t. LXXIII • nr 4/2020 (862) • DOI 10.33226/0137-5490.2020.4.2

Dr hab. Anna Golonka, prof. URz

Uniwersytet Rzeszowski
ORCID: 0000-0002-0199-2203
e-mail: anna_golonka@o2.pl

Przeciwdziałanie praniu pieniędzy w obliczu zmian wprowadzonych IV i V dyrektywą AML

Anti-money laundering in face of the amendments provided of the IVth and Vth AML directives

Streszczenie

Przedmiotem niniejszego artykułu są zagadnienia dotyczące przeciwdziałania praniu pieniędzy. Istotne zmiany w systemie prewencji przed tym zjawiskiem przyniosła ustawa z 1.03.2018 r. i przepisy wykonawcze do niej. Wejście w życie tej ustawy zostało podyktowane przede wszystkim potrzebą dostosowania krajowych przepisów do unormowań unijnych, w szczególności IV i V dyrektywy AML. Celem analizy przepisów ustawy z 1.03.2018 r. jest jednak nie tylko ukazanie zmian oraz ocena kształtu bieżących rozwiązań prawnych, ale przede wszystkim wskazanie kierunku pożądanych jej nowelizacji. Wysunięcie stosownych postulatów *de lege ferenda* jest uzasadnione w szczególności potrzebą implementacji do krajowego porządku prawnego odnośnych dyrektyw Unii Europejskiej w pełnej rozciągłości.

Słowa kluczowe: pranie pieniędzy, dyrektywa UE, ocena ryzyka, waluta wirtualna

Abstract

The subject of this study are anti-money laundering issues. Significant changes in the system of prevention against this phenomenon were brought by the Act of 1 March 2018 and its implementing provisions. The entry into force of this law was dictated primarily by the need to adapt the national provisions to EU regulations, in particular the IV and V AML directives. However, the purpose of analyzing the provisions of the Act of 1 March 2018 is not only to show changes and to assess the shape of the current legal solutions, but also to indicate the direction of desired amendments. Putting forward the appropriate *de lege ferenda* postulates is justified in particular by the need to fully implement the relevant EU directives into the national legal order.

Key words: money laundering, EU directive, *Risk Base Approach*, virtual currency

JEL: G2, K14

Wprowadzenie

Pranie pieniędzy stanowiło przedmiot niejednego opracowania, w którym było ono ukazywane w aspekcie kryminologicznym i kryminalistycznym. Wiele napisano o szkodliwych skutkach, jakie dla obrotu gospodarczego niesie wprowadzanie do niego „brudnych" wartości majątkowych, tj. wartości, które pochodzą z nielegalnych źródeł. Nie może zatem dziwić fakt, że na forum międzynarodowym i ponadnarodowym od lat były i nadal są opracowywane akty normatywne, których celem jest stworzenie mechanizmów zapewniających możliwie skuteczną prewencję przed tym procederem. Na gruncie wspólnotowym, począwszy od 1990 r. (por. dyrektywa Rady 91/308/EEC z 10.06.1991 r. w sprawie zapobiegania przed wykorzystaniem systemu finansowego dla celu prania pieniędzy, OJ L nr 166, s. 77–83), co kilka lat uchwalane są kolejne dyrektywy, bądź zmieniane są już obowiązujące, czego zasadniczym celem jest efektywne przeciwdziałanie praniu pieniędzy (*Anti-Money Laundering*, dalej w skrócie AML). Zadaniem tych aktów prawnych jest przede wszystkim wskazanie bieżących tendencji w dziedzinie zagrożenia praniem pieniędzy, a tym samym wytyczenie kierunków działań dla ustawodawców państw członkowskich UE.

Obecnie obowiązująca dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (Dz.Urz. UE nr L 141/73), zwana IV dyrektywą AML, jest tego najlepszym przykładem. Nie będzie przesady w stwierdzeniu, że

implementacji tego aktu służyło uchwalenie ustawy z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2019 r. poz. 1115) dalej u.p.p.. Uchyliła ona zarazem postanowienia obowiązującej w tym zakresie do 12.07.2018 r. ustawy z 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy (w pierwotnym stanie prawnym nosiła ona tytuł ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, Dz.U. nr 116, poz. 1216. Na mocy nowelizacji tej ustawy z 27.09.2002 r. jej zakresem objęto dodatkowo przeciwdziałanie finansowaniu terroryzmu, Dz.U. z 2002 r., nr 180, poz. 1500), czyniąc jednocześnie zadość potrzebie transponowania do krajowego porządku prawnego regulacji unijnych.

Powyższa dyrektywa nie jest jednak ostatnią, jaka aktualnie obowiązuje w prawie wspólnotowym w dziedzinie przeciwdziałania praniu pieniędzy. Uchwalono bowiem kolejne dyrektywy dotyczące zwalczania procederu „prania" (Dz.Urz. UE nr L 156/43; Dz.Urz. UE nr L 284/22). Szczególną uwagę należy zwrócić na tę z nich, której czas transponowania do krajowego prawa upłynął 10.01.2020 r., czyli tzw. V dyrektywę AML — dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/843 z 30.05.2018 r. (Dz.Urz. UE nr L 156/43), zmieniającą m.in. dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849. Szczególnie, że niektóre z jej postanowień nadal nie doczekały się odpowiednich regulacji w rodzimej ustawie AML. Taki stan rzeczy czyni zasadną analizę obowiązujących przepisów ustawy z 1.03.2018 r. oraz wybranych aktów wykonawczych do niej, w szczególności rozporządzenia Ministra Finansów z 16.05.2018 r. w sprawie zgłaszania informacji o beneficjentach rzeczywistych wydane na podstawie art. 62 u.p.p. (Dz.U. z 2018 r. poz. 968), rozporządzenia Ministra Finansów z 11.01.2019 r. w sprawie informacji o wwożonych lub wywożonych środkach pieniężnych, krajowych środkach płatniczych i walutach dewizowych, wydanego na podstawie art. 85 ust. 4 u.p.p. (Dz.U. z 2019 r. poz. 64) oraz rozporządzenia Ministra Finansów z 4.10.2018 r. w sprawie przekazywania informacji o transakcjach oraz formularza identyfikującego instytucję obowiązaną, wydanego na podstawie art. 78 ust. 3 (Dz.U. z 2018 r. poz. 1946).

Celem artykułu jest nie tylko ocena kształtu obowiązujących rozwiązań prawnych, ale również udzielenie odpowiedzi na pytanie o stan dostosowania polskich przepisów AML do obowiązujących unormowań wspólnotowych. Pozwoli to zarazem na wysunięcie pewnych wniosków w kontekście przewidywanej skuteczności i efektywności przeciwdziałania procederowi prania pieniędzy w świetle znowelizowanych przepisów.

Już tylko dla porządku wypada nadmienić, że większość z mechanizmów mających za zadanie zapobieganie praniu pieniędzy, przewidzianych w ustawie o przeciwdziałaniu praniu pieniędzy (stosownie do tytułu przedmiotowego aktu prawnego), pozostaje aktualna również w odniesieniu do przeciwdziałania finansowaniu terroryzmu. Odniesienie się w niniejszym artykule jedynie do procederu prania pieniędzy wynika przede wszystkim z praktycznego wymiaru zagrożenia obu zjawiskami[1], które jest nieporównywalnie większe w przypadku przestępstwa określonego w art. 299 ustawy z 6.06.1997 r. — Kodeks karny (Dz.U. z 2019 r. poz. 1950 ze zm.), dalej k.k. (pranie pieniędzy), niż tego, o którym mowa w art. 165a k.k. (finansowanie terroryzmu).

Risk Base Approach jako podstawa systemu przeciwdziałania praniu pieniędzy

Ustawa z 1.03.2018 r., wzorem swojej „poprzedniczki", system przeciwdziałania praniu pieniędzy opiera na wzajemnym współdziałaniu tworzących go podmiotów. Podobnie, jak w ustawie z 16.11.2000 r., podstawowymi instytucjami, na których spoczywają obowiązki związane z przeciwdziałaniem praniu pieniędzy są tzw. instytucje obowiązane (IO).

IO zostały wymienione taksatywnie w art. 2 ust. 1 pkt 1–25 u.p.p. (w kwestii postulatów dotyczących dostosowania polskich przepisów do regulacji unijnych w odniesieniu kwoty progowej por. Golonka, 2009, s. 112; co do niepełnego katalogu tych instytucji por. Golonka, 2008, s. 179–181). Przekazują one do Generalnego Inspektora Informacji Finansowej (GIIF) informacje na temat podejrzenia wprowadzenia do legalnego obrotu finansowego wartości majątkowych, które mogą pochodzić z działalności przestępczej. GIIF, przy pomocy Departamentu Informacji Finansowej, stanowiącego wyodrębnioną w strukturach Ministerstwa Finansów jednostkę organizacyjną, analizuje, gromadzi i przetwarza dane zawarte w tzw. SARach (ang. *Suspicious Activity Reports*), a także raportach w sprawie transakcji podejrzanych (ang. *Suspicious Transaction Reports on Money Laundering*, STR-ML i odpowiednio: STR-TF, ang. *Suspicious Transaction Reports on Terrorist Financing*). W przypadku zaistnienia uzasadnionego podejrzenia popełnienia przestępstwa, w którym mowa w art. 299 k.k. lub art. 165a k.k., Generalny Inspektor składa stosowne zawiadomienie do organów ścigania, będących jednostkami współpracującymi w rozumieniu art. 2 ust. 2 pkt 8, czyli do organów administracji rządowej, organów jednostek samorządu terytorialnego oraz innych państwowych jednostek organizacyjnych, a także NBP, KNF i NIK).

Tak zarysowany (naturalnie w sporym uproszczeniu) system prewencji przed omawianym procederem, jak mogłoby się zdawać, nie odbiega wobec tego zasadniczo od tego, jaki przewidywała ustawa z 16.11.2000 r., a tym samym jego bardziej szczegółowe omówienie byłoby zbędne. Tyle, że — jak wiadomo — diabeł tkwi w szczegółach. Tak więc i w tym przypadku ustawa z 1.03.2018 r. opiera się w istocie na zupełnie inaczej ujętych przesłankach, niż przewidywała to ustawa z 16.11.2000 r. Czy jednak są one diametralnie odmienne od tych, na jakich bazowała „poprzedniczka" z 1.03.2018 r.? Zanim przyjdzie się do tego odnieść, wypada w pierwszej kolejności wskazać, że w świetle postanowień tej ustawy, „trzon" systemu przeciwdziałania „praniu" stanowi tzw. „ocena ryzyka" (ang. *Risk Based Approach* — RBA). Została ona przyjęta przez ustawę z 1.03.218 r. za podstawę „konstrukcji" mechanizmu przeciwdziałania zjawiskom prania pieniędzy oraz finansowania terroryzmu

wzorem IV dyrektywy AML. Zmusza to do postawienia pytania, czym wobec tego jest owa „ocena ryzyka", a konkretnie, na czym powinny opierać się obecnie IO dokonując takiej oceny.

Jak poleca przyjmować prawodawca unijnych, przez „ocenę ryzyka" należy rozumieć „proces służący prezentacji informacji o naturze i skali prania pieniędzy/finansowania terroryzmu i powiązanych z nimi przestępstw bazowych oraz o słabych punktach w systemie AML/CFT oraz innych elementach systemu prawnego, które czynią go atrakcyjnymi dla praczy pieniędzy i finansujących terroryzm" (IV dyrektywa AML). Z kolei samo „ryzyko" odnosi się w tym przypadku do prawdopodobieństwa wystąpienia prania pieniędzy lub finansowania terroryzmu, tudzież jego możliwych skutków. Tak pojmowane ryzyko jest zatem ryzykiem inherentnym, tj. istniejącym przed jego ograniczeniem. Nie obejmuje ono natomiast ryzyka rezydualnego, czyli takiego, jakie istnieje po jego usunięciu lub zmniejszeniu (por. „Wspólne wytyczne").

Takie wskazania pozwalają na wysunięcie wniosku, że działania podejmowane przez IO powinny sprowadzać się wyłącznie do takich czynności, które eliminują możliwość (a ściślej — minimalizują prawdopodobieństwo) wykorzystania ich do celu prania pieniędzy[2].

Natomiast w świetle powyższego nie muszą one prowadzić do jego wyeliminowania, nawet jeżeliby IO stały się *in concreto* uczestnikiem tego procederu. Faktem jest zresztą, że w tej mierze główny ciężar spoczywa nie na IO, a na GIIF oraz jednostkach współdziałających, które są odpowiedzialne za zwalczanie przejawów prania pieniędzy.

Podstawowy obowiązek nałożony na IO w związku z potrzebą oceny ryzyka wynika z art. 27 ust. 1 u.p.p., zgodnie z którym IO identyfikują i oceniają ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu odnoszące się do ich działalności, „z uwzględnieniem czynników ryzyka dotyczących klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw", a działania te winny być „proporcjonalne do charakteru i wielkości IO".

Obejmuje on identyfikację oraz ocenę ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, odnoszącego się do działalności danej instytucji. Zgodnie z ust. 2 tego artykułu, przy ocenianiu ryzyka IO mogą (!) uwzględniać obowiązującą krajową ocenę ryzyka (KOR), jak również sprawozdanie Komisji Europejskiej, o którym mowa w art. 6 ust. 1–3 dyrektywy 2015/849 (ust. 2), co stanowi podstawę do sporządzenia przez nie własnej oceny ryzyka (ust. 3). Zapis przewidziany w art. 27 ust. 2 u.p.p. nasuwa jednak wątpliwość dotyczącą powodu, dla którego opieranie się na KOR ma charakter uznaniowy i wobec tego, jakie kryteria powinny być decydujące dla IO przy opracowaniu przez nie ich własnych ocen ryzyka? Oczywiste jest bowiem, że nie chodzi o kryteria ogólnie wskazane w art. 27 ust. 1 u.p.p., skoro na nich opiera się również KOR.

Temu dokumentowi ustawa poświęca 4. rozdział. Nie precyzuje w nim jednak, czym jest KOR. Próżno w niej także szukać definicji KOR, jak również szczegółowo wskazanych kryteriów oceny poziomu ryzyka. Zdaje się zresztą, że o takich in abstracto nie może być mowy. Można natomiast znaleźć w ustawie informacje, co powinien zawierać taki dokument. Zgodnie z art. 29 u.p.p., dokument KOR składa się w szczególności z: opisu metodyki krajowej oceny ryzyka, opisu zjawisk związanych z praniem pieniędzy oraz finansowaniem terroryzmu, opisu obowiązujących regulacji dotyczących ww. procederów, wskazania poziomu ryzyka dla tych zjawisk wraz z uzasadnieniem, wniosków wynikających z oceny ryzyka oraz identyfikacji zagadnień dotyczących ochrony danych osobowych związanych z ww. procederami.

Generalny Inspektor, jako organ odpowiedzialny za opracowanie KOR („we współpracy z Komitetem, jednostkami współpracującymi i instytucjami obowiązanymi" — art. 25 ust. 1 u.p.p.), jest zobowiązany wziąć pod uwagę przy jego tworzeniu sprawozdanie Komisji Europejskiej dla Parlamentu Europejskiego i Rady (Bruksela, 26.06.2017 r., COM 92017) 340 *final*, http://ec.europa.eu/transparency/regdoc/rep/1/2017/PL/COM-2017-340-F1-PL-MAIN-PART-1.PDF (12.03.2020 r.). Sprawozdanie to określa, analizuje oraz szacuje ryzyko prania pieniędzy oraz finansowania terroryzmu na szczeblu unijnym i obejmuje co najmniej zagadnienia dotyczące: obszarów rynku wewnętrznego, które są uznane za najbardziej zagrożone ich wykorzystaniem do przeprowadzenia tych procederów, ryzyka związanego z każdym odnośnym sektorem, a także najpowszechniejsze metody wykorzystywane przez przestępców do prania nielegalnych dochodów. Z przewidzianych w nim wskazówek można wyinterpretować pewne kierunki zagrożeń, tudzież tendencje, które w odniesieniu do poszczególnych branży czy szerzej — prowadzonej działalności lub charakteru świadczonych usług, stanowią swoisty wzorzec dla IO przy tworzeniu przez nie ich własnych macierzy oceny ryzyka popełnienia przestępstwa, o którym mowa w art. 299 k.k. lub art. 165a k.k. Ustawa z 1.03.2018 r. utrzymuje dotychczasowy obowiązek opracowania procedur wewnętrznych (art. 50 u.p.p.), z tym że wprowadza wymóg dotyczący zatwierdzenia („akceptacji") takich procedur, przed ich wprowadzeniem do stosowania, przez kadrę kierowniczą wyższego szczebla.

Analizując opublikowany w 2019 r. przez GIIF dokument zawierający Krajową Ocenę Ryzyka, można dojść do wniosku, że uwzględnia on nie tylko międzynarodowe standardy w zwalczaniu omawianego procederu, ale nadto także w kompleksowy sposób prezentuje je z odniesieniem do polskich realiów. Krajowa ocena ryzyka z 2019 r. zawiera informacje na temat bieżącego stanu zagrożenia procederami prania pieniędzy oraz finansowania terroryzmu, prognozy oraz tendencje panujące na rynku finansowym i pozafinansowym, które mogą sprzyjać zachowaniom kryminogennym, w tym w szczególności tym, które z punktu widzenia niebezpieczeństwa wystąpienia powyższych zjawisk mają znaczenie kardynalne. Dokument GIIF prezentuje również, co należy pozytywnie ocenić, zagrożenie innymi czynami, które stosunkowo często (bazując na sprawozdaniach z działalności GIIF) stanowią czyny bazowe dla prania pieniędzy. Ponadto KOR zawiera charakterystykę działalności instytucji objętych obowiązkami wynikającymi z realizacji ustawy z podziałem na rynki: finansowy i pozafinansowy, a także opis samego zjawiska prania pieniędzy (analogicznie —

finansowania terroryzmu) i analizę aktów normatywnych obowiązujących w tym względzie. Co ważne wskazuje nie tylko na stan zagrożenia wspomnianymi procederami, ale także „podatność" na ich wystąpienie — zob. https://www.knf.gov.pl/o_nas/komunikaty?articleId=66631&p_id=18 (25.02.2020 r.). Pozwala tona stwierdzenie, iż dokument GIIF spełnia stawiane przed nim oczekiwania, wynikające m.in. regulacji wspólnotowych.

Wobec powyższego niejasny pozostaje powód, dla którego do uznania IO pozostawiono decyzję w kwestii oparcia się na informacjach zawartych w dokumencie Generalnego Inspektora przy tworzeniu własnych ocen ryzyka. Skoro KOR zawiera wskazanie obszarów zagrożeń, jak i perspektywy ich wystąpienia, zebrane na podstawie danych dostępnych GIIF, a zatem i najbardziej wiarygodnych, a co więcej, daje się z niej wyprowadzić ocenę ryzyka zarówno dla instytucji finansowych, jak i pozafinansowych, to należałoby oczekiwać, iż ten właśnie dokument będzie podstawowym, na którym będą opierały się IO opracowując stosowne dokumenty na własny użytek. Wobec tego należałoby postulować zastąpienie zapisu przewidzianego w art. 27 ust. 2 u.p.p., dającego instytucjom obowiązanym fakultatywne prawo do oparcia się na KOR, bardziej stanowczym, który przewidywałby, iż „IO przy ocenianiu ryzyka opierają się w szczególności na obowiązującej krajowej ocenie ryzyka, a mogą uwzględniać także sprawozdanie Komisji Europejskiej, o którym mowa w art. 6 ust. 1–3 dyrektywy 2015/849". Wydaje się, że taka zmiana pozwoliłaby na nadanie właściwej rangi dokumentowi GIIF (dyktowanej celem opracowania i popartej profesjonalizmem tego organu), zarazem jednak, zważywszy na okresowy charakter KOR, nie ograniczałaby ona IO do powinności restrykcyjnego podążania za wskazaniami płynącymi z tego dokumentu i nie pozbawiała ich możliwości uwzględnienia czegoś ponadto, co z niego wynika. Z całą pewnością zaś, nie można traktować czynników ryzyka, na jakich opierają się IO podejmując ocenę, co do nich, za alternatywne wobec KOR, skoro ten ostatni dokument odnosi się właśnie do opisu tych czynników.

Natomiast w kwestii czynników, na jakich opierają się IO dokonując oceny ryzyka, uwagę zwraca przede wszystkim ich stosunkowo ogólnie zapisana charakterystyka. Jest to zresztą zrozumiałe, jeśli zważyć na praktycznie niewyczerpany katalog poszczegółowych determinantów, jakie *in concreto* wpływają na ryzyko prania pieniędzy w każdej z instytucji. Wobec powyższego, podejmując próbę konkretyzacji takich czynników, z teoretycznego punktu widzenia można by posiłkować się np. „Wspólnymi wytycznymi", opracowanymi na podstawie art. 17 i 18 ust. 4 dyrektywy (UE) 2015/849. Jednak wyprowadzony na tej podstawie *risk management* w istocie nie będzie odpowiadał oczekiwaniom płynącym z wejścia w życie nowych przepisów. Wynika to nie tylko z tego, że Wytyczne te bardzo drobiazgowo określają i grupują czynniki (np. dotyczące klienta, obszaru geograficznego, jurysdykcji, a także produktu, usługi lub transakcji, w tym kanałów dostaw), ale przede wszystkim z tego, że przewidziane w nich zapisy są często nieprecyzyjne i wysoce niedookreślone. Tytułem przykładu można wskazać na czynnik poziomu ryzyka dotyczący klienta taki, jak „reputacja" (ze wskazaniem, że należy brać pod uwagę m.in. to „czy istnieją niekorzystne doniesienia medialne lub inne istotne źródła informacji na temat klienta; czy istnieją jakiekolwiek domniemania działalności przestępczej lub terrorystycznej wobec klienta lub beneficjenta rzeczywistego, etc.); "inne źródła informacji" takie, jak „wiedza własna" (niejasne jest, czy chodzi o wiedzę pracownika czy całej instytucji); „informacje od społeczeństwa obywatelskiego" oraz pochodzące „z wiarygodnych, otwartych źródeł" (raporty w cieszących się uznaniem tytułach prasowych, informacje od wiarygodnych podmiotów prywatnych, informacje od organizacji). Decyzja w kwestii „wiarygodności" czy „wartości" i rzetelności informacji ma jednak całkowicie uznaniowy charakter.

Poza powyższym obowiązkiem związanym z oceną ryzyka, ustawa z 1.03.2018 r. nadal utrzymuje w mocy kardynalne obowiązki IO. Wynikają one przede wszystkim z:

- art. 74 u.p.p. (obowiązek niezwłocznego, dokonanego jednak nie później niż w terminie 2 dni roboczych od dnia potwierdzenia przez instytucję obowiązaną podejrzenia, złożenia zawiadomienia do Generalnego Inspektora Informacji Finansowej o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa określonego w art. 299 k.k. lub art. 165a k.k., ze wskazaniem na zakres danych uwzględnianych w takim zawiadomieniu — ust. 3 art. 74);
- art. 86 u.p.p. (obowiązek niezwłocznego zawiadomienia GIIF za pomocą środków komunikacji elektronicznej o przypadku powzięcia uzasadnionego podejrzenia, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu);
- art. 90 u.p.p. (tzw. następcze przekazanie tego zawiadomienia w przypadku, gdy jego niezwłoczne przesłanie było niemożliwe).

Obowiązki instytucji wynikające z V dyrektywy AML

Wprowadzenie do ustawy z 1.03.2018 r. kategorii podmiotów, jakimi są beneficjenci rzeczywiści, a tym samym i realizacja nowych obowiązków przez IO względem takich osób, wynika przede wszystkim z postanowień IV dyrektywy AML. Kolejna, V dyrektywa AML doprecyzowała jednak postanowienia dotyczące m.in. sposobu pozyskiwania i gromadzenia danych na temat takich osób.

Warto wskazać, że w uzasadnieniu do projektu ustawy z 1.03.2018 r. podniesiono, że sama terminologia odnosząca się do beneficjenta rzeczywistego, rzutująca ostatecznie na kształt definicji legalnej, rodzi wiele wątpliwości. Sprowadzają się one do określenia warunków, jakie należy uznać za miarodajne w tym względzie. Polski ustawodawca postanowił przyjąć za zasadnicze kryteria pozwalające nadać status beneficjenta rzeczywistego danej osobie: kryterium „kontrolne" (tj. kontrola sprawowana przez osobę/y fizyczną/e) oraz możliwość wywierania decydującego wpływu na decyzje podejmowane przez dany podmiot — *de facto* będący klientem IO. Krajowy legislator zdecydował się również na

zawężenie kręgu podmiotów zobligowanych do identyfikacji beneficjenta rzeczywistego (art. 58 u.p.p.). Jak podniósł w uzasadnieniu do projektu ustawy, powodem tego jest fakt, że art. 30 ust. 1 dyrektywy 2015/849 nakłada taką powinność jedynie na „podmioty o charakterze korporacyjnym i inne podmioty prawne". W stosunku do nich w prawie wspólnotowym przewidziano konieczność dysponowania przez instytucje zobowiązane „odpowiednimi, dokładnymi i aktualnymi informacjami o ich beneficjentach rzeczywistych", w tym zawierającymi szczegółowe informacje o stosunkach łączących te podmioty z beneficjentami rzeczywistymi. Natomiast zważywszy na obowiązujące w naszym kraju przepisy, pojęcie „podmiotów korporacyjnych" wydaje się nieprecyzyjne (por. uzasadnienie do projektu ustawy z 1.03.2018 r.; druk 2233, s. 30–33). Dostrzegł to zresztą sam projektodawca, który wywiódł, że „powszechnie przyjmuje się podział podmiotów prawa na oparte na substracie osobowym podmioty typu korporacyjnego oraz na oparte na substracie majątkowym podmioty typu zakładowego. (...) podmioty prawa typu korporacyjnego są zbiorowościami osób związanych z tym podmiotem stosunkiem członkostwa, realizującymi wspólne cele oraz decydującymi o celach i aktywności korporacji" (por. uzasadnienie do projektu ustawy z 1.03.2018 r.; druk 2233, s. 30–33). Mając na uwadze powyższe, jak również ideę podejścia opartego o analizę ryzyka, jaka przyświeca całej polityce przeciwdziałania praniu pieniędzy, rodzimy prawodawca uznał za zasadne objęcie obowiązkiem identyfikacji beneficjentów rzeczywistych tylko tych „podmiotów korporacyjnych", „ (...) których konstrukcja pozwala na ukrycie tożsamości osób fizycznych faktycznie wywierających decydujący wpływ na działania podejmowane przez takie podmioty i w stosunku do których zidentyfikowano ryzyko wykorzystania tych podmiotów w celu ukrycia tożsamości przestępców uczestniczących w procederze prania pieniędzy" (por. uzasadnienie do projektu ustawy z 1.03.2018 r.; druk 2233, s. 30–33). Dodatkowo odwołał się on do praktyki Generalnego Inspektora, z której wynika, że „ (...) nie każdy typ spółki znany prawu polskiemu w tym samym stopniu jest narażony na wykorzystanie w przestępczym procederze". Stanowiło to podstawę do wyłączenia spod obowiązku identyfikowania beneficjentów rzeczywistych spółek jawnych oraz spółek publicznych (ściślej — spółek akcyjnych w rozumieniu przepisów ustawy z 29.07.2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych).

Wyłączenie dotyczące tych pierwszych zostało podyktowane „specyficznym przeznaczeniem spółki partnerskiej jako podmiotu utworzonego przez wspólników w celu wykonywania wolnego zawodu, zasad uzyskania uprawnień pozwalających na wykonywanie tych zawodów oraz zasad odpowiedzialności za zobowiązania związane z wykonywaniem wolnego zawodu przez poszczególnych partnerów", zaś w przypadku spółki publicznej „odrębnie określonymi obowiązkami o charakterze informacyjnym, jak i znaczną fluktuacją akcjonariatu spółek publicznych" (por. uzasadnienie do projektu ustawy z 1.03.2018 r.; druk 2233, s. 33–34). Takie uzasadnienie przyjętego rozwiązania prawnego, chociaż niewątpliwie pozytywnie odebrane przez podmioty wyłączone spod omawianego obowiązku, nie może nie zastanawiać. Argumentacja podniesiona w uzasadnieniu do projektu i przytaczana w literaturze przedmiotu (Grynfelder, 2020, komentarz do art. 58 u.p.p.), z której wynika, że te typy spółek stwarzają relatywnie niższe ryzyko wykorzystania ich działalności do prania pieniędzy teoretycznie nie nasuwa obiekcji. Może jednak nasuwać uzasadnione zastrzeżenia objęcie obowiązkiem identyfikacji beneficjanta rzeczywistego przedstawicieli wolnych zawodów, którzy wykonują działalność w ramach „podmiotu korporacyjnego", w innej formie organizacyjno-prawnej niż spółka jawna. Nie wydaje się, aby istniały wystarczająco przekonujące argumenty, które przemawiałyby za takim podejściem, w szczególności dotyczące np. złożonego charakteru prowadzonych spraw lub gałęzi prawa, jakiej one w przeważającej mierze dotyczącą. Należy mieć wszakże na uwadze to, że z założenia zakres obowiązków nałożonych na takie podmioty przez ustawę został ograniczony, co jest podyktowane specyfiką czynności podejmowanych przez przedstawicieli zawodów zaufania publicznego (por. art. 2 ust. 1 pkt 14 u.p.p.). Natomiast w odniesieniu do spółki publicznej, motywy wyłączenia jej na mocy art. 58 u.p.p. wydają się racjonalne, zwłaszcza w kontekście oczekiwanej, obligatoryjnej od 1.01.2021 r. dematerializacji akcji (ustawa z 30.08.2019 r. o zmianie ustawy — Kodeks spółek handlowych oraz niektórych innych ustaw, Dz.U. z 2019 r. poz. 1798).

Celem realizacji wymagań wynikających z art. 30 ust. 3 dyrektywy 2015/849, związanych z obowiązkiem identyfikacji beneficjentów rzeczywistych, od 13.10.2019 r. działa system teleinformatyczny — Centralny Rejestr Beneficjentów Rzeczywistych (por. art. 55 i n. u.p.p.). Na mocy rozporządzenia MF z 16.05.2018 r. zgłoszenie o beneficjencie rzeczywistym jest składane przez objęte tym obowiązkiem spółki za pośrednictwem strony internetowej, której identyfikator URI (ang. Uniform Resource Identifier) jest zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych. Zgłoszenie jest szyfrowane w sposób automatyczny w systemie teleinformatycznym wykorzystywanym przez tego ministra do przyjmowania zgłoszeń (por. § 2 rozporządzenia Ministra Finansów z 16.05.2018 r. w sprawie zgłaszania informacji o beneficjentach rzeczywistych wydanego na podstawie art. 62 u.p.p., Dz.U. z 2018 r. poz. 968). Sposób organizacji Rejestru stanowi zarazem realizację postulatów płynących z V dyrektywy AML, która jednak kładzie dodatkowo nacisk na konieczność zapewnienia publicznego dostępu dodanych zgromadzonych w tym rejestrze. Zdaniem prawodawcy wspólnotowego umożliwi to m.in. „większą kontrolę informacji przez społeczeństwo obywatelskie, w tym przez prasę lub organizacje społeczeństwa obywatelskiego", a także przyczynia się do utrzymania zaufania do uczciwości transakcji finansowych oraz do systemu finansowego. Stwierdzenie to, chociaż bez wątpienia słuszne, to jednak z praktycznego punktu widzenia może budzić uzasadnione obiekcje, zwłaszcza ze strony podmiotów, na temat których — co warto w tym miejscu odnotować — bez ich wiedzy (por. art. 65 u.p.p.) gromadzone są owe dane.

Istotne zmiany w zakresie przeciwdziałania praniu pieniędzy przyniosło także poszerzenie zakresu przedmiotowego o te aspekty, które wiążą się z obrotem walutą wirtualną. Stanowi to istotne novum, o niezwykle doniosłym — z praktycznego punktu widzenia — znaczeniu (por. także Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie „walut" wirtualnych z 7.07.2018 r., http: //www. nbp. pl/home. aspx? f=/aktualnosci/wiadomosci_2017/ww-pl. html (12.03.2020 r.)). Jak trafnie sygnalizowano, rozwój walut wirtualnych, spośród których najbardziej znaną jest *Bitcoin* (BTC), jako zjawisko stosunkowo nowe i nie do końca poznane, co do swoich prawdziwych możliwości, tudzież związanych z tym zagrożeń dla obrotu gospodarczego, wymaga stałego monitorowania i analizy jako czynnika kryminogennego (por. pismo z 28.05.2015 r. Podsekretarz Stanu w Ministerstwie Finansów [FN7.054.9.2015], *Regulacje dotyczące wirtualnej waluty Bitcoin*; pismo to prezentuje wyjaśnienia Ministerstwa Finansów w przedmiocie funkcjonowania „walut wirtualnych", Monitor Prawa Bankowego 2016, 6, s. 13–17).

Z tego względu obecnie wiele organizacji i jednostek analityki finansowej z innych krajów — analogicznych do GIIF (nie tylko tych należących do UE), a także organizacje międzynarodowe powołane do życia w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, prowadzi szereg działań zmierzających do pełnego rozpoznania zagrożeń związanych z rozwojem walut wirtualnych. Waluty takie „ (...) bazują na złożonym systemie protokołów kryptograficznych. Kreacja Bitcoin polega na wygenerowaniu kodu (szyfru) przy użyciu tzw. koparki (ang. *excavator*), to znaczy określonego programu i sprzętu komputerowego o wysokiej mocy obliczeniowej w sieci *peer-to-peer*" (zob. Dąbrowska, 2017, 1, s. 55; Bala, Kopyściański i Srokosz, 2016, s. 77–81).

Definicję legalną waluty wirtualnej zawiera również ustawa z 1.03.2018 r. Zgodnie z art. 2 ust. 2 pkt 26 u.p.p., walutą wirtualna jest „cyfrowe odwzorowanie wartości, które nie jest prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej, ani międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące. Ponadto waluta wirtualna jest pieniądzem elektronicznym w rozumieniu ustawy z 19.08.2011 r. o usługach płatniczych, wekslem lub czekiem, ani instrumentem finansowym. Waluta taka jest wymienialna w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywana lub przeniesiona albo może być przedmiotem handlu elektronicznego. Ponadto przewidziano, iż obecnie wartości majątkowe w rozumieniu u.p.p. obejmują także dodatkowo waluty wirtualne (art. 2 ust. 2 pkt. 27 u.p.p.).

Warto jednak przy okazji nadmienić, że definicję waluty wirtualnej przewidziano również w projekcie ustawy o Centralnej Bazie Rachunków, której wprowadzenie zakłada dyrektywa IV dyrektywa AML (Czarnecki, 2017). Zgodnie z art. 2 pkt 6 tego projektu (poniżej jako CBR), opublikowanego z datą 22.12.2016 r., waluta wirtualna oznacza „zbywalne prawo majątkowe, którego przedmiotem jest cyfrowa reprezentacja wartości, posiadająca swój ekwiwalent w środku płatniczym, traktowana jako środek wymiany i jednostka rozrachunkowa, nieposiadające statusu legalnego środka płatniczego i niebędące pieniądzem elektronicznym w rozumieniu ustawy z 19.08.2011 r. o usługach płatniczych, które może być przekazywane, przechowywane lub sprzedawane za środki płatnicze drogą elektroniczną" — zob. https: //legislacja.rcl.gov.pl/projekt/12293403/katalog/12400913 (23.02.2020). Pomimo, że ustawa o CBR nie doczekała się wejścia w życie, to własną Centralną informację o rachunkach (tu jako CIR) wdrożyły banki oraz SKOKi — Centralna informacja jest dostępna na www. centralnainformacja. pl (21.03.2020).

W tym miejscu nie sposób byłoby jednak nie wspomnieć i o tym, że V dyrektywa AML rozszerza zakres stosowania dyrektywy (UE) 2015/849 na podmioty zajmujące się świadczeniem usług wymiany walut pomiędzy walutami wirtualnymi a walutami fiducjarnymi (więcej na temat zagrożenia dla obrotu finansowego Bala, Kopyściański i Srokosz, 2016, s. 143–144), a także dostawców kont walut wirtualnych. Uwzględniając postępujący rozwój sektora usług finansowych i przede wszystkim wzajemne „przenikanie" się obszarów zagrożeń (zyski wygenerowane z transakcji „brudnymi" wartościami majątkowymi, pochodzącymi z transakcji „bitcoinowej", mogą być legalizowane za pośrednictwem np. usług bankowych po przeprowadzeniu transakcji z jej wykorzystaniem. Mowa tu o systemie z dwukierunkowym przepływem pieniężnym, w którym wirtualna waluta może być wymieniana na inne waluty bez ograniczeń, czego przykładem jest właśnie *Bitcoin*, który jest walutą wymienialną w elektronicznych kantorach lub na giełdach — por. Mackiewicz i Musiał, 2014, s. 136–139.

Zmiana w tym względzie będzie nie tylko koniecznością, ale przede wszystkim słusznym krokiem racjonalnego prawodawcy. W tym miejscu, wypada przypomnieć, że pieniądz fiducjarny „ (...) charakteryzuje się tym, że jego wartość nie jest w żadnym przypadku powiązana z wartością nośnika, a opiera się na wierze użytkownika w możliwość wymiany go w każdym czasie na podstawową wartość" (Jurkowska, 2004, s. 273; Srokosz, 2011, s. 212–213). Takim pieniądzem jest również pieniądz elektroniczny, stanowiący swoisty, „elektroniczny surogat monet i banknotów", który jest przechowywany na elektronicznym nośniku np. karcie mikroprocesorowej (karta *pre-paid*, uprzednio opłaconej, jak np. karta telefoniczna) lub w pamięci komputera (*network*, *software money*) i przeznaczony jest głównie do dokonywania płatności elektronicznych o ograniczonej wartości (Jurkowska, 2004, s. 273; Srokosz, 2011, s. 212–213; Cyman, 2013, s. 33–44. Pieniądz fuducjarny jest uznawany za tożsamy z pieniądzem *sensu stricto* (gotówkowym). Jako taki stanowi zatem prawny środek płatniczy (ang. *legal tender*) i charakteryzuje się m.in. powszechnością jego akceptacji (połączoną z obowiązkiem jego przyjmowania, skoro odmowa przyjęcia zapłaty prowadzi do popadnięcia dłużnika w zwłokę) oraz zdolnością do umarzania zobowiązań (Cyman, 2013, s. 54).

Co istotne, V dyrektywa AML ustanawia również definicję „dostawcy konta waluty wirtualnej", którym — zgodnie z jej art. 1 pkt 2d jest „podmiot świadczący usługi polegają-

ce na przechowywaniu prywatnych danych uwierzytelniających w imieniu swoich klientów na potrzeby posiadania, przechowywania i przekazywania walut wirtualnych". Odpowiednika takiej definicji brak w polskich regulacjach. Należy zatem zgłosić stosowny postulat wprowadzenia adekwatnego uregulowania. Co prawda, jak dostrzega sam prawodawca unijny, zmiany w tym zakresie nie rozwiążą całkowicie problemu anonimowości transakcji z użyciem walut wirtualnych, „ (...) ponieważ duża część środowiska posługującego się tymi walutami pozostanie anonimowa ze względu na fakt, że użytkownicy mogą dokonywać transakcji również bez pośrednictwa takich dostawców" (Preambuła, V dyrektywy AML pkt 9), niemniej jednak wskazuje on także na to, że krajowe jednostki analityki finansowej powinny być w stanie uzyskać informacje pozwalające im na powiązanie adresu waluty wirtualnej z tożsamością jej właściciela.

Jako środek służący przeciwdziałaniu praniu pieniędzy, prawodawca unijny zalecił wobec tego „obniżenie istniejących limitów dla anonimowych kart przedpłaconych ogólnego zastosowania oraz zidentyfikowanie klienta w przypadku zdalnych transakcji płatniczych w przypadku gdy kwota transakcji przekracza 50 euro", z zastrzeżeniem, że należy mieć przy tym na uwadze „potrzeby konsumentów dotyczące korzystania z instrumentów przedpłaconych ogólnego zastosowania". Wobec czego znowelizowane przepisy nie powinny uniemożliwić im korzystania z takich instrumentów „w interesie włączenia społecznego i włączenia w rynek finansowy" (jak wskazano w V dyrektywie AML).

Wnioski

Z uwagi na obszerny charakter zmian, jakie zostały wprowadzone ustawą z 1.03.2018 r., ich wyczerpujące omówienie w tego typu opracowaniu naukowym wydaje się niemożliwe. Nie temu celowi zresztą ma ono służyć. Jego istotą jest bowiem wskazanie raczej na te z nowowprowadzonych przepisów, które w sposób odmienny od dotychczas przyjmowanego (tj. przewidzianego ustawą z 16.11.2000 r.), określają obowiązki IO. Stąd też powoływanie przepisów, w których zostały sprecyzowane środki bezpieczeństwa finansowego, a także identyfikacja oraz weryfikacji tożsamości klienta, czy tego, jakie transakcje podlegają obowiązkowi rejestracji muszą w nim zostać pominięte (por. w tym względzie art. 35 u.p.p.).

Postanowienia ustawy z 1.03.2018 r. w tych kwestiach nie odbiegają znacząco od tych, jakie przewidywała jej „poprzedniczka". Można w tym miejscu jedynie nadmienić, że środki bezpieczeństwa finansowego należy stosować „ (...) w zakresie i z intensywnością uwzględniającymi rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz jego ocenę" (art. 33 ust. 4 u.p.p.). Poza „tradycyjnymi" środkami bezpieczeństwa finansowego, IO, powinny także zapewnić, w wypadkach, o których mowa w art. 43–46 u.p.p., stosowanie „wzmożonych środków bezpieczeństwa finansowego", w szczególności w przypadku nawiązywania stosunków gospodarczych w nietypowych okolicznościach, czy wobec klientów pochodzących z państwa trzeciego wysokiego ryzyka lub mających w nim siedzibę.

Reasumując, uchwalenie ustawy z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu stanowi przede wszystkim wyraz realizacji postulatów płynących z potrzeby dostosowania polskich regulacji prawnych do unormowań wspólnotowych, a konkretnie IV i V dyrektywy AML. Rezultatem implementacji do krajowego porządku prawnego postanowień IV dyrektywy AML jest nie tylko „kosmetyczna" zmiana obowiązującej od ponad 17 lat regulacji, ale zastąpienie jej zupełnie nową ustawą.

Ustawa z 1.03.2018 r., chociaż z pozoru bazuje na systemie przeciwdziałania praniu pieniędzy znanemu ustawie z 16.11.2000 r., to jednak w wielu istotnych kwestiach znacznie różni się od poprzedniej. Dotyczy to w szczególności nowych obowiązków, jakie w związku z BRA nakłada ona na podmioty objęte zakresem jej unormowań. Ocenie pod kątem ryzyka prania pieniędzy podlegają „stosunki gospodarcze" oraz „transakcje okazjonalne", którymi to terminami zastąpiono podstawowe pojęcie „transakcji". Nadal jednak procedury przeciwdziałania omawianemu zjawisku obejmują czynności, których przedmiotem są transakcje progowe (tj. w kwocie, co do zasady przekraczającej równowartość 10.000 euro, w tym stanowiące transakcje powiązane oraz transakcje podejrzane). Efektywność tego systemu ma zapewniać także bieżące monitorowanie przez IO stosunków gospodarczych podejmowanych z klientem.

Ustawa z 1.03.2018 r. wprowadziła również inne istotne zmiany, m.in. w zakresie podmiotowym. Odnosi się to w szczególności do katalogu tych instytucji, który został zweryfikowany pod względem realnego zagrożenia udziałem danej instytucji w omawianym procederze. Podyktowane to było koniecznością dostosowania krajowych przepisów do IV dyrektywy AML. Niewątpliwie za słuszne należy uznać dostrzeżenie zagrożeń, jakie dla obrotu gospodarczego (pod kątem możliwości ich wykorzystania do celu legalizacji „brudnych" zysków) może nieść wirtualna waluta. Wysoce pożądane byłoby jednak wprowadzenie do ustawy regulacji, które pozwolą na dostosowanej krajowych przepisów także do V dyrektywy AML. Odnosi się to zarówno do charakterystyki obowiązków nałożonych na podmioty prowadzące obrót walutą wirtualną, jak i innych instytucji, które zostały już uwzględnione w ustawie, a których zakres działalności należałoby jednak zrewidować pod kątem dostosowania spoczywających na nich obowiązków do postanowień wspomnianej dyrektywy.

Pewne zastrzeżenia można natomiast zgłosić pod adresem „nowych" powinności nałożonych na IO, które *de facto* stanowią kwintesencję ustawy z 1.03.2018 r. i zarazem zasadnicze *ratio legis* jej uchwalenia. Mowa o obwiązkach związanych z oceną ryzyka. Wobec braku jasnych i precyzyjnych kryteriów oceny poziomu ryzyka, ich uwzględnienie w praktyce może być trudne do przeprowadzenia. Wiele w tej kwestii będzie zależało od dotychczasowych procedur, jakie IO wypracowały już przez lata obowiązywania ustawy przeciwdziałającej „praniu" (tj. ustawy z 16.11.2000 r.) i do których, jak należy przewidywać, będą się one nadal odwoływały szacując poziom ryzyka prania pieniędzy.

Nałożenie na IO enigmatycznie określonych obowiązków (*risk based approach*), czy tym bardziej takich, których wyegzekwowanie w przypadku wielu z nich jest praktycznie niewykonalne, nie wydają się sprzyjać efektywności przeciwdziałaniu praniu pieniędzy. Wystarczy w tym miejscu wskazać na konieczność prowadzenia „bieżącego monitoringu stosunków gospodarczych", z całym „bagażem" nieścisłości, jakie niesie za sobą to określenie. Wydaje się zatem, że skuteczna walka z omawianym procederem będzie możliwa przede wszystkim dzięki pozostawieniu w „nowej" ustawie przepisów dotyczących trybu postępowania oraz kompetencji podmiotów uczestniczących w jej wykonaniu. Ujawnienie przypadków prania pieniędzy w praktyce uzależnione jest bowiem w dużej mierze od dobrze funkcjonującej współpracy pomiędzy podmiotami tworzącymi system przeciwdziałania temu zjawisku. Poza instytucjami obowiązanymi oraz GIIF, istotny udział mają w nim także podmioty sprawujące kontrolę wykonania ustawy w ramach nadzoru i kontroli, a także jednostki współpracujące. Należy zatem wyrazić przekonanie, że wzorem dotychczasowych przepisów, zasadniczy wpływ na efektywność zapobiegania praniu pieniędzy będzie miała przede wszystkim identyfikacja klienta rzetelnie przeprowadzana przez IO, a także zastosowanie przez nie (adekwatnych do sytuacji) środków bezpieczeństwa finansowego. To zaś, bazując na współpracy z GIIF, może skutkować podjęciem przez niego wymiernych kroków takich, jak blokada rachunku, wstrzymanie transakcji lub zamrożenie środków finansowych, a na etapie postępowania przygotowawczego — zabezpieczeniem inkryminowanych wartości majątkowych przez prokuratora.

Przypisy/Notes

[1] Por. *Sprawozdanie Generalnego Inspektora Informacji Finansowej z wykonania ustawy z 1.03.2018 r. o przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu za rok 2018*, Warszawa, marzec 2019 r., s. 27. Wynika z niego, że w 2018 r. GIIR otrzymał 42.766 informacji o pojedynczych transakcjach, których okoliczności mogą wskazywać na związek z popełnieniem przestępstwa (ang. *Suspicious Transaction Reports* — STR), w tym 42.737 transakcji były oznaczonych jako mogące mieć związek z praniem pieniędzy (ang. *Suspicious Transaction Reports on Money Laundering* — STR-ML), a 29 transakcji — jako mogące mieć związek z finansowaniem terroryzmu (ang. *Suspicious Transaction Reports on Terrorist Financing* — STR-TF), https://www.gov.pl/documents/1079560/1080340/sprawozdanie_za_2018_r_.pdf/9518c498-2d45-ed87-1165-a27e7a5ebbc3 (28.03.2020 r.).

[2] „Czynniki ryzyka" to zmienne, które same w sobie, albo w połączeniu z innymi mogą zwiększać lub zmniejszać ryzyko prania pieniędzy lub finansowania terroryzmu i wynikają one z danego stosunku gospodarczego lub transakcji okazjonalnej. „Podejście z uwzględnieniem ryzyka" oznacza, że: „właściwe organy i podmioty zobowiązane określają, oceniają i rozumieją ryzyka ML/TF, na które narażone są podmioty podlegające ocenie i podejmują środki AML/CFT proporcjonalne do tych ryzyk" — Wspólne wytyczne.

Bibliografia/References

Bala, S., Kopyściański, T., Srokosz, W. (2016). *Kryptowaluty jako elektroniczne insrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego.

Cyman, D. (2013). *Elektroniczne instrumenty płatnicze a bezpieczeństwo uczestników rynku finansowego*, Warszawa: Wolters Kluwer Polska.

Czarnecki, J. (2017). Wirtualne waluty w projekcie ustawy o Centralnej Bazie Rachunków, *Biuletyn Nowych Technologii*, 2.

Dąbrowska, J. (2017). Charakter prawny bitcoin, *Studia i Artykuły*, 1.

Golonka, A. (2009). „Kolejna" dyrektywa unijna w sprawie przeciwdziałania praniu pieniędzy — czas na ocenę dostosowania polskich regulacji prawnych, *Studia Europejskie CE UW*, 1.

Golonka, A. (2008). *Prawnokarne zagadnienia przeciwdziałania wprowadzania do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.

Grynfelder, J. (2020). W: W. Kapica (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa: LEX, komentarz do art. 58 u.p.p. https://doi.org/10.21697/kpp.2015.13.2.01.

Kaczmarek, T. T., Królak-Werwińska J. (2008). *Handel międzynarodowy — zarządzanie ryzykiem — rozliczenia finansowe*, Warszawa: Wolters Kluwer Polska.

Mackiewicz, P., Musiał, M. (2014). Rozwój wirtualnych systemów monetarnych, *Nauki o finansach (Financial Sciences)*, 1. https://doi.org/10.15611/nof.2014.1.12.

Srokosz, W. (2011), *Instytucje parabankowe w Polsce*, Warszawa: Wolters Kluwer Polska.

Wójcik, J. W. (2002), *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa: Wydawnictwo Twigger.

„Wspólne wytyczne" z 4.01.2018 r. w sprawie uproszczonych i wzmożonych środków należytej staranności wobec klientów oraz czynników, które instytucje finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy lub finansowania terroryzmu w powiązaniu z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznym (JC 2017 37), https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_PL_04-01-2018.pdf (29.03.2020 r.), dalej Wspólne wytyczne. https://doi.org/10.1787/9789264308121-pl

Dr hab. Anna Golonka

Profesor Uniwersytetu Rzeszowskiego, Kierownik Zakładu Prawa Karnego w Instytucie Nauk Prawnych (Wydział Prawa i Administracji) w Kolegium nauk społecznych. Autorka blisko 90 publikacji naukowych z zakresu prawa karnego, w tym monografii poświęconych problematyce prania pieniędzy oraz niepoczytalności i poczytalności zmniejszonej.

Dr hab. Anna Golonka

A professor at the University of Rzeszow, Head of the Criminal Law Department at the Institute of Legal Sciences at the College of Social Sciences, Faculty of Law and Administration, Author of nearly 90 scientific publications in the field of criminal law, including monographs devoted to money laundering and insanity and diminished responsibility.