Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 1 (45)/2022

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.)?

DOI:10.53024/1.1.45.2022

ARKADIUSZ PAWEŁ SZAJNA*

STRESZCZENIE

Za cel niniejszej pracy obrano przedstawienie problematyki dotyczącej kwalifikacji prawnej czynu polegającego na zrealizowaniu płatności cudzą kartą płatniczą w formie tzw. płatności zbliżeniowej (do kwoty niewymagającej autoryzacji kodem PIN) przez osobę, która weszła w posiadanie przedmiotowej karty wbrew woli jej właściciela. Autor po przeprowadzeniu analizy piśmiennictwa i kierunków orzeczniczych, konkludując stwierdza, iż dokonując subsumpcji należy wziąć pod uwagę kradzież z art. 278 § 1 k.k. bądź art. 119 § 1 k.w. Powołanie się na przepis z k.k. oraz k.w. wynika z tego, iż kradzież ma charakter czynu przepołowionego, gdzie *quantum* rozdzielającym kradzież na występek oraz wykroczenie stanowi kwota 500 zł. Zatem z uwagi na fakt, iż transakcje zbliżeniowe mogą być realizowane bez autoryzacji kodem PIN do wartości 100 zł, to generalnie kwalifikacja prawna czynu będzie obejmowała art. 119 § 1 k.w. Chyba że sprawca działał w warunkach czynu ciągłego i łączna wartość kwot przekracza granicę przepołowienia (500 zł), to wtedy należałoby dokonać kwalifikacji prawnej czynu z art. 278 § 1 k.k. w zw. z art. 12 § 2 k.k.

Słowa kluczowe: kradzież, kradzież z włamaniem, płatność zbliżeniowa, karta płatnicza.

* Dr Arkadiusz Paweł Szajna, Wyższa Szkoła Zarządzania Ochroną Pracy w Katowicach, orcid. org/0000-0001-6327-4234.

1. WPROWADZENIE

Prolegomenę do niniejszej pracy należy rozpocząć od zaprezentowania celu, za który obrano próbę ustalenia, czy dokonanie płatności kartą płatniczą w formie tzw. płatności zbliżeniowej (do kwoty niewymagającej autoryzacji kodem PIN) przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, należy kwalifikować jako kradzież tzw. zwykłą (art. 278 § 1 k.k.[1] albo 119 § 1 k.w.[2]), czy może kradzież z włamaniem (art. 279 § 1 k.k.). *Ergo* przedmiotowy tekst jest kolejnym głosem w dyspucie naukowej, która wybrzmiała po wydaniu przez Sąd Najwyższy wyroku z 22.03.2017 r. (III KK 349/16), w którego tezie stwierdzono, 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.)"[3]. Chcąc zrealizować ww. cel, zaprezentowano wybrane kierunki orzecznicze oraz przeprowadzono analizę i krytykę piśmiennictwa właściwego dla podjętego tematu artykułu.

Narodowy Bank Polski (dalej jako: NBP) w dokumencie – Informacja o kartach płatniczych – I kwartał 2021 r., określił:

1) liczbę wydanych kart płatniczych wyposażonych w funkcję umożliwiającą zrealizowanie płatności zbliżeniowej;

2) skalę zjawiska polegającego na dokonywaniu transakcji zbliżeniowych kartami płatniczymi.

Odnosząc się do pierwszego punktu, należy wskazać, że na koniec marca 2021 r. było wydanych 38,935 mln kart płatniczych z funkcją umożliwiającą dokonanie płatności zbliżeniowych, które stanowiły tym samym 88,3% wszystkich kart płatniczych (na koniec 2020 r. było to 87,8%)[4]. Ponadto wszystkich zbliżeniowych instrumentów płatniczych działających w oparciu o karty płatnicze (np. gadżety, stickery, karty zainstalowane w telefonie) było 44,365 mln[5]. NBP podaje również, że w I kwartale 2021 r. ich liczba uległa zwiększeniu o 934 tys., co szacuje się na wzrost wynoszący odpowiednio 2,1%[6].

Mając na uwadze punkt drugi (w kwartale poddanym analizie), kartami płatniczymi w formie zbliżeniowej przeprowadzono 1,334 mld transakcji[7]. Ponadto w tym samym okresie udział płatności zbliżeniowych w ogólnej liczbie

---

1 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2020 r. poz. 1444, ze zm.).

2 Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2021 r. poz. 2008).

3 Wyrok SN z 22.03.2017 r., III KK 349/16, Legalis nr 1618180.

4 Informacja o kartach płatniczych – I kwartał 2021 r. (https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty/informacje_kwartalne.html), dostęp:14.07.2021 r.

5 *Ibidem*.

6 *Ibidem*.

7 *Ibidem*.

bezgotówkowych płatności kartowych wynosił odpowiednio 95,3%[8]. Natomiast w poprzednim kwartale wynosił 94,9%[9].

NBP podaje również, że:

1) łączna wartość przeprowadzonych bezgotówkowych transakcji zbliżeniowych wyniosła 80,004 mld zł;

2) udział tychże transakcji w całości obrotów bezgotówkowych przeprowadzanych kartami płatniczymi wyniósł 91,6%;

3) udział transakcji zbliżeniowych na przestrzeni poprzednich kwartałów systematycznie wzrasta;

4) średnia wartość pojedynczej transakcji zbliżeniowej wyniosła 60 zł[10].

Podejmowana problematyka będąca przedmiotem niniejszego opracowania – w świetle powyższych informacji – wydaje się być istotna, doniosła społecznie również z uwagi na to, że:

1) w marcu 2020 r. zwiększono limit płatności zbliżeniowej bez konieczności wpisywania kodu PIN do kwoty 100 zł[11];

2) ok. 70% transakcji dokonywanych kartami Mastercard dotyczy płatności na kwotę do 100 zł (transakcje do kwoty 50 zł stanowią ok. 40% wszystkich transakcji kartowych)[12];

3) zdaniem B. Ciołkowskiego, dyrektora generalnego na Polskę, Czechy i Słowację w Mastercard Europe „rok po podwyższeniu limitu transakcji zbliżeniowych bez PIN nasze dane pokazują, że ta zmiana była bardzo potrzebna. Polscy konsumenci w czasie pandemii chętniej płacą bezgotówkowo, a szczególnie zbliżeniowo, co jest już możliwe we wszystkich terminalach w naszym kraju. W badaniach Polacy deklarują, że nadal będą płacić w ten sposób, także po ustaniu pandemii. Płatności zbliżeniowe są przez nich postrzegane jako wygodne, bezpieczne i bardziej higieniczne”[13].

---

8 *Ibidem*.

9 *Ibidem*.

10 *Ibidem*.

11 https://www.forbes.pl/finanse/transakcje-zblizeniowe-karta-zwiekszenie-limitu-do-100-zl-w-visa-i-mastercard/kx0f4c7, dostęp:14.07.2021 r.

12 https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/aktualnosci/pl-pl/2021/marzec/mastercard-70-transakcji-karta-nie-przekracza-100-pln-nie-wymagaja-potwierdzenia-kodem-pin/, dostęp:14.07.2021 r.

13 *Ibidem*.

2. PŁATNOŚCI ZBLIŻENIOWE – ISTOTA I FUNKCJONALNOŚĆ

J. Harasim w swoim artykule podaje, że pojęcie płatności zbliżeniowej jest różnorodnie definiowane[14]. Jedna z definicji (najstarszych) przygotowana przez Komitet do spraw Systemów Płatności i Rozrachunku funkcjonujący przy Banku Rozrachunków Międzynarodowych odnosi się *de facto* do kart zbliżeniowych[15], pojmując je jako karty, które nie wymagają fizycznego kontaktu z czytnikiem[16].

Kolejna definicja, przywołana przez tę autorkę została opublikowana w raporcie opracowanym w 2006 r. przez Datamonitor, w którym płatność zbliżeniowa wyjaśniona została jako pewien rodzaj płatności elektronicznej, gdzie „transfer danych transakcyjnych z urządzenia płatniczego będącego w dyspozycji konsumenta do terminala POS[17] sprzedawcy nie wymaga fizycznego kontaktu między tymi urządzeniami"[18].

J. Harasim wskazuje również, iż w raportach przygotowanych przez Edgar, Dunn & Company we współpracy z Payments Cards & Mobile oraz Mastercard odnoszących się do innowacyjnych płatności zrezygnowano ze zdefiniowania (wprost) pojęcia płatności zbliżeniowych, na rzecz wyodrębnia ich kategorii:

1) „płatności wykorzystujące karty zbliżeniowe (*contactless cards*);

2) płatności z wykorzystaniem urządzeń mobilnych (*mobile proximity payments*), w tym zwłaszcza telefonów komórkowych;

3) płatności, w przypadku których nośnik pozwalający na płatność zbliżeniową jest umieszczany na innych akcesoriach konsumenta (np. w zegarku czy fragmencie ubioru) bądź nawet pod jego skórą"[19].

Z kolei M. Krzysztoszek płatność zbliżeniową rozumie jako realizację „transakcji poprzez przyłożenie do czytnika terminala płatniczego karty płatniczej lub urządzenia mobilnego, wyposażonego w bezpieczny element zawierający dane z karty płatniczej. Dokonując płatności zbliżeniowej do wartości nieprzekraczającej 50 zł[20],

---

14 J. Harasim, *Płatności zbliżeniowe jako przykład innowacji płatniczej – determinanty upowszechnienia*, „Studia Ekonomiczne" 2013, nr 173 t. I, s. 244.

15 J. Harasim w swoim artykule wskazuje, że innych nośników w tamtych czasach jeszcze nie było.

16 J. Harasim, *Płatności zbliżeniowe…*, s. 244, za: A Glossary of Terms Used in Payments and Settlemet Systems. Bank for International Settlements, Basel 2003, http://www.bis.org/publ/cpss00b.pdf, s. 15.

17 Terminal POS to urządzenie przeznaczone do przyjmowania płatności bezgotówkowych pomiędzy klientem a przedsiębiorcą, źródło: https://pospay.com.pl/strefa-wiedzy/co-to-jest-terminal-pos, dostęp: 14.07.2021 r.

18 J. Harasim, *Płatności zbliżeniowe…*, s. 244, za: Contactless Payments 2006. Datamonitor 2006, s. 12.

19 *Ibidem*, za: Advanced Payments Report 2012. Edgar Dunn & Company 2012, s. 27.

20 Aktualnie kwota ta wynosi 100 zł.

podanie kodu PIN nie jest wymagane każdorazowo, a jedynie co kilka losowych operacji”[21].

Pojęcie płatności zbliżeniowej[22] jest definiowane w regulacjach wewnętrznych (regulaminach) opracowanych przez banki. Jako przykład można podać regulamin kart płatniczych dla klientów indywidualnych w PKO Banku Polskim SA[23]. *Ergo* w świetle § 2 pkt 38 przedmiotowego regulaminu, termin zbliżeniowa transakcja płatnicza (operacja zbliżeniowa) oznacza „transakcję dokonaną przy użyciu karty w terminalu z czytnikiem zbliżeniowym realizowaną poprzez zbliżenie karty albo urządzenia mobilnego z nośnikiem zbliżeniowym do czytnika terminala; maksymalna kwota transakcji zbliżeniowej, dla której nie ma konieczności potwierdzania PIN-em lub podpisem określona jest w Komunikacie”[24].

Podsumowując powyższe rozważania, należy uznać, iż realizacja tego rodzaju płatności następuje dzięki zaimplementowaniu rozwiązań technologicznych opierających się na bezprzewodowej komunikacji krótkiego zasięgu pomiędzy czytnikiem (będącym w dyspozycji sprzedawcy) a np. kartą bądź telefonem (będącymi w dyspozycji klienta), które są wyposażone w odpowiedni system umożliwiający komunikację[25]. Warto – w ślad za J. Banasiem – zwrócić uwagę, iż na początku komunikacja bezprzewodowa była dodatkową funkcją, przypisaną jedynie kartom płatniczym[26]. Jak wskazuje on w swoim artykule, intensywny rozwój nauki doprowadził do opracowania technologii fal radiowych krótkiego zasięgu NFC (*Near Field Communication*)[27]. Podkreślmy, iż technologia ta daje możliwość bezprzewodowego łączenia się i wymiany danych między urządzeniami[28]. Ponadto – jak słusznie zauważa M. Krzysztoszek – jest ona stosowana w procesie realizacji bezstykowych płatności zbliżeniowych, w przypadku których nie jest wymagane podawanie kodu PIN[29]. Dzięki temu znaczącemu dla realizacji płatności technologicznemu osiągnięciu rozszerzono grupę urządzeń, z użyciem których możliwa

---

21 M. Krzysztoszek, *Bankowość elektroniczna w teorii i praktyce. Materiały edukacyjne dla środowiska szkolnego*, Warszawa 2017, s. 27.

22 Inaczej również jako: transakcja, operacja.

23 Regulamin kart płatniczych dla klientów indywidualnych w PKO Banku Polskim SA, obowiązujący od 15.12.2018 r., źródło: https://www.pkobp.pl/media_files/410e6e2d-b806-4b1a-b894-e64899ade456.pdf, dostęp: 20.07.2021 r.

24 *Ibidem*, § 2 pkt 38, źródło: https://www.pkobp.pl/media_files/410e6e2d-b806-4b1a-b894-e64899ade456.pdf, dostęp: 20.07.2021 r.

25 J. Banaś, *Płatności zbliżeniowe i perspektywy ich rozwoju*, „Studia Ekonomiczne” 2014, nr 186 cz. I, s. 16.

26 *Ibidem*.

27 *Ibidem*.

28 M. Krzysztoszek, *Bankowość…*, s. 26.

29 *Ibidem*.

stała się realizacja zapłaty[30]. Współcześnie można zapłacić za dany towar, wykorzystując m.in. kartę bezstykową, smartfon, zegarek[31].

Jako zasadne jawi się w tym miejscu odtworzenie kilku istotnych etapów procesu zapłaty kartą, który to jest wysoce skomplikowany, ale w przystępny sposób zaprezentowany został w artykule P. Opitka[32]. Zatem w ślad za przywołanym autorem należy uznać, iż wprowadzając kartę do czytnika, generuje się napięcie elektryczne na styku chipa z czytnikiem i wówczas mikroprocesor wysyła do terminala ciąg bajtów wyposażonych w informacje o logicznej strukturze informatycznej obsługującej kartę oraz – jak to ujmuje P. Opitek – wymogi aplikacyjne niezbędne do zrealizowania operacji[33]. Następnie ma miejsce czynność uwierzytelnienia, realizowana przez „przesłanie z terminalu informacji dotyczących środka płatniczego oraz wpisanego na klawiaturze numeru PIN"[34]. Podkreślić należy, iż konieczność autoryzacji kodem PIN nie dotyczy transakcji zbliżeniowych poniżej 100 zł. Wprowadzony za pośrednictwem klawiatury kod PIN przesyłany jest na „serwer banku przy zastosowaniu tajnego klucza w postaci 15-bitowej liczby zaszyfrowanej algorytmem DES"[35]. Kolejno z dostarczonego szyfrogramu wyznaczana jest wartość PIN-u, podlegająca porównaniu z wartością wprowadzoną przez osobę użytkującą kartę i jeżeli są one identyczne, transakcja uzyskuje status uwierzytelnionej[36]. Zdaniem P. Opitka „wynika z tego, że w karcie płatniczej całym procesem zapłaty steruje mikroprocesor i uwierzytelnia ją za pomocą dwóch informacji: znanej posiadaczowi karty (tj. PIN-u)[37] oraz unikatowego klucza bezpieczeństwa zapisanego w chipie"[38]. Istotne jest również to, że w odniesieniu do:

---

30 J. Banaś, *Płatności…*, s. 16.

31 *Ibidem*.

32 Przedstawiając proces zapłaty oparto się na informacjach zaprezentowanych w artykule P. Opitka, *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017, nr 2. Jest to bowiem – zdaniem autora – publikacja, która w sposób przystępny, czytelny odtwarza ten wysoce skomplikowany proces zapłaty – mówiąc kolokwialnie – krok po kroku. Mając przy tym na uwadze wysoce złożony charakter tego rodzaju płatności oraz fakt, iż nie wszystkie jego elementy zostały odtworzone w niniejszym artykule, odsyłam czytelników do ww. artykułu, w którym P. Opitek szczegółowo dokonał jego wyjaśnienia.

33 P. Opitek, *Kwalifikacja prawna…*, s. 87.

34 *Ibidem*.

35 *Ibidem*.

36 *Ibidem*, za: D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, [w:] *Bankowość elektroniczna*, A. Gospodarowicz (red.), Warszawa 2005, s. 100.

37 Podkreślona przez P. Opitka rola mikroprocesora i kodu PIN jest bardzo istotna w kontekście dalszych rozważań nad kwestią kwalifikacji prawnej czynu pod kradzież z włamaniem.

38 P. Opitek, *Kwalifikacja prawna…*, s. 87.

1) kart zbliżeniowych nawiązanie swoistego połączenia tegoż instrumentu płatniczego z terminalem następuje za pomocą zainstalowanego nadajnika funkcjonującego w ramach dedykowanych systemów płatności zbliżeniowych[39];

2) kart bezstykowych wykorzystywana jest komunikacja oparta na wcześniej wspomnianej technologii NFC. Jak podaje P. Opitek, tego typu operacje wykonywane są za pośrednictwem wprowadzonego do karty miniaturowego układu scalonego oraz anteny radiowej, które to za pomocą fal radiowych[40] umożliwiają przeprowadzenie bezprzewodowej transmisji danych między chipem i terminalem[41].

Kolejno, system bankowy – celem udzielenia zgody na finalizację danej operacji finansowej – przeprowadza weryfikację autentyczność karty, potwierdza również możliwość realizacji zapłaty z jej użyciem w ramach przydzielonego limitu[42]. Jak podkreśla P. Opitek „wskazane parametry mogą być przesyłane na bieżąco do banku w celu autoryzacji (mówi się wtedy o trybie *online*), ale w wypadku terminali sklepowych POS transakcja najczęściej realizowana jest w trybie *offline*. Oznacza to, że po odczytaniu karty system operacyjny maszyny ma wystarczające dane do przeprowadzenia zlecenia bez obowiązku komunikowania się z jej wydawcą w czasie rzeczywistym"[43]. Finalnie każda z osób, tj. posiadacz karty, jej wydawca[44], akceptant[45] i agent rozliczeniowy[46] przeprowadza „określony zestaw przekształceń danych zawartych w komunikacie zgodnie z przydzieloną jej rolą w systemie płatniczym"[47].

Na zakończenie bank powiadamia centrum autoryzacyjne o zatwierdzeniu (lub odmowie) danej operacji i z kolei ww. centrum instruuje POS o tym, aby daną transakcję zrealizował lub odrzucił[48].

Bez wątpienia karty z chipem, wyposażone w specjalistyczny system operacyjny, są instrumentami odznaczającymi się wysokim poziomem zaawansowania

---

39 *Ibidem*, podaje: PayPass dla MasterCard i PayWave dla Visa.

40 *Ibidem*, podaje ich częstotliwość: 13,56 Mhz z użyciem standardu komunikacyjnego ISO 14443.

41 *Ibidem*, s. 87.

42 *Ibidem*.

43 *Ibidem*, s. 87-88.

44 Dostawca wydający kartę płatniczą do dyspozycji płatnika, źródło: art. 2 pkt 35c ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907, ze zm.; dalej: o.u.p.).

45 Odbiorca inny niż konsument, na rzecz którego agent rozliczeniowy świadczy usługę płatniczą, źródło: art. 2 pkt 1b o.u.p.

46 Dostawca prowadzący działalność w zakresie świadczenia usługi płatniczej, o której mowa w art. 3 ust. 1 pkt 5, w tym agent rozliczeniowy w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29.4.2015 r. w sprawie opłat *interchange* w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz. Urz. UE L 123 z 19.05.2015, s. 1); dalej: „rozporządzenia (UE) 2015/751", źródło: art. 2 pkt 1a o.u.p.

47 P. Opitek, *Kwalifikacja prawna…*, s. 88.

48 *Ibidem*.

technologicznego[49]. Na potwierdzenie powyższego można zasygnalizować, iż na karcie znajduje się kwadrat (najczęściej o złotej brawie), a w nim wgłębienie, w którym „za pokrytą cienką warstwą żywicy powłoką ochronną, osadzono kilkudziesięciobitowy mikroprocesor oraz moduł z pamięcią do ponownego zapisu (EEPROM)"[50]. Ponadto ów procesor zawiera oprogramowanie kontrolujące „odczyt i zapis danych zawartych w pamięci elektronicznej (…)"[51].

3. KWALIFIKACJA PRAWNA CZYNU – STANOWISKA PRZEDSTAWICIELI DOKTRYNY ORAZ WYBRANE KIERUNKI ORZECZNICZE

Istotnym dla rozważań będących przedmiotem niniejszego punktu będzie przedstawienie rozumienia pojęcia „włamanie" – znamienia dwuaktowego typu czynu zabronionego opisanego w art. 279 § 1 k.k., będącego – w stosunku do art. 278 § 1 k.k. – kwalifikowanym typem kradzieży. Jednakże zanim to nastąpi należy zwrócić uwagę na przykładowe, pojawiające się w orzecznictwie odmienne – od powyżej jedynie zasygnalizowanych – kwalifikacje prawne czynu:

1. Art. 286 § 1 k.k. (oszustwo). Jako przykład można podać wyrok Sądu Rejonowego w Bielsku Podlaskim z 24.9.2014 r. (VIII K 217/14), w którym to uznano, iż „stypizowane w art. 286 § 1 k.k. oszustwo polega na doprowadzeniu innej osoby do niekorzystnego rozporządzenia mieniem własnym lub cudzym między innymi za pomocą wprowadzenia jej w błąd. Czyn ten ma być dokonany w celu osiągnięcia korzyści majątkowej, a zatem zachodzić musi zamiar bezpośredni. (…) A.B. udał się do sklepu z zamiarem zakupu papierosów przy wykorzystaniu karty należącej do pokrzywdzonego. Przekazując tę kartę sprzedawczyni i wskazując na zamiar zakupu papierosów dążył do wprowadzenia jej w błąd, co do faktu, że jest uprawnionym do korzystania z karty. Posiadanie bowiem legitymizuje posiadacza jako uprawnionego. Cel jego działania był nastawiony na osiągnięcie korzyści majątkowej związanej z otrzymaniem towaru za środki pieniężne innej osoby. Jest również oczywiste, że zaakceptowanie transakcji przy użyciu karty spowodowałoby rozporządzeniem przez kasjerkę środkami pieniężnym P.P. Z jego punktu widzenia byłoby to rozporządzenie niekorzystne, gdyż nie otrzymałby z tego tytułu żadnego ekwiwalentu"[52].

Odnosząc się do kwalifikacji prawnej czynu z art. 286 § 1 k.k., podkreślmy, iż przedmiotem czynności wykonawczej przestępstwa oszustwa jest osoba, która

---

[49] *Ibidem*.

[50] *Ibidem*, za: P. Opitek, *Wpływ standardu EMV na nielegalne działania z wykorzystaniem kart płatniczych w kontekście przestępstwa skimming*, „Bezpieczny Bank" 2016, nr 1, s. 136-137.

[51] P. Opitek, *Kwalifikacja prawna…*, s. 88.

[52] Wyrok SR w Bielsku Podlaskim z 24.09.2014 r., VIII K 217/14, Legalis nr 1982672.

przez sprawcę (poprzez oszukańcze metody) zostaje skłoniona do aktywnego udziału w realizacji jego zamiaru, ale również mienie – przedmiot podlegający rozporządzeniu przez tę osobę[53]. W doktrynie słusznie podkreśla się przy tym, że może to być mienie rozporządzającego czy też innego podmiotu[54]. Istotne jednak w kontekście przedmiotowych rozważań jest to, iż warunkiem odpowiedzialności karnej jest istnienie tożsamości osoby wprowadzonej w błąd i rozporządzającej mieniem[55]. Z samego brzmienia art. 286 § 1 k.k. wynika ponadto wskazany powyżej wymóg. Tak więc oczywiste jest, iż w sytuacji, w której inna osoba została wprowadzona w błąd, a jeszcze inna rozporządziła mieniem, brak jest podstaw do zakwalifikowania danego czynu pod art. 286 § 1 k.k. Słusznie w swoim dziele zauważa B. Gadecki, iż „(…) należy zauważyć, że sprzedawca w sklepie nie jest osobą uprawnioną do rozporządzenia mieniem pokrzywdzonego (właściciela karty)"[56]. Dlatego też pociągnięcie do odpowiedzialności z przedmiotowego przepisu należy uznać za bezpodstawne.

2. Art. 287 § 1 k.k. (oszustwo komputerowe). Jako przykład na tego rodzaju kwalifikację prawną czynu można podać wyrok Sądu Okręgowego w Gliwicach z 29.9.2017 r. (VI Ka 639/17), w którym to Sąd uznał, iż „działanie oskarżonego, który na skutek przyłożenia karty zbliżeniowej do terminala płatniczego, powodował automatyczny przesył danych informatycznych pomiędzy rachunkiem właściciela sklepu a rachunkiem właściciela karty, a w zamian za to otrzymywał korzyść majątkową w postaci zakupionego towaru, którą obejmował swoim zamiarem, w sposób najbardziej pełny wypełnia znamiona art. 287 § 1 k.k."[57].

Komentując pokrótce tego typu czyn zabroniony, należy zwrócić uwagę, iż odznacza się on dwiema odmianami – w pierwszej ma miejsce wpływanie przez sprawcę na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, a w drugiej – dochodzi do zmiany, usuwania albo wprowadzenia nowego zapisu danych informatycznych[58]. Zaprezentowane czynności sprawcze – co istotne – są zakazane wówczas, gdy dochodzi do ich realizacji bez upoważnienia[59]. Sprawcy przestępstwa z art. 287 § 1 k.k. ma towarzyszyć określony cel, za jaki ustawodawca uznał chęć osiągnięcia korzyści majątkowej lub wyrządzenie

---

53 M. Gałązka, [w:] *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, Legalis, komentarz do art. 286, pkt II C 2 (5).

54 *Ibidem*.

55 Wyrok SA w Rzeszowie z 30.01.2014 r., II AKa 112/13, Legalis nr 1079533.

56 B. Gadecki, *Kradzież i użycie karty bankomatowej oraz karty płatniczej (wybrane zagadnienia praktyczne)*, „Przegląd Policyjny" 2016, nr 1 (121), s. 153.

57 Wyrok SO w Gliwicach z 29.09.2017 r., VI Ka 639/17, Legalis nr 1809221.

58 M. Gałązka, [w:] *Kodeks karny…*, komentarz do art. 287, pkt III 1.

59 *Ibidem*.

szkody majątkowej innej osobie[60]. Przedmiotem wymienionych czynności sprawczych[61] są dane informatyczne, które w świetle art. 1 lit. b konwencji Rady Europy z 28.11.2001 r. o cyberprzestępczości[62] pojmuje się jako „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"[63]. Zdaniem L. Wilka, chodzi więc o takie informacje, które mają znaczenie dla sfery majątkowej określonego podmiotu[64]. Warto ponadto wskazać na przedmiot wykonawczy, którym w świetle komentowanego przepisu nie jest człowiek, ale urządzenie stanowiące część systemu informatycznego działającego w sposób automatyczny lub nośnik, na którym to dane informatyczne są zapisane[65]. Podkreśla się również, iż sprawca czynu nie ukierunkowuje swoich działań na proces decyzyjny człowieka (innego), ale na procesy, które zachodzą automatycznie[66]. Dodajmy również, iż występek ten nie ma miejsca przykładowo w sytuacjach, w których sprawca (co prawda) realizuje znamiona określone w art. 287 § 1 k.k., ale zachowanie to stanowi sposób do wprowadzenia innej osoby w błąd i doprowadzenia jej (tym samym) do niekorzystnego rozporządzenia mieniem[67]. Zdarzenia tego typu powinno się kwalifikować pod art. 286 § 1 k.k., ponieważ czyn sprawcy ukierunkowany jest przeciwko mieniu, ale również osobie[68]. Zdaniem B. Michalskiego taki złożony przedmiot ochrony charakteryzuje „klasyczne oszustwo"[69]. Do prawidłowych wniosków dochodzi B. Gadecki, zaznaczając że „(…) w przypadku użycia skradzionej karty (…) następuje zmiana kwoty pieniędzy na koncie pokrzywdzonego. Jednakże nie można przyjąć, że sprawca dokonał «zmiany» kwoty pieniędzy na koncie i dzięki temu uzyskał korzyść majątkową, bowiem zmiana wskazanej kwoty na koncie jest «naturalną konsekwencją» (…) dokonania zakupu przy użyciu karty (…)"[70]. Wtóruje mu A. Lach, pisząc że „(…) przepis ten znajduje zastosowanie, gdy przedmiotem czynności wykonawczej jest

---

60 T. Oczkowski, komentarz do art. 287, pkt B 2, [w:] *Kodeks karny. Komentarz*, R.A, Stefański (red.), Warszawa 2021.

61 Użyto liczby mnogiej, ponieważ jest ich sześć.

62 Konwencja Rady Europy o cyberprzestępczości z dnia 23.11.2001 r. (Dz. U. z 2015 r. poz. 728), art. 1 pkt b.

63 L. Wilk, komentarz do art. 287, pkt V B 1 (19), [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222-316*, M. Królikowski, R. Zawłocki (red.), Warszawa 2017.

64 *Ibidem*.

65 M. Gałązka, [w:] *Kodeks karny…*, komentarz do art. 287, pkt III 6.

66 *Ibidem*.

67 B. Michalski, komentarz do art. 287, pkt II 9 16, [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316. Tom II*, A. Wąsek, R. Zawłocki (red.), Warszawa 2010.

68 *Ibidem*.

69 *Ibidem*.

70 B. Gadecki, *Kradzież i użycie*…, s. 153.

bezpośrednio zapis danych informatycznych, nie zaś kiedy działanie sprawcy powoduje w rezultacie zmianę tych danych"[71].

3. Art. 286 § 1 k.k. w zbiegu z art. 287 § 1 k.k. w związku z art. 11 § 2 k.k. Tego typu kwalifikacja została przyjęta przez Sąd Rejonowy w Zielonej Górze w wyroku z 16.03.2015 r., ale nie będzie ona w tym miejscu omawiana, ponieważ komentarze odpowiednio do art. 286 § 1 i art. 287 § 1 k.k. zostały zawarte w punkcie 1 i 2 niniejszej części pracy. Zatem, jak napisał sąd w uzasadnieniu: „(…) oskarżony użył znalezionej wcześniej karty w taki sposób, że w sklepie (...) w K. przy ul. (...) zapłacił nią za towar wprowadzając pracownika sklepu w błąd co do właściciela karty. Na skutek tego pracownik ten rozporządził niekorzystnie mieniem B.D. w kwocie 11,95 zł, ponieważ umożliwił oskarżonemu dokonanie zapłaty przy pomocy terminala zbliżeniowego, co spowodowało zmniejszenie środków na rachunku B.D. Oskarżony działał w celu osiągnięcia korzyści majątkowej w postaci artykułów spożywczych. Transakcja ta została odnotowana na rachunku bankowym pokrzywdzonej, a więc oskarżony wpłynął na automatyczne przetwarzanie danych i zrobił to bez upoważnienia. Nie dysponował bowiem zgodą właścicielki karty. To zachowanie oskarżonego wypełniło znamiona występku z art. 286 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. P.P. nie pokonał żadnego zabezpieczenia karty – płatności dokonał zbliżeniowo, nie używał kodu PIN, a karta ta nie była zabezpieczona w inny sposób w przypadku dokonywania płatności zbliżeniowych, a zatem nie sposób mówić o wypełnieniu przez niego również znamion występku z art. 279 § 1 k.k. Następnie P.P. ponownie w tym samym sklepie działając w taki sam sposób kupił papierosy. Również to jego zachowanie wypełnia znamiona występku z art. 286 § 1 k.k. i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. Tego samego dnia P.P. jeszcze dwukrotnie w taki sam sposób jak opisany powyżej płacił za paliwo na stacji (...) w M. przy ul. (...) oraz za posiłek w barze (...) w J. za każdym razem posługując się kartą B.D. i płacąc odpowiednio kwoty 43,98 zł i 41,80 zł"[72].

Przechodząc do realizacji założeń wskazanych we wprowadzeniu do trzeciego punktu niniejszej pracy, przyjmuje się (choć niektórzy uważają inaczej[73]), że włamanie – będące znamieniem typu czynu zabronionego określonego w art. 279 § 1 k.k. – możliwe jest wtedy, gdy dana rzecz znajduje się w pomieszczeniu zamkniętym[74].

---

[71] A. Lach, *Glosa do wyroku SN z dnia 22 marca 2017 r., sygn. III KK 349/16*, „Prokuratura i Prawo" 2018, nr 5, s. 174.

[72] Wyrok SR w Zielonej Górze z 16.03.2015 r., II K 1662/14, Legalis nr 2151940.

[73] M. Gałązka, [w:] *Kodeks karny…*, komentarz do art. 279, pkt III B 1 (6), za: G. Łabuda, [w:] *Kodeks karny. Część szczególna*, J. Giezek (red.), Warszawa 2014, s. 1074.

[74] M. Gałązka, [w:] *Kodeks karny…*, komentarz do art. 279, pkt III B 1 (6).

Istotne – zanim nastąpi wyjaśnienie pojęcia „pomieszczenie zamknięte" – jest zwrócenie uwagi na znamię „włamanie". Otóż po przeprowadzeniu analizy piśmiennictwa i orzecznictwa można dojść do konstatacji o funkcjonującej w sferze prawa karnego wykładni *sensu largo* tegoż pojęcia oraz, iż nie jest ono niejako „zawężane" jedynie do kwestii użycia siły ukierunkowanej na przełamanie przeszkody fizycznej[75]. Uznać należy, w ślad za M. Gałązką, że zastosowana metoda (techniczna) pokonania przeszkody nie ma większego znaczenia, dzięki czemu jej przełamanie może polegać na: zastosowaniu – wspomnianej powyżej – siły fizycznej, wykorzystaniu szczególnych umiejętności, jak również niezgodnym z prawem uzyskaniu dostępu do oryginalnego klucza[76]. Jednakże przyjmuje się w judykaturze, iż zabezpieczenie ma być „wyraźną manifestacją woli właściciela czy posiadacza mienia – woli właśnie zabezpieczenia go przed innymi osobami"[77]. Za wystarczające uznaje się przy tym „stworzenie zewnętrznej bariery jednoznacznie sygnalizującej, że celem jej zainstalowania było wykluczenie dostępu do tych przedmiotów przez osoby nieuprawnione"[78]. Mając powyższe na uwadze, poniżej prezentuję kilka przykładów (zawartych w dwóch orzeczeniach), w których stwierdzono, iż poddany osądowi czyn nie wyczerpał znamion kradzieży z włamaniem:

1. Pomieszczenie nie w pełni zamknięte.

„Sprawca, który zabiera mienie w celu przywłaszczenia po usunięciu przeszkody materialnej stanowiącej specjalne zamknięcie pomieszczenia, w wypadku gdy pomieszczenie to nie jest w pełni (całkowicie) zamknięte, nie dokonuje kradzieży z włamaniem"[79].

2. Zabór mienia w następstwie wdarcia się do wnętrza pomieszczeń poprzez wykorzystanie m.in. niezamkniętych drzwi.

„Natomiast kradzieżą zwykłą, a nie kradzieżą z włamaniem, jest zabór mienia w celu przywłaszczenia z wszelkiego rodzaju pomieszczeń w następstwie wdarcia się do ich wnętrza dokonanego przez wykorzystanie:

a) otworów przeznaczonych do normalnego wkraczania do wnętrza (np. drzwi, bramy), lecz niezamkniętych,

b) otworów, które nie są przeznaczone do normalnego wkraczania do wnętrza (np. otworów okiennych, przewodów kominowych, wentylacyjnych) i nie są zamknięte,

---

[75] T. Oczkowski, komentarz do art. 279, pkt A I 2, [w:] *Kodeks karny. Komentarz*, R.A. Stefański (red.), Warszawa 2021.

[76] M. Gałązka, [w:] *Kodeks karny...*, komentarz do art. 279, pkt III B 4 (9).

[77] *Ibidem*, pkt III B 3 (8), za: postanowienie SN z 24.06.2010 r., V KK 388/09, Legalis nr 24372.

[78] *Ibidem*, za: wyrok SA w Białymstoku z 8.10.2002 r., II AKa 505/02, „Prokuratura i Prawo" – wkł. 2004, nr 10, poz. 21.

[79] Teza wyroku SN z 5.03.1985 r., III KR 53/85, Legalis nr 24648.

c) wymienionych przykładowo otworów zamkniętych, np. na pozostawiony w zamku klucz, zwykły haczyk, klamkę zewnętrzną, zasuwkę itp. urządzenia"[80].

W świetle wywodów poczynionych w powyższym akapicie, istoty włamania nie powinno się sprowadzać jedynie do fizycznego uszkodzenia lub zniszczenia przeszkody chroniącej dostęp do rzeczy. Włamanie charakteryzuje się zachowaniem, którego fundamentalną cechą jest „nieposzanowanie wyrażonej przez dysponenta rzeczy woli zabezpieczenia jej przed innymi osobami"[81]. Za zasadne należy uznać ponadto postulaty wysuwane przez część przedstawicieli doktryny, dotyczące zakresu znaczeniowego pojęcia „włamanie", które to powinno obejmować także zabezpieczenia elektroniczne, cyfrowe[82]. W świetle powyższego T. Oczkowski w swoim komentarzu do art. 279 k.k. wspomina, że pokonanie „zabezpieczeń na komputerze, systemie komputerowym, elektronicznych urządzeniach bankowych (bankomatach) i dokonanie dzięki temu zaboru cudzych pieniędzy, powinno być oceniane na podstawie art. 279 § 1 k.k., a nie na podstawie oszustwa komputerowego z art. 287 k.k."[83].

Odnosząc się do terminu „pomieszczenie zamknięte" zwróćmy uwagę na to, iż zdaniem L. Wilka podlega ono swego rodzaju podziałom, klasyfikacjom[84]. Tak więc do grupy tzw. pomieszczeń zasadniczych zamkniętych zalicza się: budynki, lokale mieszkalne i użytkowe[85]. Natomiast do grupy tzw. pomieszczeń specjalnych powinniśmy kwalifikować np.: sejfy, szafy pancerne, skrytki, biurka, kufry[86]. Dostanie się do tego typu pomieszczeń uznawane jest za „odpowiadające z pewnością pojęciu włamania, gdyż ich zasadniczym celem jest zabezpieczenie mienia przed kradzieżą"[87]. Trzeba przy tym zasygnalizować, iż wymienione pojęcia nie są wyczerpywane przez wolne przestrzenie, nawet jeżeli został do nich częściowo ograniczony dostęp przez postawienie płotów, zamontowanie barierek lub innego typu ogrodzeń[88]. Chociaż w jednym judykacie Sąd Najwyższy uznał, że pokonanie, przez zniszczenie (uszkodzenie) przeszkody w postaci ogrodzenia zabezpieczającego mienie, dokonane w celu zaboru cudzego mienia, może wypełniać znamiona typu czynu zabronionego

---

80 Uchwała pełnego składu Izby Karnej SN z 25.06.1980 r., VII KZP 48/78, Legalis nr 22111.

81 Wyrok SA we Wrocławiu z 1.03.2013 r., II AKa 39/13, Legalis nr 742336.

82 T. Oczkowski, komentarz do art. 279, pkt A III 7, [w:] *Kodeks karny. Komentarz*, R.A. Stefański (red.), Warszawa 2021.

83 *Ibidem*, za np.: A. Marek, *Kodeks karny*, Warszawa 2007, s. 510; M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks karny*, t. III, A. Zoll (red.), Warszawa 2008, s. 84.

84 L. Wilk, komentarz do art. 279, pkt V A 18 (34), [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222-316*, M. Królikowski, R. Zawłocki (red.), Warszawa 2017.

85 *Ibidem*.

86 *Ibidem*.

87 L. Wilk komentarz do art. 279…

88 T. Oczkowski, komentarz do art. 279, pkt A I 5, [w:] *Kodeks karny. Komentarz*, R.A. Stefański (red.), Warszawa 2021, za: M. Dąbrowska-Kardas, P. Kardas, [w:] A. Zoll (red.), *Kodeks karny*, t. III, 2008, s. 85.

kradzieży z włamaniem, ale pod pewnymi warunkami[89]. *Ergo* pierwszym jest „całkowite ogrodzenie określonego miejsca przestrzeni, wydzielające je i zabezpieczające przed dostępem osób postronnych"[90]. Za drugi uznano to, że „ogrodzenie musi stanowić realną przeszkodę uniemożliwiającą «prosty» zabór określonego mienia, przeszkodę manifestującą wolę dysponenta mienia zabezpieczenia go właśnie w ten sposób"[91]. Przedostatni warunek „związany jest ze sposobem pokonania tej przeszkody – fizycznym jej usunięciem (zniszczenie, uszkodzenie), wymagającym użycia stosownej siły, środków czy narzędzi, przy czym niewystarczające byłoby pokonanie przeszkody poprzez niewymagające znacznej siły np. wypchnięcie czy odsunięcie, nie mówiąc już o przeskoczeniu ogrodzenia"[92]. Ostatni odnosi się do „samego przedmiotu zaboru – musi on charakteryzować się takimi właściwościami, aby bez pokonania zabezpieczenia nie był możliwy jego zabór (np. przerzucenie przez ogrodzenie)"[93].

Skoro powyżej wykazano, że czyn polegający na zrealizowaniu płatności kartą płatniczą w formie tzw. płatności zbliżeniowej (do kwoty niewymagającej autoryzacji kodem PIN) przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, nie powinien być – zdaniem autora[94] – kwalifikowany z art. 286 § 1 k.k., art. 287 § 1 k.k., art. 286 § 1 k.k. w zbiegu z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k., to warto w tym miejscu przejść do rozważań nad jeszcze jedną możliwością, dotyczącą przeprowadzenia subsumpcji pod art. 278 § 1 k.k.[95], art. 119 § 1 k.w.[96] i art. 279 § 1 k.k.[97].

Odnosząc się do tak zakreślonego problemu (kwestia kwalifikacji prawnej danego czynu jako kradzieży albo kradzieży z włamaniem) widoczne jest, iż zarówno w doktrynie, jak i judykaturze wybrzmiały dwa odmienne podejścia. Chcąc rozstrzygnąć, które podejście winno wieść prym, być wiodącym, należy je w tym miejscu przedstawić.

Swoistym rdzeniem, rozdzielającym problem kwalifikacji prawnej tego typu czynu na dwa odmienne stanowiska[98] wydaje się być mikroprocesor, będący na wyposażeniu karty posiadającej funkcję płatniczą. Uściślając, można zadać następujące pytania:

---

89 Postanowienie SN z 24.06.2010 r., V KK 388/09, Legalis nr 24372.
90 *Ibidem*.
91 *Ibidem*.
92 *Ibidem*.
93 *Ibidem*.
94 Przedmiotowe stanowisko wynika z przeprowadzonej w niniejszej pracy analizy i krytyki piśmiennictwa.
95 Kradzież z k.k.
96 Kradzież z k.w.
97 Kradzież z włamaniem z k.k.
98 Zarówno w doktrynie, jak i judykaturze.

1. Czy wystarczającym zabezpieczeniem – w odniesieniu do znamion kradzieży z włamaniem – jest wspomniany mikroprocesor?

2. Jaka jest rola kodu PIN w kontekście dostępu do środków finansowych zgromadzonych na rachunku bankowym?

Zwolennicy pierwszego stanowiska, wskazujący na kwalifikację prawną czynu z art. 279 § 1 k.k., podnoszą m.in., że kod PIN stanowi istotne zabezpieczenie dostępu do środków finansowych, lecz dodatkowe[99]. Tym pierwotnym, wręcz najistotniejszym jest konstrukcja karty płatniczej, wyposażona w mikroprocesor umożliwiający realizację transakcji, w tym również zbliżeniowych, bez użycia wspomnianego kodu PIN[100].

Przykładowe orzeczenia – subsumpcja pod kradzież z włamaniem:

1. Wyrok Sądu Najwyższego z 22.03.2017 r., III KK 349/16.

„Przybliżenie karty płatniczej do terminalu skutkuje przedostaniem się 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, w celu dokonania płatności za określony towar lub usługę, dokonuje kradzieży z włamaniem"[101].

2. Wyrok Sądu Okręgowego w Gliwicach z 8.12.2017 r., VI Ka 952/17.

„Przybliżenie karty płatniczej do terminalu skutkuje przedostaniem się 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, w celu dokonania płatności za określony towar lub usługę, dokonuje kradzieży z włamaniem. Dokonując w takich warunkach płatności kartą, doprowadza do zmniejszenia aktywów na rachunku bankowym właściciela karty. W istocie dokonuje więc włamania w drodze przełamania zabezpieczeń elektronicznych i zaboru mienia w postaci wartości pieniężnych zapisanych w systemie informatycznym banku, mimo że fizycznie nie obejmuje ich w posiadanie, otrzymując w zamian od razu ich ekwiwalent w postaci towaru lub usługi[102]".

3. Wyrok Sądu Okręgowego w Świdnicy z 28.12.2017 r., IV Ka 726/17.

„Dokonanie płatności kartą płatniczą w formie zbliżeniowej przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, stanowi

---

[99] Z tak konstruowanego poglądu wybrzmiewa – można rzec – marginalizacja zabezpieczenia pod postacią kodu PIN.

[100] Wyrok SN z 22.03.2017 r., III KK 349/16, Legalis nr 1618180.

[101] *Ibidem*.

[102] Wyrok SO w Gliwicach z 8.12.2017 r., VI Ka 952/17, Legalis nr 1809215.

przestępstwo kradzieży z włamaniem, ponieważ dochodzi do przełamania bariery elektronicznej w systemie bankowej płatności bezgotówkowej"[103].

Z kolei zwolennicy drugiego stanowiska, opowiadający się za kwalifikacją prawną czynu pod kradzież tzw. zwykłą, argumentują m.in., że mikroprocesor jako taki nie stanowi zabezpieczenia, umożliwia bowiem komunikowanie się z systemem informatycznym banku[104], a osoba dysponująca prawem do używania karty rezygnuje – w przedmiocie realizacji transakcji zbliżeniowych – z zabezpieczenia pod postacią kodu PIN[105].

Przykładowe orzeczenia – subsumpcja pod kradzież tzw. zwykłą:

4. Wyrok Sądu Okręgowego w Piotrkowie Trybunalskim z 7.01.2015 r., III K 74/14.

„Z kolei istota przestępstwa z art. 278 § 1 k.k. polega na tym, że sprawca wyjmuje rzecz z władztwa innej osoby wbrew jej woli i obejmuje we własne posiadanie, mając faktyczną możliwość dysponowania tą rzeczą. W przedmiotowej sprawie niewątpliwym jest, że oskarżony dokonując zaboru pieniędzy z konta pokrzywdzonego poprzez dokonanie siedmiu nieuprawnionych transakcji, przy pomocy zabranej mu wcześniej karty bankomatowej, z takim zamiarem działał. Przed dokonaniem tych transakcji K.M. wszedł wbrew woli pokrzywdzonego w posiadanie karty bankomatowej bezstykowej (...) o numerze (...) wydanej przez (...) na osobę L.M. uprawniającej do dokonywania zakupów w obrocie bezgotówkowym"[106].

5. Wyrok Sądu Apelacyjnego w Gdańsku z 27.11.2018 r., II AKa 307/18.

„Dokonanie płatności kartą płatniczą w formie tzw. płatności zbliżeniowej przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, stanowi – w zależności od przywłaszczonej kwoty – przestępstwo kradzieży zwykłej określone w art. 278 § 1 k.k. lub też wykroczenie z art. 119 § 1 k.w."[107].

Należy – zdaniem autora – w ślad za M. Krukiem przyjąć, że „samemu mikroprocesorowi, choć steruje on procesem od strony technicznej, nie sposób przypisać roli zabezpieczenia, gdyż w przypadkach transakcji niewymagających autoryzacji jest on, a właściwie karta, której jest integralną częścią, bezbronnym narzędziem w rękach aktualnego posiadacza"[108]. Słusznie podkreśla Sąd Apelacyjny w Gdańsku w wyroku

---

[103] Wyrok SO w Świdnicy z 28.12.2017 r., IV Ka 726/17, Legalis nr 1809214.

[104] Rolę mikroprocesora w procesie realizacji transakcji płatniczej przedstawiono w punkcie 2 niniejszego artykułu.

[105] M. Gałązka, [w:] *Kodeks karny...*, komentarz do art. 279, pkt III B 2 (7), m.in. za: wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.

[106] Wyrok SO w Piotrkowie Trybunalskim z 7.01.2015 r., III K 74/14, Legalis nr 1809219.

[107] Wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.

[108] M. Kruk, *Pojęcie „włamanie" w świetle transakcji zbliżeniowej – uwagi na tle wyroku SN z 22 marca 2017 r., III KK 349/16*, „IUS NOVUM" 2019 nr 4, s. 86.

z 27.11.2018 r., 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 za pomocą karty płatniczej. Mikroprocesor sam w sobie nie stanowi natomiast zabezpieczenia przed nieuprawnionym dostępem do środków pieniężnych"[109]. A. Lach celnie argumentuje podkreślając, że przecież kradzież z włamaniem jest przestępstwem dwuaktowym, na które to z jednej strony składa się zabór w celu przywłaszczenia, z drugiej zaś włamanie – pojmowane jako przełamanie zabezpieczeń[110]. Zatem gdy użyjemy karty z funkcją płatniczą, kodem PIN i następnie ów kod wprowadzimy i zatwierdzimy np. za pośrednictwem klawiatury terminala POS, to wówczas możemy mówić o momencie, w którym „sprawca «włamuje się» (lub usiłuje to zrobić)"[111]. Natomiast w sytuacji, gdy mamy do czynienia z funkcją zbliżeniową[112], to tego zachowania nie da się wyróżnić[113].

4. PODSUMOWANIE

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[114]. 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.

Odnosząc się jeszcze do istoty kodu PIN w związku z realizacją transakcji finansowej poprzez użycie karty z funkcją płatniczą, należy uznać że pełni on – zdaniem

---

[109] Wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.

[110] A. Lach, *Glosa do wyroku SN z dnia 22 marca 2017 r., sygn. III KK 349/16*, „Prokuratura i Prawo" 2018, nr 5, s. 172.

[111] *Ibidem*.

[112] Należy pamiętać, iż wprowadzanie kodu PIN nie jest wymagane w przypadku transakcji do 100 zł.

[113] A. Lach, *Glosa…*, s. 172.

[114] Następuje przywłaszczenie mienia właściciela karty przez zabór, a nie np. rozporządzenie mieniem albo zmianę danych informatycznych, za: B. Gadecki, *Kradzież i użycie…*, s. 153–154.

autora bez wątpienia – funkcję zabezpieczającą[115]. Warto wzbogacić przedstawienie znaczenia kodu PIN, odnosząc się do dwóch przypadków, zasygnalizowanych przez Sąd Apelacyjny w Gdańsku w wyroku z 27.11.2018 r.[116]. Otóż pierwszy z nich dotyczy realizacji płatności zbliżeniowej do kwoty 100 zł (bez konieczności podawania kodu PIN). Natomiast w drugim płatność dokonywana jest przy użyciu tej samej karty, jednak po wpisaniu do terminala zdobytego wcześniej kodu PIN. W pierwszym przypadku właściciel karty, podpisując z bankiem umowę zgodził się, że do wysokości ustalonej wartości transakcji będzie mógł realizować płatność w formie zbliżeniowej bez konieczności wprowadzania kodu PIN[117]. Biorąc to pod uwagę, zdaniem sądu – słusznie – „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"[118]. Rzecz jasna – zdaniem sądu – wyrażanie zgody na tego rodzaju ryzyko w żadnym wypadku nie eliminuje bezprawności takich zachowania[119]. Należy przy tym w pełni zaakceptować stanowisko, iż „nie sposób uznać, że owa bezprawność kryminalna jest identyczna z sytuacją, gdy dla uzyskania dostępu do środków pieniężnych sprawca przełamał zabezpieczenie w postaci kodu PIN"[120].

Zdaniem autora – podzielającego stanowisko Sądu Apelacyjnego w Gdańsku wyrażone w wyroku z 27.11.2018 r. – za *ratio legis* wyodrębnienia czynu zabronionego kradzieży z włamaniem, będącego przecież kwalifikowanym typem kradzieży tzw. zwykłej, uznaje się zwiększone nasilenie złej woli sprawcy przestępstwa, jego determinację w kontekście osiągnięcia obranego celu[121].

Konkludując, należy wyjaśnić przyczynę przywołania – we wcześniejszych częściach niniejszego artykułu – obok art. 278 § 1 k.k. regulacji dot. kradzieży z kodeku wykroczeń, tj. art. 119 § 1 k.w. Wynika ona z tego, iż *de iure* kradzież

---

115 Nie jest zasadne umniejszanie roli kodu PIN poprzez wskazywanie, że jest on czymś dodatkowym w stosunku to pierwotnej formy zabezpieczenia. Warto również za R. Sosikiem podkreślić, że „biorąc pod uwagę rachunek prawdopodobieństwa, a więc fakt, że istnieje 10 000 możliwych kombinacji cyfr w czterocyfrowym kodzie PIN, prawdopodobieństwo użycia właściwego kodu w 3 dopuszczalnych próbach można porównać do wprowadzenia przypadkowego klucza do zamka zabezpieczającego pomieszczenie z gotówką z nadzieją na jego otwarcie. W takim stanie faktycznym nie sposób zatem stwierdzić, że samo posiadanie narzędzia w postaci klucza przesądza o tym, że owo narzędzie nadaje się do dokonania kradzieży z włamaniem", za: R. Sosik, *Wykorzystanie skradzionej karty płatniczej do wykonania płatności zbliżeniowych – Glosa do wyroku SN z 22.03.2017 r., III KK 349/16*, „Glosa – Prawo Gospodarcze w Orzeczeniach i Komentarzach" 2018, nr 2, s. 126.

116 Wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.

117 *Ibidem*.

118 *Ibidem*.

119 *Ibidem*.

120 *Ibidem*.

121 Wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.

ma charakter czynu przepołowionego, gdzie swoistym progiem, rozdzielającym kradzież na występek oraz wykroczenie jest kwota 500 zł. *Ergo* z uwagi na fakt, iż transakcje zbliżeniowe mogą być realizowane bez autoryzacji kodem PIN do wartości 100 zł, to generalnie kwalifikacja prawna czynu będzie obejmowała art. 119 § 1 k.w. Chyba że sprawca działał w warunkach czynu ciągłego (art. 12 k.k.) i łączna wartość kwot przekracza granicę przepołowienia (500 zł), to wtedy należałoby uznać właściwą subsumpcję z art. 278 § 1 k.k. w zw. z art. 12 § 2 k.k.

BIBLIOGRAFIA

Literatura

Banaś J., *Płatności zbliżeniowe i perspektywy ich rozwoju*, „Studia Ekonomiczne" 2014, nr 186, cz. I.
Gadecki B., *Kradzież i użycie karty bankomatowej oraz karty płatniczej (wybrane zagadnienia praktyczne)*, „Przegląd Policyjny" 2016, nr 1(121).
Gałązka M., [w:] *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, Legalis.
Harasim J., *Płatności zbliżeniowe jako przykład innowacji płatniczej – determinanty upowszechnienia*, „Studia Ekonomiczne" 2013, nr 173 t. I.
Kruk M., *Pojęcie „włamanie" w świetle transakcji zbliżeniowej – uwagi na tle wyroku Sądu Najwyższego z 22 marca 2017 r., III KK 349/16*, „IUS NOVUM" 2019, nr 4.
Krzysztoszek M., *Bankowość elektroniczna w teorii i praktyce. Materiały edukacyjne dla środowiska szkolnego*, Warszawa 2017.
Lach A., *Glosa do wyroku Sądu Najwyższego z dnia 22 marca 2017 r., sygn. III KK 349/16*, „Prokuratura i Prawo" 2018, nr 5.
Łabuda G., [w:] *Kodeks karny. Część szczególna*, J. Giezek (red.), Warszawa 2014.
Michalski B., komentarz do art. 287, pkt II 9 16, [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316. Tom II*, A. Wąsek, R. Zawłocki (red.), Warszawa 2010.
Oczkowski T. [w:] *Kodeks karny. Komentarz*, R.A. Stefański (red.), Warszawa 2021.
Opitek P., *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017, nr 2.
Sosik R., *Wykorzystanie skradzionej karty płatniczej do wykonania płatności zbliżeniowych – Glosa do wyroku Sądu Najwyższego z 22.03.2017 r., III KK 349/16*, „Glosa – Prawo Gospodarcze w Orzeczeniach i Komentarzach" 2018, nr 2.
Wilk L., [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222-316*, M. Królikowski, R. Zawłocki (red.), Warszawa 2017.

Źródła prawa

Konwencja Rady Europy o cyberprzestępczości z dnia 23.11.2001 r. (Dz. U. z 2015 r. poz. 728).
Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2021 r. poz. 2008).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2020 r. poz. 1444, ze zm.).
Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907, ze zm.).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29.04.2015 r. w sprawie opłat *interchange* w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz. Urz. UE L 123 z 19.05.2015, str. 1).

Orzecznictwo

Uchwała pełnego składu Izby Karnej SN z 25.06.1980 r., VII KZP 48/78, Legalis nr 22111.
Wyrok SN z 22.03.2017 r., III KK 349/16, Legalis nr 1618180.

Wyrok SN z 5.03.1985 r., III KR 53/85, Legalis nr 24648.
Postanowienie SN z 24.06.2010 r., V KK 388/09, Legalis nr 24372.
Wyrok SA w Białymstoku z 8.10.2002 r., II AKa 505/02, „Prokuratura i Prawo" – wkł. 2004, nr 10, poz. 21.
Wyrok SA we Wrocławiu z 1.03.2013 r., II AKa 39/13, Legalis nr 742336.
Wyrok SA w Rzeszowie z 30.01.2014 r., II AKa 112/13, Legalis nr 1079533.
Wyrok SA w Gdańsku z 27.11.2018 r., II AKa 307/18, Legalis nr 1969941.
Wyrok SO w Piotrkowie Trybunalskim z 7.01.2015 r., III K 74/14, Legalis nr 1809219.
Wyrok SO w Gliwicach z 29.09.2017 r., VI Ka 639/17, Legalis nr 1809221.
Wyrok SO w Gliwicach z 8.12.2017 r., VI Ka 952/17, Legalis nr 1809215.
Wyrok SO w Świdnicy z 28.12.2017 r., IV Ka 726/17, Legalis nr 1809214.
Wyrok SR w Zielonej Górze z 16.03.2015 r., II K 1662/14, Legalis nr 2151940.
Wyrok SR w Bielsku Podlaskim z 24.09.2014 r., VIII K 217/14, Legalis nr 1982672.

Źródła internetowe

Informacja o kartach płatniczych – I kwartał 2021 r. (https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty/informacje_kwartalne.html).
https://www.forbes.pl/finanse/transakcje-zblizeniowe-karta-zwiekszenie-limitu-do-100-zl-w-visa-i-mastercard/kx0f4c7.
https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/aktualnosci/pl-pl/2021/marzec/mastercard-70-transakcji-karta-nie-przekracza-100-pln-nie-wymagaja-potwierdzenia-kodem-pin/.
https://www.pkobp.pl/media_files/410e6e2d-b806-4b1a-b894-e64899ade456.pdf.

A contactless transaction made with someone else's payment card up to an amount that does not require authorization with a PIN code – theft or theft with burglary?

SUMMARY

The aim of this publication is to present the issues related to the legal qualification of an act consisting in making a payment with someone else's payment card in the form of a contactless payment (up to an amount that does not require authorization with a PIN code) by a person who came into possession of the card against the will of its owner. After analyzing the literature and jurisprudence, the author concludes that the theft under the Penal Code or the Code of Petty Offences should be taken into account when classifying the act in law. The indication of the legal provision from the Criminal Code and the Code of Petty Offences results from the fact that theft is a halved act, where the *quantum* that separates the theft into a crime and an petty offence is the amount of PLN 500.

Keywords: theft, burglary, contactless payment, payment card.