Pojęcia kluczowe: *płatność zbliżeniowa, karta płatnicza, kradzież, kradzież z włamaniem, oszustwo*

Artykuły

Anna Czesnowicka

TRANSAKCJA NIEAUTORYZOWANA Z PERSPEKTYWY PRAWNOKARNEJ – KWALIFIKACJA PRAWNA DOKONANIA TZW. PŁATNOŚCI ZBLIŻENIOWEJ ZA POMOCĄ CUDZEJ KARTY PŁATNICZEJ

Rynek płatności bezgotówkowych staje się faktem, a jednocześnie obszarem przynoszącym coraz to nowe wyzwania z punktu widzenia bezpieczeństwa takich transakcji. Szczególną popularność na przestrzeni ostatnich lat zyskują transakcje nieautoryzowane w formie tzw. płatności zbliżeniowej, pozwalające na dokonanie płatności za towary jedynie poprzez samo przyłożenie karty płatniczej do terminalu płatniczego, bez konieczności posłużenia się zabezpieczającym kodem PIN, składania podpisu na wydruku czy przeciągania karty przez czytnik.

Stały wzrost wykorzystania innowacyjnych technologii powoduje konieczność poszukiwania instrumentów w celu skutecznej reakcji karnej oraz odpowiedniej interpretacji obowiązujących regulacji prawnych, w tym właściwej kwalifikacji prawnej czynów realizowanych z wykorzystaniem elektronicznych instrumentów płatniczych. Analiza tak określonego problemu poprzedzona zostanie poszukiwaniem odpowiedzi na pytanie, czy skorzystanie z metody płatności zbliżeniowej stanowi samo w sobie neutralizację zabezpieczenia elektronicznego chroniącego rachunek bankowy, wobec czego niezbędne pozostanie zarysowanie technicznych aspektów tego rodzaju płatności.

Kwalifikacja prawna dokonania płatności zbliżeniowej za nabywane towary lub usługi za pomocą cudzej karty płatniczej, która została uprzednio skradzio-

 DOI: 10.54383/0031-0344.2022.7-8.5

na, wciąż sprawia wiele problemów w praktyce. O ile posłużenie się taką kartą przy dokonaniu płatności za pomocą wpisania kodu PIN, zgodnie z ugruntowaną linią orzeczniczą, kwalifikowane jest jako przestępstwo kradzieży z włamaniem, o tyle dokonanie płatności zbliżeniowej skradzioną kartą płatniczą nie doczekało się do chwili obecnej jednoznacznego stanowiska judykatury i doktryny. Sytuacji nie ułatwia fakt, że w zależności od okoliczności działania przestępnego możliwe jest przyjęcie realizacji nawet czterech różnych kwalifikacji prawnych. Zauważalne tym samym pozostają istotne rozbieżności w przedmiocie zarysowanego problemu.

Do najczęściej spotykanych rozwiązań należy przyjmowanie w takim przypadku realizacji znamion kradzieży z włamaniem określonej w art. 279 § 1 Kodeksu karnego[1], ze wskazaniem, że przełamanie zabezpieczenia polega już na samym przyłożeniu karty do terminalu, bądź też kradzieży w typie podstawowym, o której mowa w art. 278 § 1 k.k. lub – w zależności od kwoty – wykroczenia z art. 119 § 1 Kodeksu wykroczeń[2]. Drugi pogląd warunkowany jest stwierdzeniem, że dokonanie płatności zbliżeniowej nie prowadzi do przełamania zabezpieczenia. W judykaturze można również niekiedy spotkać się z kwalifikacją takiego zachowania jako oszustwa informatycznego realizującego dyspozycję z art. 287 k.k., jak też oszustwa „zwykłego" z art. 286 § 1 k.k. Problematyka nie ma charakteru tylko teoretycznego, pozostaje bowiem istotna z punktu widzenia rozgraniczenia pomiędzy przestępstwem a wykroczeniem.

Celem artykułu jest zatem dokonanie szerszej analizy zarysowanego problemu i próba jego rozwiązania przy uwzględnieniu kryteriów różnicujących kradzież w typie podstawowym i kradzież z włamaniem. Należy się zastanowić nad tym, czy dokonanie płatności zbliżeniowej cudzą kartą płatniczą za nabywaną w sklepie tabliczkę czekolady należy traktować jako kradzież z włamaniem, który to czyn jako niemający swojego odpowiednika w Kodeksie wykroczeń zawsze pozostaje przestępstwem. W dalszej kolejności rozważania zostaną skoncentrowane wokół próby odpowiedzi na pytanie, czy taka transakcja może być uznana za realizującą znamiona oszustwa z art. 286 § 1 k.k. lub oszustwa komputerowego z art. 287 § 1 k.k. Udzielenie odpowiedzi na tak postawione pytania nie jest jednak możliwe bez odniesienia się do technicznej strony funkcjonowania kart płatniczych, w tym przede wszystkim do sposobu uwierzytelniania transakcji oraz rodzaju stosowanych zabezpieczeń elektronicznych.

KARTA PŁATNICZA – MECHANIZM PŁATNOŚCI ZBLIŻENIOWEJ

Pierwsze karty płatnicze pojawiły się około 1900 r. w Stanach Zjednoczonych, dynamiczny rozwój kart nastąpił zaś po II wojnie światowej[3]. W Polsce pierwsze

[1] Ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2022 r. poz. 1138 ze zm.), dalej k.k.
[2] Ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2021 r. poz. 2328 ze zm.), dalej k.w.
[3] A. Michór, *Karty płatnicze* (w:) *Problemy współczesnej bankowości*, red. W. Góralczyk, Warszawa 2014, LEX/el.

karty płatnicze pojawiły dopiero pod koniec lat 70. XX wieku. W 1998 r. funkcjonowało na polskim rynku niespełna 4 mln kart, w 2012 r. zaś już 32 mln kart płatniczych, przy użyciu których wykonano 461 mln transakcji gotówkowych oraz bezgotówkowych na łączną kwotę 95 mld złotych[4]. Do dziś zauważalne pozostaje bardzo szybkie tempo wzrostu liczby transakcji dokonywanych przy użyciu kart zbliżeniowych, a także wartość przeprowadzanych transakcji. Wystarczy wspomnieć, że na koniec I kwartału 2021 r. znajdowało się na rynku polskim 44,1 mln kart płatniczych, w tym 38,9 mln sztuk kart zbliżeniowych. Udział kart zbliżeniowych w ogólnej liczbie kart płatniczych wyniósł 88,3%. W tym samym okresie przeprowadzono 1,6 mld transakcji kartami płatniczymi, w tym 1,5 mld transakcji bezgotówkowych, o łącznej wartości 198,2 mld zł. Transakcje bezgotówkowe stanowiły już 92,6% łącznej liczby wszystkich transakcji kartami. Pojedyncza płatność bezgotówkowa wynosiła średnio 67 zł[5]. Warto dodać, że w ramach kategorii kart płatniczych wyróżnić należy karty magnetyczne (informacje identyfikujące kartę zapisane są na pasku magnetycznym), karty mikroprocesorowe (informacje zapisane na mikroprocesorze), karty hybrydowe (informacje zapisane jednocześnie na pasku magnetycznym i mikroprocesorze). W Polsce dominującą kategorią kart na rynku są karty hybrydowe.

Rozwój rynku obrotu bezgotówkowego w naturalny sposób spowodował konieczność przyjęcia odpowiednich regulacji prawnych. Problematyka instrumentów płatniczych, w tym kart płatniczych, uregulowana została nie tylko w prawie krajowym, ale też na gruncie prawa unijnego. Pojęcie „karta płatnicza" znalazło swoją normatywną definicję w art. 2 pkt 15 rozporządzenia Parlamentu Europejskiego i Rady 2015/751 z 29.04.2015 r., zgodnie z którym jest to instrument płatniczy, który umożliwia płatnikowi zainicjowanie transakcji kartą debetową lub kredytową[6]. Z kolei „instrument płatniczy" definiowany jest jako każde zindywidualizowane urządzenie lub urządzenia lub każdy zbiór procedur uzgodniony przez użytkownika usług płatniczych i dostawcę usług płatniczych, wykorzystywane w celu zainicjowania zlecenia płatniczego. Trybunał Sprawiedliwości UE w wyroku z 11.11.2020 r. w sprawie *DenizBank*, sygn. C-287/19[7], w którym analizował problematykę kwalifikowania funkcji NFC kart płatniczych jako instrumentu płatniczego, wskazał, że przywołany przepis należy interpretować w ten sposób, iż funkcja NFC zindywidualizowanej wielofunkcyjnej karty bankowej, umożliwiająca dokonywanie płatności niskokwoto-

[4] Narodowy Bank Polski, *Informacja o kartach płatniczych – I kwartał 2012 r.*, Warszawa 2012, http://www.nbp.pl/systemplatniczy/karty/q_01_2012.pdf (dostęp: 21.01.2022 r.).

[5] Narodowy Bank Polski, Departament Systemu Płatniczego, *Informacja o kartach płatniczych I kwartał 2021 r.*, Warszawa 2021, https://www.nbp.pl/systemplatniczy/karty/q_01_2021.pdf (dostęp: 5.02.2022 r.).

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z 29.04.2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz.Urz. UE. L z 2015 r. nr 123, s. 1).

[7] Wyrok TSUE z 11.11.2020 r., C-287/19, w sprawie *Denizbank AG v. Verein für Konsumenteninformation*, LEX nr 3082739.

wych obciążających powiązany z nią rachunek bankowy, stanowi „instrument płatniczy" zgodnie z definicją ustanowioną w tym przepisie.

Podobnie termin „karta płatnicza" definiowany jest w polskim porządku prawnym. Ustawodawca w art. 2 pkt 15a ustawy z 19.08.2011 r. o usługach płatniczych[8] wskazał, że jest to karta uprawniająca do wypłaty gotówki lub umożliwiająca złożenie zlecenia płatniczego, w tym karta płatnicza w rozumieniu art. 2 pkt 15 rozporządzenia (UE) 2015/751, z kolei w art. 2 pkt 10 ustawy została zawarta normatywna definicja „instrumentu płatniczego". Karta płatnicza stanowi w konsekwencji jeden z desygnatów terminu „instrument płatniczy". Posłużenie się przez ustawodawcę alternatywą łączną prowadzi do wniosku, że kartą płatniczą może być zarówno karta uprawniająca tylko do wypłaty gotówki, czyli tzw. karta bankomatowa, jak też karta umożliwiająca tylko złożenie zlecenia płatniczego, a także karta zarówno uprawniająca do wypłaty gotówki, jak i złożenia zlecenia płatniczego. Słusznie zauważył Sąd Apelacyjny w Katowicach, że karta płatnicza nie służy tylko do wypłaty gotówki z bankomatu, ale również do zapłaty za towary i usługi, co powoduje, że spełnia funkcję pieniądza gotówkowego[9].

Z kolei na gruncie prawa karnego karta płatnicza, ale już nie karta bankomatowa, w myśl art. 115 § 9 k.k., kwalifikowana jest jako rzecz ruchoma, stanowiąc „inny środek płatniczy", tym samym aktualizacji ulegają wszystkie typy czynów przeciwko mieniu. Odrębnie penalizowany w art. 278 § 5 k.k. jest czyn polegający na kradzieży karty uprawniającej do podjęcia pieniędzy z automatu bankowego, czyli tzw. karty bankomatowej, która – jak wskazano powyżej – również może być kartą płatniczą. W konsekwencji kradzież karty płatniczej innej niż bankomatowa kwalifikowana będzie – w zależności od wartości przedmiotu zaboru – z art. 278 § 1 k.k. lub art. 119 k.w., kradzież zaś karty bankomatowej – z art. 278 § 5 k.k. Wychodząc poza zakres tematu, jedynie nadmienić wypada, że taka konstrukcja przepisów spowodowała pewien chaos interpretacyjny, bowiem przed dokonaną w 2013 r. nowelizacją ustawy o usługach płatniczych[10] dość jednolicie przyjmowano, że karta bankomatowa nie jest innym środkiem płatniczym, gdyż nie może być uznana za surogat pieniądza[11]. W aktualnym stanie prawnym taka linia orzecznicza ulega modyfikacji. Niemniej zdaje się przeważać stanowisko, zgodnie z którym kwalifikacja z art. 278 § 5 k.k. powinna być przyjmowana w przypadku kradzieży każdej karty uprawniającej do podjęcia pieniędzy z automatu bankowego niezależnie od tego, czy karta taka uprawnia do skorzystania z innych funkcji (w tym funkcji płatniczej), czy też nie[12]. Problem ten nie jest li tylko teoretyczny, art. 278 § 5 k.k. nie ma bowiem swojego odpowiednika w Kodeksie wykroczeń,

[8] Ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2021 r. poz. 1907).

[9] Wyrok Sądu Apelacyjnego w Katowicach z 26.11.2004 r. (II AKa 295/04), Legalis nr 70507.

[10] Ustawa z 12.07.2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. poz. 1036).

[11] Uchwała SN z 23.10.2002 r. (I KZP 31/02), OSNKW 2002/11–12, s. 95.

[12] Tak też postanowienie SN z 15.09.2016 r. (I KK 129/16), OSNKW 2016/11, poz. 78; wyrok Sądu Apelacyjnego w Szczecinie z 12.11.2015 r. (II AKa 171/15); przeciwne stanowisko wyrok Sądu Apelacyjnego we Wrocławiu z 28.12.2011 r. (II AKa 385/11), LEX nr 1103521.

wobec czego przyjęcie tej kwalifikacji powoduje, że nie aktualizuje się problematyka tzw. przepołowienia takiego czynu.

Obecnie karta płatnicza jest powszechnie wykorzystywanym instrumentem płatniczym, płatności bezgotówkowe stanowią zaś jeden z najbardziej powszechnych systemów płatności. Na gwałtowny wzrost transakcji bezgotówkowych niewątpliwie wpływ ma nie tylko rozwój technologii i coraz większa cyfryzacja, ale także pandemia COVID-19. Korzystanie z kart płatniczych wyposażonych w funkcję komunikacji bliskiego zasięgu (tzw. funkcja płatności zbliżeniowej, funkcja NFC) stanowi coraz bardziej popularną metodę płatności, ułatwia realizację transakcji płatniczych i zapłatę za nabywane towary i usługi. Funkcja płatności zbliżeniowej pozwala na dokonywanie płatności do określonej kwoty (obecnie do 100 zł) bez konieczności wprowadzania osobistego numeru identyfikacyjnego w kasach wyposażonych w odpowiednie urządzenie. Stały wzrost wykorzystania innowacyjnych technologii powoduje konieczność poszukiwania instrumentów w celu skutecznej reakcji karnej oraz odpowiedniej interpretacji obowiązujących regulacji prawnych, w tym właściwej kwalifikacji prawnej czynów realizowanych z wykorzystaniem elektronicznych instrumentów płatniczych.

Istotne z punktu widzenia tematyki opracowania jest ustalenie, czy skorzystanie z metody płatności zbliżeniowej stanowi samo w sobie neutralizację zabezpieczenia elektronicznego chroniącego rachunek bankowy, wobec czego niezbędne jest zarysowanie technicznych aspektów tego rodzaju płatności.

Przebieg transakcji bezgotówkowej to skomplikowany proces, angażujący kilka podmiotów. Najczęściej w praktyce występuje system czterostronny, w którym występują wystawcy (podmioty odpowiedzialne za przekazanie kart płatniczych na rynek oraz rozliczenia operacji finansowych), akceptanci (podmioty, u których dokonuje się elektronicznych płatności), instytucje rozliczeniowe (transmisja, przetwarzanie i rozliczanie zleceń dokonywanych w punktach akceptujących) oraz posiadacze kart płatniczych (zobowiązani do właściwego zabezpieczenia instrumentu płatniczego oraz zapewnienia odpowiednich środków finansowych na swoim rachunku bankowym)[13]. Wieloetapowy pozostaje także sam przebieg procesu transakcyjnego, w ramach którego zasadnicze znaczenie odgrywa uwierzytelnianie oraz autoryzacja transakcji. Pierwszy ze wskazanych procesów to potwierdzenie tożsamości użytkownika jako uprawnionego do korzystania ze środków zgromadzonych na rachunku bankowym, z kolei autoryzacja to zatwierdzenie dostępu do środków zgromadzonych na rachunku (PIN)[14]. Zindywidualizowana karta płatnicza powiązana jest bowiem z rachunkiem bankowym określonej osoby. Przyłożenie karty do terminalu zaopatrzonego w czytnik mikroprocesora znajdującego się w karcie płatniczej powoduje zainicjowanie wymiany danych pomiędzy chipem a termi-

[13] E. Ślązak, *Nowoczesne instrumenty płatnicze* (w:) *Bankowość detaliczna*, red. J. Koleśniak, Warszawa 2016, s. 205–206.

[14] M. Małecki, P. Dudek, *Paragrafy adaptują się do technologii*, „Rzeczpospolita – Rzecz o prawie" z 13.02.2018 r.

nalem, które to informacje następnie przesyłane są do centrum rozliczeniowego. W dalszej kolejności ma miejsce tzw. zapytanie autoryzacyjne, czyli przesłanie odczytanych informacji do wystawcy karty, który dokonuje weryfikacji środków dostępnych na koncie oraz innych danych, w tym czy karta nie została zastrzeżona, a następnie przesyła do terminalu komunikat zwrotny co do możliwości przeprowadzenia zamierzonej transakcji. Na tym etapie posiadacz karty zobowiązany zostanie do dokonania autoryzacji transakcji kodem PIN (w przypadku niekorzystania z funkcji zbliżeniowej bądź przekroczenia limitu lub liczby transakcji)[15]. W przypadku wykorzystania funkcji płatności zbliżeniowej rachunek ten zostaje obciążony już po dokonaniu płatności i wymaga jedynie posiadania tej karty z aktywną funkcją NFC. W konsekwencji każda osoba posiadająca dostęp do takiej karty płatniczej może dokonać płatności w granicach dopuszczalnego limitu, niezależnie od tego, czy posiadacz karty wyraził na to zgodę, czy też nie. Zwrócenie uwagi na ten fakt ma szczególne znaczenie w przypadku utraty, kradzieży lub przywłaszczenia karty. Prawidłowy przebieg transakcji kartą płatniczą umożliwia dostęp do środków zgromadzonych na rachunku bankowym powiązanym z używaną kartą[16].

Transakcje zbliżeniowe są możliwe dzięki nowej technologii, która wykorzystuje umieszczony w karcie miniaturowy układ scalony oraz wbudowaną antenę radiową[17]. Elementem koniecznym do korzystania z karty płatniczej jest kod elektroniczny stanowiący swoisty i niepowtarzalny klucz elektroniczny zabezpieczający dostęp do rachunku bankowego. Poza tym karty płatnicze wyposażone są w mikroprocesor, oparty na standardzie EMV[18], w którym zapisywane są informacje o posiadaczu karty i o karcie. Mikroprocesor umieszczony na karcie pozwala ukryć i zabezpieczyć przed odczytaniem część danych, ale przede wszystkim do każdej transakcji – również wykonanej zbliżeniowo – generuje unikalne, cyfrowe podpisy, stosując do tego zaawansowane techniki kryptograficzne[19]. Mechanizm płatności zbliżeniowej polega na połączeniu kart wyposażonych w mikroprocesor z technologią łączności bezprzewodowej bliskiego zasięgu, umożliwiając tym samym bezprzewodową transmisję danych między chipem i terminalem płatniczym za pomocą fal radiowych[20]. Uwierzy-

[15] M. Grabowski, *Instrumenty płatnicze w prawie polskim*, rozprawa doktorska, Uniwersytet Warszawski, Wydział Prawa i Administracji, Instytut Nauk Prawno-Administracyjnych, Warszawa 2013, s. 158–159, http://depotuw.ceon.pl (dostęp: 5.03.2022 r.).

[16] M. Kruk, *Pojęcie „włamanie" w świetle transakcji zbliżeniowej – uwagi na tle wyroku Sądu Najwyższego z 22.03.2017 r., III KK 349/16*, „Ius Novum" 2019/4, s. 83.

[17] P. Opitek, *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017/2, s. 87.

[18] Standard zapewniający wyższy poziom bezpieczeństwa w transakcjach płatniczych, dzięki któremu kartę płatniczą bardzo trudno wykorzystać w procederze skopiowania zawartości mikroprocesora w celu wykonywania nieuprawnionych płatności.

[19] Pismo z 27.09.2012 r., wydane przez Ministerstwo Finansów – Podsekretarz Stanu, SPS-023-6402/12, Zabezpieczenie kart bankomatowych przed kradzieżą danych, www.sejm.gov.pl.

[20] P. Opitek, *Kwalifikacja...*, s. 87.

telnienie w przypadku płatności zbliżeniowej dokonywane jest za pomocą unikatowego klucza bezpieczeństwa zapisanego w chipie i stanowiącego integralną część karty[21]. Karta płatnicza wyposażona jest również w aplikację pozwalającą na weryfikację liczby lub wartości transakcji wykonanych w formie zbliżeniowej. Przekroczenie ustalonego limitu powoduje konieczność przeprowadzenia transakcji z użyciem kodu PIN.

Z punktu widzenia tematu opracowania istotne jest zauważenie, że funkcja płatności zbliżeniowej nie ma charakteru obligatoryjnego. Jest to bowiem dodatkowa funkcjonalność, która może być dodana do kart płatniczych różnego typu i na którą musi wyrazić zgodę posiadacz rachunku bankowego. Bank ma bowiem obowiązek zapewnić posiadaczowi rachunku możliwość posiadania karty płatniczej bez funkcjonalności zbliżeniowej, który to obowiązek może być zrealizowany albo poprzez wyłączenie możliwości dokonywania płatności w tej formie na karcie płatniczej, albo też poprzez wydanie karty płatniczej niewyposażonej w funkcjonalność płatności zbliżeniowych.

KRADZIEŻ A KRADZIEŻ Z WŁAMANIEM – INTERPRETACJA TERMINU „POKONANIE PRZESZKODY MATERIALNEJ"

Kradzież to w myśl art. 278 § 1 k.k. pozbawienie władztwa nad rzeczą uprawnionej osoby i przejęcie tego władztwa przez osobę dokonującą zaboru. Szczególnym przypadkiem kradzieży stanowiącym odrębny typ czynu zabronionego jest kradzież z włamaniem, o której mowa w art. 279 § 1 k.k. W tym wypadku nie jest wystarczające „jedynie" wyjęcie rzeczy z posiadania innej osoby i objęcie jej w posiadanie przez sprawcę, ale niezbędne jest dokonanie takiego przywłaszczenia w wyniku usunięcia przeszkody materialnej chroniącej przedmiot czynności wykonawczej przed kradzieżą, stanowiącej fizyczne lub cyfrowe (elektroniczne) zabezpieczenia chroniące rzecz przed kradzieżą[22]. Tym samym jest to przestępstwo dwuaktowe, którego pierwszy etap stanowi włamanie, czyli przełamanie zabezpieczenia chroniącego przedmiot przed kradzieżą, drugi zaś – kradzież.

Zgodnie ze słownikową definicją „włamanie" oznacza „napad rabunkowy połączony z włamaniem, zniszczeniem urządzeń zabezpieczających" czy też „dostanie się do zamkniętego pomieszczenia siłą, niszcząc urządzenia zabezpieczające"[23]. Włamanie zostało bowiem scharakteryzowane jako dwie czynności: użycie siły fizycznej i przełamanie zabezpieczenia[24]. Warto jednak zauważyć, że to nie jedyna słownikowa definicja tego terminu. Uwzględniając rozwój tech-

[21] Por. P. Opitek, *Kwalifikacja...*, s. 87.

[22] Por. *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, komentarz do art. 279 k.k., teza 4, Warszawa 2021, LEX/el.

[23] *Słownik języka polskiego*, t. 3, red. M. Szymczak, Warszawa 1983, s. 732; *Uniwersalny słownik języka polskiego*, t. 4, red. S. Dubisz, Warszawa 2003, s. 466.

[24] J. Wróblewski, *Kradzież z włamaniem. Z zagadnień rozumienia tekstów prawnych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1966/2, s. 235.

nologiczny, współczesny słownik wskazuje także, że o włamaniu można mówić wówczas, gdy po pokonaniu zabezpieczeń dochodzi do bezprawnego odczytania lub zapisania danych w komputerze lub w sieci komputerowej[25].

Analizując to określenie na gruncie prawnokarnym, trudno jednak poprzestać na słownikowym jego definiowaniu, jak bowiem słusznie wskazał Sąd Najwyższy, pojęcie włamania to termin z języka prawnego (i prawniczego), którego znaczenie odbiega od znaczenia tego słowa w języku ogólnym[26]. O ile każde użycie siły fizycznej do usunięcia przeszkody zabezpieczającej rzecz przed kradzieżą stanowi realizację znamienia „włamanie", o tyle zakres desygnatów tego znamienia jest szerszy i nie zawsze będzie wymagał pokonania przeszkody przy zastosowaniu siły fizycznej. Nie można wobec tego tracić z pola widzenia wypracowanej w doktrynie i orzecznictwie, jak też będącej przedmiotem bogatej literatury prawniczej wykładni terminu „kradzież z włamaniem". Konieczne pozostaje również odkodowanie współczesnego rozumienia tego pojęcia.

Przyjęcie znamienia kwalifikującego z art. 279 § 1 k.k. wymaga posłużenia się przez sprawcę stosownym sposobem działania, określonymi środkami, narzędziami czy też odpowiednim natężeniem siły, przy czym sama intensywność siły niezbędnej do pokonania przeszkody ma mniejsze znaczenie. Dla bytu przestępstwa kradzieży z włamaniem nie jest istotne to, czy dojdzie do fizycznego zniszczenia lub uszkodzenia przeszkody materialnej, ale istotne pozostaje nieposzanowanie woli dysponenta rzeczy zabezpieczenia jej przed innymi osobami. Przeszkoda chroniąca dostęp do rzeczy musi mieć charakter realny, czyli w sposób faktyczny w konkretnych okolicznościach chronić rzecz przed kradzieżą. Warunkiem zakwalifikowana czynu jako włamanie jest bowiem przełamanie zabezpieczenia, które stanowi wyraz zabezpieczenia rzeczy przed kradzieżą, a zatem element służący jako zabezpieczenie nie może mieć charakteru tzw. zwykłego zamknięcia. W doktrynie słusznie wskazuje się, że nie stanowi włamania otwarcie drzwi pozostawionym w zamku kluczem albo zaopatrzonych tylko w zewnętrzny haczyk lub skobel, który każdy bez trudu może odsunąć, w takim bowiem wypadku trudno mówić o woli właściciela lub posiadacza zabezpieczenia przedmiotu przed kradzieżą[27]. Do kategorii desygnatów terminu „zabezpieczenie" nie można także zaliczyć tzw. zwykłych zamknięć[28]. O ile słusznie przyjmuje się, że otwarcie drzwi oryginalnym kluczem należy traktować jako kradzież z włamaniem[29], o tyle takiej kwalifikacji nie będzie można przyjąć w przypadku otwarcia niezamkniętych na klucz drzwi. W sytuacji gdy sprawca ma otwarty, bezpośredni dostęp do rzeczy ruchomej,

[25] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/slowniki/w%C5%82amywaczka.html (dostęp: 6.02.2022 r.).

[26] Postanowienie SN z 6.12.2006 r. (III KK 358/06), OSNKW 2007/2, poz. 17.

[27] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, komentarz do art. 279.

[28] P. Kardas, J. Satko, *Przestępstwa przeciwko mieniu: przegląd problematyki, orzecznictwo (SN 1918–2000, piśmiennictwo)*, Kraków 2002, s. 48.

[29] Wyrok Sądu Apelacyjnego we Wrocławiu z 1.03.2013 r. (II AKa 39/13), LEX nr 1294878.

nie realizuje znamion czynu z art. 279 k.k., nie pokonuje bowiem przeszkody stanowiącej zabezpieczenie dostępu do przedmiotu zaboru. Irrelewantne jednak pozostaje to, czy otwarcie zamkniętych drzwi nastąpi za pomocą skradzionego oryginalnego klucza, dopasowanego klucza, czy przy użyciu innych narzędzi. Bez znaczenia pozostaje także rodzaj zabezpieczenia, jego skuteczność czy też łatwość pokonania[30]. Do przyjęcia realizacji znamion wskazanego przestępstwa nie wystarczy jednak samo istnienie przeszkody materialnej, ale musi być ona także aktywowana i uruchomiona w czasie dokonywania przez sprawcę zamachu na zabezpieczone mienie[31].

Skoro zatem – podzielając zdanie M. Dąbrowskiej-Kardas i P. Kardasa – istota kradzieży z włamaniem polega na usunięciu przeszkody materialnej zabezpieczającej dostęp do mienia, a jednocześnie niekwestionowana pozostaje możliwość zabezpieczenia elektronicznego, które odnosi się do urządzeń elektronicznych i nie pozostaje związane z pomieszczeniem, to pojęcie włamania należy również odnieść do „zachowania polegającego na przełamaniu zabezpieczenia rzeczy przed zaborem"[32]. Zestawiając tak zdekodowane znamiona kradzieży z zachowaniem osoby dokonującej zaboru odzieży w sklepie poprzez zerwanie zawieszki jej zabezpieczającej, warto zauważyć, że bez większych wątpliwości w drugim przypadku należy przyjąć realizację znamion kradzieży w typie podstawowym. Zawieszka bowiem nie chroni dostępu do mienia, ale pozwala na ujawnienie kradzieży poprzez uruchomienie alarmu w momencie pokonywania bramek ochronnych. Nie chodzi zatem o to, czy rzecz ma jakieś zabezpieczenie, ale o to, czy to zabezpieczenie może stanowić realną przeszkodę przed zaborem oraz faktyczną manifestację woli dysponenta rzeczy zabezpieczenia jej przed innymi osobami.

Cechą konstytutywną włamania nie jest charakter zabezpieczenia (fizyczne, elektroniczne czy cyfrowe), ale istotne jest samo przełamanie takiego zabezpieczenia. Stąd też włamanie nie zawsze będzie się wiązało z użyciem siły fizycznej, ale może wiązać się również z wysiłkiem umysłowym, do realizacji tego znamienia może bowiem dojść także poprzez przełamanie elektronicznych kodów zabezpieczających dostęp do bankomatu albo do programu komputerowego[33]. Słusznie w judykaturze wskazuje się, że włamaniem jest pokonywanie zabezpieczeń elektronicznych, chroniących dostęp osób nieuprawnionych do systemu komputerowego, elektronicznej bazy danych, elektronicznego urządzenia bankowego czy rachunku bankowego[34]. Co prawda w orzecznictwie wskazuje się, że przeszkoda materialna chroniąca mienie przed kradzieżą powinna być „częścią konstrukcji pomieszczenia zamkniętego lub specjalnym zamknięciem

[30] Wyrok SN z 15.08.1985 r. (I KR 212/85), OSNKW 1986/11–12, poz. 97.
[31] Por. wyrok SN z 3.02.1999 r. (V KKN 566/98), „Prokuratura i Prawo" 1999/7–8, wkładka, poz. 7.
[32] M. Dąbrowska-Kardas, P. Kardas (w:) *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. W. Wróbel, A. Zoll, Warszawa 2022, komentarz do art. 279.
[33] M. Dąbrowska-Kardas, P. Kardas (w:) *Kodeks...*, komentarz do art. 279.
[34] Postanowienie SN z 29.10.2012 r. (I KZP 11/12), Legalis nr 538445.

tego pomieszczenia, utrudniającym dostęp do jego wnętrza"[35]. Niemniej wykładnia literalna dyspozycji art. 279 § 1 k.k. nie pozwala na ograniczenie kradzieży z włamaniem jedynie do pomieszczeń czy też innych lokali zamkniętych. Takie też stanowisko przyjmowane jest w nowszej judykaturze i w doktrynie. W procesie ewolucji sposobu interpretacji tego pojęcia, u podstaw której leży dostrzeżenie rozwoju technologicznego, przyjmuje się, że urządzenia elektroniczne, bazy danych czy rachunki bankowe tworzą wirtualne pomieszczenie, do którego dostępu chroni specjalny klucz (kod) elektroniczny, stanowiący swoisty ekwiwalent fizycznego zamknięcia rzeczy w pomieszczeniu. W wyroku Sądu Najwyższego z 9.09.2004 r.[36] słusznie stwierdzono, że zabezpieczenie takie „stanowi *sui generis* zamknięcie dostępu dla każdej osoby, która zamierza władać rzeczą, także dla osoby uprawnionej. Jest więc swoistym ekwiwalentem fizycznego zamknięcia rzeczy w pomieszczeniu".

KWALIFIKACJA PRAWNA PŁATNOŚCI ZBLIŻENIOWEJ DOKONANEJ SKRADZIONĄ KARTĄ PŁATNICZĄ

W związku z rozwojem systemów płatniczych w orzecznictwie i doktrynie pojawił się problem z oceną zachowania polegającego na dokonaniu płatności kartą płatniczą w formie tzw. *płatności zbliżeniowej* przez osobę nieuprawnioną, która weszła w posiadanie karty wbrew woli jej właściciela, prowadzący do znacznych rozbieżności w ocenie prawnej takiego zachowania. Wyrazistym przykładem omawianego problemu może być stan faktyczny sprawy będącej przedmiotem rozpoznania w wyroku Sądu Najwyższego z 11.10.2016 r.[37]. Prokurator w akcie oskarżenia przyjął, że dokonanie płatności zbliżeniowych skradzioną kartą płatniczą należy kwalifikować z art. 286 § 1 k.k. i zarzucił oskarżonej dopuszczenie się czterdziestu przestępstw, polegających na doprowadzeniu kasjerek różnych placówek handlowych do niekorzystnego rozporządzenia środkami pieniężnymi na rachunku bankowym osoby, której karta płatnicza została uprzednio skradziona. Sąd rejonowy wobec niewskazania w akcie oskarżenia znamienia wprowadzenia w błąd przyjął, że nie jest możliwe zakwalifikowanie tego działania jako oszustwa i uznał oskarżoną za winną dokonania kradzieży środków pieniężnych znajdujących się na rachunku bankowym przy użyciu skradzionej karty zbliżeniowej, kwalifikując ten czyn z art. 278 § 1 k.k. w zw. z art. 12 k.k. Sąd okręgowy rozpoznający apelację od wyroku sądu pierwszej instancji uniewinnił oskarżoną od popełnienia zarzucanych jej czynów, uznając, że sąd pierwszej instancji niezasadnie orzekł w zakresie innej kwalifikacji prawnej. Sąd Najwyższy w wyniku rozpoznania kasacji uchylił wyrok sądu drugiej instancji i przekazał sprawę do ponownego rozpoznania w postępowaniu od-

[35] Uchwała SN z 25.06.1980 r. (VII KZP 48/78), OSNKW 1980/8, poz. 65.
[36] Wyrok SN z 9.09.2004 r. (V KK 144/04), LEX nr 137749.
[37] Wyrok SN z 11.10.2016 r. (V KK 122/16), LEX nr 2148659.

woławczym, wskazując, że niezrozumiałe było uniewinnienie oskarżonej w tak opisanym stanie faktycznym.

PŁATNOŚĆ ZBLIŻENIOWA JAKO KRADZIEŻ CZY KRADZIEŻ Z WŁAMANIEM?

Pogląd prawny sprowadzający się do uznania, że płatność zbliżeniowa cudzą kartą płatniczą powinna być kwalifikowana jako kradzież z włamaniem, znajduje swoje najmocniejsze uwarunkowanie w wyroku Sądu Najwyższego z 22.03.2017 r. (III KK 349/16), w którym wskazano, że „przybliżenie karty płatniczej do terminalu skutkuje uzyskaniem dostępu do rachunku bankowego właściciela karty, dochodzi zatem do przełamania bariery elektronicznej w systemie bankowej płatności bezgotówkowej". Sąd Najwyższy nie dostrzegł powodu, by różnicować sytuacje dokonania płatności za pomocą wpisania kodu PIN i sytuacje, w których dochodzi jedynie do dokonania transakcji przy użyciu płatności zbliżeniowej. Wskazał bowiem na istotę zabezpieczenia samej karty płatniczej, podkreślając, że kod PIN jest istotnym zabezpieczeniem dostępu do środków zgromadzonych przez właściciela karty płatniczej, ale zabezpieczeniem dodatkowym. W ocenie Sądu Najwyższego pierwotne zabezpieczenie stanowi sama konstrukcja karty płatniczej, która zawiera mikroprocesor umożliwiający dokonywanie wszelkich transakcji, w tym również zbliżeniowych, bez użycia kodu PIN. Zgodnie z tym poglądem samo przybliżenie karty płatniczej do terminalu płatniczego prowadzi do uzyskania dostępu do rachunku bankowego właściciela karty, przez co dochodzi do przełamania bariery elektronicznej w systemie bankowej płatności bezgotówkowej.

Przeciwny pogląd prawny został wyrażony niewiele ponad dwa lata później w wyroku Sądu Apelacyjnego w Gdańsku z 27.11.2018 r.[38], w którym stwierdzono, że dokonanie płatności kartą płatniczą w formie płatności zbliżeniowej przez osobę nieuprawnioną 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. W uzasadnieniu takiego stanowiska podniesiono, że mikroprocesor nie pełni funkcji zabezpieczenia przed nieuprawnionym dostępem do środków pieniężnych, stanowi on bowiem „jedynie mechanizm umożliwiający komunikowanie się z systemem informatycznym banku". Sąd Apelacyjny podkreślił, że aktywując płatność zbliżeniową, „posiadacz karty płatniczej rezygnuje z zabezpieczenia karty kodem PIN do określonej kwoty z uwagi na szybkość i wygodę". Innymi słowy, posiadacz karty rezygnuje „z zabezpieczenia będącego przejawem jego woli ustanowienia bariery w dostępie do rzeczy", a to zaś powoduje, że „w przypadku płatności zbliżeniowej bez podania kodu PIN brak dwuetapowości działania sprawcy tak charakterystycznej dla kradzieży z włamaniem".

[38] Wyrok Sądu Apelacyjnego w Gdańsku z 27.11.2018 r. (II AKa 307/18), LEX nr 2690748. Podobnie wyrok Sądu Rejonowego w Grudziądzu z 29.10.2019 r. (II K 294/19), LEX nr 2758145.

Ujmując plastycznie analizę tego skomplikowanego problemu prawnego, Sąd Najwyższy przywołał przykład otwarcia drzwi w typowym pokoju hotelowym kluczem magnetycznym w formie plastikowej karty. Wychodząc bowiem od stwierdzenia, że posłużenie się takim kluczem przez sprawcę i dokonanie zaboru pozostawionych w pokoju przez klienta hotelu przedmiotów stanowi czyn stypizowany jako kradzież z włamaniem, analogicznie przyjęto w przypadku kradzieży karty płatniczej i dokonania płatności za towary metodą zbliżeniową. Z kolei Sąd Apelacyjny w Gdańsku użył obrazowego przykładu, porównując dokonanie płatności zbliżeniowej cudzą kartą do dokonania płatności za zakupy kolejnymi banknotami znajdującymi się w uprzednio skradzionym portfelu.

Ze stanowiskiem Sądu Najwyższego kwalifikującym omawiane zachowanie jako wypełniające znamiona kradzieży z włamaniem nie sposób się zgodzić. O ile nie ma wątpliwości, że dokonanie otwarcia drzwi kluczem magnetycznym kwalifikowane być powinno jako kradzież z włamaniem, o tyle nie można tego przykładu przenosić w drodze analogii na grunt problemu płatności zbliżeniowej. Funkcją karty magnetycznej jest zabezpieczenie dostępu do pokoju hotelowego, wobec czego pełni ona rolę tradycyjnego klucza. Funkcja zbliżeniowa karty płatniczej inicjuje jedynie proces przekazywania danych informatycznych, który dopiero po pozytywnej weryfikacji tzw. zapytania autoryzacyjnego przechodzi w fazę autoryzacji danej transakcji prowadzącą do zmiany danych na rachunku bankowym właściciela rachunku bankowego oraz podmiotu, na którego rzecz wpłynie określona kwota. Błędne zatem pozostaje podstawowe założenie, które legło u podstaw takiej argumentacji, a mianowicie to, że karta płatnicza sama w sobie zawiera zabezpieczenie przed dostępem do rachunku bankowego. Co prawda „kod jako swoisty i niepowtarzalny klucz elektroniczny zabezpieczający dostęp do konta bankowego danej osoby za pośrednictwem bankomatu wraz z kartą bankomatową stanowią przeszkodę do zawładnięcia mieniem innej osoby”[39], jednakże nie można podobnego wniosku przerzucać na grunt transakcji zbliżeniowej. Dokonanie płatności w tej formie nie wymaga użycia jakiejkolwiek siły fizycznej wobec zabezpieczeń, szczególnych umiejętności lub środków technicznych (elektronicznych), ani też żadnego wysiłku umysłowego. Następuje ono bowiem jedynie poprzez przyłożenie karty do czytnika. Niezasadnie zatem Sąd Najwyższy dokonał porównania dokonania płatności zbliżeniowej do otwarcia drzwi za pomocą karty magnetycznej. Problem bowiem jest w tym, że uwzględnienie technicznych aspektów karty płatniczej nie może prowadzić do wniosku, jakoby karta ta, sama w sobie, stanowiła zabezpieczenie rachunku bankowego. Analizując ten problem, należałoby zadać pytanie, czy otwarcie zamkniętych drzwi do pokoju przy użyciu klamki można kwalifikować tak samo jak otwarcie takich drzwi dorobionym kluczem bądź innym narzędziem, na które to pytanie odpowiedź negująca taką możliwość pozostaje oczywista.

[39] Wyrok Sądu Apelacyjnego we Wrocławiu z 9.07.2014 r.(II AKa 180/14), LEX nr 1506771.

Przyjęta przez Sąd Najwyższy teza stojąca u podstaw wzmiankowanego orzeczenia, jakoby mikroprocesor stanowił owo zabezpieczenie, pozostaje wobec tego co najmniej dyskusyjna, a nawet chybiona. Wydaje się, że większych wątpliwości nie budzi stwierdzenie, iż sam pasek magnetyczny, w jaki wyposażona jest karta płatnicza, nie stanowi zabezpieczenia w rozumieniu art. 279 § 1 k.k. Z kolei mikroprocesor to nowa generacja tradycyjnych kart z paskiem magnetycznym bądź też swoisty „pasek magnetyczny +", stanowiący nowy standard kart płatniczych, uwzględniający rozwój technologiczny i pozwalający na większe możliwości poprzez kompatybilność z terminalami płatniczymi oraz zapewniający większe bezpieczeństwo poprzez brak możliwości skopiowania mikroprocesora. Mikroprocesor to narzędzie chroniące informacje w nim przechowywane przed skopiowaniem ich przez inne osoby, nie zaś stanowiące barierę przed nieuprawnionym użyciem karty płatniczej. Wręcz przeciwnie, mikroprocesor działa automatycznie, aktywując kartę w czasie dokonywania transakcji, stanowiąc swego rodzaju przekaźnik, umożliwiający wpływ na przesył danych informatycznych. Tym samym mikroprocesor nie utrudnia dostępu do środków finansowych zgromadzonych na rachunku bankowym, ale ten dostęp umożliwia. Takie też stanowisko zajął TSUE w przywołanym na wstępie wyroku, wskazując, że funkcja NFC umożliwia, nie zaś zabezpiecza, dokonywanie płatności za towary. Istotą włamania jest pokonanie realnej, faktycznej przeszkody materialnej czy elektronicznej zabezpieczającej rzecz przed kradzieżą. Brak istnienia aktywnego zabezpieczenia powoduje, że niemożliwe jest przyjęcie realizacji znamion kradzieży z włamaniem. Aktywowanie płatności zbliżeniowych dezaktywuje konieczność każdorazowej autoryzacji transakcji za pomocą kodu PIN. Samo uwierzytelnienie transakcji bez konieczności autoryzacji należy traktować jako wyjęcie określonej kwoty z cudzego portfela, nie zaś jako przełamanie zabezpieczenia. Dopiero przekroczenie wartości dokonywanej płatności lub limitu transakcji zbliżeniowych powoduje konieczność wpisania kodu PIN, a co za tym idzie zasadność przyjęcia kwalifikacji kradzieży z włamaniem. Tym samym brak aktywnego zabezpieczenia dostępu do mienia dezaktualizuje możliwość przyjęcia realizacji znamienia „włamanie" w przypadku nieuprawnionego użycia karty płatniczej w formie płatności zbliżeniowej.

Trafnie przyjmuje się w orzecznictwie, że „nie stanowi kradzieży z włamaniem takie zachowanie sprawcy, który kradnie cudzą rzecz ruchomą, uniemożliwiając zadziałanie zabezpieczenia tejże rzeczy"[40]. Aktywacja płatności zbliżeniowej przez posiadacza karty powoduje naturalną konsekwencję w postaci rezygnacji ze stworzenia zewnętrznej bariery mającej na celu wykluczenie dostępu do mienia przez osoby nieuprawnione do wysokości określonej kwoty, wobec czego nie można mówić o realizacji przez sprawcę jednego z konstytutywnych elementów składających się na „włamanie", a mianowicie zaboru mienia po uprzednim przełamaniu chroniącego go zabezpieczenia, co słusznie zauważa

[40] Postanowienie SN z 29.10.2012 r.(I KZP 11/12), „Prokuratura i Prawo" 2013/2, wkładka, poz. 3.

Sąd Apelacyjny w Gdańsku. W takim przypadku dopiero zablokowanie karty przez jej posiadacza będzie stanowić manifestację dysponenta rzeczy woli zabezpieczenia jej przed innymi osobami. Tym samym na błędnej konstrukcji logicznej oparte zostało także stanowisko Sądu Apelacyjnego w Gdańsku w wyroku z 2.04.2019 r.[41], kwestionujące zasadność zróżnicowania kwalifikacji prawnej w przypadku dokonywania płatności zbliżeniowej przez osobę nieuprawnioną i dokonywania takiej płatności z użyciem kodu PIN, w dalszej zaś kolejności podzielające przedstawione powyżej stanowisko Sądu Najwyższego. Argumentację ku temu ma stanowić fakt, że niejednokrotnie „terminal nie realizuje płatności zbliżeniowych, pomimo że karta płatnicza ma charakter zbliżeniowy, a kwota płatności nie przekracza 50 zł i dla zrealizowania takiej płatności wymagany jest kod PIN". Otóż należy zauważyć, że takie sytuacje będą miały miejsce wówczas, gdy zostanie przekroczony limit transakcji, których można dokonać w formie płatności zbliżeniowej. Przenosząc problem na grunt obrazowy: kradzież radia z otwartego samochodu (np. wówczas, gdy drzwi pojazdu nie zostały zamknięte za pomocą kluczyka lub pilota) kwalifikowana będzie z art. 278 § 1 k.k., jednakże zamknięcie pojazdu powoduje, że dokonanie kradzieży będzie powodowało konieczność przyjęcia kwalifikacji z art. 279 § 1 k.k.

Nie sposób także zgodzić się z twierdzeniem Sądu Rejonowego w Grudziądzu, jakoby zbliżenie karty do terminalu powodowało „sforsowanie zabezpieczenia w postaci procesora umieszczonego w karcie płatniczej"[42]. Zbliżenie karty do terminalu to bowiem nic innego jak sposób płatności analogiczny do przekazania banknotu sprzedawcy. Nie mają zatem racji M. Małecki i P. Dudek, twierdząc, że „złodziej zbliżający do terminalu cudzą kartę wbrew woli jej posiadacza dokonuje uwierzytelnienia transakcji i już tym sposobem bezprawnie pokonuje zabezpieczenie dostępu do pieniędzy (zapisów w systemie informatycznym)"[43]. Nie sposób przecież przyjąć, aby sprawca w momencie przekazywania sprzedawcy banknotu stanowiącego zapłatę za nabywany towar lub usługę dokonywał przełamania zabezpieczenia, są to bowiem dwa różne etapy transakcji płatniczej. Terminal nie stanowi zamkniętego pomieszczenia ani jego surogatu. Co więcej, terminal płatniczy nie stanowi miejsca przechowywania środków finansowych, ale pozwala „jedynie" na przyjmowanie płatności.

Podsumowując tę część rozważań, należy stwierdzić, że dla ustalenia prawidłowej kwalifikacji prawnej zachowania polegającego na dokonaniu płatności zbliżeniowej cudzą kartą płatniczą zasadnicze znaczenie ma prawidłowe odkodowanie technicznego aspektu systemu płatności bezgotówkowych. Nie budzi przy tym wątpliwości, że nieuprawnione użycie karty zbliżeniowej w celu zapłaty za nabywane rzeczy może zostać zakwalifikowane jako realizujące znamiona kradzieży, sprawca bowiem włącza do swojego majątku towary, za które płaci kosztem środków finansowych zdeponowanych na cudzym ra-

[41] Wyrok Sądu Apelacyjnego w Gdańsku z 2.04.2019 r.(II AKa 9/19), LEX nr 3222745.
[42] Wyrok Sądu Rejonowego w Grudziądzu z 29.10.2019 r. (II K 294/19), LEX nr 2758145.
[43] M. Małecki, P. Dudek, *Paragrafy...*

chunku bankowym. Niemniej użycie cudzej karty płatniczej w formie płatności zbliżeniowej nie prowadzi do przełamania bariery elektronicznej w systemie bankowej płatności bezgotówkowej, chodzi tu bowiem o formę płatności, ale nie o zabezpieczenie środków na rachunku bankowym.

DOKONANIE PŁATNOŚCI ZBLIŻENIOWEJ JAKO OSZUSTWO?

Czy zapłata za zakupiony towar lub usługi cudzą kartą płatniczą przy wykorzystaniu jej funkcji zbliżeniowej może być kwalifikowana jako oszustwo lub oszustwo komputerowe? Niewątpliwie w praktyce przypadki takiej kwalifikacji nie należą do rzadkości. Bez trudu można bowiem odnaleźć orzeczenia sądów przyjmujące w takim przypadku realizację znamion z art. 286 § 1 k.k. lub art. 287 § 1 k.k.

W mojej ocenie przyjęcie kwalifikacji z art. 286 k.k. jest co najmniej wątpliwe. Zauważyć bowiem trzeba, że do znamion oszustwa należą wprowadzenie określonej osoby w błąd albo też wyzyskanie jej błędu. Powstaje zatem pytanie, kogo sprawca wprowadza w błąd tudzież czyj błąd wykorzystuje, dokonując płatności zbliżeniowej. Trudno uznać, aby tym koniecznym dla realizacji znamion oszustwa tzw. czynnikiem ludzkim był sprzedawca w sklepie, posiadacz rachunku bankowego czy też pracownik banku. Podobnie, nie można zasadnie twierdzić, aby sprawca wyzyskiwał błąd sprzedawcy co do tego, że jest uprawniony do posługiwania się kartą, sprzedawca nie jest bowiem przedstawicielem banku czy właściciela rachunku bankowego i nie legitymuje się upoważnieniem do rozporządzania środkami pieniężnymi znajdującymi się na rachunku bankowym określonej osoby. Jego rola sprowadza się do fizycznego wydania towaru ze sklepu, która to czynność co prawda stanowi rozporządzenie, ale nie można jej uznać za rozporządzenie niekorzystne w świetle interesów właściciela sklepu. Co prawda zgodnie z art. 59b ustawy o usługach płatniczych akceptant przy dokonywaniu płatności z użyciem karty płatniczej identyfikującej osobę upoważnioną do jej używania może żądać okazania przez osobę korzystającą z tej karty dokumentu potwierdzającego jej tożsamość, aczkolwiek takie sytuacje nie wystąpią często w praktyce. Będzie to miało miejsce przykładowo bezpośrednio po dokonaniu kradzieży karty płatniczej. Jednakże nawet w przypadku, gdy kasjer dostrzegł, że karta została skradziona, a następnie udostępnił terminal sprawcy tej kradzieży, trudno zasadnie przyjmować realizację czynu z art. 286 § 1 k.k., problematyczne pozostaje bowiem określenie osoby, która została wprowadzona w błąd lub też której błąd wykorzystano. Nie będzie taką osobą kasjer, nieprzeszkodzenie bowiem przez niego w realizacji transakcji mogłoby być wartościowane prawnokarnie jako pomocnictwo w realizacji czynu zabronionego, nie można zaś wprowadzić w błąd samego siebie lub też wyzyskać własnego błędu[44]. Należy zatem stwierdzić, że zachowanie kasjera mogłoby być oceniane jako pomocnictwo w kradzieży (art. 18 § 3 k.k. w zw. z art. 278 § 1 k.k.).

[44] Podzielam w tym zakresie stanowisko M. Małeckiego i P. Dudka, *Paragrafy...*

Z kolei przepis art. 287 § 1 k.k. penalizuje tzw. oszustwo komputerowe i „znajduje zastosowanie, gdy przedmiotem czynności wykonawczej jest bezpośrednio zapis danych informatycznych, nie zaś kiedy działanie sprawcy powoduje w rezultacie zmianę tych danych”[45]. Zgodnie ze wskazanym przepisem karze podlega ten, kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych.

Przykładem orzeczenia, w którym dokonanie płatności w formie zbliżeniowej cudzą kartą płatniczą zakwalifikowano jako realizujące znamiona czynu z art. 287 § 1 k.k., jest wyrok Sądu Okręgowego w Gliwicach z 29.09. 2017 r.[46] W wyroku tym sąd uznał, że „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.”. Sąd odwoławczy wskazał, że w przypadku zastrzeżonej karty zbliżeniowej przestępstwo oszustwa komputerowego nie zostaje popełnione w chwili przyłożenia tejże karty do terminalu płatniczego w sklepie, skutkiem przestępstwa z art. 287 § 1 k.k. jest bowiem dokonanie wpływu w procesie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych, a zatem dokonanie zmiany przez sprawcę w autentycznym procesie przetwarzania, gromadzenia lub przekazywania danych informatycznych, która powoduje, że ich gromadzenie, przetwarzanie lub przekazywanie odbywa się w inny sposób, niż był założony. Zastrzeżenie karty przez właściciela rachunku bankowego powoduje, że przybliżenie do terminalu karty płatniczej nie doprowadza do żadnej zmiany w procesie obróbki danych informatycznych na rachunku bankowym należącym do właściciela karty, uniemożliwia bowiem jakąkolwiek ingerencję w dane informatyczne zapisane na rachunku bankowym posiadacza karty. Jednocześnie sąd w przywołanym wyroku zakwestionował możliwość przyjęcia w takiej sytuacji kwalifikacji z art. 279 § 1 k.k., karta bankomatowa nie umożliwia bowiem przełamania przeszkody elektronicznej chroniącej dostęp do rachunku bankowego, przyłożenie zaś karty zbliżeniowej do terminalu nie może być uznane za przełamanie zamkniętego pomieszczenia, terminal nie jest bowiem zamkniętym pomieszczeniem chroniącym dostęp do zgromadzonych na rachunku bankowym jakiegoś podmiotu środków pieniężnych. W ocenie sądu przyłożenie karty zbliżeniowej do terminalu płatniczego powoduje automatyczny przesył danych informatycznych pomiędzy rachunkiem właściciela sklepu a rachunkiem właściciela karty, sprawca zaś w wyniku takiego działania otrzymuje korzyść majątkową w postaci zakupionego towaru.

[45] B. Gadecki, *Kradzież i użycie karty bankomatowej oraz karty płatniczej (wybrane zagadnienia praktyczne)*, „Przegląd Policyjny” 2016/1, s. 153.

[46] Wyrok Sądu Okręgowego w Gliwicach z 29.09.2017 r. (VI Ka 639/17), LEX nr 2396474.

Wydaje się, że zasadnicze znaczenie dla przyjęcia określonej kwalifikacji prawnej ma znamię czynnościowe „wpływa", które według ujęcia słownikowego oznacza wywarcie na kogoś lub coś wpływu, nacisku, oddziaływanie na kogoś lub coś, dostanie się gdzieś lub do czegoś[47]. Przywołując stanowisko M. Dąbrowskiej-Kardas i P. Kardasa, należy podkreślić, że wpływanie to „dokonywanie zmiany przez sprawcę w autentycznym procesie przetwarzania, gromadzenia lub przekazywania danych informatycznych, która powoduje, że ich gromadzenie, przetwarzanie lub przekazywanie odbywa się w inny sposób, niż był założony"[48]. W przypadku płatności zbliżeniowej – w mojej ocenie – nie sposób uznać, aby sprawca „wpływał", dokonując zniekształcenia bądź innej transformacji automatycznego procesu rozliczeniowego. Ten proces przebiegać bowiem będzie dokładnie w ten sam sposób, jak w przypadku dokonania płatności przez osobę uprawnioną. Sam mechanizm płatności, w tym uwierzytelniania i autoryzacji, nie ulegnie zmianie. Sprawca nie utrudnia jego przebiegu, nie zniekształca ani go nie uniemożliwia, ale powoduje „jedynie" uszczuplenie zgromadzonych na rachunku bankowym środków finansowych określonej osoby na jego rzecz. Jednakże użycie karty płatniczej przez podmiot uprawniony spowodowałoby takie uszczuplenie dokładnie w ten sam sposób i dokładnie przy działaniu tego samego mechanizmu, a jedynie na rzecz innej osoby. Trudno także uznać, aby sprawca wprowadzał w systemie informatycznym banku nowe zapisy danych informatycznych, działanie osoby nieuprawnionej do korzystania z karty płatniczej nie polega bowiem na wprowadzeniu nowych danych, ale na uruchomieniu technicznego schematu płatności, którego dopiero końcowym etapem będzie automatyczny nowy zapis danych.

WNIOSKI

Konsekwencją powyższych rozważań jest stwierdzenie, że prawidłową kwalifikacją prawną czynu polegającego na nieautoryzowanym wykorzystaniu funkcji zbliżeniowej karty płatniczej jest art. 278 § 1 k.k. Funkcja zbliżeniowa karty płatniczej nie stanowi bowiem zabezpieczenia, wobec czego nie dochodzi do realizacji znamienia włamania. Argumentacji za przyjęciem realizacji znamion kradzieży z włamaniem w przypadku płatności zbliżeniowej w żadnym razie nie może stanowić postulat jednorodności kwalifikacji prawnej zaboru pieniędzy za pomocą karty płatniczej. Sposób dokonania czynu zabronionego wpływa bowiem na stopień społecznej szkodliwości czynu. Ponadto taka argumentacja może prowadzić do wniosku, że zabór portfela niezależnie od tego, czy dokonany jest po uprzednim sforsowaniu zabezpieczenia lokalu mieszkalnego, czy też poprzez wyjęcie z niezabezpieczonej torebki, nie powinien wpływać na kwalifikację prawną czynu, z czym w sposób naturalny nie można się zgodzić. Niemniej jednak po analizie orzecznictwa sądów powszechnych wydaje

[47] *Słownik...*, red. M. Szymczak, s. 703.

[48] M. Dąbrowska-Kardas, P. Kardas (w:) *Kodeks...*, komentarz do art. 287.

się słuszna konstatacja Sądu Apelacyjnego w Lublinie w wyroku z 20.12.2019 r. (II AKa 235/19) wskazująca, że aktualnie dominujący okazał się pogląd przyjmowania w przypadku dokonania przez osobę nieuprawnioną płatności zbliżeniowej kwalifikacji prawnej z art. 279 § 1 k.k. Niewątpliwie znaczenie w tym wypadku ma autorytet najwyższej instancji sądowej. Niemniej jednak stanowisko takie w kontekście przywołanej argumentacji należy ocenić jako nietrafne.

ABSTRACT

Anna Czesnowicka

The author is a graduate of the administration and law of the Faculty of Law and Administration of the Jagiellonian University, deputy judge District Court for the Metropolitan City of Warsaw in Warsaw.

The penality of unauthorised contactless transactions – legal qualification of contactless payments with appropriated payment cards

While cashless payments market is steadily increasing its range and gross value, it simultaneously poses new safety challenges. One of the most common offences over the last few years have been unathorised contactless payments that allow for the closing the transaction by touching the card to the terminal without the use of such measures as entering the PIN number, signing the receipt or passing the card through the scanner. While innovative payment technologies take over the market, therefore, it is expedient to search for efficient legal instruments by applicable interpretation of already existing regulations, involving the fitting legal qualification of illegal electronic transactions. The following article presents a discussion of the matter, preceded by an analysis of the question whether contactless payments inherently pre-empt electronic bank safety measures, and an overview of the technological aspects of contactless payments.

Keywords: *unathorised contactless payments, payment card, robbery, burglary, fraud*

Anna Czesnowicka
ORCID: 0000-0001-9604-5729; e-mail: aniaczesnowicka@wp.pl

Autorka jest absolwentką administracji i prawa Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego, asesorem sądowym Sądu Rejonowego dla m.st. Warszawy w Warszawie

BIBLIOGRAFIA ZAŁĄCZNIKOWA

Dąbrowska-Kardas Małgorzata, Kardas Piotr (w:) *Kodeks karny. Część szczególna*, t. 3, *Komentarz do art. 278–363 k.k.*, red. W. Wróbel, A. Zoll, Warszawa 2022, komentarz do art. 279

Gadecki Bartłomiej, *Kradzież i użycie karty bankomatowej oraz karty płatniczej (wybrane zagadnienia praktyczne)*, „Przegląd Policyjny" 2016/1

Grabowski Michał, *Instrumenty płatnicze w prawie polskim*, rozprawa doktorska, Uniwersytet Warszawski, Wydział Prawa i Administracji, Instytut Nauk Prawno-Administracyjnych, Warszawa 2013

Kardas Piotr, Satko Jacek, *Przestępstwa przeciwko mieniu: przegląd problematyki, orzecznictwo (SN 1918–2000, piśmiennictwo)*, Kraków 2002

Kodeks karny. Komentarz aktualizowany, red. M. Mozgawa, komentarz do art. 279 k.k.

Kruk Maciej, *Pojęcie „włamanie" w świetle transakcji zbliżeniowej – uwagi na tle wyroku Sądu Najwyższego z 22.03.2017 r., III KK 349/16*, „Ius Novum" 2019/4, s. 83

Małecki Mikołaj, Dudek Paweł, *Paragrafy adaptują się do technologii*, „Rzeczpospolita – Rzecz o prawie" z 13.02.2018 r.

Marek Andrzej, *Kodeks karny. Komentarz*, Warszawa 2010, komentarz do art. 279

Michór Andrzej, *Karty płatnicze* (w:) *Problemy współczesnej bankowości*, red. Góralczyk Wojciech, Warszawa 2014

Opitek Paweł, *Kwalifikacja prawna przestępstw związanych z transakcjami kartą płatniczą*, „Prokuratura i Prawo" 2017/2

Słownik języka polskiego, t. 3, red. M. Szymczak, Warszawa 1983

Ślązak Emil, *Nowoczesne instrumenty płatnicze* (w:) *Bankowość detaliczna*, red. J. Koleśniak, Warszawa 2016

Uniwersalny słownik języka polskiego, t. 4, red. S. Dubisz, Warszawa 2003

Wróblewski Jerzy, *Kradzież z włamaniem. Z zagadnień rozumienia tekstów prawnych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1966/2