RUCH PRAWNICZY, EKONOMICZNY I SOCJOLOGICZNY
Rok LXIV — zeszyt 2 — 2002

MAREK PRENGEL

TECHNICZNO-FINANSOWE ASPEKTY PRZESTĘPCZEGO WYKORZYSTANIA TZW. NOWYCH TECHNOLOGII PŁATNICZYCH W DOBIE GLOBALIZACJI NA PRZYKŁADZIE PRANIA PIENIĘDZY*

1. MIĘDZYNARODOWO DZIAŁAJĄCA PRZESTĘPCZOŚĆ ZORGANIZOWANA W EPOCE GLOBALIZACJI

W toku globalizacji pokonuje ogromne odległości i przekracza granice państw nie tylko kapitał lub towar legalnego pochodzenia, turystyka wypoczynkowa albo szukająca pracy ludność, lecz także przestępcy i nielegalne towary oraz „brudny" kapitał[1].

W przeciągu ostatnich dziesięcioleci miała miejsce wzmożona internacjonalizacja (umiędzynarodowienie) przestępczości zorganizowanej i jej nieuniknione następstwo, internacjonalizacja prania pieniędzy[2]. Najważniejszym czynnikiem wpływającym na umiędzynarodowienie przestępczości i jej zwalczanie jest wzrastające ułatwienie międzynarodowej współpracy i rozwoju w dziedzinie przepływu informacji i technologii[3]. Obecnie nie ma większych problemów z dotarciem, w stosunkowo krótkim czasie niemal każdego punktu kuli ziemskiej. Postęp w wielu dziedzinach pozwala przestępczości zorganizowanej, działającej „ponad granicami" poszczególnych państw, względnie łatwo planować popełnianie przestępstw i je dokonywać[4]. Komputer i możliwości, jakie stwarza Internet, otwierają przed przestępczością zorganizowaną niemal nieograniczone perspektywy. Podsumowując: internacjonalizacja przestępczości odbywa się przy udziale rozwoju w dzie-

* Autor dziękuje za wieloletnią opiekę naukową zarówno Czcigodnemu Panu Profesorowi Andrzejowi Markowi z Katedry Prawa Karnego i Kryminologii Uniwersytetu im. Mikołaja Kopernika w Toruniu, jak również Fundacji Gottlieb Daimler- und Karl Benz-Stiftung z Ladenburga.

[1] Por. „Neue Zürcher Zeitung" (NZZ) 9/10 czerwiec 1985, s. 11. Zob. także A. Wöß, *Geldwäscherei und Banken, Methoden und Formen*, Europarecht, Anpassungsbedarf für Österreichs Banken, Wien 1994, s. 21 - 22; L. Violante, *Das Organisierte Verbrechen, Ein europäisches Problem*, w: Friedrich-Ebert-Stiftung (wyd.), *Strategien und Gegenstrategien*, Organisierte Kriminalität in Deutschland und Italien, Dokumentation, Berlin 1993, s. 25 - 26; K. Schelter, *Innere Sicherheit in einem Europa ohne Grenzen, Illusion oder realistisches Ziel einer entschlossenen Politik?*, w: R. C. Meier-Walser i n. (red.), *Organisierte Kriminalität, Bestandsaufnahme, Transnationale Dimension, Wege der Bekämpfung*, München 1999, s. 15 i n.

[2] Zob. H. U. Endres, *Internationale Verbrechensbekämpfung, Verfassungs- and verwaltungsrechtliche Probleme*, München 1990, s. 5 i n.

[3] Zob. Endres, *Verbrechensbekämpfung* (monografia). Por. także Dyrektywę Rady EWG z 10 czerwca 1991, w: A. Fülbier, R. R. Aepfelbach, *Kommentar zum Geldwäschegesetz*, wyd. 4, Köln 1999, s. 471 oraz B. Bukovc, *Die Bekampfung der Geldwäsche in der Europäischen Union*, Schriftenreihe Euro-Jus, t. 1, Manz 1998, s. 5, 11, 38; M. Mirak-Weißbach, *Der gerechte Krieg, Das Rauschgiftkartell besiegen*, Wiesbaden 1990, s. 185 i n.

[4] Pod. Violante, *Problem*, s. 25 - 26. Zob. C. Kern, *Geldwäsche und organisierte Kriminalität*, Regensburg 1993, s. 5; Wöß, *Geldwäscherei*, s. 21 - 22.

dzinie technologii, z którego korzysta światowy handel i wszelkiego rodzaju współpraca między poszczególnymi państwami.

2. TRANSAKCJE PRZEPROWADZANE W RAMACH TZW. NOWYCH TECHNOLOGII PŁATNICZYCH

2.1. Przedstawienie problemu

Wyróżnia się trzy najważniejsze techniczne systemy płatnicze w ramach tzw. nowych technologii płatniczych, które są szczególnie atrakcyjne w procederze prania pieniędzy, są to[5]:

— system oparty na tzw. zasadzie jednolitości, tj. sieci zamkniętej z powszechnie znanymi uczestnikami;
— system „smart card" zwany systemem kart chipowych (zaopatrzone w chip karty płatnicze do ponownego „załadowania");
— otwarty system płatniczy (rozrachunkowy): przeprowadzanie operacji przy użyciu takich sieci, jak np. Internetu[6].

W niniejszych rozważaniach istotne jest znalezienie odpowiedzi na dwa podstawowe pytania. Po pierwsze – czy będzie można ulokować wartości majątkowe za granicą przy wykorzystaniu tych systemów. Po drugie – czy będzie wiązało się to z możliwością prześledzenia śladu na „papierze" (w dokumentacji) – zwanego w literaturze paper trail – względnie śladu „elektronicznego" (np. na twardym dysku komputera) – tzw. electronic trail – po przeprowadzanych operacjach finansowych[7]? Istnienie tego „śladu" zaprowadzi organy ścigania nie tylko do „pracza", lecz również do sprawcy przestępstwa pierwotnego, najczęściej parającego się handlem narkotykami.

Pierwszy z nich, system płatniczy oparty na tzw. zasadzie jednolitości, wykorzystuje się od dłuższego czasu do przemieszczania wartości majątkowych. Zazwyczaj można ustalić, kto był zlecającym przekaz, a kto jego odbiorcą. W związku z powyższym jego nadużycie do prania pieniędzy będzie praktycznie ograniczone.

W kolejnym systemie, „napełnianie" pieniądzem depozytowym (księgowym) lub elektronicznym kart chipowych (smart card) jest porównywalne z pobraniem gotówki z rachunku bankowego. Co prawda, w banku zostanie zarejestrowany przepływ pobranej sumy z danej karty, natomiast jest niemożliwe ustalenie na podstawie tejże ewidencji, kto kartę „napełnił", względnie później ją użył: jest to najsłabszy punkt, który daje możliwość wykorzystania tej karty przez osobę piorącą pieniądze w momencie zapłaty z jej użyciem.

---

[5] Zob. P. Hoyer, J. Klos, *Regelungen zur Bekämpfung der Geldwäsche und ihre Anwendung in der Praxis*, wyd. 2, Bielefeld 1998, s. 21 i n.

[6] Zob. NZZ 17 czerwiec 1997, s. B1 i n.; NZZ 14 lipiec 1997, s. 7; E. Kube, *Technische Entwicklung und neue Kriminalitätsformen*, „Kriminalistik" 10/1996, s. 618 i n.

[7] Por. Mirek-Weißbach, *Krieg*, s. 185 i n. W dalszych wywodach zostanie użyte wyłącznie określenie paper trail.

W kwestii wykorzystania ostatniego z wyżej wymienionych systemów płatniczych do prania pieniędzy Ackermann jest zdania, iż szybki rozwój Internetu wiąże się jedynie z obawami jego przestępczego wykorzystania[8]. W istocie rzeczy transakcje finansowe przeprowadza się nie tylko w tzw. zamkniętych sieciach, lecz również w Internecie. Jednakże przeprowadzanie legalnych transakcji finansowych w otwartych sieciach nie zyskało jeszcze na popularności. Powodem tego stanu rzeczy jest brak zadowalających systemów zabezpieczeń tych ostatnich tak, aby zabezpieczyć w stopniu wystarczającym dostęp osób niepowołanych do korzystania z nie przeznaczonych dla nich danych, np. numerów kart kredytowych podawanych wsieci[9]. W 1998 Ackermann był przekonany, iż wykorzystanie tzw. otwartych sieci do celów przestępczych, w tym do prania pieniędzy, będzie nieuniknioną czekającą nas niedługo przyszłością[10]. Obecnie można bez wahań rzec, że stało się to już rzeczywistością.

W istocie rozrachunek z wykorzystaniem tzw. otwartych sieci, np. Internatu, do niedawna odgrywał mało znaczącą rolę. Było to wynikiem braku możliwości wystarczającego zabezpieczenia przepływu wszelkich danych. Pewne trudności występowały przy tzw. autentyfikacji; związane ze stwierdzeniem osoby uprawnionej. Obecnie przezwyciężono większość z wyżej wymienionych problemów techniczno-finansowych tak, iż Internet stwarza nieograniczone możliwości dla nowoczesnych systemów finansowo-rozliczeniowych[11]. Większość z liczących się w świecie banków lub innych instytucji finansowych wkroczyła w erę Internet bankingu[12]. Otwarte systemy płatnicze obecnie wykorzystuje się do transferu wszelkich wartości majątkowych, w tym „brudnych". Ważną kwestią jest możliwość prześledzenia paper trail. W kryptologicznych pracach naukowo-badawczych rozważa się możliwość przeciwdziałania wykorzystania anonimowych systemów płatniczych dla celów prania pieniędzy i propozycji technicznych rozwiązań umożliwiających tam, gdzie zachodzi potrzeba zniesienia anonimowości poszczególnych operacji, np. przez wprowadzenie jako ogniw pośrednich upoważnionych do tego osób trzecich[13]. Nie jest jeszcze jasne, jakich digitalnych systemów płatniczych powinno to dotyczyć i za pomocą, jakich metod zniesienia anonimowości będzie się to odbywało. Duże praktyczne znaczenie dla korzystania z otwartych systemów płatniczych do przepływu wartości majątkowych, szczególnie „ponad granicami" państwowymi, ma możliwość prześledzenia paper trail, gdyż to właśnie one dają nowe dotychczas jeszcze mało znane możliwości szybkiego, anonimowego i bezpiecznego przeprowadzenia procesu prania pieniędzy. Wykorzystanie otwartych systemów płatniczych do wewnątrzkrajowego prania pieniędzy będzie odgrywało rolę drugoplanową.

---

[8] Zob. J.-B. Ackermann i in., *Kommentar, Einziehung – Organisiertes Verbrechen – Geldwäscherei*, t. 1, Zürich 1998, s. 533.

[9] Szerzej Raepple, *Sicherheitskonzepte für das Internet, Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung*, wyd. 1, Heidelberg 1998 (monografia); G. Müller, K.-H. Stapf (red.), *Mehrseitige Sicherheit in der Kommunikationstechnik*, t. 2, Erwartung, Akzeptanz, Nutzung, Bonn 1998 (monografia).

[10] Ackermann, *Kommentar*, s. 533.

[11] Por. Ackermann, *Kommentar*, s. 533.

[12] Zob. D. Rosenthal, *Projekt im Internet*, Zürich 1997, s. 320 - 321.

[13] Pod. Ackermann, *Kommentar*, s. 533.

Studia typologiczne Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (Financial Action Task Force on Money Laundering »FATF«) przeprowadzone w latach 1997 - 1998 wskazują na aktualne tendencje prania pieniędzy, ze szczególnym uwzględnieniem nowych systemów i technologii[14]. W jednym z zaleceń (zalecenie nr 13 znowelizowane 28 czerwca 1996) FATF apeluje o wczesne wykrywanie niebezpieczeństw związanych z wykorzystaniem nowych technologii i o przedsiębranie odpowiednich środków do przeciwdziałania ich wykorzystania do prania pieniędzy[15].

Chociaż w dziedzinie nowych technologii płatniczych, w szczególności: „elektronicznych giełd pieniężnych", direct bankingu lub operacji bankowych w Internecie, nie wykryto jak dotychczas przypadków prania pieniędzy, to eksperci FATF zwracają uwagę na istniejące wysokie zagrożenie wykorzystania ich w tym celu. Szybki, tani i powszechny dostęp do nowych technologii, które z jednej strony są niezbędnymi elementami rozwoju nowoczesnego systemu gospodarczego, z drugiej strony sprzyjają nadużyciu i utrudnieniu zwalczania przestępczości zorganizowanej.

Konieczność wnikliwej kontroli nad nowymi technologiami płatniczymi w aspekcie prania pieniędzy jest spowodowana nie tylko dynamicznym rozwojem tej dziedziny, lecz również błyskawicznym rozprzestrzenianiem się technologii. Obie tendencje dają coraz to nowe możliwości wraz z powszechniejszym i tańszym do nich dostępem. Największe banki (np. w Szwecji) posiadają setki tysięcy klientów mających otwarty rachunek bankowy w Internecie, dający możliwość dwudziestoczterogodzinnego dostępu do prawie wszystkich usług bankowych: coraz więcej instytucji finansowych proponuje swoim klientom własne strony internatowe z tzw. wirtualnym stanowiskiem bankowym, umożliwiającym dokonanie większości tradycyjnych operacji finansowych, jak np. sprawdzenie stanu rachunku, przekaz lub innych. W niektórych państwach usługi są ograniczone do wewnątrzkrajowych operacji finansowych[16].

2.2. „Elektroniczne giełdy pieniężne"

Powszechnie używany termin „elektroniczne giełdy pieniężne" należy do tzw. pojęć nieostrych. Pozwoli on się przybliżyć przez inny termin „z góry zapłacone karty" (prepaid cards). „Elektroniczne giełdy pieniężne", tj. multi-purpose prepaid cards, są nieimiennymi (personalnie neutralnymi) kartami o charakterze globalnym (światowym), na których „zapisano" elektronicznie sumy pieniężne po to, aby móc z ich pomocą dokonywać operacji finansowych. Tradycyjne karty kredytowo-debitowe służą do identyfikacji dostępu do związanego z nimi rachunku bankowego i umożliwiają

[14] Por. W. Jasiński, *Nowe zalecenia Grupy Specjalnej ds. Przeciwdziałania Praniu Brudnych Pieniędzy*, „Przegląd Ustawodawstwa Gospodarczego" 10/1997, s. 10 i n.; Hoyer, Klos, *Regelungen*, s. 21.

[15] Zalecenie nr 13 omawia Hoyer, Klos, *Regelungen*, s. 38 i n., 551 i n., a także Jasiński, *Nowe zalecenia*, s. 10.

[16] Por. Hoyer, Klos, *Regelungen*, s. 22.

„zapisanie" na nich znacznie mniejszych sum pieniężnych, w przeciwieństwie do „elektronicznych giełd pieniężnych"[17]. Te ostatnie występują pod postacią karty chipowej, combi card, karty pieniężnej, pay card, p-card, smart card, system card i innych kart służących zwłaszcza do zapłaty za towary i usługi. Jako karty o charakterze globalnym (światowym) z szerokim zakresem użytkowania są one częścią tzw. trójstronnego systemu składającego się z emitenta karty, akceptanta karty i posiadacza karty[18].

Możliwość realizacji tzw. płynnego (float) zysku stanowi finansowe uzasadnienie interesu do wydania prepaid cards. Korzyść ta pochodzi z oprocentowania równowartości będącej do dyspozycji emitenta od momentu „załadowania" karty aż do dokonania zapłaty z jej użyciem i zaspokojenia roszczenia akceptanta. Dodatkowym elementem jest zaoszczędzenie wydatków, związanych ze zwyczajnym obrotem gotówkowym, jak np. koszty przechowywania, transportu lub bezpieczeństwa. Posiadacz „elektronicznej giełdy pieniężnej" płaci z góry (w momencie „załadowania" karty) emitentowi równowartość „zapisanych" na karcie jednostek rozliczeniowych. Suma stanowiąca zawartość karty pełni rolę elektronicznych jednostek rozliczeniowych stanowiących roszczenie każdorazowego ich dysponenta względem emitenta przenaszalne bez ograniczeń na inne podmioty: wszelkie roszczenia innych podmiotów względem posiadacza karty mogą zostać zaspokojone z samej karty[19].

Zasadniczo zadaniem „elektronicznych giełd pieniężnych" jest substytucja pieniądza gotówkowego, choć są one bardziej uniwersalnym nośnikiem wartości niż sam pieniądz gotówkowy. Z tego powodu wydają się budzić szczególne zainteresowanie wśród osób piorących pieniądze. Tradycyjne karty pieniężne nie posiadają tak dużej atrakcyjności dla piorącego pieniądze chociażby ze względu na mniejszą mobilność i anonimowość, a pozostawiany po dokonanych z ich pomocą operacjach paper trail, umożliwia dojście do sprawcy prania pieniędzy, a nierzadko do sprawców przestępstw pierwotnych poprzedzających pranie pieniędzy[20].

Dla oceny potencjalnego zagrożenia praniem pieniędzy duże znaczenie ma podział kart pieniężnych na imienne (spersonifikowane), tj. związane z posiadanym rachunkiem rozliczeniowym (ec-karta, karta bankowa z funkcją giełdy pieniężnej) i nieimienne (niespersonifikowane) w postaci karty wartościowej z funkcją giełdy pieniężnej[21].

W przypadku karty pieniężnej imiennej zapłata z jej użyciem następuje podobnie jak przy zapłacie pieniądzem gotówkowym. Jednostki rozliczeniowe znajdujące się na karcie zostaną potrącone o sumę stanowiącą tytuł zapłaty, jednakże bez identyfikacji posiadacza karty. Natomiast sam proces

---

[17] Zob. J. Krzyżewski, *Obrót pieniężny przy użyciu kart płatniczych i kredytowych*, „Prawo Bankowe" 2/1997, s. 80 i n.

[18] Pod. Hoyer, Klos, *Regelungen*, s. 22; M. Findeisen, *Geldwäschebekämpfung im Zeitalter des Electronic Banking*, „Kriminalistik" 2/1998, s. 113 - 114.

[19] Hoyer, Klos, *Regelungen*, s. 23; Findeisen, *Zeitalter*, s. 113 - 114.

[20] Zob. Hoyer, Klos, *Regelungen*, s. 23.

[21] Ibidem, s. 23.

„załadowania" karty odbywa się bezgotówkowo przy terminalu, który pozostawia po dokonanej operacji paper trail, będący następstwem autoryzacji w systemie on line: podobnie jak w przypadku pobrania pieniądza gotówkowego z bankomatów.

Karty pieniężne w formie nieimiennej są związane z rachunkiem rozliczeniowym karty wartościowej, tzw. white card, które mogą zostać „załadowane" w terminalu za pobraniem pieniądza gotówkowego. Podczas tej operacji nie ma miejsca żadnego rodzaju identyfikacja posiadacza karty lub jej użytkownika. Zarówno proces „załadowania", jak i późniejsze operacje płatnicze z jej użyciem, odbywają się w pełni anonimowo.

Zdaniem ekspertów FATF powstawanie „elektronicznych giełd pieniężnych" przedstawia poważne zagrożenie wykorzystania ich do celów prania pieniędzy, szczególnie wtedy, gdy górne granice transakcji zostaną podniesione lub nawet całkowicie zniesione. Niektóre z tych górnych granic są już relatywnie wysokie, np. w Wielkiej Brytanii już od końca lat 90-tych XX w. większość kart pieniężnych posiada możliwości płatnicze nawet do kilkuset funtów, tj. kilku tysięcy złotych[22].

System „elektronicznych giełd pieniężnych" stanie się atrakcyjniejszy w przypadku transakcji o charakterze międzynarodowym. Wykorzystanie sieci Internetu do przeprowadzanych transakcji stanowić będzie dodatkowe utrudnienie dla wykrycia procederu „prania": umożliwi bezpośrednie przeniesienie elektronicznie „zapisanych" wartości od jednego posiadacza karty do drugiego bez pozostawiania śladów po przeprowadzonej operacji[23].

2.3. Bezpośrednie transakcje (direct banking)

Według FATF direct banking może zostać wykorzystany szczególnie przez sprawców zorganizowanych do utrudnienia wykrycia operacji mających na celu pranie pieniędzy. Obawy te wynikają z braku tradycyjnych metod kontroli, będących następstwem zredukowanego kontaktu pomiędzy pracownikiem bankowym a klientem[24]. W direct bankingu dochodzi do założenia rachunku bankowego lub przeprowadzania dalszych operacji finansowych pomiędzy klientem a instytucją finansową bez konieczności bezpośredniego „fizycznego" kontaktu, tj. klient jest znany jedynie z drogi korespondencyjnej, telefonicznej, faxowej lub najczęściej internetowej[25]. W tego rodzaju transakcjach klient i posiadacz rachunku bankowego nie jest znany jako „osoba". Należy dodać, że w takiej sytuacji trudno jest sprawdzić choćby dane podane podczas zakładania rachunku rozliczeniowego[26].

---

[22] Ibidem, s. 24.

[23] Ibidem, s. 24.

[24] Ibidem, s. 24.

[25] Zob. R. Müller i n., *Wirtschaftskriminalität, Eine Darstellung der typischen Erscheinungsformen mit praktischen Hinweisen tur Bekämpfung*, wyd. 4, München 1997, s. 66 i n.

[26] Zob. Findeisen, *Zeitalter*, s. 110 - 111.

2.4. Cybermoney

Podczas, gdy w środkach przekazu coraz więcej uwagi zwraca się na wzrost pornografii z udziałem nieletnich w Internecie oraz na wykorzystywanie tego medium przez skrajnych ekstremistów, staje się coraz bardziej jasne, iż eksploatacja praktycznie nieprzejrzystej sieci komunikacyjnej rodzi jeszcze bardziej daleko idące niebezpieczeństwa: obecnie jest wykorzystywany przez prawie każdy rodzaj przestępczości. Można bez wątpienia stwierdzić, iż przestępcze jego wykorzystanie jest bardziej powszechne niż się sądzi[27].

Powstanie tzw. „cybermoney" jest związane z rozwojem Internetu[28]. Ta o światowym zasięgu sieć komputerowa rozwinęła się w przeciągu zaledwie kilku lat, stając się jedną z najważniejszych dróg komunikacyjnych, oferujących towary i usługi w skali globalnej[29].

Pod pojęciem „cybermoney" *sensu largo* rozumie się pieniądz elektroniczny, tj. jednostki rozrachunkowe, które zakodowano („zapisano") elektronicznie na twardym dysku komputera („pieniądz sieciowy") lub na chipach krzemowych kart plastikowych (kart pieniężnych)[30]. W sensie *stricto* „cybermoney" to tylko pieniądz sieciowy, służący do zapłaty z wykorzystaniem międzynarodowych sieci komputerowych[31].

W przypadku pieniądza sieciowego mamy do czynienia, podobnie jak przy kartach pieniężnych, z „z góry" zapłaconymi elektronicznymi jednostkami rozliczeniowymi, które są wypuszczane przez bank lub inną instytucję finansową jako środki płatnicze w miejsce pieniądza gotówkowego lub księgowego. „Zapisany" na twardym dysku posiadacza komputera pieniądz sieciowy wykorzystywany jest do przeprowadzania operacji płatniczych w drodze przepływu między posiadaczami komputerów, biorących w nim udział. Zapłata pieniądzem sieciowym odbywa się anonimowo, a do obrotu elektronicznymi jednostkami rozliczeniowymi dochodzi bez włączenia do tej operacji rachunków bankowych i udziału, tzw. centralnego clearingu, tj. bezpośrednio z zapisu płacącego do zapisu odbiorcy przekazu[32].

---

[27] Por. Müller, *Wirtschaftskriminalität*, s. 37 i n., 54 i n.; T. Janovsky, *Internat und Verbrechen, Die virtuelle Komponente der Kriminalität*, „Kriminalistik" 7/1998, s. 500; J. Ziegler, *Die Barbaren kommen, Kapitalismus und organisiertes Verbrechen*, München 1999, s. 226 i n.

[28] Szerzej S. Dreher, *Cyber Money, Entwicklungstendenzen und Abwicklungstechniken im Internet, Studien zum Finanz-, Bank- und Versicherungsmanagement des Lehrstuhls für Finanzierung und Investition*, t. 4, Kaiserslautern 1999 (monografia).

[29] Internet łączy komputery w ogólnoświatową sieć. Pierwotnie technologię internetową rozwijano dla amerykańskiego wojska. Miała ona za cel stworzenie sieci komputerowej, która umożliwiłaby bezproblemową komunikację na wypadek zmagań wojennych podczas awarii pojedynczych komputerów. Połączenie między komputerem x a komputerem y w tej sieci nastąpi automatycznie poprzez z góry nieokreślony komputer. Każdy komputer posiada niepowtarzalny w skali globalnej IP-adres i poszukuje samodzielnie „drogę" do komputera docelowego. Nawet, gdy jeden z komputerów ulegnie awarii połączenie będzie kontynuowane automatycznie przez jakiś inny. Zob. Janovsky, *Virtuelle Komponente*, s. 500; Müller, *Wirtschaftskriminalität*, s. 54 i n.

[30] Zob. Fülbier, Aepfelbach, *Kommentar*, s. 148 - 149; Findeisen, *Zeitalter*, s. 107. Por. także K. J. Jakubski, *Przestępstwa związane z użyciem kart*, „Prawo Bankowe" 2/1998, s. 83 i n.

[31] Pod. Hoyer, Klos, *Regelungen*, s. 25.

[32] Najzwyklejsza jednorazowa operacja finansowa dokonana przez Internet kosztuje nie więcej niż parę euro-centów, z wykorzystaniem bankomatu już kilkanaście euro-centów, telefonicznie przeprowadzona nierzadko kilkadziesiąt euro-centów, natomiast przy okienku bankowych nawet do jednego euro. Por. Findeisen, *Zeitalter*, s. 108, 114 - 115.

Podczas, gdy pieniądz elektroniczny jest wykorzystywany w pierwszej kolejności do operacji płatniczych o stosunkowo niskich sumach (np. w RFN kilkuset euro, tj. kilku tysięcy złotych), to pieniądz sieciowy nadaje się oraz został przewidziany przez większość emitentów do znacznie większych operacji[33].

O światowym zasięgu anonimowa ogólnie dostępna sieć komunikacyjna Internetu ułatwia wszelką wymianę informacji, towarów i usług. Poniżej wymienione najważniejsze cechy tej globalnej sieci dają zupełnie nowe dotychczas jeszcze nieznane możliwości dla rozwoju nowej generacji przestępczości, w tym „cyber-prania"[34].

Po pierwsze, granice geograficzne nie stanowią żadnej przeszkody w świecie Internetu.

Następstwem tego jest globalizacja rynków finansowych. Nawet dla drobnych klientów nie stanowi przeszkody otwarcie, np. będąc „fizycznie" na terytorium Polski, wielu rachunków bankowych w wielu różnych zagranicznych instytucjach finansowych i szybki, nie budzący podejrzeń transfer, o charakterze światowym, przez nie pieniędzy. Możliwość ekspansji aktywności „praczy" stała się rzeczywistością: mamy do czynienia z równie szybkim rozwojem zarówno legalnego, jak i nielegalnego wykorzystania zjawiska zwanego „globalizacją". Ponadto Internet banking umożliwia przeprowadzenie skuteczniejszych czynności maskujących w każdym z etapów prania pieniędzy, np. przez lokatę w inne wartości majątkowe (papiery wartościowe).

Poszczególne operacje można wykonać z wykorzystaniem komputera podłączonego do sieci w dowolnym miejscu kuli ziemskiej, wkładając w nie minimum wysiłku, czasu i kosztów[35]. Dodatkową zaletą Internet bankingu jest praktycznie nieograniczona możliwość przeprowadzania następujących po sobie błyskawicznych operacji z wykorzystaniem wielu rachunków bankowych, nierzadko w różnych instytucjach finansowych tego samego dnia, a w dodatku 24 godziny na dobę. Do tego wszystkiego wystarczy jedynie sprawny komputer podłączony do sieci Internetu i niewiele tzw. kliknięć myszką[36]. Działania „pracza" wspomaga Internet banking państw offshore.

Systemy sieci pieniężnych nadają się, w przeciwieństwie do „załadowanych" kart, do wewnątrzkrajowego i międzynarodowego transferu z wyko-

---

[33] Findeisen, *Zeitalter*, s. 113 - 114.

[34] Por. Hoyer, Kłos, *Regelungen*, s. 25; Findeisen, *Zeitalter*, s. 109. Szerzej K. Bremer, *Strafbare Internet-Inhalte in internationaler Hinsicht, Ist der Nationalstaat wirklich überholt?*, Frankfurt a.M. 2001, w szczególności s. 42 i n., 66 i n., 72 i n., 107 i n., 173 i n.

[35] W skład kosztów użytkownika wchodzą koszty za rozmowy telefoniczne wg taryfy połączenia telefonicznego swojego service providera. Są to najczęściej: miesięczna opłata ryczałtowa i opłata za użytkowanie – czasowa lub opłata zależna od objętości przekazu. Natomiast samo korzystanie z oferty internetowej jest często (jeszcze) bezpłatne. Dostęp do tej oferty zazwyczaj otwarty dla każdego lub tylko częściowo chroniony za pomocą hasła. Por. Janovsky, *Virtuelle Komponente*, s. 500.

[36] Do korzystania z sieci internetowej oprócz komputera z modemem lub kartą ISDN, telefonu i odpowiedniego programu podłączeniowego potrzeba także umowy z ofiarującym usługi internetowe tzw. service providerem, który umożliwi dostęp do tej sieci. Po uzyskaniu połączenia telefonicznego z komputerem service providera trzeba już tylko podać oznaczenie użytkownika (tzw. login) i hasło. Teraz już mamy otwarty dostęp do globalnej sieci internetowej. Por. Janovsky, *Virtuelle Komponente*, s. 500.

rzystaniem wysokich sum pieniężnych. Nieodzowna wydaje się tendencja zastąpienia przez te systemy tradycyjnych instrumentów bezgotówkowego przepływu pieniędzy.

Po drugie, podczas ścigania karnego dodatkowe problemy stwarza anonimowość przestępcy[37].

Nawet, gdy przez tzw. IP-adres rozpoznano komputer, z którego dane z niedozwoloną zawartością wysłano lub na którym się one znajdują, nie daje to jeszcze możliwości ustalenia miejsca stacjonowania komputera[38]. Adresy internetowe są nadawane przez odpowiedzialne za pojedyncze domeny instytucje. Co prawda, można dojść do osoby, która złożyła wniosek o przydzielenie adresu internetowego, ale czy chodzi tu o tak naprawdę faktycznie istniejącą osobę i czy przy zgłoszeniu podane miejsce stacjonowania komputera jest jednoznaczne z jego rzeczywistym miejscem, nie jest to takie pewne. W tych rozważaniach pominięto niezwykle skomplikowaną kwestię zarówno komputerów przenaszalnych (laptopów), jak również nowoczesnej telefonii komórkowej wyposażonej w Internet.

Rozpoznanie komputera nie pozwala jeszcze ustalić, jaka osoba miała dostęp do niego i kto faktycznie wysłał dane. Pojedynczy użytkownicy meldują się loginem i hasłem[39]. Jednakże pod tym rozpoznaniem użytkownika najczęściej nie biorą oni udziału w komunikacji internatowej. Wielokrotnie zostaje im dany przez komputer service providera tzw. dynamiczny adres, który obowiązuje tylko na czas danego połączenia z tymże komputerem. IP-adres pokazuje się na tzw. dalszym komputerze lub na nagłówku przekazu e-mailowego dopiero po wykorzystaniu protokołu danych na komputerze service providera. Można dojść do konkretnego loginu, z którego korzystano podczas serfowania po Internecie, natomiast jaka osoba login internetowy używała, nie jest to zawsze łatwe do ustalenia.

W rzeczywistości dowody można będzie dostarczyć po przeprowadzeniu przeszukania u podejrzanego, w szczególności jego komputera. Czynności dochodzeniowe utrudni lub nawet uniemożliwi ich dalsze prowadzenie, wykonanie przez podejrzanego wielu następujących po sobie w bardzo krótkim okresie czasu operacji.

W przypadku poczty elektronicznej (e-mailowej) zasadniczo czołówka wiadomości zawiera IP-adres komputera, z którego wysłano pocztę. Jeżeli nagłówek przekazu byłby automatycznie wymazany, to nie można by ustalić drogi e-maila i jego pochodzenia. Czasami ułatwi to automatyczne otrzymanie e-mailowego adresu bez jednoczesnego obowiązku sprawdzania identyfikacji.

Po trzecie, międzynarodowa sieć Internetu przyczynia się do internationalizacji ścigania karnego[40].

---

[37] Zob. Janovsky, *Virtuelle Komponente*, s. 503 - 504; Müller, *Wirtschaftskriminalität*, s. 43 - 44, 55 - 56.
[38] Internet Protocol.
[39] Słowo rozpoznawcze identyfikujące użytkownika i stanowiące jego jakby imię i nazwisko.
[40] Zob. Janovsky, *Virtuelle Komponente*, s. 503.

Tylko znikoma część sprawców i komputerów, za pomocą których dokonano przestępstw lub na których znajdują się dane potrzebne w postępowaniu, albo też z którymi takowe połączenie z Internetem ustalono, znajdują się w kraju. Sprawcy zasłaniają się międzynarodową anonimowością i korzystają z praktycznie ograniczonego granicami państwowymi ścigania karnego. Aby móc dotrzeć do komputera, który znajduje się za granicą i do danych potrzebnych w ramach prowadzonego dochodzenia, wielokrotnie trzeba przebrnąć przez bardzo żmudną drogę pomocy prawnej. Do tego czasu – w zależności od konkretnego państwa, są to często tygodnie lub miesiące trwających procedur pomocy prawnej i prowadzących do sukcesu poszukiwań – przestępca ma możliwość przeprowadzenia czynności maskujących. W przypadku wyszukania przez „pracza" państwa, w którym przez niego popełniony czyn nie jest przestępstwem, usiłowania pomocy prawnej okażą się bezowocne. Udzielenie pomocy prawnej uzależnione jest od tego, aby czyn był przestępstwem zarówno w państwie proszącym o pomoc prawną, jak i w państwie udzielającym pomocy prawnej[41].

Podsumowując: przeprowadzanie operacji z użyciem pieniądza sieciowego stwarza dogodne możliwości wykorzystania ich do prania pieniędzy[42]. Pieniądz sieciowy nie przepływa z jednego rachunku bankowego na inny, lecz przybiera formę dalej idącej, gotówko podobnej operacji o zwiększonej anonimowości. Mówi się o tzw. wirtualnym pieniądzu, który z reguły nie pozostawia żadnego paper trail. Pozwala on klientowi emitującego banku na przenoszenie go niemalże bez ograniczeń na osoby trzecie. Dla samego emitującego jest niemożliwe do ustalenia, kto, komu, ile i jakim tytułem przesłał pieniędzy[43].

2.5. Inne tendencje

Oprócz operacji bankowych z wykorzystaniem Internetu, systemów „elektronicznych giełd pieniężnych" i direct bankingu, istnieje stosunkowo łatwa możliwość przeprowadzenia procederu prania pieniędzy z wykorzystaniem rozwijającego się telefonicznego bankingu (np. w Hongkongu) i kasyn internatowych (np. w Finlandii).

Powszechna, łatwo i tanio dostępna, coraz bardziej anonimowa, dwudziestoczterogodzinna oferta usług w zakresie telefonicznego bankingu utrudnia sprawność przeprowadzonej kontroli, w tym co do wykorzystania jego do prania pieniędzy[44]. Podobnie wygląda sytuacja w przypadku internetowej kasyno-oferty. Dodatkowym elementem wspierającym piorącego pieniądze może okazać się prowadzenie przez kasyna rachunków rozliczeniowych swoich internetowych klientów[45].

---

[41] Por. zwłaszcza art. 111 § 1 Kodeksu karnego.
[42] Zob. Findeisen, *Elektronisches Geld*, s. 48 - 49.
[43] Pod. Findeisen, *Zeitalter*, s. 114 - 115.
[44] Müller, *Wirtschaftskriminalität*, s. 68.
[45] Pod. Hoyer, Klos, *Regelungen*, s. 27.

3. PODSUMOWANIE

Metody wykorzystujące tzw. nowe technologie płatnicze w procesie prania pieniędzy są tak skomplikowane, jak i sam system gospodarczy, który wspomaga piorącego pieniądze w jego przestępczej działalności. System ten podlega ciągłym przeobrażeniom; częściowo przez nieustannie zmieniające się metody zwalczania i dochodzenia. Te zmiany wymagają jeszcze szybszego dostosowania technik prania pieniędzy do nowo powstałej rzeczywistości, do tego stopnia, iż enumeratywne wyliczenie wszystkich możliwych ich konstelacji wydaje się niemożliwe[46]. Fantazja i pomysłowość „praczy" są praktycznie niczym nieograniczone, wyprzedzają one mechanizmy przeciwdziałania temu procederowi przynajmniej o jedno, jak nie o dwa lub trzy posunięcia[47]. Prawie każdy rodzaj transferu wartości majątkowych może zostać wykorzystany w procesie prania pieniędzy. Częstokroć operacje w ramach tego procesu są na tyle skomplikowane i zagmatwane, iż samym ekspertom gospodarczym trudno je rozpoznać jako pranie pieniędzy. Wszystkie te operacje najczęściej posiadają jedną cechę wspólną: „wplątanie" w nie jak największej liczby państw, szczególnie państw offshore[48].

TECHNICAL AND FINANCIAL ASPECTS OF UNLAWFUL USE OF NEW PAYMENT TECHNOLOGIES IN THE AGE OF GLOBALISATION BY THE EXAMPLE OF MONEY LAUNDERING

S u m m a r y

This article is a discussion of the issue of new payment technologies along with a comprehensive view of their possible unlawful use. The notion of „new payment technologies", virtually unknown until recently, denotes a system of closed networks, chip cards system, and open payment systems.

The author puts special emphasis upon problems related to the interconnection and mutual influence between the following four new phenomena of the 20th century: intensive organized criminal activity and such crime-fostering phenomena as: abuse of new payment technologies, ongoing globalisation, and intensified money laundering. The author sets out to present the arising socio-economic threats connected with the discussed processes and above all to shed light upon the technical and financial mechanisms connected with them.

[46] Por. J. Knorz, *Der Unrechtsgehalt des § 261 StGB*, Frankfurt a.M. 1996, s. 32.

[47] Pod. F. Bresler, *Interpol, Der Kampf gegen des internationale Verbrechen von den Anfängen bis heute*, München 1993, s. 285. Jedyną barierą dla „pracza" jest jego własna fantazja wspierana przez ciągły rozwój usług techniczno-finansowych, które banki oferują swoim klientom, a które jednocześnie wspierają „pracza". P. Bernasconi, *Erscheinungsformen der Geldwäscherei in der Schweiz*, w: Schweizerischer Anwaltsverband (wyd.), *Geldwäscherei und Sorgfaltspflichten, Schriftenreihe des Schweizerischen Anwaltsverbandes*, t. 8, Zürich 1991, s. 8. Bliższe, połączone z rozrywką, zapoznanie się z powyżej przedstawioną tematyką proponuje bestseller *Firma* amerykańskiego obrońcy w sprawach karnych i autora wielu powieści Johna Grishama. W *Firmie* autor przedstawia, w sposób wyjątkowo ciekawy, siatkę amerykańskich powiązań przestępczych, które występują w lekturze „pod płaszczem" dobrze prosperującej międzynarodowej kancelarii doradztwa podatkowego, prowadzącej „brudne" interesy w bankach na Kajmanach.

[48] I. Klippl, *Geldwäscherei*, Wien 1994, s. 6.

The author arrives at the following conclusions. Methods of applying new payment technologies, especially in money laundering, are as complicated as the economic system itself. The criminals' unlimited imagination and resourcefulness is still ahead of any preventive measures. Additionally, the constantly transforming globalisation process makes it even more difficult to enumerate all the possibilities of unlawful use of these technologies.