultury prawnej³⁵, a więc kluczowe decyzje postępowania karnego wydawane przez sędziego, czy prokuratora muszą cechować się poprawnością i stosownością językową oraz etyką i estetyką wypowiedzi³⁶. Dotyczy to

³² P. Siemkowicz, *Przestępstwa skierowane przeciwko poufności...*, *op. cit.*, s. 4.

³³ Wyrok Trybunału Konstytucyjnego z dnia 11 stycznia 2000 r., sygn. K. 7/99, OTK ZU 2000, nr 1, poz. 2.

³⁴ W. Jakimowicz, *Aktualność pojęć prawa administracyjnego*, WKP 2021, źródło: LEX.

³⁵ W. Grzeszczyk, *Uzasadnienie wyroku sądu odwoławczego*, *Prokuratura i Prawo* 2008, nr 6, s. 43.

³⁶ Nieprzypadkowo w programie nauczania dla studentów prawa jednego z uniwersytetów wyznaczono, jako cel dydaktyczny, nabycie przez nich następujących kompetencji: „zna status zasad ortograficznych i interpunkcyjnych oraz akty prawne odnoszące się do języka; zna rodzaje błędów językowych oraz norm poprawnościowych; wie, z jakich źródeł skorzystać w wypadku wątpliwości poprawnościowych”, <https://usosweb.umk.pl/>

szczególnie tak doniosłego wydarzenia, jak wydanie wyroku w którym decyduje się o losie oskarżonego, a pośrednio wpływa także na sytuację życiową innych osób: pokrzywdzonego (zadośćuczynienie za doznaną krzywdę), czy członków najbliższej rodziny sprawcy (np. kara więzienia niszczy więzy ojcowskie, a niekiedy pozbawia rodzinę jej jedyne go żywiciela). I chociaż prawo przemawia „tysiącem ust” (słowa Gerarda Cornu), a dyskurs prawny ma charakter polifoniczny³⁷, to jednak moment ferowania wyroku, znajdujący odzwierciedlenie w jego treści, powinien odznaczać się doniosłością chwili i precyzją słów. Stąd czerpie on swoją siłę, respekt i szacunek społeczny; a *contrario*, wyrok zawierający błędy ortograficzne, nielogiczną budowę, czy słowa potoczne może powodować zaniżenie jego rangi u adresatów wyroku, a niekiedy wręcz kpinę z sędziego sprowadzającą się do kontestacji: „ocenia innych, a sam nie umie poprawnie pisać”.

Przechodząc do konkretów, to przeprowadzone badania spraw dotyczących przestępczości teleinformatycznej pokazały, że treść orzeczeń wydawanych przez sędziów i prokuratorów pozostawia niekiedy wiele do życzenia w zakresie kultury języka prawniczego. Postulować należy, aby sąd w opisie czynu posługiwał się zwrotami prawnymi, a więc takimi, jakie zostały zamieszczone w ustawie, literalnie odzwierciedlającymi znamiona przestępstwa, a nie powszednimi.

W sprawie prowadzonej przez Sąd Rejonowy dla Krakowa-Krowdrzy w Krakowie sprawca został uznany za winnego tego, 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.”³⁸ W Kodeksie cywilnym jest mowa o „umowie sprzedaży”, a nie „kupna-sprzedaży” i pierwszą z wymienionych nazw należało zastosować. Wskazano niepoprawną nazwę firmy: „Swarowski” zamiast „Swarovski”. Prawidłowy opis czynu i jego kwalifikacja prawna powinny brzmieć następująco: „w dniu 16 grudnia 2011 roku w Krakowie bez

kontroler.php?_action=katalog2/przedmioty/pokazPrzedmiot&kod=1300-KJP-1FS, data odczytu: 18.08.2022.

³⁷ M. Sobieszewska, Juryslingwistyka: między językiem i prawem, *Studia Iuridica Lublinensia* 2015, nr 4, s. 126.

³⁸ Wyrok Sądu Rejonowego dla Krakowa-Krowdrzy w Krakowie II Wydział Karny, sygn. II K 549/12/K (zbiory własne autora).

uprawnienia uzyskał dostęp do konta A. /.../ założonego na portalu www.allegro.pl i działając w celu wyrządzenia A. /.../ szkody bez upoważnienia wprowadził zapisy nowych 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 oraz 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 § 2 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.”

Raził niekiedy brak znaków interpunkcyjnych w treści decyzji lub niepotrzebnie stosowane skróty językowe; dotyczy to m.in. postanowienia u umorzeniu dochodzenia zalegającego w aktach 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”³⁹ Stawia się kropkę po skrócie, który jest początkową literą skróconego wyrazu, a więc w postanowieniu powinno widnieć „k.k.” zamiast „kk”. W tak doniosłej decyzji procesowej, jak postanowienie kończące postępowanie karne, nie powinno się pisać „ok.”. Choć skróty przyjęte są na mocy pewnej konwencji i można skrócić prawie każdy wyraz, to należy to robić tylko wtedy, kiedy jest to naprawdę potrzebne. Do sytuacji takich nie należy sporządzanie wyroku, czy postanowienia, które przygotować można dokładnie i bez pośpiechu po to, aby odznaczały się „dostojną” formą. Poza tym prokurator popełnił błąd merytoryczny akceptując decyzję w której jednostki bitcoina nazwano „walutą”; nie są nią w rozumieniu ustawy z dnia 27 lipca 2002 r. Prawo dewizowe⁴⁰, gdyż nie stanowią znaków pieniężnych (banknotów i monet) będących prawnym środkiem płatniczym w Polsce lub poza jej granicami.

Jednak zdarzają się wyroki, których treść w ogóle odbiega od *meritum* sprawy i nie wiadomo do końca za co podsądny został skazany.

³⁹ Akta Prokuratury Rejonowej Katowice-Południe w Katowicach, sygn. PR 3 Ds. 778.2018 (zbiory własne autora).

⁴⁰ Tekst jedn. Dz. U. z 2022 r., poz. 309. Zgodnie z art. 2 ust. 2 pkt 8 i 9 ustawy wartościami dewizowymi są zagraniczne środki płatnicze oraz złoto dewizowe i platyna dewizowa; zagranicznymi środkami płatniczymi są waluty obce i dewizy.

Sprawa prowadzona w Sądzie Rejonowym dla Krakowa-Nowej Huty w Krakowie dotyczyła sytuacji, gdy oskarżony zamontował w samochodzie urządzenie podsłuchowe, aby śledzić mężczyznę poruszającego się tym pojazdem. Sąd uznał go za winnego przestępstwa i skazał za to, że: „w okresie od nieustalonego dnia lipca 2013 roku do dnia 21 sierpnia 2013 roku w miejscowości D. woj. małopolskiego, w celu uzyskania nieuprawnionej informacji o trasie poruszania się samochodu marki Renault Megane 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 przestępstwo z art. 267 § 3 k.k.”⁴¹ Z treści wyroku wynika, że zamiarem oskarżonego było śledzenie trasy przemieszczania się samochodu, a nie ustalonej osoby. Sprawca została więc skazany za monitorowanie trasy przejazdu Renault Megane, ale taki czyn nie podlega penalizacja na podstawie art. 267 § 3 k.k. jeśli nie jest powiązany z naruszeniem prawa do prywatności pokrzywdzonego.

6. Podsumowanie

W niniejszym artykule zaprezentowano kilka kluczowych kwestii związanych z konstruowaniem opisu czynu i jego kwalifikacji prawnej w sprawach dotyczących przestępczości teleinformatycznej. Jednak krąg problemów, które pojawiają się na omawianym polu, jest znacznie szerszy i dotyczy także rozróżnienia pomiędzy „danymi” i „informacją”, określenia relacji art. 278 § 1 k.k. lub art. 279 § 1 k.k. do art. 287 § 1 k.k., kwalifikacji prawnej przestępstw związanych z artefaktami gamingowymi (skinami, lootbox’ami), czy walutami wirtualnymi o charakterze pochodnych instrumentów finansowych. Wszystkie wymienione problemy zostaną przeanalizowane w przygotowywanej monografii po to, aby na końcu zaproponować rozwiązania dyskusyjnych kwestii. Jak pokazuje bowiem cząstkowa analiza tematu, jest wiele niejasności lub punktów spornych w kwalifikowaniu i opisie przestępstw teleinformatycznych, zarówno w doktrynie, jak i orzecznictwie. Sytuacja taka stanowi wdzięczne i ciekawe pole badań dla autora.

⁴¹ Wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie VIII Wydział Karny, sygn. VIII K 911/13/N (zbiory własne autora).

Akty prawne

1. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz. U. z 2022 r., poz. 1138).
2. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (tekst jedn. Dz. U. z 2022 r., poz. 1375).
3. Ustawa z dnia 27 lipca 2002 r. Prawo dewizowe (tekst jedn. Dz. U. z 2022 r., poz. 309).

Bibliografia

1. Błachnio A., Res extra commercium jako przedmiot czynności wykonawczej przestępstwa przeciwko mieniu, *Wojskowy Przegląd Prawniczy* 2017, nr 2.
2. Bojarski T., *Odmiany podstawowych typów przestępstw w polskim prawie karnym*, Warszawa 1982.
3. Chauvin T., Stanecki T., Winczorek P., *Wstęp do prawoznawstwa*, Warszawa, Wydawnictwo C. H. Beck 2009.
4. Grzeszczyk W., Uzasadnienie wyroku sądu odwoławczego, *Prokuratura i Prawo* 2008, nr 6.
5. Jakimowicz W., Aktualność pojęć prawa administracyjnego, *WKP* 2021, źródło: LEX.
6. Pietras A., Kawecki M., *Ustawowe znamiona czynów zabronionych w części wojskowej kodeksu karnego w tabelach*, Wydawnictwo Difin 2017.
7. Sobieszewska M., *Juryslingwistyka: między językiem i prawem*, *Studia Iuridica Lublinensia* 2015, nr 4.
8. 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, data odczytu: 18 sierpnia 2022 r.
9. Sowiński P. K., Znaczenie wskazania kwalifikacji prawnej czynu oraz jej zmiany w toku postępowania karnego dla realizacji przez oskarżonego prawa do obrony, *Roczniki Nauk Prawnych*, Tom XXVIII, nr 3, 2018.
10. Wróbel W., Art. 267. Znamiona określające typ czynu zabronionego, (w:) W. Wróbel, A. Zoll (red.), *Kodeks karny. Część szczególna*. Tom

- II. Część II. Komentarz do art. art. 212–277d, opublikowano: LEX, teza 15.
11. Uzasadnienie projektu ustawy wprowadzającej karalność za przest. Z art. 267 § 2 k.k., druk sejmowy nr 458 Sejmu VI kadencji (zbiory własne autora).

Orzeczenia

1. Wyrok Trybunału Konstytucyjnego z dnia 11 stycznia 2000 r., sygn. K. 7/99, OTK ZU 2000, nr 1, poz. 2.
2. Wyrok Sądu Najwyższego z dnia 4 października 2017 r., sygn. II K.K. 162/17, LEX nr 2397594.
3. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 28 września 2017 r., sygn. II AKa 192/16, LEX nr 2391897.
4. Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 września 2014 r., sygn. II AKa 242/14, LEX nr 1527320.
5. Wyrok Sądu Apelacyjnego we Wrocławiu II Wydział Karny z dnia 9 lipca 2014 r., sygn. II AKa 180/14, LEX nr 1506771.
6. Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 stycznia 2014 r., sygn. II AKa 397/13, LEX nr 1428051.
7. Wyrok Sądu Okręgowego w Olsztynie z dnia 4 lutego 2015 r., sygn. VII Ka 1181/14, LEX nr 1835967.
8. Wyrok Sądu Okręgowego w Nowym Sączu z dnia 17 czerwca 2014 r., sygn. II Ka 188/14, LEX nr 1859693.
9. Wyrok Sądu Okręgowego we Wrocławiu z dnia 5 lutego 2014 r., sygn. IV Ka 1233/13, LEX nr 1882446.
10. Wyrok Sądu Rejonowego w Jeleniej Górze II Wydział Karny z dnia 28 września 2020 r., sygn. II K 739/20, LEX nr 3102107.
11. Wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie Wydział II Karny, sygn. II K 228/17/N (zbiory własne autora).
12. Wyrok Sąd Rejonowy w Goleniowie z dnia 27 lutego 2018 r., sygn. II K 424/17, LEX nr 2730262.
13. Wyrok Sądu Rejonowego dla Krakowa Nowej Huty w Krakowie II Wydział Karny, sygn. II K 724/17/N (zbiory własne autora).
14. Wyrok Sądu Rejonowego w Radomsku VI Wydział Karny z dnia 17 listopada 2016 r., sygn. VI K 288/16, LEX nr 2342576.
15. Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie VIII Wydział Karny z dnia 6 czerwca 2016 r., sygn. VIII K 654/11, LEX nr 2096681.

16. Wyrok Sądu Rejonowego w Giżycku II Wydział karny z dnia 3 sierpnia 2015 r., sygn. II K 84/14, LEX nr 2070430.
17. Wyrok Sądu Rejonowego w Nowym Sączu II Wydział Karny z dnia 28 stycznia 2014 r., sygn. II 1 K 322/13 (zbiory własne autora).
18. Wyrok Sądu Rejonowego dla Wrocławia-Śródmieścia we Wrocławiu II Wydział karny z dnia 14 sierpnia 2013 r., sygn. II K 87/12, LEX nr 1903395.
19. Wyrok Sądu Rejonowego dla Krakowa-Podgórze w Krakowie II Wydział Karny, sygn. II K 1085/13/P (zbiory własne autora).
20. Wyrok Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie VIII Wydział Karny, sygn. VIII K 911/13/N (zbiory własne autora).
21. Wyrok Sądu Rejonowego dla Krakowa-Krowodrzy w Krakowie II Wydział Karny, sygn. II K 549/12/K (zbiory własne autora).
22. Postanowienie Sądu Rejonowego w Dzierżonowie z dnia 16 kwietnia 2014 r., sygn. II Kp 44/14, LEX nr 1906875.

Akta prokuratury

1. Akta Prokuratury Okręgowej w Krośnie o sygn. PO I Ds. 3.2018 (zbiory własne autora).
2. Akta Prokuratury Rejonowej Katowice-Południe w Katowicach o sygn. PR 3 Ds. 778.2018 (zbiory własne autora).
3. Akta Prokuratury Rejonowej Częstochowa-Południe w Częstochowie o sygn. 1 Ds. 23.2018 (zbiory własne autora).

Legal qualification and the description of forbidden acts regarding information and communications technology crimes (chosen issues)

Abstract

The article presents chosen issues regarding legal qualification information and communications technology crimes, that is punishable acts committed when using information and communications technology systems. In the beginning, the author presents the range of research done. This serves as basis for formulating particular thesis and conclusions.

The first two chapters regard mistakes made by trial bodies in the description of the crime and its legal qualification. What follows next is marking borderlines between the appearances of Article 267 § 1 of the Criminal Code and Article 267 § 2 of the Criminal Code. The fifth chapter of the article is devoted to the culture of legal language in passing trial decisions. The paper ends with a summary of the undertaken topic.

Key words

Information and communications technology crimes, cybercrime, description of the act, legal classification of the act, interpretation of the law, issuing a judgment by a court.