Pojęcia kluczowe: *kryptowaluta, bitcoin, cyberprzestępstwo, blockchain, e-terroryzm*

Artykuły

Aleksander Petrys

BITCOIN – WSPÓŁCZESNA ALTERNATYWA WOBEC PIENIĄDZA FIDUCJARNEGO W PERSPEKTYWIE POSTĘPOWANIA KARNEGO

W zeszłorocznym wrześniowym numerze czasopisma „Palestra" opublikowany został artykuł dotyczący prawnokarnej perspektywy funkcjonowania kryptowalut w polskim porządku prawnym[1]. Celem niniejszego opracowania jest uchwycenie tej tematyki z perspektywy regulacji Kodeksu postępowania karnego[2]. W oparciu o wybrane przykłady przestępstw z Kodeksu karnego[3], tj.: prania pieniędzy, hackingu, kradzieży, a także e-terroryzmu, autor wyraża swoje obawy związane z ciągłym brakiem ustawy komplementarnie regulującej materię kryptowalut w polskim porządku prawnym, niemniej jednak zauważa, że pierwszym tak znaczącym krokiem ku temu była implementacja przez Polskę unijnej dyrektywy Anti-Money Laundering and Countering Financing of Terrorism Act (AML-V), czego dowodem będą tezy przedstawione w niniejszym opracowaniu[4].

[1] A. Petrys, *Bitcoin – współczesna alternatywa wobec pieniądza fiducjarnego w aspekcie prawnokarnym*, „Palestra" 2021/9, s. 62.

[2] Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2021 r. poz. 1023 ze zm.), dalej k.p.k.

[3] Ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2021 r. poz. 2345 ze zm.), dalej k.k.

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z 30.05.2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE, dalej AML.

 DOI: 10.54383/0031-0344.2022.5.4

Od momentu wyemitowania pierwszego bitcoina po dziś dzień kryptowaluty wciąż zyskują swoich nowych użytkowników, rezygnujących z powszechnie przyjętego bankowego systemu płatności. Bitcoin jest dla nich w pełni niezależną i wolną walutą przyszłości, umożliwiającą szybkie, niekontrolowane przez żadne organy państwowe przelewy. Są także jego przeciwnicy, upatrujący w bitcoinie znakomite narzędzie przestępcze. Ta kryminalna „odnoga" bitcoina przejawia się m.in. w oszustwach finansowych, kradzieżach, praniu pieniędzy, dark-marketingu i finansowaniu terroryzmu. O ile dla jego użytkowników bitcoin stanowi niezależny, poufny i niekontrolowany instytucjonalnie środek płatniczy, o tyle z perspektywy państwa będącego gwarantem bezpieczeństwa prezentowane cechy bitcoina wpływają na stosunkowo niechętne wdrażanie go w krajowe systemy finansowe. Asumptem do powstania waluty bitcoin była chęć skończenia z inwigilacyjną polityką państw Zachodu (głównie USA) wynikającą m.in. z państwowego monopolu na dystrybucję pieniądza. Kryptowalut nie należy się obawiać, gdyż stanowiły one inspirację dla wielu pozytywnych zmian, jakie już zaszły w światowym systemie transakcji finansowych (np. skrócenie czasu realizacji międzynarodowych przelewów, uproszczenie obsługi kont bankowych itd.). Kluczem do tego, aby kryptowaluty stały się w pełni bezpiecznym narzędziem z perspektywy zarówno jego użytkowników, jak i państwowych gospodarek, jest nadanie im prawnie ugruntowanego statusu.

BITCOIN – ANALIZA NA TLE POSTĘPOWANIA KARNEGO

Chcąc określić „rolę", jaką pełni bitcoin w postępowaniu karnym, ważne jest, aby zwrócić uwagę na to, na jakim etapie procesu występuje, gdyż wraz ze zmianą statusu procesowego zmienia się status bitcoina. W związku z powyższym należy stwierdzić, że bitcoin w Kodeksie postępowania karnego podlega wielu procesowym metamorfozom. Przykładowe postacie, w jakie wciela się bitcoin w polskim procesie karnym, to:

- informacja,
- ślad,
- dowód,
- przedmiot zabezpieczenia majątkowego,
- przedmiot poręczenia majątkowego.

Na pierwszym etapie, jeszcze przed wszczęciem procesu, informacja to określony zbiór danych na temat pewnego wycinka rzeczywistości. Podmiot (np. organ ścigania) otrzymujący informację dotyczącą np. pewnego zdarzenia, rzeczy lub osoby może na jej podstawie podjąć ewentualne kroki proceduralne w sytuacji, gdy z jej treści wynika konkretny, mogący mieć swoje odzwierciedlenie w rzeczywistości fakt. Za T. Hanauskiem należy przyjąć, że informacje to wszelkie dane o świecie zewnętrznym, pozyskane przez bezpośrednie poznanie zmysłowe lub przez opis jakiegoś stanu rzeczy podany przez osobę

trzecią[5]. Dane te pełnią dla organów ścigania funkcję zarówno poznawczą, jak i inspirującą. Jako przykład takiej informacji można sobie wyobrazić sytuację, w której w przedsiębiorstwie Y. doszło do popełnienia przestępstwa przy użyciu kryptowalut. Jeden z pracowników tego przedsiębiorstwa posiada wiedzę na temat tego, że jedna z osób zatrudnionych – pracownik X. – interesuje się tematyką związaną z np. cyberprzestępczością. Ta wiedza, będąca informacją, podlegać będzie weryfikacji przez organy ścigania w toku dalszych ustaleń[6]. Można skonkludować, że bitcoin na pierwszym etapie procesu może pełnić rolę szeroko rozumianej informacji.

W kolejnym stadium postępowania informacja może przerodzić się w ślad. Śladem, według zaproponowanej definicji przez Jana Sehna, nazywamy „zmiany w obiektywnej rzeczywistości, które jako spostrzegalne znamiona po zdarzeniach będących przedmiotem postępowania, mogą stanowić podstawę do odtworzenia i ustalenia przebiegu tych zdarzeń zgodnie z rzeczywistością"[7]. W ujęciu wąskim ślad to materialna pozostałość pewnego zdarzenia[8], podczas gdy w ujęciu szerokim to każda zmiana, zarówno ta rzeczywista, jak i nierzeczywista. Bitcoin, będący pewnego rodzaju cyfrowym zapisem, pełni rolę niematerialnego śladu zwanego w kryminologii śladem cyfrowym[9]. Każda aktywność użytkowników sieci internetowej pozostawia po sobie pewną informację. Informacja ta dostarcza danych na temat m.in. przeglądanych przez nas stron internetowych, treści wysłanych e-maili, polubionych zdjęć na portalach społecznościowych, słuchanej muzyki czy dokonanych przez nas transakcji bankowych. Zrealizowana w sieci blockchain transakcja również pozostawia po sobie ślad w postaci bloku danych na temat: daty przelewu, wartości poszczególnej transakcji, jak i zaszyfrowanej nazwy konta, z którego doszło do jej realizacji. Organy ścigania, chcąc odszukać nielegalnie wykradzione z konta środki, mogą posłużyć się łańcuchem bloków bitcoina do tego, aby zidentyfikować ewentualnego sprawcę kradzieży. Odnosząc powyższe rozważania do przykładu z punktu A (obrazującego bitcoina w charakterze informacji), organy ścigania, po pozytywnym zweryfikowaniu otrzymanej od osoby zatrudnionej w przedsiębiorstwie Y. wiadomości na temat zainteresowań pracownika X., mogą podjąć poszukiwania ewentualnych śladów cyfrowych pozostawionych przez pracownika X. w sieci internetowej. Takim śladem cyfrowym może być m.in. historia dokonanych przy użyciu bitcoina transakcji, zatem bitcoin może pełnić w postępowaniu karnym funkcję tzw. śladu.

Na podstawie opublikowanego przez MSWiA raportu dotyczącego cyberprzestępczości wynika, że liczba przestępstw dokonanych za pośrednictwem

[5] T. Hanausek, *Prywatny detektyw. Przewodnik zawodu*, Poznań 1992, s. 53.

[6] *Prawo a blockchain i kryptowaluty #7* Crypto@Cracow, https://www.youtube.com/watch?v=wR5-R5ZIn0Dk (dostęp: 20.02.2022 r.).

[7] J. Sehn, *Ślady kryminalistyczne*, „Z Zagadnień Kryminalistyki" 1960/1, s. 25.

[8] T. Hanausek, *Prywatny...*, s. 25.

[9] A. Hyła, *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018/5, s. 158.

Internetu systematycznie wzrasta[10]. W związku z tym faktem 1.12.2016 r. decyzją Komendanta Głównego Policji i Ministra Spraw Wewnętrznych i Administracji powołano nową komórkę organizacyjną ds. walki z cyberprzestępczością[11].

Rosnąca liczba cyberprzestępstw spowodowała także, że znaczenie cyfrowego dowodu w postępowaniu karnym zyskało na wartości. W związku z brakiem definicji dowodu cyfrowego w polskim postępowaniu karnym należy wziąć pod uwagę stosunkowo szeroką definicję zaproponowaną przez Międzynarodową Organizację do spraw Dowodów Komputerowych[12], nadającą dowodowi cyfrowemu następujące znaczenie: „dowód cyfrowy to informacja przechowywana lub transmitowana w formie binarnej, która może mieć znaczenie w postępowaniu sądowym"[13]. W polskim postępowaniu karnym ustawowym zapisem umożliwiającym organom ścigania wykorzystanie dowodu cyfrowego w postępowaniu jest art. 236a k.p.k., który stanowi, że „przepisy rozdziału niniejszego stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną". Z treści niniejszego artykułu wynika, że organy ścigania mają prawo do zatrzymania bądź przeszukania cyfrowych danych mogących stanowić dowód w sprawie. Przykładami takich dowodów mogą być: pliki przechowywane na komputerze, historia przeglądanych stron internetowych, wciąż możliwe do odzyskania dane usunięte z komputera, a także wszelkie wiadomości e-mailowe.

W związku ze stosunkowo szeroką definicją cyfrowego dowodu także bitcoiny mogą stanowić przedmiot zatrzymania bądź przeszukania. Organy ścigania po dokonaniu tych czynności procesowych podejmują działania związane z zabezpieczeniem zebranych danych, wraz ze sporządzeniem odpowiedniego protokołu (art. 236a k.p.k. w zw. z art. 228 § 1 w zw. z art. 229 k.p.k.). Wszelkie zgromadzone informacje w sposób wyżej wymieniony uzyskują status tzw. dowodu w sprawie. Zestawiając rozważania z przykładem dotyczącym przestępstwa w przedsiębiorstwie Y., po wykonaniu przez odpowiednie organy ścigania wszelkich niezbędnych czynności procesowych, związanych z m.in. zgromadzeniem danych informatycznych, dotyczących np. historii bitcoinowych transakcji, świadczących o możliwości popełnienia przez pracownika X. przestępstwa,

[10] *PAP, Raport MSWiA: Systematycznie wzrasta zagrożenie cyberprzestępczością, 2017*, https://www.gazetaprawna.pl/artykuly/1023542,raport-mswia-systematycznie-wzrasta-zagrozenie-cyberprzestepczoscia.html (dostęp: 4.04.2021 r.).

[11] *Komenda Główna Policji, Biuro do walki z cyberprzestępczością Komendy Głównej Policji rozpoczęło działalność, 2016*, http://www.policja.pl/pol/aktualnosci/135801,Biuro-do-walki-z-Cyberprzestepczoscia-Komendy-Glownej-Policji-rozpoczelo-dzialal.html (dostęp: 20.02.2022 r.).

[12] Z ang. The International Organisation on Computer Evidence (IOCE).

[13] International Organisation on Computer Evidence, G8 Proposed Principles For the Procedures Relating to Digital Evidence, za A. Lach, *Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne*, Toruń 2004, s. 1.

przechodzi się do dalszego etapu procesu, w którym zebrane dowody stanowić będą istotną z perspektywy dalszego toku postępowania wartość procesową. Bitcoin może pełnić zatem rolę dowodu w postępowaniu karnym.

W kolejnym etapie postępowania, po zgromadzeniu przez organy ścigania niezbędnych dowodów świadczących o dużym prawdopodobieństwie popełnienia przestępstwa przez (będącego przykładem) oskarżonego pracownika X., Kodeks postępowania karnego przewiduje możliwie powiązaną z prezentowanym tematem bitcoina instytucję tzw. zabezpieczenia majątkowego. Jak stanowi art. 291 § 1 k.p.k., „w razie zarzucenia oskarżonemu popełnienia przestępstwa, za które lub w związku z którym można orzec:

1) grzywnę,
2) świadczenie pieniężne,
3) przepadek,
4) środek kompensacyjny,
5) zwrot pokrzywdzonemu lub innemu uprawnionemu podmiotowi korzyści majątkowej, jaką sprawca osiągnął z popełnionego przestępstwa, albo jej równowartości – może z urzędu nastąpić zabezpieczenie wykonania tego orzeczenia na mieniu oskarżonego lub na mieniu, o którym mowa w art. 45 § 2 k.k., jeżeli zachodzi uzasadniona obawa, że bez takiego zabezpieczenia wykonanie orzeczenia będzie niemożliwe albo znacznie utrudnione".

Abstrahując od kwestii przesłanek proceduralnych, z jakimi wiąże się możliwość zastosowania instytucji zabezpieczenia majątkowego, przedmiotem niniejszego akapitu będzie próba odpowiedzi na pytanie, czy pomimo braku kodeksowego i instytucjonalnego potwierdzenia portfel bitcoinowy będzie mógł stanowić przedmiot majątkowego zabezpieczenia. W pierwszej kolejności warto zwrócić uwagę na to, że bitcoin dzięki statusowi prawa majątkowego pełni na podstawie art. 44 k.c.[14] rolę tzw. mienia. O ile charakter mienia, stanowiącego przedmiot art. 291 § 1 k.p.k., jest w doktrynie różnie interpretowany[15], o tyle kwestia konieczności zastosowania zabezpieczenia ze względu na uzasadnioną obawę utraty mienia czy niemożliwość jego późniejszego wyegzekwowania, a nawet intencjonalnego ukrycia czy wyzbycia się go przez oskarżonego, stanowi wspólny głos doktryny w sprawie[16]. Bitcoin jako byt spełniający kodeksowe

[14] Ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740), dalej k.c.

[15] W doktrynie zdania na temat „mienia" są stosunkowo podzielone. Dla części doktryny mienie to jedynie dobro rzeczywiste (fizyczne) – K. Wojtaszyn, *Stosowanie instytucji tymczasowego zajęcia mienia ruchomego w postępowaniu przygotowawczym – aspekty praktyczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011/4, s. 90. Z kolei dominującym poglądem jest ten, nadający pojęciu „mienie" szerokie znaczenie, zgodne z art. 44 k.c. – P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017/6, s. 51; S. Zabłocki (w:) *Kodeks postępowania karnego. Komentarz do art. 167–296*, red. R.A. Stefański, Warszawa 2019, t. 2.

[16] D. Skowron, *Bitcoin jako przedmiot zabezpieczenia w postępowaniu karnym*, „Prawo Karne i Kryminologia", Warszawa 2018. s. 17; B. Augustyniak, K. Eichstaedt, M. Kurowski, *Kodeks postępowania karnego*, t. 1, *Komentarz aktualizowany*, red. D. Świecki, Warszawa 2019.

przesłanki mienia (często mienia o znacznej wartości), będący dobrem możliwie szybkim do wyzbycia bądź jego ukrycia, wymaga od organów procesowych chcących skutecznie go zabezpieczyć wnikliwego, szybkiego oraz niezwłocznego działania. O ile w aspekcie teoretycznym bitcoin pełniący rolę zabezpieczonego w postępowaniu mienia nie rodzi większych wątpliwości, o tyle w ujęciu praktycznym taka możliwość przekłada się na szereg proceduralnych przeszkód i technicznych utrudnień z tym związanych. Pierwszym problemem, na który zwraca uwagę w swojej pracy D. Skowron, jest pytanie związane z tym, skąd organy procesowe będą pozyskiwały wiedzę na temat posiadanych przez oskarżonego środków bitcoinowych[17]. Konto kryptowalutowe, w przeciwieństwie do konta bankowego, nie jest kontrolowane przez scentralizowanego regulatora posiadającego informacje na temat swoich klientów. Dodatkowo każdy posiadacz konta bitcoinowego podczas realizowania płatności identyfikowany jest nie z imienia i nazwiska, a jedynie z losowo wygenerowanego ciągu znaków (*username*).

Na ten moment najskuteczniejszą możliwością pozyskania informacji dotyczących posiadanych bitcoinów jest przeprowadzenie gruntownego śledztwa bądź dochodzenia obnażającego oskarżonego z wszelkich posiadanych przez niego aktywów. Po skutecznym zidentyfikowaniu tzw. portfela kryptowalutowego istotny problem stanowi sposób technicznego zabezpieczenia zdeponowanych na nim środków. Ponownie, w przeciwieństwie do konta bankowego, które można zablokować, dostęp do portfela bitcoinowego uzależniony jest jedynie od posiadanego hasła dostępu. Sam fakt poznania hasła przez organ prokuratury nie daje gwarancji zablokowania środków, gdyż oskarżony może zapamiętać swoje hasło i zrealizować szybki przelew z konta zablokowanego na nowe, niezajęte konto. Pojawiającym się w doktrynie potencjalnym rozwiązaniem tego problemu jest ewentualne stworzenie konta prokuratorskiego, na którym byłyby zdeponowane bitcoinowe środki oskarżonego[18]. Po przelaniu środków na potencjalne prokuratorskie konto bitcoinowe kolejnym problemem jest fluktuacyjna wartość samego bitcoina. Sąd Najwyższy w swoim postanowieniu orzekł, że „zgodnie z art. 293 § 2 k.p.k. i art. 291 § 4 k.p.k., rozmiar zabezpieczenia powinien odpowiadać jedynie potrzebom tego, co ma zabezpieczać, natomiast należy je uchylić niezwłocznie w całości lub w części, jeśli ustaną przyczyny, wskutek których zostało ono zastosowane w określonym rozmiarze lub powstaną przyczyny uzasadniające jego uchylenie choćby w części”[19].

Ciągłe spadki oraz wzrosty cen bitcoina, a w konsekwencji jego niestabilna wartość, tworzą kolejną przeszkodę w zabezpieczeniu konkretnej jego wartości. O ile z perspektywy *sensu stricto* prawnej regulacje zawarte w Kodeksie postępowania karnego umożliwiają względnie skuteczne egzekwowanie postanowień

[17] D. Skowron, *Bitcoin...*, s. 17.

[18] Prawo a blockchain i kryptowaluty #7 Crypto@Cracow, https://www.youtube.com/watch?v=wR5R5ZIn0Dk (dostęp: 20.02.2022 r.).

[19] Postanowienie SN z 13.08.2018 r. (VII KZ 8/18), Legalis nr 1832867.

o zabezpieczeniu majątku kryptowalutowego, o tyle to aspekt praktyczny przysparza wielu problemów technicznych w zastosowaniu takiego środka przymusu. Niezbędny czynnik, jaki musi wystąpić, aby niniejsza procedura mogła funkcjonować bez zarzutu, to ujednolicenie niniejszych procedur operacyjnych, a w konsekwencji wypracowanie wspólnego w skali państwa mechanizmu działania.

Ostatnie, procesowe oblicze bitcoina związane jest z instytucją poręczenia majątkowego, będącego jednym ze środków zapobiegawczych stosowanych w postępowaniu karnym. Poręczenie majątkowe, to instytucja uregulowana w rozdziale 28 Kodeksu postępowania karnego, w którym to art. 266 § 1 stanowi, że „poręczenie majątkowe w postaci pieniędzy, papierów wartościowych, zastawu lub hipoteki może złożyć oskarżony albo inna osoba". Ustawowe pojęcia takie jak „pieniądz", „papier wartościowy" i „hipoteka" nie stanowią zakresu definicyjnego kryptowalut, a w tym także bitcoina. Ciekawą interpretacyjnie możliwością porządkującą bitcoina na tle postępowania karnego jest instytucja tzw. zastawu, regulowanego na gruncie Kodeksu cywilnego[20]. O ile artykuł 306 § 1 k.c. nie uwzględnia w swej treści niematerialnej istoty bitcoina, o tyle art. 327 k.c., regulujący tzw. zastaw na prawach, interpretowany jest przez doktrynę w następujący sposób – „by można było mówić o zastawialności konkretnego dobra, musi się ono legitymować łącznie trzema cechami. Po pierwsze, dobro to musi być wystarczająco odróżnialne (oznaczalne) od innych dóbr i kategorii mienia, dla potrzeb zastawu. Po drugie, przedmiot zastawu musi posiadać wymierną wartość ekonomiczną. Po trzecie, musi być zbywalne"[21]. Bitcoin, będący zbywalnym prawem majątkowym, reprezentującym przy tym konkretną (odróżnialną od innych kryptowalut) wartość ekonomiczną, spełnia kryteria przedmiotu zastawu. Mając na uwadze szereg czynności ustawowych, jakie wymagane są do tego, aby skutecznie ustanowić zastaw, należy stwierdzić, że w przypadku niektórych z nich procedura zastawu na bitcoinie odbiegać będzie od tych standardowo przyjętych[22]. Zakres potencjalnych problemów, z jakimi bezpośrednio wiąże się instytucja poręczenia majątkowego w odniesieniu do kryptowalut, to przede wszystkim: ich niejasny status własności sprowadzający się jedynie do wiedzy na temat hasła dostępu, niestabilna wartość finansowa, a to co najważniejsze, to brak prokuratorskich portfeli kryptowalutowych, na które trafiałyby wszelkie poręczone wartości. Celem niniejszej refleksji nie jest proceduralne omówienie instytucji poręczenia majątkowego na bitcoinie, a jedynie uzmysłowienie czytającemu, z jak szerokim spektrum możliwości de-

[20] Ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2021 r. poz. 2459 ze zm.), dalej k.c.

[21] M. Balwicka-Szczyrba, A. Bieranowski, M. Jankowska, E. Klat-Górska, J. Kozińska, A. Kozioł, K. Krziskowska, D.J. Łobos-Kotowska, J. Naczyńska, M. Stańko, A. Sylwestrzak, J. Widło, *Kodeks cywilny. Komentarz. Własność i inne prawa rzeczowe (art. 126–352)*, red. M. Fras, M. Habdas, Warszawa 2018, t. 2.

[22] Art. 307 § 1 k.c. Do ustanowienia zastawu potrzebna jest umowa między właścicielem a wierzycielem oraz, z zastrzeżeniem wyjątków w ustawie przewidzianych, wydanie rzeczy wierzycielowi albo osobie trzeciej, na którą strony się zgodziły.

finicyjnych wiąże się istota bitcoina w postępowaniu karnym. Zaczynając od pierwszego stadium – „informacji", a kończąc na „poręczeniu majątkowym", otrzymujemy pełen obraz poszczególnych szczebli procesowych postępowania karnego, w których bitcoin odgrywa ważną, a niekiedy wręcz kluczową rolę procesową. Pomimo braku jakichkolwiek regulacji bezpośrednio odnoszących się do materii kryptowalutowej zakres interpretacyjnych możliwości bitcoina w Kodeksie postępowania karnego jest zdecydowanie najszerszy.

BITCOIN JAKO PRZEDMIOT KRADZIEŻY I HACKINGU

Powodów wciąż niskiej popularności kryptowalut w Polsce jest stosunkowo wiele. Abstrahując od kwestii konieczności posiadania fachowej wiedzy z zakresu systemu P2P i mechanizmu działania blockchain, a także ciągle zmieniającej się ceny kryptowalut, najczęstszym powodem odrzucenia *a priori* technologii blockchain jest poczucie braku bezpieczeństwa nad posiadanymi środkami w portfelu bitcoinowym. Brak jakichkolwiek przepisów ugruntowujących instytucję bitcoina i zapewniających przy tym państwową ochronę jego posiadaczom nie wpływa korzystnie na jego obraz w oczach potencjalnych zainteresowanych. Czy prezentowane obawy mają swoje odzwierciedlenie w rzeczywistości i czy faktycznie na gruncie znanych nam prawnokarnych instytucji bezpieczeństwo własności bitcoina stoi pod znakiem zapytania?

Niniejsze prawnokarne rozważania rozpocznę od art. 278 § 1 k.k., który stanowi, że „kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". Jedną z przesłanek kradzieży jest zatem zabór cudzej rzeczy ruchomej (rzeczy definiowanej na podstawie art. 115 § 9 k.k.). Bitcoin na gruncie Kodeksu karnego nie spełnia ustawowych wymogów rzeczy ruchomej, zatem można postawić tezę, że ze względu na niematerialny charakter bitcoina jego kradzież na podstawie art. 278 § 1 k.k. nie będzie karana[23]. Warto jednak wziąć pod uwagę, czym tak naprawdę jest kradzież bitcoina. O ile w wypadku rzeczy materialnych uzmysłowienie sobie istoty kradzieży jest stosunkowo łatwe, o tyle w wypadku dóbr niematerialnych (takich jak bitcoin) stanowi to już przedmiot doktrynalnych rozważań. Przywłaszczenie cudzych bitcoinów z prywatnego konta jest *de facto* niemożliwe, gdyż wbrew wszelkim obawom, konto bitcoinowe chronione jest hasłem dopuszczającym do konta jedynie jego posiadacza. Zatem cyfrowy zabór bitcoinów nie będzie możliwy. Aby można było mówić o jakiejkolwiek formie kradzieży kryptowalut, niezbędnym elementem jest wejście w posiadanie hasła dostępu do kryptoportfela jego posiadacza. Wówczas osoba X logująca się za osobę Y będącą posiadaczem zdeponowanych na koncie środków może przetransferować pozostawione tam środki na swoje konto, stając się przy tym właścicielem wszystkich zgromadzonych bitcoinów. Dochodzimy zatem do wniosku,

[23] A. Petrys, *Bitcoin...*, s. 62.

że kradzież bitcoinów powinna być interpretowana jako kradzież prywatnego hasła dostępu do konta, a nie bezpośredni zabór samych bitcoinów[24]. Jednakże, z perspektywy art. 278 § 1 k.k., kradzież hasła będącego bitowym zapisem (niespełniającego ustawowej przesłanki rzeczy ruchomej) również nie będzie traktowana na gruncie tego artykułu jako czyn zabroniony. O ile kradzież samych bitcoinów, jak i hasła dostępu do konta nie będzie uznana za kradzież w rozumieniu art. 278 § 1 k.k., o tyle zabór rzeczywistego portfela, będącego fizycznym nośnikiem kodu dostępu do konta bitcoinowego, w którym zapisany jest kod dostępu do konta walutowego, traktowany będzie jako kradzież odnosząca się do wartości tego portfela, a nie zdeponowanych na koncie środków bitcoinowych. W art. 278 § 2 k.k. ustawodawca wprowadził penalizację czynu mogącego pozornie odpowiadać istocie kryptowalut, zapisując, że „tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej".

W związku z brakiem ustawowej definicji programu komputerowego kluczowym elementem będzie zapoznanie się z doktrynalną interpretacją tego pojęcia. Według przeważających w doktrynie opinii program komputerowy to pewien zamknięty algorytm połączonego ze sobą w jedną całość zbioru danych[25]. Co odróżnia cyfrowe hasło od programu komputerowego to fakt, że kod dostępu do portfela kryptowalutowego, będący algorytmicznym zapisem bitów, nie jest w przeciwieństwie do programu komputerowego zamkniętą całościowo strukturą danych. Klucz dostępu do konta bitcoinowego „jest fragmentem kodu informatycznego, który pozwala na identyfikację konkretnej «bit-monety». Nie można zatem jednoznacznie zakwalifikować bitcoina jako programu komputerowego"[26].

Mając na uwadze powyższe rozważania, należy stwierdzić, że na gruncie art. 278 § 1 k.k. i art. 278 § 2 k.k. kradzież zarówno bitcoina, jak i prywatnego klucza nie będzie traktowana jako ustawowe przestępstwo przeciwko mieniu. Na gruncie prawa karnego zakwalifikowanie bitcoina jako swoiste prawo majątkowe powinno zostać w doktrynie zaaprobowane. Wynika to z faktu jednakowego definiowania terminu „prawo majątkowe", gdyż tak jak w prawie cywilnym, tak i w prawie karnym desygnatem odniesienia jest wartość ekonomiczna danego dobra, którą bitcoin bezsprzecznie posiada.

W związku powyższą konstatacją bitcoin będzie stanowić przedmiot prawnokarnej ochrony przed tzw. bezprawnym jego przywłaszczeniem. Zgodnie z treścią art. 284 § 1 k.k. „kto przywłaszcza sobie cudzą rzecz ruchomą lub pra-

[24] J. Czarnecki, *Raport o wirtualnych walutach: Wybrane zagadnienia prawnokarne związane z bitcoinem*, Warszawa 2014.

[25] M. Kulik (w:) *Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2015, s. 645; M. Janowski, *Pojęcie programu komputerowego w obowiązującym Kodeksie karnym (rozważania na tle art. 278 § 2 k.k.)*, „Przegląd Sądowy" 2011/2, s. 5; P. Czaplicki, *Wybrane przestępstwa gospodarcze związane z obrotem walutą Bitcoin w prawie polskim, Unii Europejskiej oraz Stanów Zjednoczonych*, „Studenckie Zeszyty Naukowe" 2017/20, s. 42.

[26] P. Czaplicki, *Wybrane...*, s. 42.

wo majątkowe, podlega karze pozbawienia wolności do lat 3". O ile sam bitcoin nie będzie mógł zostać uznany za rzecz, a jedynie za prawo majątkowe, o tyle portfel bitcoinowy będzie spełniać ustawowy desygnat rzeczy ruchomej. Dlatego też posiadacze bitcoina na gruncie art. 284 § 1 k.k. mają zagwarantowaną prawnokarną ochronę swojej „kryptowłasności" przed bezprawnym jej przywłaszczeniem. Pogląd ten uznawany jest także przez wielu autorów prac z dziedziny kryptowalut[27].

Pomimo jedynie pozornego braku ochrony własności bitcoina w polskiej ustawie karnej z pomocą przychodzi nam również art. 267 § 2 k.k. stanowiący, że „kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2" (przestępstwo tzw. hackingu). O ile na gruncie art. 278 k.k. przedmiotem ochrony była własność, o tyle art. 267 k.k. chroni prawo do dysponowania informacją. Ustawowo chronionym przed nielegalnym dostępem do zawartej w nim treści jest tzw. system informatyczny, który na gruncie konwencji Rady Europy z 2001 r. o cyberprzestępczości definiowany jest w następujący sposób – „system informatyczny oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych"[28]. Bitcoin, opierający swój mechanizm działania na systemie blockchain (będącym siecią powiązanych ze sobą wzajemnie komputerów), posiada cechy systemu informatycznego. Zatem nieuprawnione wejście w posiadanie informacji na temat hasła do kryptowalutowego konta będzie traktowane jako przestępstwo. Z tej perspektywy karane będzie wyłącznie bezprawne wejście w posiadanie kodu dostępu, a nie powiązana z tym możliwa kradzież kryptowalutowych środków.

Oznacza to, że na gruncie polskiego Kodeksu karnego karane jest przestępstwo hackingu związane z nielegalnym pozyskaniem danych z systemu informatycznego, jakim jest konto bitcoinowe (art. 267 § 2 k.k.), podczas gdy czyn kradzieży pozostaje w zasadzie bezkarny (art. 278 § 1 w zw. z art. 278 § 2 k.k.).

PRANIE PIENIĘDZY I KORUPCJA

Z perspektywy stabilnie funkcjonującej gospodarki państwowej największym zagrożeniem związanym z popularyzacją bitcoina jest możliwość posłużenia się nim jako skutecznym narzędziem korupcyjnym i środkiem umożliwiającym wypranie pieniędzy (będące aktem legalizacji dochodów uzyskanych wbrew prawu). W wypadku przestępstwa z art. 229 § 1 k.k. ustawodawca przyjął szeroką definicję korzyści, uwzględniającą w swej konstrukcji także cyfrowy charak-

[27] J. Liberacki, *Karnoprawne aspekty walut kryptograficznych (bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2018/13, s.13–14; D. Skowron, *Bitcoin...*, s. 11; J. Dąbrowska, *Charakter prawny bitcoin*, „Człowiek w Cyberprzestrzeni" 2017/1, s. 70.

[28] Konwencja Rady Europy o cyberprzestępczości (Dz.U. z 2015 r. poz. 728).

ter bitcoina, zapewniając przy tym gwarancje karnej odpowiedzialności osoby przyjmującej korzyść majątkową w formie kryptowalut. Nie należy zapominać, że bitcoin, jako niekontrolowana i autonomiczna kryptowaluta, funkcjonująca w oparciu o rozproszony i zdecentralizowany system blockchain, anonimizujący tożsamość wszystkich jego użytkowników, stanowi wysoce niebezpieczne narzędzie przestępcze. Z opublikowanego przez agencję Reutera raportu wynika, że w latach 2017–2021 liczba dotychczas wypranych środków finansowych z wykorzystaniem szeroko pojętych kryptowalut to około 33 miliardy dolarów, co w skali całego świata być może nie stanowi poważnego zagrożenia dla stabilności finansowej, jednak jedynie ścisła międzynarodowa współpraca jest w stanie zatrzymać ewentualny przyszły wzrost tychże wskaźników[29].

Metod prania pieniędzy jest wiele. W ramach przykładu wymienić można:
- *smurfing* – polegający na małych wpłatach realizowanych przez wielu podstawionych wpłacających,
- mieszanie – związane z łączeniem brudnych pieniędzy z legalnie prowadzonymi biznesami, w których trudno oszacować faktyczne dochody (restauracje, puby, bary),
- tzw. fikcyjne kredyty – polegające na braniu fikcyjnych kredytów spłacanych pieniędzmi pochodzącymi z przestępstw.

Zarówno organy ścigania, jak i przestępcy nieustannie modernizują swoje metody działania, ucząc się na swoich błędach i wyciągając z nich niezbędne wnioski na przyszłość. Taką potencjalnie nową metodą od pierwszych dni jego funkcjonowania był bitcoin, który szybko zyskał opinię współczesnej maszynki do prania pieniędzy. Złą atmosferę wokół bitcoina dodatkowo podgrzewały światowe afery przestępcze, które obnażały kolejne niebezpieczne oblicza kryptowalut. Mając na uwadze wiele nadużyć, jakie mogłoby spowodować pozostawienie kryptowalut poza zakresem przedmiotowym przestępstwa prania pieniędzy, polski ustawodawca w art. 299 k.k. zastosował bardzo szerokie znamiona przedmiotowe przestępstwa prania pieniędzy, gdyż zgodnie z treścią tego artykułu „kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

W przeciwieństwie do innych prawnokarnych przepisów uwzględniających

[29] G. Chavez, *Crypto money laundering rises 30% in 2021 – Chainalysis*, „Reuters" 2022, https://www.reuters.com/technology/crypto-money-laundering-rises-30-2021-chainalysis-2022-01-26/ (dostęp: 28.02.2022 r.).

jedynie pieniądz, środki płatnicze czy instrumenty finansowe, art. 299 k.k. uzupełnia swój zakres o szeroko rozumiane prawa majątkowe, które „obejmują wszelkie możliwe prawa majątkowe na rzeczach i na dobrach niematerialnych”[30]. Bitcoin, jak i wszelkie inne kryptowaluty, stanowi skuteczne narzędzie na drodze do popełnienia przestępstwa prania pieniędzy. Niniejsze rozważania należy jednak wzbogacić o treść istotnej z tej perspektywy ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, zobowiązującej podmioty pośredniczące w transakcjach kryptowalutowych do realizowania konkretnych, mających na celu zwiększenie bezpieczeństwa obrotu kryptowalutami czynności[31]. W ramach krótkiej dygresji warto zauważyć, że niniejsza ustawa jako pierwsza w polskim porządku prawnym wprowadza zarys pojęcia kryptowalut zwanych ustawowo „wirtualnymi walutami”. Zgodnie z art. 2 ust. 2 pkt 26 tej ustawy pojęcie waluty wirtualnej oznacza „cyfrowe odwzorowanie wartości, które nie jest:

a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
c) pieniądzem elektronicznym w rozumieniu ustawy z 19.08.2011 r. o usługach płatniczych[32],
d) instrumentem finansowym w rozumieniu ustawy z 29.07.2005 r. o obrocie instrumentami finansowymi[33],
e) wekslem lub czekiem

– oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego”[34].

Niniejsza nowelizacja jest wynikiem implementacji unijnych przepisów w sprawie zapobiegania praniu pieniędzy i finansowaniu terroryzmu[35]. Z tre-

[30] A. Barczak-Oplustil, M. Bielski, G. Bogdan, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, J. Raglewski, M. Szewczyk, W. Wróbel (w:) *Kodeks karny. Część szczególna. Komentarz do art. 278–363*, red. A. Zoll, Warszawa 2016, t. 3.

[31] Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r. poz. 2447).

[32] Ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2021 r. poz. 2140).

[33] Ustawa z 29.07.2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2021 r. poz. 2140).

[34] Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r. poz. 2447).

[35] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z 30.05.2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

ści przyjętej ustawy można wyprowadzić wniosek, że ustawodawca niejako potwierdził wcześniejsze opinie doktryny odrzucające nadanie kryptowalutom statusu środka płatniczego, pieniądza elektronicznego i instrumentu finansowego. Należy jednak podkreślić, że treść polskiej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nieco różni się od unijnej dyrektywy AML. Abstrahując od odmiennego zakresu adresatów podpadających pod treść obu ustaw, najistotniejszą różnicą jest brak wyłączenia z polskiej definicji wirtualnych walut tzw. walut cyfrowych reprezentujących umowną wartość w świecie gier komputerowych (np. WoW Gold – jednostka wartości w grze World of Warcraft). Brak rozróżnienia obu terminów nie został wyjaśniony, niemniej jednak powodem takiego niedopatrzenia może być fakt językowego nierozróżnienia obu pojęć, tzn. *„virtual currency"* i *„digital currency"*.

Z perspektywy prawidłowego funkcjonowania przepisów ustawowe niedopatrzenie nie będzie generowało ewentualnych problemów interpretacyjnych w związku z tym, że – co do zasady – obowiązuje unijny nakaz interpretacyjny. Z treści ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wynika, że ustawodawca narzuca konkretne cele na podmioty w niej wskazane, mające zwiększyć bezpieczeństwo przeciwko możliwym defraudacjom finansowym. Ustawa zobowiązuje podmioty świadczące usługi wymiany walut wirtualnych na prawne środki płatnicze, a także na inne waluty wirtualne (poprzez np. kantory bitcoinowe), pośredników wymiany wirtualnych walut, dostawców kont wirtualnych, jak i podmioty, których działalność polega na prowadzeniu cudzych kont bądź rachunków kryptowalutowych. Wszystkie podmioty zostały nazwane zbiorczo „instytucjami obowiązanymi", na które ustawodawca nałożył wiele obowiązków, takich jak m.in. prowadzenie rejestrów transakcji, weryfikowanie danych osobowych podmiotów realizujących transakcje, kontrolowanie i zgłaszanie do Generalnego Inspektora Informacji Finansowej (GIIF) ewentualnych podejrzeń i w ostateczności nawet blokowanie transakcji możliwie nielegalnych.

Niniejsze zmiany mają wielu przeciwników, którzy uważają, że dyrektywa AML ostatecznie zakończyła erę wolnego i niekontrolowanego przepływu kryptowalut. Z jednej strony wymóg okazywania danych osobowych wpisuje się w inwigilacyjny trend znany nam ze scentralizowanych systemów bankowych, z drugiej zaś strony należy zwrócić uwagę, że dzięki podjętym środkom ostrożności ryzyko wyprania pieniędzy drastycznie spadnie. Zwiększenie w polskim porządku prawnym kompetencji GIIF również zniechęci potencjalnych zainteresowanych do defraudowania pieniędzy. Celem tych zmian było także ograniczenie możliwości finansowania terrorystycznych grup przestępczych za pomocą wirtualnych walut, co z perspektywy ataków terrorystycznych zwłaszcza w Europie nie należało do rzadkości. Wprowadzona w życie ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu ma kilka praktycznych nieścisłości, takich jak np. obowiązek zgłaszania przez podmioty zobowiązane do GIIF transakcji powyżej 15.000 euro. O ile w wypadku krajo-

wych środków płatniczych punktem odniesienia będzie średni kurs NBP, o tyle w wypadku wartości kryptowalutowych takie odniesienie nie będzie możliwe (art. 72 ust. 1 pkt 1)[36]. Wprowadzone zmiany, jakie wiążą się z obowiązywaniem niniejszej ustawy, uznać należy za ważny krok do formalnego ugruntowania pozycji bitcoina w Polsce. Ważne jest, aby przepisy dotyczące wirtualnych walut były wciąż aktualizowane i nowelizowane w związku z tym, że zasięg możliwości Internetu jest z każdym rokiem większy i oferuje większe możliwości finansowych defraudacji.

E–TERRORYZM

Z opublikowanego raportu „Terrorist Use of Cryptocurrencies"[37] wynika, że kryptowaluty pełnią współcześnie kluczową rolę w procesie finansowania terroryzmu. Powodów nielegalnego przeznaczenia kryptowalut jest wiele, m.in.:

- anonimowość wpłacających,
- szybkość przelewów,
- brak ich kontroli przez organy państwowe,
- niejednolite przepisy kryptowalutowe,
- wciąż podążające „krok za" światowymi trendami przestępczymi regulacje prawne.

Z uwagi na to, że zjawisko ataków terrorystycznych stanowi realny problem już nie tylko dla poszczególnych nacji, ale dla całego świata, polityka bezpieczeństwa cybernetycznego powinna być tworzona wspólnie przez wszystkie zagrożone atakami państwa w celu jak najlepszego i komplementarnego systemowego uszczelnienia. Cyberterroryzm, nazywany często „współczesnym terroryzmem", w doktrynie definiowany jest jako „politycznie umotywowany atak na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów"[38]. Strategia walki z cyberprzestępczością jest różna. W Rosji i Chinach bitcoin – tak jak i inne kryptowaluty – ma status waluty zakazanej i jakikolwiek nim obrót traktowany jest jak przestępstwo. Z kolei państwa Zachodu takie jak np. USA, Niemcy starają się znaleźć rozwiązania nadające kryptowalutom status instytucji prawnie regulowanej[39]. Ważne jest, aby wprowadzane przepisy nie tylko regulowały skutki już popełnionych przestępstw,

[36] Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r. poz. 2447).

[37] C. Dion-Schwarz, D. Manheim, P.B. Johnston, *Terrorist use of Cryptocurrencies, Technical and Organizational Barriers and Future Threats*, „Rand Corporation" 2019, s. 22.

[38] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011/1, s. 11.

[39] Zespół Comparic.pl, *Władze USA sklasyfikują kryptowaluty i ICO jako produkt finansowy?*, https://comparic.pl/wladze-usa-sklasyfikuja-kryptowaluty-ico-jako-produkt-finansowy/ (dostęp: 20.02.2022 r.).

ale antycypowały możliwość ich wystąpienia, tworząc prewencyjne systemy bezpieczeństwa. Kluczową wartością w skali europejskiej kryptopolityki jest dyrektywa AML-V, rozszerzająca zakres regulowanej materii o politykę kryptowalutową. Sam fakt wprowadzenia tzw. instytucji zobowiązanych znacząco zwiększył bezpieczeństwo obrotu kryptowalutami, a przy tym zmniejszył skalę finansowania terroryzmu za pomocą kryptowalut. Polska implementacja przepisów unijnych dotycząca finansowania terroryzmu odwołuje się wprost na podstawie art. 2 ust. 2 pkt 6 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu do treści art. 165a ustawy z 6.06.1997 r. – Kodeks karny – „kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w zamiarze sfinansowania przestępstwa o charakterze terrorystycznym lub przestępstwa, o którym mowa w art. 120, art. 121, art. 136, art. 166, art. 167, art. 171, art. 252, art. 255a lub art. 259a, podlega karze pozbawienia wolności od lat 2 do 12".

Polski ustawodawca, w przypadku zarówno art. 299 k.k., jak i art. 165a k.k., zastosował rozległy zakres przedmiotowy, dzięki czemu gromadzenie środków w kryptowalucie z zamiarem finansowego wspomagania ataków terrorystycznych podlegać będzie karze pozbawienia wolności. Szeroki zakres przedmiotowy przepisów odnoszących się zarówno do bezpieczeństwa powszechnego, jak i obrotu gospodarczego nie jest przypadkowy, gdyż oba regulują wysoce istotne z perspektywy stabilności państwa obszary, tworząc szczelny system penalny.

WNIOSKI

Od 2008 r., tj. od czasu wyemitowania pierwszej kryptowaluty, jaką był bitcoin, wraz z nim powstała także alternatywna niekontrolowana rzeczywistość cyberprzestępcza, pozwalająca posiadaczom jednostek kryptowalutowych m.in. na niekontrolowany zakup narkotyków oraz broni palnej, a także zlecanie zabójstw czy przeprowadzanie cyberataków, a w tym także finansowanie szeroko rozumianego terroryzmu. Momentem odejścia od globalnej polityki legislacyjnej deprecjacji tychże zmian technologicznych był zamach w Paryżu w 2015 r., do którego przyznało się Państwo Islamskie, finansowane m.in. poprzez wpłaty kryptowalutowe. Od tamtego tragicznego w skutkach zdarzenia kryptowaluty zaczęto postrzegać już nie tylko jako swoistą nowinkę technologiczną, a jako potencjalne narzędzie terrorystyczne. Pierwszą tak istotną regulacją w skali państw Unii Europejskiej normalizującą obrót kryptowalutowymi środkami była przywołana w tekście dyrektywa AML-V, dzięki której obrót wartościami kryptowalutowymi stał się znacznie bezpieczniejszy oraz zaczął opierać się na podstawie usystematyzowanych reguł zachowania. Dlatego też implementację tejże regulacji do polskiego porządku prawnego należy ocenić jako bardzo pozytywną. Wykorzystanie technologicznego dorobku kryptografii w krajowym porządku prawnym i gospodarczym to warunek *sine qua non* następnych kilku lat.

ABSTRACT

Aleksander Petrys

The author is an advocate trainee (District Bar Association in Warsaw), a graduate of the Faculty of Law an Administration of the Jagiellonian University in Krakow, a lawyer in a law firm in Warsaw.

Bitcoin – a modern alternative to fiat money in a criminal procedure perspective

The article is an overview of cryptocurrencies from the perspective of the regulation of the Criminal Procedure Code and on the background of selected types of crimes from the Penal Code, i.e.: money laundering, hacking, theft, and e-terrorism. The author expresses his concern about the continuous lack of a complementary law regulating the matter of cryptocurrencies in the Polish legal system, but he also notes that the first such significant step forward was the implementation by Poland of the EU Directive AML-V.

Keywords: *cryptocurrency, bitcoin, cybercrime, blockchain, e-terrorism*

Aleksander Petrys
ORCID: 0000-0002-2291-3957; e-mail: petrysaleksander@gmail.com

Autor jest aplikantem adwokackim III roku (ORA w Warszawie), absolwentem Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnikiem w jednej z warszawskich kancelarii.

BIBLIOGRAFIA ZAŁĄCZNIKOWA

Augustyniak Barbara, Eichstaedt Krzysztof, Kurowski Michał (w:) *Kodeks postępowania karnego*, t. 1, *Komentarz aktualizowany*, red. D. Świecki, Warszawa 2019

Balwicka-Szczyrba Małgorzarta, Bieranowski Adam, Jankowska Marlena, Klat-Górska Elżbieta, Kozińska Joanna, Kozioł Agata, Krziskowska Katarzyna, Łobos-Kotowska Dorota, Naczyńska Joanna, Stańko Marek, Sylwestrzak Anna, Widło Jacek (w:) *Kodeks cywilny. Komentarz*, t. 2, *Własność i inne prawa rzeczowe (art. 126–352)*, red. M. Fras, M. Habdas, Warszawa 2018

Barczak-Oplustil Agnieszka, Bielski Marek, Bogdan Grzegorz, Ćwią-

kalski Zbigniew, Dąbrowska-Kardas Małgorzata, Kardas Piotr, Majewski Jarosław, Raglewski Janusz, Szewczyk Maria, Wróbel Włodzimierz, *Kodeks karny. Część szczególna. Komentarz do art. 278–363*, red. A. Zoll, Warszawa 2016, t. 3

Chavez Gertrude, *Crypto money laundering rises 30% in 2021 – Chainalysis,* „Reuters" 2022

Czaplicki Piotr, *Wybrane przestępstwa gospodarcze związane z obrotem walutą Bitcoin w prawie polskim, Unii Europejskiej oraz Stanów Zjednoczonych*, „Studenckie Zeszyty Naukowe" 2017/20, s. 32

Czarnecki Jacek, *Raport o wirtualnych walutach: Wybrane zagadnienia prawnokarne związane z bitcoinem*, Warszawa 2014

Dąbrowska Justyna, *Charakter prawny bitcoin*, „Człowiek w Cyberprzestrzeni" 2017/1

Dion-Schwarz Cynthia, Manheim David, Johnston Patrick B., *Terrorist use of Cryptocurrencies, Technical and Organizational Barriers and Future Threats,* „Rand Corporation" 2019

Hanausek Tadeusz, *Prywatny detektyw. Przewodnik zawodu*, Poznań 1992

Hyła Aleksandra, *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018/5, s. 157

Janowski Maciej, *Pojęcie programu komputerowego w obowiązującym Kodeksie karnym (rozważania na tle art. 278 § 2 k.k.)*, „Przegląd Sądowy" 2011/2, s. 80

Kulik Magdalena (w:) *Kodeks karny. Komentarz,* red. M. Mozgawa, Warszawa 2015

Lach Arkadiusz, Lachowski Jerzy, Oczkowski Tomasz, Zgoliński Igor, Ziółkowska Agata (w:) *Kodeks karny. Komentarz,* red. V. Konarska-Wrzosek, Warszawa 2018

Liberacki Jędrzej, *Karnoprawne aspekty walut kryptograficznych (Bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2018/13, s. 7

Liedel Krzysztof, Piasecka Paulina, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011/1, s. 15

Opitek Paweł, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego,* „Prokuratura i Prawo" 2017/6, s. 37

Petrys Aleksander, *Bitcoin – współczesna alternatywa wobec pieniądza fiducjarnego w aspekcie prawnokarnym*, „Palestra" 2021/9, s. 62

Sehn Jan, *Ślady kryminalistyczne*, „Z Zagadnień Kryminalistyki" 1960/1, s. 3

Skowron Damian, *Bitcoin jako przedmiot zabezpieczenia w postępowaniu karnym*, „Prawo Karne i Kryminologia", Warszawa 2018

Wojtaszyn Katarzyna, *Stosowanie instytucji tymczasowego zajęcia mienia ruchomego w postępowaniu przygotowawczym – aspekty praktyczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011/4, s. 87

Zabłocki Stanisław (w:) *Kodeks postępowania karnego. Komentarz do art. 167–296*, red. R.A. Stefański, Warszawa 2019, t. 2

 DOI: 10.54383/0031-0344.2022.5.4