

Pranie pieniędzy

KRYPTOWALUTY • AML • OBRONA KARNA

Jak legalnie ograniczać ryzyko odpowiedzialności
i bronić się przed zarzutem z art. 299 k.k.

PRAWO POLSKIE I UNIJNE

MiCA • Travel Rule • Blockchain • Orzecznictwo SN
Dowody cyfrowe • AML/KYC • Strategia procesowa

Mapa opracowania

REDAKCYJNY PRZEWODNIK PO ZAGADNIENIACH

01

RAMY ODPOWIEDZIALNOŚCI

Znamiona art. 299 k.k., źródło aktywów i umyślność

02

PREWENCJA I COMPLIANCE

Bezpieczny obrót, KYC i dokumentowanie transakcji

03

KRYPTOAKTYWA I BLOCKCHAIN

MiCA, TFR, DeFi, stablecoiny i ślady on-chain

04

STRATEGIA OBRONY

Zarzut, dowody, biegli i zabezpieczenie majątku

05

ORZECZNICTWO I ŹRÓDŁA

Polskie i unijne podstawy argumentacji procesowej

ZASADA, OD KTÓREJ ZACZYNA SIĘ DOBRA OBRONA

Sygnal alarmowy AML nie jest dowodem winy.

Każdy element zarzutu wymaga odrębnego ustalenia i weryfikacji.

PRANIE PIENIĘDZY

Prewencja odpowiedzialności i obrona przed zarzutem z art. 299 k.k.

Poradnik ekspercki: kwalifikacja prawna • źródło majątku • umyślność • AML/KYC • obrona dowodowa • zabezpieczenie mienia • orzecznictwo SN i prawo UE

Stan prawny i stan weryfikacji: 20 października 2026 r.

Opracowanie ma charakter analityczny i edukacyjny. Nie jest opinią dotyczącą konkretnych akt sprawy. Zastosowanie też wymaga weryfikacji dat czynów, czasowego obowiązywania przepisów, materiału dowodowego i statusu uczestników. Zapobieganie zarzutowi oznacza legalność i transparentność działań, nigdy zatajenie dowodów, fałszywe dokumentowanie transakcji ani obchodzenie obowiązków AML.

STRESZCZENIE DLA PRAKTYKI

TEZA. Obrona w sprawie o pranie pieniędzy nie polega na wykazaniu, że transakcja była typowa, zyskowa lub dokonana przez bank. Koncentruje się na zakwestionowaniu elementów ustawowego typu czynu: przestępczego źródła określonych wartości, konkretnego zachowania przypisanego podejrzanemu, strony podmiotowej, kwalifikacji ilościowej oraz – w granicach odpowiedniej części przepisu – ustawowych cech działania.

Trzy poziomy trzeba od siebie oddzielić: (1) „red flag” w systemie AML, czyli czynnik ryzyka wymagający analizy przez instytucję obowiązującą; (2) procesowe podejrzenie przestępstwa, uzasadniające czynności organów; (3) udowodnienie znamion przestępstwa w postępowaniu karnym. Próg dla zgłoszenia AML nie jest tym samym co standard prawomocnego skazania. Sam raport do GILF nie zastępuje dowodu winy.

Fundamenty judykatury: uchwała SN (7) z 18.12.2013 r., I KZP 19/13: majątek może pochodzić bezpośrednio lub pośrednio z czynu, a sprawca czynu źródłowego może odpowiadać również za pranie; uchwała SN (7) z 24.06.2015 r., I KZP 5/15: nie wolno automatycznie kwalifikować całego salda mieszanego rachunku jako majątku „brudnego”, a końcowy zwrot o utrudnieniu wykrycia odnosi się do „innych czynności”, nie zaś do każdej czynności nazwanej. Wyrok SN z 05.03.2015 r., III KK 407/14, chroni przed utożsamianiem źródła nieudokumentowanego z przestępczym. [O1–O3]

CZĘŚĆ I. RAMY PRAWNE I WARUNKI ODPOWIEDZIALNOŚCI

I. Aktualne źródła prawa i zasada międzyczasowa

Podstawę odpowiedzialności karnej stanowi art. 299 ustawy z 6 czerwca 1997 r. – Kodeks karny. Na dzień sporządzenia opracowania uwzględniono tekst jednolity ogłoszony 16 października 2026 r. w Dz.U. 2026 poz. 1342. Obowiązki zapobiegawcze wynikają zasadniczo z ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst jednolity Dz.U. 2025 poz. 644 z późn. zm., w tym nowelizacją Dz.U. 2026 poz. 1206). Postępowanie reguluje Kodeks postępowania karnego (tekst jednolity Dz.U. 2026 poz. 490 z późn. zm.). [P1–P3]

UWAGA. W sprawie konkretnej transakcji należy odtworzyć brzmienie art. 299 k.k. w dacie czynu i zastosować art. 4 § 1 k.k., jeżeli doszło do zmiany ustawy. Przepisy o przeciwdziałaniu praniu pieniędzy i przepisy karne nie są tożsame: niewykonanie określonego obowiązku AML może rodzić odrębną odpowiedzialność administracyjną albo – w odpowiednich wypadkach – karną, lecz nie dowodzi samo przez się popełnienia czynu z art. 299 § 1 k.k.

Na poziomie unijnym odróżnić należy dyrektywę (UE) 2018/1673 o zwalczaniu prania pieniędzy za pomocą środków prawnokarnych, będącą istotnym kontekstem wykładni, od regulacji prewencyjnych AML. Rozporządzenie (UE) 2024/1624 (AMLR) będzie co do zasady stosowane od 10 lipca 2027 r., nie od daty jego przyjęcia w 2024 r. Dyrektywa (UE) 2024/1640 przewiduje etapowe terminy transpozycji, dlatego poszczególnych przyszłych obowiązków nie można bezkrytycznie przedstawiać jako już obowiązujących w październiku 2026 r. [UE1–UE3]

2. Konstrukcja art. 299 k.k. – sześć poziomów badania

1. Przedmiot czynności: zindywidualizowane środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome albo nieruchomości.
2. Pochodzenie: związek tego mienia z korzyścią powstałą przy popełnieniu czynu zabronionego; dopuszczalny jest związek pośredni, jednak musi zostać dowodowo wykazany.
3. Czynność: jedna z ustawowo wymienionych postaci działania, np. przyjęcie, posiadanie, używanie, przekazanie, ukrycie, transfer, konwersja, pomoc w przeniesieniu własności albo inne zachowanie spełniające warunki końcowej klauzuli.
4. Podmiot: co do zasady sprawcą § 1 może być każda osoba, natomiast § 2 ma charakter szczególny związany z wykonywaniem czynności w określonych podmiotach.
5. Strona podmiotowa: umyślność; dowody wiedzy i godzenia się na okoliczności przestępczego pochodzenia podlegają indywidualnej ocenie.
6. Zakres: data, miejsce, kwoty, uczestnicy, ewentualne porozumienie, znaczna korzyść, przygotowanie, przepadek i ewentualne przesłanki z § 8.

Zagrożenie dla czynu podstawowego z art. 299 § 1 i § 2 wynosi od 6 miesięcy do 8 lat pozbawienia wolności; przy działaniu w porozumieniu z innymi osobami (§ 5) lub osiągnięciu znacznej korzyści (§ 6) – od roku do 10 lat. Karalne jest także przygotowanie opisane w § 6a (do 3 lat). Art. 299 § 7 ustanawia szczególną podstawę obligatoryjnego przepadku z zastrzeżeniem zwrotu osobie uprawnionej, a § 8 – wyjątkowe rozwiązania dotyczące współpracy ze ściganiem, o ściśle określonych warunkach. [P1]

3. Przestępstwo źródłowe: co właściwie należy udowodnić?

Związek korzyści z czynem zabronionym nie może zostać zastąpiony ogólną narracją o „niejasnej działalności”, gotówce lub rzekomej „fikcyjności biznesu”. Dla obrony fundamentalne jest żądanie odpowiedzi: jaki czyn zabroniony ma być

źródłem korzyści; kiedy i w jakim mechanizmie doszło do jego popełnienia; na czym polega uzyskana korzyść; jak i w której części przełożyła się na mienie objęte zarzutem; jak organ wyklucza alternatywne legalne źródła?

Orzeczenie SN III KK 407/14 nie ustanawia wymogu prawomocnego skazania za przestępstwo bazowe ani obowiązku poznania każdej okoliczności tego czynu. Nakazuje natomiast powiązanie ustaleń o pochodzeniu mienia z czynem zabronionym, nie z samą nieudokumentowaną historią transakcji. Dyrektywa 2018/1673 w art. 3 ust. 3 wyraźnie wyklucza wymóg uprzedniego skazania za aktywność źródłową oraz dopuszcza ustalenie kryminalnego pochodzenia bez odtworzenia wszystkich elementów tej aktywności, w tym tożsamości jej sprawcy. W konkretnej sprawie zakres ustaleń musi jednak odpowiadać polskiej ustawie i standardom dowodowym procesu karnego. [O3; UE1]

Nie należy utożsamiać czterech różnych tez: „osoba nie ujawniła źródła” – „źródło jest sprzeczne z prawem” – „mienie pochodzi z czynu zabronionego” – „oskarżony umyślnie uczestniczył w praniu”. Każda wymaga odrębnej podstawy faktycznej. Deficyt dokumentów może uruchomić czynności sprawdzające i ocenę ryzyka, ale nie jest logicznym substytutem dowodu wszystkich kolejnych tez.

4. Autopranie, przyjęcie środków i czynności o charakterze neutralnym

Po uchwale I KZP 19/13 nie da się skutecznie twierdzić, że sprawca czynu bazowego z definicji nie może popełnić przestępstwa z art. 299 k.k. Jednocześnie nie wolno rezygnować z analizy, czy zarzucane zachowanie realizuje odrębny typ czynu: fakt wcześniejszego przestępstwa nie powinien prowadzić do mechanicznego wielokrotnego przypisywania tej samej czynności, bez wyjaśnienia czasowego, przedmiotowego i prawnego rozdzielenia poszczególnych zachowań.

Przykładowo – legalne w swej naturze prowadzenie rachunku, księgowanie faktury lub odbiór należności nie są automatycznie „bezpieczne”, jeżeli osoba umyślnie wykonuje czynność na mieniu pochodzącym z czynu zabronionego. Z drugiej strony sama nazwa czynności gospodarczej nie wystarcza do przypisania winy. Obrona bada ekonomiczną treść świadczenia, kontekst czasowy, zakres dostępnej wiedzy, rzeczywiste uprawnienia do rachunku i cele operacyjne.

5. „Inne czynności” i ograniczenie argumentu o braku zamiaru ukrycia

W uchwale I KZP 5/15 SN wskazał, że zamieszczony w końcowej części art. 299 § 1 k.k. zwrot o możliwości udaremnienia lub znacznego utrudnienia wykrycia dotyczy tylko kategorii „innych czynności”, a nie wszystkich ustawowo nazwanych sposobów działania. Nie jest więc trafną obroną uniwersalne stwierdzenie: „nie chciałem ukryć pieniędzy, więc nie mogłem ich prac”. Dla czynności nazwanych trzeba zbadać ich ustawowy charakter i umyślność względem pochodzenia mienia; w odniesieniu do „innych czynności” dochodzi analiza obiektywnej zdolności do utrudnienia wykrycia. [O2]

6. Strona podmiotowa: wiedza, zamiar bezpośredni i ewentualny

Art. 299 § 1 k.k. jest przestępstwem umyślnym. W praktyce oskarżenie rekonstruuje wiedzę lub godzenie się na przestępcze pochodzenie ze śladów pośrednich: ostrzeżeń, korespondencji, negocjacji ceny, nienaturalnego podziału ról, sprzecznych instrukcji, realnej kontroli nad środkami, powtarzalności nietypowych operacji, wcześniejszych doświadczeń i zachowania po uzyskaniu informacji ostrzegawczych. Sam fakt posiadania znaczącego majątku albo przeprowadzenia operacji gotówkowej nie stanowi samodzielnie dowodu zamiaru.

Dokumenty z okresu sprzed transakcji mają szczególną wartość: zapytania KYC, konsultacje z działem księgowości, wpisy o weryfikacji beneficjenta rzeczywistego, sprawdzanie podstawy płatności, żądanie faktury lub umowy, e-maile o wstrzymaniu czynności do czasu wyjaśnień. Ich znaczenia nie należy jednak przeceniać: formalna lista kontrolna nie chroni, gdy oskarżony równocześnie faktycznie wie o przestępczym pochodzeniu mienia.

Dyrektywa 2018/1673 w art. 3 ust. 2 dopuszcza, aby państwa penalizowały również sytuacje, w których sprawca podejrzewał lub powinien był wiedzieć o źródle majątku. Nie oznacza to automatycznego przeniesienia każdej przewidzianej tam opcji na art. 299 § 1 polskiego k.k.; o granicach odpowiedzialności przesądza krajowa ustawa, a dyrektywa nie może sama rozszerzać przestępstwa na niekorzyść jednostki. [UE1]

CZĘŚĆ II. LEGALNE ZAPOBIEGANIE RYZYKU ZARZUTU

7. Organizacja przepływu pieniędzy i dowodów legalnego pochodzenia

Najskuteczniejsza prewencja to zorganizowanie obrotu tak, aby prawdziwy cel i treść ekonomiczna czynności były możliwe do wykazania bez rekonstrukcji dokonywanej dopiero po wszczęciu dochodzenia. Dla podmiotów gospodarczych oznacza to spójność umów, faktur, wydań towaru, sprawozdawczości, wpisów księgowych, deklaracji podatkowych, rachunków i dokumentów transportowych; dla osób prywatnych – zachowanie dokumentacji sprzedaży majątku, darowizny, spadku, pożyczki, wynagrodzenia, oszczędności i innych rzeczywistych źródeł.

7.1. Minimalny pakiet dowodowy dla większej transakcji

- Podstawa prawna i gospodarcza: pisemna umowa z załącznikami, opisem świadczenia i rzeczywistym harmonogramem.
- Weryfikacja stron: dokumenty rejestrowe, umocowanie reprezentantów, beneficjent rzeczywisty, podstawowe relacje właścicielskie oraz zakres rzeczywistej działalności.
- Dokumenty wykonania: protokoły odbioru, raporty prac, korespondencja, dokumenty dostawy, potwierdzenia usług i praw do przedmiotu transakcji.
- Ścieżka pieniądza: potwierdzenia przelewów, wyciągi, rozrachunki, rozliczenie zaliczek i zwrotów, dokumentacja walutowa oraz powiązanie kwoty z konkretnym zobowiązaniem.
- Źródło środków, jeśli charakter transakcji tego wymaga: akty notarialne, dowody uzyskania dochodu, dziedziczenia lub darowizny, dokumenty pożyczek i sprzedaży aktywów; weryfikacja autentyczności.
- Nota ryzyka: jakie czerwone flagi zauważono, jakie wyjaśnienia uzyskano, kto podjął decyzję i dlaczego były one racjonalne na datę transakcji.
- Retencja i bezpieczeństwo: integralność plików, uprawnienia dostępu, oryginały, kopie zgodne z prawem i datowana historia zmian.

Dla instytucji obowiązanych art. 49 ustawy AML ustanawia jako regułę pięcioletni okres przechowywania wskazanych danych i dowodów, liczony według ustawowych punktów początkowych, z odrębnymi wyjątkami. Nie oznacza to pięcioletniego „bezpiecznego terminu” niszczenia dowodów w toczącej się sprawie karnej ani zniesienia innych obowiązków retencyjnych. [P2]

8. Kontrahent wysokiego ryzyka: co sprawdzić przed zawarciem umowy?

Standard staranności nie jest jednolity dla wszystkich. Osoba fizyczna niezawodowo sprzedająca swój używany samochód ma inne możliwości i obowiązki niż bank, kantor, dostawca usług kryptoaktywów czy kancelaria działająca w zakresie czynności objętych art. 2 ust. 1 pkt 14 ustawy AML. Uczciwa transakcja nie powinna być oceniana wyłącznie w świetle późniejszej wiedzy o kontrahencie; kluczowe jest to, co było wiadome albo racjonalnie dostępne uczestnikowi w chwili działania.

1. Potwierdź tożsamość i umocowanie osoby występującej za kontrahenta; porównaj deklarowaną działalność z dokumentami publicznymi i historią współpracy.
2. Wyjaśnij rzeczywisty przedmiot i gospodarczy sens operacji; szczególnie gdy struktura płatności odbiega od umowy.
3. Zweryfikuj, kto jest uprawnionym odbiorcą płatności i dlaczego ewentualna płatność ma zostać wykonana osobie trzeciej.
4. Przeanalizuj ryzyko sankcyjne, korupcyjne, podatkowe oraz pochodzenie aktywów w skali adekwatnej do charakteru czynności.
5. W przypadku sygnałów alarmowych wstrzymaj decyzję biznesową i zasięgnij porady prawnej; instytucja obowiązana realizuje dodatkowo ustawowe reguły AML i ewentualne zawiadomienia.

6. Zapisz faktyczny rezultat analizy i tożsamość osoby decyzyjnej; nie twórz dokumentacji pozornej ani wstecznie datowanej.

9. Sygnały ostrzegawcze – przesłanki kontroli, nie domniemanie winy

Sytuacja	Ryzyko wymagające wyjaśnienia	Bezpieczna reakcja zgodna z prawem
Niewyjaśniona płatność od osoby trzeciej	Niejasna podstawa świadczenia i właściciel środków	Ustalić podstawę prawną, stronę świadczenia i źródło finansowania
Duża gotówka bez racjonalnego kontekstu	Trudniejsza rekonstrukcja źródła i obiegu	Dokumentować rzeczywistą przyczynę oraz spełnić obowiązki właściwe dla danej czynności
Krótką sekwencją wielu przelewów	Możliwe ukrycie ścieżki pieniądza	Weryfikować cel i kontrahentów, zachować autentyczne dowody
Spółki bez realnej działalności	Pozorne świadczenie lub niejawna kontrola	Zweryfikować gospodarcze wykonanie umów oraz beneficjentów
Aktywa cyfrowe i zewnętrzne portfele	Niepełna identyfikacja stron i transferów	Korzystać z legalnych usług, dokumentować nabycie i rozliczenie
Podejrzenie karuzeli fakturowej	Związek płatności z czynem podatkowym	Audyt dostaw i faktur, badanie dostawców, konsultacja prawna

UWAGA. Celowe dzielenie transakcji, posługiwanie się cudzym rachunkiem dla ukrycia dysponenta, tworzenie fikcyjnych tytułów przelewów, antydatowanie faktur czy niszczenie korespondencji nie stanowią sposobów „ograniczania ryzyka”. Mogą tworzyć osobne podstawy odpowiedzialności i istotne dowody zamiaru. Nie wolno utożsamiać przejrzystego planowania podatkowego lub korporacyjnego z tworzeniem struktur pozornych.

10. Kto jest instytucją obowiązaną i jakie ma obowiązki?

Art. 2 ustawy AML wskazuje katalog instytucji obowiązanych. Obejmuje on podmioty finansowe i liczne kategorie zawodowe lub działalności regulowanych, a także – w ustawowo określonym zakresie – adwokatów, radców prawnych, prawników zagranicznych i doradców podatkowych. Nie każda porada prawna czyni z adwokata instytucję obowiązaną w tej konkretnej sprawie. Dla kancelarii decyduje czynność objęta katalogiem ustawowym, np. określone transakcje nieruchomościowe, korporacyjne lub finansowe, oraz faktyczny zakres zaangażowania. Aktualny zakres trzeba analizować z uwzględnieniem nowelizacji obowiązującej od 29.09.2026 r. [P2]

Podstawowe grupy obowiązków podmiotów objętych reżimem AML: ocena ryzyka działalności i klienta (art. 27, 33), identyfikacja klienta i beneficjenta rzeczywistego, weryfikacja tożsamości, rozpoznanie celu relacji oraz bieżący monitoring (art. 34–35), stosowanie środków wzmożonych w sytuacjach ustawowych (art. 43 i nast.), analiza transakcji nietypowych, procedury wewnętrzne (art. 50), szkolenie (art. 52), retencja (art. 49) oraz wymagane informacje do GILF. [P2; I1]

Warto odróżnić przesłanki zawiadomienia o podejrzanych okolicznościach (art. 74) od zawiadomienia dotyczącego określonej transakcji lub wartości majątkowych (art. 86). W każdym przypadku właściwy jest aktualny tryb ustawowy oraz oficjalne wskazówki GILF. Nie wolno ujawniać informacji objętych zakazem „tipping-off” ani informować kontrahenta o zawiadomieniu w sposób sprzeczny z art. 54 ustawy; wyjątki mają granice ustawowe. [P2; I1]

11. Specyfika kancelarii adwokackiej: tajemnica, obrona i transakcje

Ochrona tajemnicy obrończej i doradztwa związanego z procesem wymaga autonomicznej analizy. Art. 75 ustawy AML przewiduje wyłączenie wskazanych obowiązków przekazywania informacji i zawiadomień dla profesjonalnych

prawników z art. 2 ust. 1 pkt 14, gdy informacje uzyskano podczas ustalania sytuacji prawnej klienta w związku z postępowaniem sądowym, jego obrony, reprezentacji lub zastępstwa w takim postępowaniu albo porady o wszczęciu lub uniknięciu postępowania. Znaczenie ma rzeczywisty charakter usługi, nie sama nazwa umowy. [P2]

Wyłączenie art. 75 nie oznacza immunitetu wobec działalności polegającej na świadomym uczestnictwie w praniu pieniędzy, ani generalnego zwolnienia z obowiązków przy obsłudze operacji gospodarczych objętych reżimem AML. Granicę pomiędzy ochroną informacji uzyskanych w celu prowadzenia obrony a udziałem prawnika w organizacji transakcji trzeba oceniać oddzielnie. Orzecznictwo TSUE C-305/05 oraz ETPC Michaud przeciwko Francji potwierdza znaczenie tej granicy i szczególny status zawodowego sekretu prawnego w kontekście praw podstawowych. [UE5–UE6]

Rekomendowany standard kancelarii: przy przyjęciu zlecenia sklasyfikować, czy dotyczy reprezentacji procesowej, doradztwa transakcyjnego czy modelu mieszanego; określić zakres zastosowania ustawy AML, oddzielić zespoły i zasoby informacyjne stosownie do tajemnicy, prowadzić proporcjonalne czynności KYC, dokumentować konflikt interesów, a honorarium i rachunki rozliczać w sposób możliwy do odtworzenia. W razie wątpliwości zastosować indywidualną ocenę prawną i etyczną.

12. Nieruchomości, pożyczki prywatne, darowizny i transakcje rodzinne

Przeniesienie środków w rodzinie nie jest samo przez się praniem. W praktyce jednak deklaracja „to oszczędności rodziny” może być niewystarczająca, gdy kwoty i przebieg zdarzeń wymagają wykazania ich rzeczywistego źródła. Dokumenty nabycia aktywów, umowy pożyczek, oświadczenia o pochodzeniu kapitału poparte obiektywnymi dowodami, przelewy, podatkowe zgłoszenia darowizn i akty notarialne umożliwiają odtworzenie ciągu gospodarczego. Formalna umowa pożyczki zawarta wyłącznie dla stworzenia pozoru legalnego źródła nie stanowi ochrony.

W transakcji nieruchomościowej warto zestawić cenę z rozliczeniem, umowę przedwstępną z ostateczną, środki własne z kredytem i faktycznego odbiorcę zapłaty z treścią aktu. Gdy stroną jest podmiot korporacyjny, dokumentować decyzje organów i umocowanie. Jeżeli w sprawie występują rozliczenia gotówkowe, należy odrębnie ocenić obowiązki dotyczące danej kategorii transakcji i podmiotu; samo użycie gotówki nie realizuje wszystkich znamion art. 299 k.k.

13. Obrót międzynarodowy i kryptoaktywa

W obrocie transgranicznym nie wystarczy formalna zgodność płatności z regułami bankowymi. Weryfikacja obejmuje możliwy związek z jurysdykcją wysokiego ryzyka, sankcjami, właścicielem faktycznym, uzasadnieniem gospodarczym oraz spójnością dokumentacji dostaw. W odniesieniu do kryptoaktywów istotne są dokumenty ich nabycia, historii transferów, dane podmiotu świadczącego usługi, transferów do i z portfeli własnych oraz rozliczenia księgowo-podatkowe. Rozporządzenie (UE) 2023/1113 wprowadza obowiązki informacyjne w odniesieniu do transferów funduszy i określonych kryptoaktywów – zależnie od podmiotowego i przedmiotowego zakresu aktu. [UE4; I2]

Komunikat GIIF nr 113 zaznacza, że samo naruszenie wymogów informacyjnych transferu nie musi automatycznie uzasadniać zawiadomienia o praniu pieniędzy bez analizy innych czynników ryzyka; zarazem brak informacji powinien zostać wyjaśniony stosownymi środkami zgodnymi z ustawą. Jest to cenne rozróżnienie pomiędzy niespełnieniem wymogu regulacyjnego a dowodem przestępstwa. [I2]

CZĘŚĆ II-A. KRYPTOAKTYWA, BLOCKCHAIN I OBRONA PRZED ZARZUTEM PRANIA PIENIĘDZY

ROZDZIAŁ SPECJALNY • aktualizacja stanu prawnego na 20 października 2026 r. • perspektywa prawa polskiego i Unii Europejskiej • standard dowodu cyfrowego i obrony z art. 299 k.k.

TEZA. Samo posiadanie bitcoina, etheru, stablecoinów, prowadzenie portfela self-custody, korzystanie z protokołu DeFi lub dokonanie transferu pomiędzy własnymi adresami nie oznacza popełnienia prania pieniędzy. Jednocześnie kryptoaktywa mogą stanowić przedmiot czynności wykonawczej z art. 299 k.k., jeżeli spełniono wszystkie ustawowe znamiona, w szczególności wykazano powiązanie określonych wartości z korzyścią pochodzącą z czynu zabronionego oraz umyślne zachowanie konkretnej osoby. Postać cyfrowa mienia nie tworzy ani immunitetu, ani domniemania winy.

Metodyka obrony w sprawach krypto wymaga połączenia analizy prawnokarnej, analizy transakcyjnej i kryminalistyki cyfrowej. Pytanie nie brzmi jedynie „dokąd wysłano tokeny?”, lecz: jakie wartości i w której chwili przemieszczono; kto kontrolował środki; czy rzeczywisty beneficjent był tą samą osobą; jakie znaczenie ma rachunek powierniczy, depozyt giełdy lub inteligentny kontrakt; jaki był prawny tytuł transferu; co oskarżony wiedział w czasie czynności; i czy w ogóle istnieje dostateczny dowód źródła przestępczego.

13A. Mapa regulacyjna: art. 299 k.k., MiCA, Travel Rule i polska ustawa AML

Art. 299 k.k. jest przepisem karnym. Rozporządzenie MiCA (UE) 2023/1114 reguluje zasadniczo rynek kryptoaktywów, emitentów i dostawców usług w zakresie kryptoaktywów (CASP); rozporządzenie (UE) 2023/1113, często określane jako Travel Rule / TFR, określa informacje towarzyszące transferom środków i kryptoaktywów; ustawa AML z 1 marca 2018 r. oraz odpowiednie przepisy i wytyczne unijne organizują system prewencji, identyfikacji klientów, analizy ryzyka i raportowania. Naruszenie obowiązku regulacyjnego należy badać według jego własnej podstawy prawnej; samo w sobie nie przesądza ono o popełnieniu przestępstwa z art. 299 § 1 k.k. [K1–K4].

MiCA stosuje się w kluczowym zakresie od 30 grudnia 2024 r.; odrębne części dotyczące tokenów powiązanych z aktywami i tokenów będących pieniądzem elektronicznym stosowane są od 30 czerwca 2024 r. Art. 143 ust. 3 przewidywał przejściową możliwość kontynuowania działalności określonych dotychczasowych dostawców usług do 1 lipca 2026 r. lub do wcześniejszego udzielenia bądź odmowy zezwolenia. W komunikacie z 23 czerwca 2026 r. KNF przypominała o zakończeniu okresu przejściowego 1 lipca 2026 r.; dlatego historyczny wpis do polskiego rejestru działalności w zakresie walut wirtualnych nie powinien być dziś utożsamiany z zezwoleniem CASP MiCA. Status konkretnego usługodawcy należy zweryfikować według rodzaju usługi, właściwego organu, decyzji i aktualnego rejestru ESMA. [K1, K5, K6].

UWAGA. Projekt polskiej ustawy o rynku kryptoaktywów uchwalony w maju 2026 r. został zawetowany, a 4 września 2026 r. Sejm nie uchwalił ustawy ponownie. W październiku 2026 r. nie wolno przedstawiać tego projektu jako obowiązującej polskiej ustawy. Nie zmienia to bezpośredniego stosowania odpowiednich przepisów unijnych ani dalszego obowiązywania właściwych przepisów polskiej ustawy AML i kodeksów. Kolejne inicjatywy legislacyjne mają status projektu do chwili skutecznego uchwalenia i wejścia w życie. [K7].

Rozporządzenie AMLR (UE) 2024/1624, mimo że już weszło w życie, zasadniczo będzie stosowane od 10 lipca 2027 r. Zawarte w nim przyszłe wymogi – w tym art. 40 w sprawie adresów niehostowanych i art. 79 dotyczący anonimowych rachunków kryptoaktywów – trzeba odróżniać od wymogów obowiązujących obecnie. Używanie tych przepisów jako samoistnej podstawy zarzutu dotyczącego transakcji z października 2026 r. bez szczególnej podstawy prawnej byłoby błędem intertemporalnym. [K8].

13B. Jak art. 299 k.k. działa w środowisku blockchain?

Przedmiotem obrotu może być bitcoin, ether, stablecoin, określone tokeny użytkowe, tokeny odzwierciedlające prawa lub inne zbywalne wartości. Nie wszystkie aktywa cyfrowe mają ten sam status cywilnoprawny, regulacyjny czy podatkowy; ich kwalifikację w art. 299 należy uzasadnić poprzez właściwą kategorię mienia lub prawa majątkowego, zamiast automatycznie zakładać, że każdy token jest „walutą” albo „instrumentem finansowym”. W razie sporu konieczna jest analiza natury tokena, dokumentacji emitenta, jego faktycznej funkcji i praw przysługujących posiadaczowi.

Przedmiot czynności musi pochodzić bezpośrednio lub pośrednio z korzyści związanej z czynem zabronionym. Jeżeli oskarżyciel powołuje się na oszustwo inwestycyjne, wymuszenie ransomware, przestępstwo podatkowe, bezprawny dostęp do systemu lub przywłaszczenie kryptoaktywów, należy oddzielnie ustalić: czyn źródłowy, rodzaj i wartość korzyści, konkretną ścieżkę jej przekształceń oraz osobę przypisaną do zachowania ujętego w art. 299. Nie wystarcza ogólne stwierdzenie, że dany protokół, grupa adresów lub podmiot był wcześniej używany w przestępczości.

W przypadku w pełni identyfikowalnego łańcucha przepływ tokenów może być dobrze udokumentowany; to jednak nie zastępuje ustalenia ich przestępczego pochodzenia, kontroli nad adresem ani świadomości uczestnika. Nawet jeśli narzędzie analityczne oznaczy transfer jako „high risk”, etykieta ta jest wskaźnikiem analitycznym, nie samodzielnym rozstrzygnięciem sądu co do znamion art. 299 k.k.

Orzecznictwo SN dotyczące przestępnego źródła (I KZP 19/13; III KK 407/14) i rachunków mieszanych (I KZP 5/15) wymaga adaptacji do kryptoaktywów, a nie mechanicznego przeniesienia pojęcia salda bankowego na każdy blockchain. W systemach UTXO i account-based „wymieszanie” środków może następować inaczej; metoda śledzenia musi zostać zdefiniowana, zweryfikowana i zestawiona z modelem faktycznym danego aktywa. [O1–O3].

13C. Adres, klucz prywatny, konto giełdowe i faktyczny dysponent — cztery odrębne kwestie

Należy rozróżniać: (a) publiczny adres blockchain, (b) zdolność podpisania transakcji przy użyciu właściwych kluczy, (c) konto użytkownika prowadzone przez CASP i jego księgowanie wewnętrzne oraz (d) rzeczywiste prawo do środków albo działanie na cudzy rachunek. Jedna osoba może kontrolować wiele adresów, a jeden adres lub klucz może być kontrolowany przez kilka osób albo przez strukturę multisig. Konto depozytowe giełdy agreguje środki wielu klientów; transfer na adres giełdowy nie oznacza automatycznie, że jego beneficjent jest właścicielem wszystkich aktywów na tym adresie.

W systemie UTXO wskazanie wejścia lub wyjścia transakcji nie jest identyfikacją osoby fizycznej. W sieciach account-based operacje z kontraktami, kontami abstrakcyjnymi, podpisami wielostronnymi i delegacją mogą prowadzić do błędnych uproszczeń dotyczących sprawstwa. W tokenach na sieci EVM należy analizować zdarzenia transferu i wywołania kontraktów razem z kontekstem technicznym, a nie wyłącznie saldo eksploratora blockchain.

W PRAKTYCE. Procesowe twierdzenie „oskarżony używał adresu X” wymaga wskazania podstawy przypisania: autoryzowanych danych KYC giełdy, urządzeń i logów, korespondencji, faktów dotyczących podpisywania transakcji, zeznań oraz testów technicznych dokonanych w kontrolowany i bezpieczny sposób. Adres przypisany heurystycznie do „klastra” przez prywatnego dostawcę analityki nie jest z natury równoważny dowodowi wyłącznej kontroli oskarżonego. Z drugiej strony wielokrotna zgodność danych on-chain, logowań i instrukcji może zbudować mocny dowód pośredni; należy analizować całość, a nie jeden wskaźnik.

13D. Travel Rule: portfele niehostowane i próg 1 000 EUR bez uproszczeń

Od 30 grudnia 2024 r. rozporządzenie (UE) 2023/1113 nakłada na objętych nim dostawców usług określone obowiązki uzyskania, przekazania i przechowywania informacji o inicjatorze i beneficjencie transferów kryptoaktywów.

Dane, zgodnie z art. 14 ust. 4, mogą towarzyszyć transferowi niezależnie od samego łańcucha – nie muszą być osadzone w transakcji blockchain. Oceniając domniemane naruszenie, trzeba odróżnić podmiot zobowiązany (CASP) od użytkownika prywatnego portfela i sprawdzić zakres stosowania rozporządzenia. [K2].

Przy transferze z CASP na adres niehostowany lub odwrotnie CASP ma obowiązek uzyskania i przechowywania odpowiednich informacji. Dodatkowo, gdy transfer przekracza 1 000 EUR, właściwy CASP stosuje odpowiednie środki oceniające, czy niehostowany adres jest własnością odpowiedniego klienta lub jest przez niego kontrolowany – szczegółowo art. 14 ust. 5 i art. 16 ust. 2. Próg nie jest „limitem bez AML”: nie zwalnia niższych transferów z pozostałych obowiązków, nie tworzy legalnej metody unikania weryfikacji i nie stanowi kryterium legalności źródła aktywów. [K2, K3].

Transakcje wyłącznie pomiędzy dwiema osobami działającymi we własnym imieniu, bez CASP uczestniczącego w transferze, wymagają odrębnej analizy zakresu rozporządzenia; nie należy automatycznie traktować każdego prywatnego przesłania krypto jako operacji, do której użytkownik musi technicznie dołączyć komplet danych Travel Rule. Równie błędne byłoby uznanie transferu P2P za z definicji poza ryzykiem karnym: brak obowiązku konkretnego CASP nie usuwa art. 299 k.k., sankcji ani obowiązków podatkowych.

Z perspektywy obrony należy uzyskać politykę CASP obowiązującą w dacie operacji, zapis żądanych danych, przyczynę oznaczenia transferu, sposób ustalania wartości w EUR, ewentualną korespondencję wyjaśniającą i komplet informacji towarzyszących transferowi. Brak danych po stronie usługodawcy nie jest dowodem, że jego klient świadomie prał pieniądze.

13E. Analiza blockchain i typowe ograniczenia metod atrybucji

Dane on-chain są wartościowymi zapisami technicznymi, ale należy wyraźnie oddzielić obserwację bezpośrednią (hash transakcji, identyfikator łańcucha, czas bloku, adresy, wolumen, log zdarzeń, opłata) od wniosku analitycznego (konkretna osoba kontroluje portfel; transfer był zapłatą za usługę; token pochodzi z czynu zabronionego). Poziom pewności tych twierdzeń jest różny. Warto zweryfikować, na jakiej wersji łańcucha i stanu sieci oparto raport, czy ustalenia są reprodukowalne oraz czy historyczne etykiety adresów zachowano na datę analizy.

Modele analizy klastrów stosują heurystyki, takie jak wspólne wydawanie wejść w modelu UTXO albo identyfikacja charakterystycznych przepływów i depozytów. Heurystyka nie jest aksjomatem: działania wielu uczestników, portfele zbiorcze, modele depozytowe, agregatory i struktury multisig mogą prowadzić do błędnego przypisania. Obrona powinna badać nie tylko trafność danych wyjściowych, lecz również zastosowaną regułę łączenia adresów, miary niepewności, próbę walidacyjną i możliwość wskazania alternatywnego wyjaśnienia.

Tokeny przechodzące przez giełdy centralne zwykle generują dwa różne rodzaje materiału: zapisy on-chain transferów do portfeli giełdy i wewnętrzną księgę usługodawcy. Bez drugiego elementu nie zawsze można dowodowo powiązać konkretny depozyt z konkretnym późniejszym wypływem z portfela omnibus. W przypadkach transgranicznych obrona powinna wnioskować o pozyskanie źródłowych danych od właściwej giełdy w dopuszczalnym trybie procesowym, zamiast akceptować dowolny schemat graficzny jako „trasę tych samych monet”.

W systemach DeFi konieczne jest odtworzenie semantyki wywołań kontraktu. Zakup tokena, dostarczenie płynności, pożyczka zabezpieczona, likwidacja pozycji, staking, swap za pośrednictwem routera lub bridge są odmiennymi zdarzeniami gospodarczymi. Sama współobecność środków w smart kontrakcie nie oznacza porozumienia jego wszystkich użytkowników ani tożsamości ich właścicieli. Powinno się sprawdzić stan puli, transakcje zależne, strukturę kontraktu i dokumentację protokołu z właściwego okresu.

13F. Mixery, privacy coins, mosty, giełdy zagraniczne i stablecoiny

Mechanizmy podwyższające prywatność i złożoność przepływów mogą być czynnikami ryzyka AML i obszarem zainteresowania organów. FATF zalicza do wskaźników ostrzegawczych m.in. korzystanie z usług miksowania, nietypowe sekwencje transferów, nieprzejrzyste źródła środków i powiązania z adresami znanymi z działalności przestępczej. Są to jednak wskaźniki do zbadania w kontekście, nie automatyczne dowody popełnienia przestępstwa. [K10].

W sprawach dotyczących miksera, narzędzia privacy lub wielokrotnej konwersji organ powinien dowieść związku konkretnych aktywów z przestępstwem źródłowym i ustalić wiedzę oraz czynność oskarżonego. Obrona powinna domagać się przedstawienia drogi rozumowania analityka: co jest faktem on-chain, co przypisaniem probabilistycznym, a co hipotezą operacyjną. Nie wolno sprowadzać postępowania do wniosku: „stosowano narzędzie prywatności, zatem celem było pranie pieniędzy”. Odmienna może być ocena, gdy istnieją dodatkowo jednoznaczne instrukcje ukrycia przestępczego pochodzenia lub wiedza o nim.

W bridge token może zostać zablokowany w jednej sieci i odtworzony jako reprezentacja w drugiej; czasem dochodzi do zmiany emitenta, aktywa lub mechaniki rozliczenia. Rzetelna analiza wymaga mapy obu sieci, identyfikacji kontraktów i dowodu korelacji operacji. Niewłaściwe jest sumowanie transferu wejściowego i wyjściowego jako dwóch różnych przysporzeń, jeśli ekonomicznie chodzi o jedną wartość.

Stablecoiny wymagają weryfikacji emitenta, sieci, prawa wykupu, ewentualnych mechanizmów zamrażania tokenów i relacji do pieniądza fiducyjnego. Zbieżne oznaczenie tickerem, np. USDT lub USDC, nie wystarcza do zindywidualizowania instrumentu i konkretnego łańcucha. W ocenie ryzyka CASP istotne mogą być też sankcje i geografia przepływu, ale ich naruszenie lub podejrzenie stanowi odrębny problem prawny, którego nie wolno w procesie zastępować skrótem myślowym o art. 299.

13G. Prewencja dla osób prywatnych i podmiotów prowadzących działalność

Właściciel kryptoaktywów nie powinien tworzyć dokumentów „pod kontrolę”, lecz zachowywać wiarygodne, pierwotne dane transakcji od chwili ich powstania. Dla historycznie nabytych aktywów konieczne jest odtworzenie pochodzenia środków wykorzystanych na zakup oraz ciągłości posiadania lub kontroli. Korzystne jest gromadzenie eksportów danych z platform, potwierdzeń bankowych, wiadomości transakcyjnych, zapisów księgowych i potwierdzeń wcześniejszych wypłat. Dokumentacja powinna być prowadzona proporcjonalnie, z poszanowaniem prywatności i bezpieczeństwa informacji.

Dla spółek i podmiotów mogących być instytucją obowiązującą kluczowe są: ocena charakteru usługi i statusu CASP, udokumentowana ocena ryzyka, weryfikacja klienta i beneficjenta rzeczywistego, analiza źródła pochodzenia środków odpowiednio do ryzyka, screening sankcyjny w wymaganym zakresie, reakcja na transakcje atypowe, wewnętrzna procedura AML i jej faktyczne stosowanie, dokumentacja decyzji oraz zasady przechowywania danych. Procedury marketingowe lub fikcyjne checklista bez wdrożenia nie redukują prawidłowo ryzyka.

Przy operacjach OTC (pozagiełdowych) należy weryfikować tożsamość i umocowanie kontrahenta, ekonomiczną funkcję świadczenia, sposób ustalenia ceny, istnienie rachunku lub adresu rzeczywiście uzgodnionego przez strony oraz dokumentować wydanie i otrzymanie świadczenia. Szczególną ostrożność uzasadniają propozycje przelewów przez niepowiązane osoby trzecie, nieuzasadnione prowizje, transakcje bez realnego świadczenia i sprzeczne dane o stronach. Brak możliwości wyjaśnienia poważnych niezgodności powinien prowadzić do legalnej weryfikacji, wstrzymania lub rezygnacji z transakcji, a w wypadku podmiotów obowiązanych – do wykonania obowiązków ustawowych.

UWAGA. Nie należy dzielić operacji dla uniknięcia identyfikacji, podstawiać cudzych rachunków, posługiwać się fikcyjnymi umowami, usuwać historii transakcji ani zlecać osobom trzecim pozorne „udokumentowanie” źródła środków. Takie czynności mogą zwiększyć ryzyko odrębnej odpowiedzialności, osłabić wiarygodność wyjaśnień i naruszać przepisy AML.

13H. Dokumentowanie legalnego nabycia: standard dowodu i „crypto source of wealth”

1. Pierwotne finansowanie: historia rachunku bankowego, na który wpływało wynagrodzenie, przychód ze sprzedaży, środki pożyczki lub darowizny, wraz z autentycznymi dokumentami ich pochodzenia.

2. Pierwszy zakup: zlecenie, data, para handlowa, cena, prowizja, potwierdzenie giełdowe albo dowód autentycznego zakupu OTC i identyfikacja kontrahenta.
3. Kontynuacja łańcucha wartości: eksport historii z giełdy, depozyty/wypłaty, hashe, logi swapów, świadectwa transferów między własnymi portfelami i ewentualnych migracji sieci.
4. Zdarzenia bez transferu on-chain: zapisy wewnętrznych ksiąg giełdy, rozliczenia sald, dokumenty upadłości platform, historię zmian konta i spraw dotyczących dostępu.
5. Operacje niehandlowe: spadek, darowizna, wynagrodzenie, zwrot pożyczki lub świadczenie w krypto — ich tytuł prawny, moment otrzymania i dokumentacja podatkowa.
6. Weryfikacja wartości: historyczny kurs pary handlowej, źródło notowania, strefa czasowa, liczba jednostek i opłaty; nie należy mieszać kwoty wpłaty fiat z późniejszą wyceną w innym dniu.
7. Integralność i proces: eksporty CSV/JSON lub inne dane pierwotne, sumy kontrolne plików, kopie źródłowe, wskazanie dat i osób zabezpieczających dowód. Nie udostępniać fraz seed ani kluczy prywatnych w sposób niekontrolowany.

Z punktu widzenia ciężaru dowodu zasadniczą powinnością organu jest wykazanie wszystkich znamion czynu. Oskarżony nie musi „udowodnić niewinności”, choć przedłożenie istniejących, legalnych źródeł finansowania może obalić wadliwe założenia prokuratury i ograniczyć ryzyko długotrwałego zabezpieczenia. Brak pełnej dokumentacji sprzed wielu lat wymaga oceny realiów rynku i możliwości odtworzenia danych, a nie automatycznego utożsamienia luki archiwalnej z pochodzeniem przestępczym.

Dokumenty podatkowe mogą mieć znaczenie poszlakowe, lecz samo rozliczenie PIT nie legalizuje przestępczej korzyści, tak samo jak brak PIT nie przesądza o praniu pieniędzy. Ministerstwo Finansów wskazuje, że w typowych rozliczeniach odpłatnego zbycia walut wirtualnych stosuje się PIT-38, a wymiana waluta wirtualna na walutę wirtualną zasadniczo nie stanowi odpłatnego zbycia; wymogi i wyjątki należy ustalić według konkretnej czynności i roku podatkowego. [K9].

13I. Wycena, przepływy mieszane, wielokrotne liczenie tych samych środków

Zarzut w sprawach blockchain często opiera się na wielkich sumach brutto „obrotu” policzonych jako łączna wartość wielu wejść i wyjść. Może to być prawidłowa miara aktywności sieci, ale niekoniecznie wartość korzyści, przedmiotu prania, zysku albo szkody. Wielokrotny obrót tym samym tokenem, przesunięcia między własnymi adresami, swapy, zastaw, uwolnienie zabezpieczenia, bridge i prowizje muszą zostać ujęte w analizie ekonomicznej bez dublowania wartości.

Dla mienia mieszanego wymagane jest uzasadnienie sposobu przypisania części przepływu do źródła przestępczego, a części do legalnych środków. Warianty metod tracowania (w zależności od sieci i stanu faktycznego) mogą dawać różne wyniki: nie wolno ich przemilczeć, arbitralnie przyjąć maksymalnej kwoty lub ignorować depozytów osób trzecich. Uchwała SN I KZP 5/15, dotycząca m.in. rachunku mieszanego, ma znaczenie jako ostrzeżenie przed automatycznym utożsamianiem całości salda z majątkiem pochodzącym z przestępstwa; techniczny sposób zastosowania tej idei do blockchain wymaga jednak odrębnego uzasadnienia.

Należy wyróżnić co najmniej cztery liczby: wolumen obrotu (sumę transferów), kwotę faktycznego przysporzenia, wartość określonych aktywów w dacie czynności i wartość podlegającą ewentualnemu zabezpieczeniu lub przypadkowi według właściwej podstawy prawnej. Analiza wartości w PLN wymaga określenia kursu, chwili wyceny, aktywa, źródła notowań, płynności i ewentualnej różnicy między wartością rynkową a sumą rzeczywiście osiągniętą.

13J. Standard ekspertyzy analitycznej i biegły z zakresu informatyki śledczej

Ekspertyza powinna być odtwarzalna i pozwalać sądowi odróżnić dane źródłowe od hipotez. Nie wystarcza zrzut ekranu z platformy analitycznej z czerwonym kolorem i procentowym „ryzykiem”. Rzetelny materiał powinien ujawniać istotne parametry metodologii, dane źródłowe, okres analizy, zasady etykietowania i klastrowania, dokładne identyfikatory, rodzaj sieci, logikę wyłączeń, granice wiarygodności oraz istotne zastrzeżenia. Jeżeli sposób obliczania wskaźnika jest tajemnicą handlową, sąd powinien rozważyć, czy istnieje wystarczający poziom weryfikowalności istotnego wniosku dla realizacji prawa do obrony.

W rozumieniu art. 193 k.p.k. wiadomości specjalne uzasadniają rozważenie opinii biegłego. Obrona powinna wyznaczyć tezy nie tylko potwierdzające hipotezę oskarżenia, ale testujące jej alternatywy: wspólne adresy giełd, mechanizmy custody, działanie smart kontraktów, skutki reorganizacji łańcucha, zmiany klasyfikacji adresu, możliwości kompromitacji klucza oraz niezależność błędów wielu narzędzi opartych na tym samym zbiorze etykiet. Prywatna ekspertyza może pomóc ukierunkować wnioski dowodowe, lecz jej status procesowy i wartość należy oceniać zgodnie z k.p.k.

Łańcuch dowodowy obejmuje nie tylko plik raportu, lecz także sposób pozyskania danych z urzędów, eksportów giełdowych i serwerów. Trzeba ustalić: kto wykonywał kopię, kiedy, jak ją zabezpieczono, czy zachowano metadane i sumy kontrolne, czy stosowano konto administratora, czy dochodziło do późniejszych modyfikacji plików i czy biegły pracował na kopii dowodowej. Wątpliwości należy konkretyzować; sama ogólna możliwość błędu informatycznego nie wystarcza do zakwestionowania każdego dowodu cyfrowego.

13K. Zabezpieczenie kryptoaktywów, klucze prywatne i proporcjonalność ingerencji

W postępowaniu karnym mogą pojawiać się zabezpieczenia majątkowe, zajęcia urzędów i nośników, żądania danych od giełd, a także międzynarodowe instrumenty współpracy. Ich dopuszczalność, organ wydający, tryb kontroli i zakres należy ustalić z uwzględnieniem właściwych przepisów k.p.k., podstawy materialnoprawnej i daty czynności. W ramach UE odpowiednie znaczenie może mieć rozporządzenie (UE) 2018/1805 o wzajemnym uznawaniu nakazów zabezpieczenia i konfiskaty; jego art. 1 wymaga poszanowania konieczności i proporcjonalności. [K11].

Właściwa obrona powinna rozdzielać zabezpieczenie określonych, zindywidualizowanych tokenów od zabezpieczenia całego portfela, który może zawierać majątek osoby trzeciej lub środki o różnych źródłach. Wnioski powinny dotyczyć zakresu majątku, wyceny, istnienia uzasadnionej podstawy i prawa osoby uprawnionej; tam, gdzie ustawa przewiduje właściwy środek zaskarżenia, należy podnosić także nieproporcjonalność i skutki gospodarcze.

Zabezpieczenie klucza prywatnego wymaga szczególnej ostrożności technicznej: ujawnienie frazy seed w protokole dostępnym szerokiemu kręgowi osób może doprowadzić do nieodwracalnej utraty majątku. Pełnomocnik powinien wnioskować o formalny, poufny i technicznie bezpieczny sposób przeprowadzenia czynności, udokumentowanie łańcucha dowodowego i ograniczenie ujawnienia wrażliwych danych do niezbędnego zakresu; nie należy samowolnie przenosić, niszczyć ani ukrywać składników majątku objętych zajęciem lub zabezpieczeniem.

13L. Sześć modeli spraw, które należy rozróżnić

Stan faktyczny	Główna kwestia obrony	Dowody priorytetowe
Inwestor kupił BTC przed laty, a dziś wypłaca zysk	Źródło fiat, ciągłość aktywów, interpretacja braków archiwum	Rachunek bankowy, historia giełd, TXID, PIT-38
Przelew na adres giełdy powiązany z oszustwem	Czy adres był wspólny i do jakiego subkonta przypisano depozyt?	Księga giełdowa, dane KYC, znaczniki czasu, korespondencja

Stan faktyczny	Główna kwestia obrony	Dowody priorytetowe
Osoba otrzymała zapłatę w USDT za realną usługę	Tytuł transferu, świadomość źródła, wartość wykonanej usługi	Umowa, wykonanie, faktura, logi, komunikacja
Podmiot uczestniczył w swapie i bridge	Czy operacja stanowiła jedynie techniczną konwersję i jaką wartość obejmowała?	ABI/zdarzenia kontraktu, mapowanie sieci, analiza wyceny
Użytkownik DeFi otrzymał tokeny z puli	Czy przypisanie źródła i kontrahenta jest w ogóle uprawnione?	Dane protokołu, historia puli, biegly, test heurystyk
Użytkownik portfela został oznaczony jako „high risk”	Czy raport ma wartość dowodową dla znamion art. 299, czy tylko AML?	Raport metodologiczny, etykiety, dane źródłowe, niezależna ekspertyza

Każdy model wymaga oddzielnego badania elementów czynu. Dobrze udokumentowana działalność gospodarcza nie wyklucza automatycznie przestępnego pochodzenia środków, a udział w nietypowym modelu technicznym nie dowodzi automatycznie winy. Obrona nie może polegać na budowaniu wersji faktycznej sprzecznej z autentycznymi danymi; jej siła wynika z metodologicznej kontroli hipotez organu i przedstawienia prawdziwych okoliczności sprawy.

13M. Macierz dowodowa obrony w sprawie o pranie kryptoaktywów

Twierdzenie oskarżenia	Pytanie krytyczne	Żądany materiał
Adres kontrolował podejrzany	Czy kontrola była wyłączna i w dacie czynu?	Urządzenia, logi, KYC, multisig, role i uprawnienia
Aktywo pochodzi z przestępstwa	Jaki czyn źródłowy i jakie połączenie ekonomiczne?	Dokumenty źródłowe, mapa przepływów, warianty alternatywne
Klaster to jedna osoba	Jakie heurystyki i jaki błąd atrybucji?	Parametry klastrowania, dane walidacyjne, biegly
Obrót równa się wartości prania	Czy policzono wielokrotnie te same jednostki?	Zestawienie netto, deduplikacja, wycena na moment czynu
Klient znał przestępcze źródło	Co realnie wiedział przed transakcją?	Korespondencja chronologiczna, dokumenty KYC, ostrzeżenia
Naruszenie Travel Rule dowodzi art. 299	Kto był podmiotem zobowiązanym i jaki obowiązek naruszono?	Status CASP, polityka, dane żądane i przekazane
Zajęcie całego portfela jest konieczne	Które aktywa należą do osoby podejrzanej i jak je wyceniono?	Dowody praw osób trzecich, przegląd sald i tytułów prawnych

13N. Przykładowe wnioski dowodowe dla obrońcy

- Wnoszę o pozyskanie od operatora platformy dokumentacji pełnej historii rachunku klienta, obejmującej identyfikatory depozytów i wypłat, ruchy wewnętrzne, dane księgi subkont, znaczniki czasu wraz ze strefą czasową oraz materiały identyfikacyjne dostępne zgodnie z prawem – na okoliczność ustalenia rzeczywistego beneficjenta poszczególnych transferów.
- Wnoszę o dopuszczenie dowodu z opinii biegłego z zakresu analizy sieci blockchain na okoliczność odróżnienia przepływów on-chain od operacji wewnętrznych CASP, oceny podstaw atrybucji adresów oraz ustalenia ograniczeń użytej heurystyki klastrowania.
- Wnoszę o zobowiązanie do ujawnienia danych źródłowych i możliwych do udostępnienia parametrów metodologicznych raportu analitycznego, w szczególności etykiet źródłowych, dat ich nadania, kryteriów przypisania i poziomów niepewności – na okoliczność kontroli prawidłowości wniosków stanowiących podstawę zarzutu.

4. Wnoszę o sporządzenie porównawczego zestawienia przepływów i wyceny, oddzielającego swapy, transfery pomiędzy własnymi adresami, bridge, transakcje klientów i rzeczywiste wpływy majątkowe, z wyraźnym wskazaniem momentów wyceny oraz uniknięciem podwójnego liczenia.
5. Wnoszę o przeprowadzenie dowodu z oryginalnych dokumentów finansowania inwestycji, historii bankowej i dokumentacji podatkowej na okoliczność istnienia rzeczywistego legalnego źródła środków oraz chronologii wejścia w posiadanie kryptoaktywów.
6. Wnoszę o weryfikację podstaw i zakresu zabezpieczenia majątkowego w odniesieniu do oznaczonych aktywów, ich faktycznego dysponenta, wartości i praw osób trzecich, z rozważeniem środka mniej dolegliwego, jeśli dopuszcza to prawo.

Każdy wniosek wymaga adaptacji do konkretnego etapu postępowania, podstawy dowodowej, przedmiotu zarzutu i dyspozycji przepisów k.p.k. Należy wskazać konkretną okoliczność mającą znaczenie dla rozstrzygnięcia, a nie kierować do sądu nieograniczonego żądania „zbadania wszystkich kryptowalut”.

13O. Checklista klienta: co zabezpieczyć przed pierwszą analizą akt?

- Identyfikatory kont na platformach i dokumenty KYC oraz ich daty, bez ujawniania hasła osobom nieuprawnionym.
- Nazwy sieci i tokenów, adresy publiczne, identyfikatory transakcji i daty zdarzeń; rozróżnienie custody / non-custody / multisig.
- Komplet dokumentów nabycia z historycznymi potwierdzeniami płatności oraz materiał dotyczący źródła majątku.
- Autentyczne umowy, faktury, korespondencję, protokoły wykonania usług i dokumenty pożyczki lub darowizny.
- Zestawienie transferów między własnymi portfelami, swapów, bridge, stakingu oraz operacji DeFi z ich rzeczywistym celem.
- Informację o utraconych dostępach, awariach giełd, rachunkach zbiorczych i innych okolicznościach mogących wyjaśnić luki w danych.
- Akta blokady, zajęcia i zabezpieczenia, decyzje CASP oraz korespondencję o wymaganiach AML i Travel Rule.
- Istniejące zeznania podatkowe i historię rozliczeń; ewentualne błędy wyjaśniać z uprawnionym doradcą zgodnie z prawem.
- Kopię materiału elektronicznego w pierwotnej postaci oraz informację, kto, kiedy i w jakich warunkach ją wykonał.
- Chronologię zdarzeń sporządzoną dla obrońcy; unikać kontaktowania się z uczestnikami w celu uzgadniania wersji zeznań lub zmieniania danych.

13P. Wniosek strategiczny: cztery niezależne linie obrony

Pierwsza: obrona na poziomie czynu bazowego — zakwestionowanie istnienia zidentyfikowanej korzyści z czynu zabronionego i ścieżki powiązania jej z oznaczonymi aktywami. Druga: obrona na poziomie sprawstwa — wykazanie, że publiczny adres, rachunek omnibus lub interakcja z kontraktem nie przesądzają o konkretnej czynności i osobie ją kontrolującej. Trzecia: obrona na poziomie strony podmiotowej — analiza rzeczywistej wiedzy i zachowania oskarżonego w chwili działania, a nie na podstawie wiedzy zdobytej dopiero po zatrzymaniu. Czwarta: obrona w zakresie wartości i środków przymusu — ocena wartości netto, deduplikacji przepływów, praw osób trzecich i proporcjonalności zabezpieczenia.

Skuteczna obrona nie ogranicza się do negowania raportu z blockchain. Powinna tworzyć alternatywny, dowodowo falsyfikowalny model chronologii i finansowania, ujawniać słabe ogniwa w atrybucji osoby oraz identyfikować tezy biegłego, które dają się odtworzyć lub obalić. Z drugiej strony, gdy dowody wskazują na istotną świadomość przestępczego źródła i celowe zachowania, strategia procesowa musi uczciwie uwzględniać ryzyko skazania, sposób ograniczenia szkód oraz dopuszczalne instrumenty ustawowe — bez tworzenia fałszywej dokumentacji i bez ingerowania w dowody.

13Q. Źródła specjalistyczne: kryptoaktywa, AML, kryminalistyka cyfrowa

[K1] Rozporządzenie (UE) 2023/1114 (MiCA), w szczególności art. 59–63, 109, 143 i 149.
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R1114>

[K2] Rozporządzenie (UE) 2023/1113 (TFR), w szczególności art. 14, 16 i 40. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R1113>

[K3] European Banking Authority, Travel Rule Guidelines, aktualne wytyczne do rozporządzenia 2023/1113.
<https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-counter-terror-financing-terror/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>

[K4] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (z późn. zm.).
<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000723>

[K5] KNF, komunikat z 23 czerwca 2026 r. o zakończeniu okresu przejściowego MiCA dla CASP.
https://www.knf.gov.pl/?articleId=98874&p_id=18

[K6] ESMA, Markets in Crypto-Assets Regulation, Interim MiCA Register i rejestr CASP.
<https://www.esma.europa.eu/pl/node/201529>

[K7] Sejm RP, przebieg prac nad ustawą o rynku kryptoaktywów, weto i wynik głosowania 4 września 2026 r.
<https://www.sejm.gov.pl/Sejm10.nsf/PrzebiegProc.xsp?nr=2363>

[K8] Rozporządzenie (UE) 2024/1624 (AMLR), w szczególności art. 40, 79 i 90. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1624>

[K9] Ministerstwo Finansów, oficjalna informacja o rozliczeniu zbycia kryptowalut, aktualizacja 24 czerwca 2026 r.
<https://www.podatki.gov.pl/podatki-osobiste/pit/informacje-podstawowe/co-jest-opodatkowane/zbycie-kryptowalut>

[K10] FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020) i Targeted Update (2025). <https://www.fatf-gafi.org/en/publications/Methodsand Trends/Virtual-assets-red-flag-indicators.html>

[K11] Rozporządzenie (UE) 2018/1805 w sprawie wzajemnego uznawania nakazów zabezpieczenia i konfiskaty.
<https://eur-lex.europa.eu/eli/reg/2018/1805>

[K12] GIIF / Ministerstwo Finansów, publikacje i wytyczne dla instytucji obowiązanych.
<https://www.gov.pl/web/finanse/-publikacje-i-wytyczne-giif-dla-instytucji-obowiazanych>

[K13] Dyrektywa (UE) 2023/2226 (DAC8) o współpracy administracyjnej w dziedzinie opodatkowania – odrębny reżim sprawozdawczy. <https://eur-lex.europa.eu/eli/dir/2023/2226>

Źródła [O1–O3] odnoszą się do orzeczeń Sądu Najwyższego omówionych w części V zasadniczego poradnika. Zastosowanie wytycznych EBA, dokumentów FATF i komunikatów organów wymaga odróżnienia ich rangi oraz charakteru od bezpośrednio obowiązujących przepisów prawa. Materiał stanowi aktualizację opracowania, nie zastępuje analizy akt konkretnej sprawy.

CZĘŚĆ III. STRATEGIA OBRONY OD PIERWSZEJ CZYNNOŚCI

14. Pierwsze 24–72 godziny po powzięciu informacji o sprawie

Nie istnieje jedna procedura dla każdego podejrzanego. Rzeczywiste priorytety zależą od etapu sprawy, zastosowanego środka, dostępnych akt i rodzaju ryzyka. Poniższe działania są zgodne z prawem i nie obejmują utrudniania postępowania.

1. Ustalić formalny status: świadek, osoba podejrzana, podejrzan po przedstawieniu zarzutów, oskarżony; uzyskać dokładną podstawę i opis czynu.
2. Zapewnić kontakt z obrońcą, omówić prawo do milczenia i zakres ewentualnych wyjaśnień; nie składać improwizowanej „pełnej historii” bez podstawowej orientacji w faktach i zarzucie.
3. Zabezpieczyć bez ingerencji autentyczną dokumentację: historię rachunków, faktury, umowy, księgi, zapisy systemowe, korespondencję, dokumenty dostaw i dokumentację urzędów zgodnie z prawem.
4. Sporządzić wewnętrzną chronologię według dat, oddzielając fakt od przypuszczenia; przy dokumentach elektronicznych zachować metadane i dane o pochodzeniu.
5. Ustalić, czy istnieje blokada rachunku, wstrzymanie transakcji, zabezpieczenie majątkowe lub zatrzymanie rzeczy; niezwłocznie uzyskać i poddać kontroli ich formalne podstawy.
6. Rozważyć konflikt interesów współpodejrzanych, interesy osób trzecich i konieczność powołania specjalistów finansowych lub biegłych.
7. Nie kontaktować się ze świadkami w celu uzgadniania relacji; wszelki kontakt z osobami w sprawie musi pozostawać zgodny z prawem i wolny od nacisków.

15. Prawo do obrony i wybór taktyki procesowej

Osoba mająca status podejrzanego powinna otrzymać pouczenia i korzystać z prawa do obrońcy oraz prawa do odmowy składania wyjaśnień lub odpowiedzi na pytania (art. 175 k.p.k.). Jej wybór nie może być interpretowany jako samodzielny dowód winy. Prawo wglądu do akt na etapie przygotowawczym funkcjonuje w granicach art. 156 k.p.k., które różnią się od uprawnień po wniesieniu aktu oskarżenia. Wnioski dowodowe i zastrzeżenia dotyczące sposobu zabezpieczenia danych należy składać w formach i terminach właściwych dla stadium sprawy. [P3]

Model A – aktywna obrona od początku: gdy komplet dokumentów i szybka ekspertyza potrafią wykazać legalne źródło środków oraz błędy identyfikacji osoby. Model B – obrona stopniowana: gdy zasadniczy materiał jest niedostępny, a pochopne wyjaśnienia grożą utrwaleniem sprzeczności. Model C – obrona łączona z legalnym wyjaśnieniem okoliczności AML i ochroną majątku: przy blokadzie działalności. Wybór musi być jawny dla klienta, nie może obejmować podawania nieprawdy.

16. Macierz obrony: zarzut – kontrteza – dowód

Element zarzutu	Pytania obrony	Właściwa inicjatywa dowodowa
Przestępcze źródło	Który czyn i jaka korzyść? Czy są alternatywne źródła?	Dokumenty bazowe, opinia finansowa, analiza przepływów
Tożsamość mienia	Czy ta kwota faktycznie jest tą korzyścią?	Mapowanie wpłat, sald i transferów w czasie
Zachowanie	Kto wydał dyspozycję i miał kontrolę?	Logi autoryzacji, upoważnienia, bankowe potwierdzenia

Element zarzutu	Pytania obrony	Właściwa inicjatywa dowodowa
Umyślność	Co podejrzany wiedział w danym dniu?	Korespondencja, procedury, niezależni świadkowie
Porozumienie – § 5	Czy dowody wykazują wspólne uzgodnienie?	Historia kontaktów, komunikacja, podział obowiązków
Znaczna korzyść – § 6	Czy to korzyść osiągnięta przez sprawcę, jak obliczona?	Ekspertyza ekonomiczna, korekta wyliczeń
Przepadek/zabezpieczenie	Czy mienie podlega przepadkowi i komu przysługuje?	Tytuły własności, wartość, interes osób trzecich

17. Analiza przepływów finansowych – praca na danych, a nie na etykietach

W sprawach o pranie pieniędzy obrona powinna przygotować odtwarzalną rekonstrukcję „source-to-use”: od pojawienia się korzyści, przez każde istotne przeniesienie i przeliczenie waluty, po miejsce przeznaczenia. Dokument ten powinien rozróżniać przepływ gotówki, przepływ praw, przysporzenie netto, obrót brutto, zwrot własnych środków, wartości rachunkowe i transakcje pozorne. Nie można bez wyjaśnienia sumować każdej operacji na tym samym kapitale, gdy prowadzi to do podwójnego liczenia jednych wartości.

Wymagana mapa dowodowa obejmuje: rachunek/portfel, datę i walutę, kwotę, zleceniodawcę, beneficjenta, identyfikator dokumentu, opis rzeczywistej podstawy, pochodzenie i stopień pewności ustalenia oraz alternatywne wyjaśnienia. Analizę należy zlecać niezależnemu ekspertowi, który ujawni metodykę i ograniczenia. Wnioski biegłego bada się również pod względem przesłanek z art. 201 k.p.k., jeżeli opinia jest niepełna, niejasna lub wewnętrznie sprzeczna. [P3]

18. Rachunek mieszany: znaczenie uchwały I KZP 5/15

Częsty błąd polega na uznaniu, że wpływ 300 000 zł mających przestępcze pochodzenie „skaża” każde kolejne saldo i wszystkie późniejsze obroty na rachunku do wysokości sumy wszystkich transferów. SN odrzucił automatyczne kwalifikowanie wszystkich wartości zgromadzonych na rachunku jako przedmiotu prania tylko dlatego, że część środków ma takie źródło. Konieczne jest przypisanie wartości korzyści do konkretnych czynności, w odpowiednim horyzoncie czasowym. [O2]

Hipotetyczny przykład: rachunek zawiera 700 000 zł legalnych wpływów i 100 000 zł, których przestępcze pochodzenie zostało dowodowo wykazane. Organ bada późniejszy przelew 150 000 zł. Obrona nie powinna twierdzić automatycznie, że przelew był „legalny”, ponieważ legalne środki stanowiły większość salda, ani że „brudne” środki zniknęły w wyniku kolejności księgowania. Powinna sprawdzić – z właściwą metodologią wynikającą z prawa i dowodów – które wartości były przedmiotem konkretnej czynności i jak wyliczono kwotę zarzutu. Sumaryczny obrót rachunku jest innym pojęciem niż wartość przestępczej korzyści.

19. Umyślność: dowody przeciw domniemaniom

Skuteczna linia obrony nie redukuje się do zaprzeczenia wiedzy. Należy zidentyfikować zdarzenia poprzedzające czynność, wyjaśnić, dlaczego dana osoba mogła racjonalnie uznawać transakcję za zgodną z prawem, i przeciwstawić temu materiał wykazujący rzeczywistą świadomość ryzyka. Szczególnie ważne są: dostęp do informacji na dany dzień, zakres obowiązków zawodowych, kompetencje w spółce, treść zaleceń specjalistów, standardowa ścieżka akceptacji oraz brak decyzyjności przy operacji.

Samo zastosowanie KYC czy brak alertu banku nie tworzy domniemania braku umyślności. Z kolei pozycja w zarządzie spółki nie tworzy domniemania osobistej wiedzy o każdym przelewie. W obu kierunkach potrzebna jest indywidualizacja. Ustalenia powinny wskazać dokładny moment, w którym oskarżony miał powziąć wiadomość o pochodzeniu mienia, i porównać go z momentem zarzucanej czynności.

20. Błędy śledztwa i prawidłowa kontrargumentacja

- Wnioskowanie „nie wykazano legalnego źródła, zatem źródło było przestępcze” – należy zakwestionować jako przeskok logiczny i żądać ustaleń odpowiadających znamionom art. 299.
- Traktowanie raportu GIIF, alertu compliance lub decyzji banku jak rozstrzygnięcia o winie – należy wskazać różnicę standardów oceny ryzyka i odpowiedzialności karnej.
- Automatyczne przenoszenie wiedzy jednej osoby na pozostałych członków zarządu, księgowych lub pełnomocników – należy wymagać konkretnych dowodów indywidualizacji.
- Sumowanie kolejnych transferów tych samych wartości bez identyfikacji rzeczywistych przysporzeń – należy żądać metodyki i korekty wyliczeń.
- Pominięcie legalnych przychodów, zwrotów, pożyczek i transakcji neutralnych ekonomicznie – należy przeprowadzić alternatywną analizę finansową.
- Niewyjaśnienie, czy dana czynność była „nazwana” czy „inna” w rozumieniu art. 299 § 1 – należy użyć wykładni I KZP 5/15.
- Brak chronologii wiedzy podejrzanego i wyciąganie z późniejszych faktów wniosków o wcześniejszym zamiarze – należy zbudować oś czasu i ustalić źródła informacji.
- Niedostateczna kontrola czynności technicznych zabezpieczenia danych – należy zbadać kompletność, łańcuch przechowywania i autentyczność zapisów.

21. Wnioski dowodowe – hierarchia i uzasadnienie

1. O dopuszczenie wyciągów ze wszystkich rachunków istotnych dla konkretnego przepływu wraz z pełnymi historiami transakcji, nie tylko wybranymi fragmentami.
2. O dane bankowe dotyczące autoryzacji, pełnomocnictw i kanału zlecenia dyspozycji w zakresie prawnie dopuszczalnym.
3. O dokumenty gospodarcze dowodzące wykonania świadczeń oraz źródeł finansowania kontrahentów, jeżeli ich ustalenie jest możliwe i istotne.
4. O przesłuchanie konkretnych świadków na ściśle określone okoliczności, a nie ogólnie „na brak winy”.
5. O opinię biegłego z rachunkowości/finansów oraz uzupełnienie dotychczasowej opinii, jeśli zachodzą przesłanki procesowe.
6. O dołączenie dokumentów z postępowania dotyczącego czynu źródłowego, z wyraźnym rozdzieleniem ich znaczenia dowodowego od prejudycjalności.
7. O zabezpieczenie oryginalnych danych cyfrowych i analizę integralności metadanych, o ile związana jest z autentycznością lub kontekstem transakcji.

W każdym wniosku trzeba wskazać dokładną tezę dowodową, znaczenie dla znamion czynu oraz możliwy do pozyskania nośnik danych; zbędne lub pozorne wnioski mogą zostać oddalone według reguł art. 170 k.p.k. Zasadne jest prowadzenie tabeli „fakt wymagający dowodu – dowód oskarżenia – kontrdowód – status weryfikacji”.

22. Blokada rachunku i zabezpieczenie majątkowe

Blokada realizowana na podstawie mechanizmów AML, zabezpieczenie majątkowe z k.p.k., zajęcie rzeczy i przepadek mają odmienne przesłanki, funkcje, organy i sposoby kontroli. Samo postanowienie o blokadzie nie jest dowodem winy. Należy ustalić dokładnie: podstawę prawną, datę i okres obowiązywania, organ, wskazane środki, wymagany stopień

uprawdopodobnienia, prawo do zaskarżenia i przesłanki dalszego utrzymywania. Terminy mogą różnić się w zależności od trybu – nie należy ich ustalać na podstawie ogólnych porad internetowych. [P2–P3]

Art. 291 k.p.k. wiąże zabezpieczenie m.in. z uzasadnioną obawą niemożności lub znacznego utrudnienia wykonania przyszłego orzeczenia. Linia obrony powinna obejmować zarówno kwestionowanie zarzutu i zakresu przypadku, jak i samoistne podważenie potrzeby, wysokości, proporcjonalności oraz sposobu zabezpieczenia. Osoba trzecia, której przysługuje prawo do mienia, wymaga odrębnej ochrony proceduralnej. [P3]

Praktyczne dowody: dokumenty własności przed uzyskaniem rzekomej korzyści, wyciągi dowodzące legalnego źródła wartości, wycena majątku, bilans zobowiązań, zakres ograniczenia działalności i propozycja dopuszczalnego ustawowo mniej dolegliwego sposobu zabezpieczenia. Nie wolno dokonywać czynności mających udaremnić wykonanie legalnego zabezpieczenia.

23. Tymczasowe aresztowanie – odrębna strategia

Zarzut art. 299 k.k. sam w sobie nie przesądza o konieczności stosowania izolacyjnego środka zapobiegawczego.

Wymaga odrębnej oceny przesłanki ogólnej z art. 249 k.p.k., podstaw szczególnych z art. 258 k.p.k., proporcjonalności i możliwości zastosowania środków wolnościowych. Obrona powinna konfrontować rzeczywiste ryzyko procesowe z ustaleniami dotyczącymi miejsca pobytu, więzi, postawy procesowej i dostępności dowodów. [P3]

W sprawach dokumentowych istotna jest argumentacja, że większość materiału znajduje się już w bankach, systemach księgowych, aktach urzędowych i niezależnych repozytoriach, co może ograniczać realne możliwości bezprawnego wpływania na dowody; nie znosi to jednak automatycznie obawy matactwa w każdej sprawie. Każde odwołanie od aresztu powinno być skonstruowane na podstawie rzeczywistych, a nie deklaracyjnych okoliczności.

24. Czy warto skorzystać z art. 299 § 8 k.k.?

Art. 299 § 8 przewiduje szczególne następstwa dobrowolnego ujawnienia organowi ścigania informacji dotyczących osób uczestniczących w przestępstwie i jego okoliczności, jeżeli doprowadziło to do zapobieżenia innemu przestępstwu, a także nadzwyczajne złagodzenie kary w sytuacji wskazanej w drugiej części przepisu. Nie jest to automatyczny „program amnestii”, a przesłanki wymagają ścisłego spełnienia i udowodnienia. Decyzja musi zostać podjęta po analizie aktualnego statusu procesowego i ryzyka samooskarżenia, z poszanowaniem praw innych osób. [P1]

Należy unikać składania deklaracji, których prawdziwości nie da się zweryfikować, lub dostosowywania opowieści do oczekiwań organu. Sens przepisu wymaga rzeczywistej, dobrowolnej i prawdziwej współpracy spełniającej warunki ustawowe.

CZĘŚĆ IV. PRZYKŁADOWE MODELE OBRONY

25. Sześć studiów hipotetycznych

Przedsiębiorca i „puste” faktury

Zarzut opiera się na kwotach brutto ze wszystkich faktur i założeniu, że brak potwierdzenia niektórych dostaw dowodzi przestępczego pochodzenia całego obrotu. Należy oddzielić rzeczywiste dostawy od fikcyjnych dokumentów, ustalić mechanizm ewentualnej korzyści z czynu bazowego i wyodrębnić środki, których dotyczyły konkretne czynności. Ryzyko: autentyczne fałszerstwa i świadome obchodzenie zasad fakturowania mogą stanowić istotne dowody oskarżenia.

Członek zarządu i rachunek spółki

Prokuratura przypisuje wiedzę na podstawie funkcji. Obrona identyfikuje moment powołania, zakres obowiązków, faktyczną obsługę płatności, wewnętrzne akceptacje i ostrzeżenia. Ryzyko: formalne przeniesienie kompetencji nie wyklucza rzeczywistej kontroli.

Osoba prywatna i duża darowizna

Bank zgłasza nietypowy wpływ. Należy wykazać autentyczność relacji darowizny, źródło pieniędzy darczyńcy, daty, zgłoszenia podatkowe i tożsamość rzeczywistego dysponenta. Brak zgłoszenia podatkowego może rodzić inny problem prawny, ale sam nie przesądza o art. 299.

Pośrednik otrzymujący prowizję

Pośrednik może nie odpowiadać za cały majątek, który przechodził przez rachunki kontrahentów. Trzeba dokładnie odtworzyć przedmiot jego czynności, źródło przysporzenia, zakres wiedzy i ewentualne porozumienie. Sama prowizja nie jest „tarczą”, jeśli stanowi zapłatę za świadome pranie.

Kryptowaluty nabyte wcześniej

Użytkownik przedstawia historyczne potwierdzenia zakupu, zapis transferów, dokumenty platform i rozliczenia, które pozwalają wiarygodnie ustalić legalne źródło aktywów. Ryzyko: brak raportów lub anonimowość portfela nie dowodzi przestępstwa, ale utrudnia ustalenia i może zwiększać uwagę organów.

Nieruchomość zakupiona przez osobę trzecią

Głównym zagadnieniem jest, czy osoba występująca w akcie była rzeczywistym nabywcą, kto finansował cenę, jaki był tytuł prawny zapłaty oraz jakie informacje znała każda z osób. Obrona musi dokumentować realną relację; pozorna umowa lub podstawiona osoba może obciążać.

26. Model konstrukcji pisma obrony – do adaptacji procesowej

Tytuł: „Wniosek dowodowy i stanowisko obrony co do przesłanek art. 299 § 1 k.k.”. Pismo powinno zidentyfikować właściwy organ, sygnaturę, uprawnionego składającego i podstawę procesową. Poniższa sekwencja jest wzorcem argumentacyjnym, a nie gotowym pismem do podpisu:

1. Petitum: o przeprowadzenie ściśle określonych dowodów, ewentualnie o ich uzupełnienie, a na odpowiednim etapie o rozważenie decyzji kończącej postępowanie zgodnie z materiałem.
2. Okoliczności bezsporne: precyzyjna oś czasu, rachunki, kontrahenci, kwoty, dokumenty i zidentyfikowane czynności.

3. Zastrzeżenie do identyfikacji źródła: brak wskazania dostatecznie ustalonego czynu zabronionego i ścieżki pochodzenia określonego mienia albo błąd w tym ustaleniu.
4. Zastrzeżenie do przypisania sprawstwa: brak potwierdzenia, że podejrzany wykonał ustawowo relewantną czynność lub posiadał rzeczywistą kontrolę nad dyspozycją.
5. Zastrzeżenie do umyślności: brak dowodów, z których wynikałaby świadomość i godzenie się na przestępstwo źródło, oraz wskazanie konkretnych kontrdowodów.
6. Analiza kwot i rachunków: weryfikacja sum, eliminacja zdublowań, wyodrębnienie źródeł legalnych i niedowodowych.
7. Argument prawny: odniesienie do uchwał I KZP 19/13, I KZP 5/15 i wyroku III KK 407/14 oraz standardu procesowego z k.p.k.
8. Konkluzja: wnioski wyłącznie w zakresie uzasadnionym faktami, bez twierdzeń wykraczających poza materiał dowodowy.

27. Checklista audytu akt przez obrońcę

- Czy zarzut identyfikuje datę, miejsce, środek płatniczy lub mienie i czynność wykonawczą?
- Czy w aktach opisano określony czyn zabroniony będący źródłem korzyści?
- Czy dostępne dowody rzeczywiście łączą mienie z korzyścią z tego czynu?
- Czy organ prawidłowo ustalił zakres przestępczej części mieszanego rachunku?
- Czy istnieje podwójne liczenie kwot i brak rozróżnienia obrotu od korzyści?
- Czy ustalono indywidualną rolę klienta, jego dyspozycje i źródła informacji w odpowiednim czasie?
- Czy ustalenia o zamiarze mają oparcie w dowodach, a nie wyłącznie w typologii AML?
- Czy zbadano legalne wersje alternatywne i dowody odciążające?
- Czy uzasadniono przesłanki porozumienia, znaczną korzyść albo przygotowanie?
- Czy zabezpieczenie, blokada i środki zapobiegawcze mają aktualne podstawy?
- Czy opinia finansowa ujawnia komplet danych i metodologię obliczeń?
- Czy zachowano pouczenia, dostęp do obrońcy, zasady dostępu do akt i kontrolę terminów?

CZĘŚĆ V. ORZECZNICTWO I ŹRÓDŁA

28. Kluczowe orzeczenia – wykładnia i praktyczne znaczenie

Orzeczenie	Teza istotna dla art. 299 k.k.	Wniosek dla obrony
SN (7), 18.12.2013, I KZP 19/13	Pochodzenie bezpośrednie i pośrednie; możliwe „autopranie”	Nie opierać obrony na wyłączeniu sprawcy czynu bazowego
SN (7), 24.06.2015, I KZP 5/15	Granica wartości na rachunku mieszanym; klauzula „innych czynności”	Badać kwotę przypisaną konkretnym operacjom i rodzaj czynności
SN, 05.03.2015, III KK 407/14	Nieudokumentowane/nielegalne źródło nie zastępuje dowodu związku z czynem zabronionym	Żądać konkretyzacji czynu źródłowego i sposobu pochodzenia
SN, 20.05.2013, III KK 455/12	Znaczenie ustalenia znamion prania i czynu źródłowego	Kontrolować opis przypisanego czynu i podstawę dowodową
TSUE, 26.06.2007, C-305/05	Przy stosowaniu AML do prawników chronić prawo do rzetelnego procesu	Rozróżniać obronę procesową i działalność transakcyjną
ETPC, 06.12.2012, Michaud p. Francji	Dopuszczalność ograniczonego raportowania AML z poszanowaniem tajemnicy adwokackiej	Badać rzeczywisty charakter usługi i gwarancje tajemnicy

Ważna uwaga metodologiczna: uchwały i wyroki nie są „magicznymi cytataми” rozstrzygającymi sprawę. Ich znaczenie zależy od rodzaju czynności przypisanej podejrzanemu, zmian brzmienia ustawy w czasie oraz faktów. Trzeba argumentować ratio decidendi, a nie mechanicznie zestawiać sygnatury.

29. Główne źródła normatywne, orzecznicze i instytucjonalne

[P1] Ustawa z 6.06.1997 r. – Kodeks karny; tekst jednolity Dz.U. 2026 poz. 1342, ogłoszony 16.10.2026

<https://www.dziennikustaw.gov.pl/DU/2026/1342>

[P2] Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu; t.j. Dz.U. 2025 poz. 644 z późn. zm.; art. 2, 27, 33–35, 43, 49, 50, 52, 54, 74–75, 86

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000723>

[P3] Ustawa z 6.06.1997 r. – Kodeks postępowania karnego; t.j. Dz.U. 2026 poz. 490 z późn. zm.

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260000490>

[O1] SN, uchwała składu siedmiu sędziów z 18.12.2013 r., I KZP 19/13 (zasada prawna)

<https://www.sn.pl/pl/sprawy/zagadnienia-prawne/i-kzp-19-13>

[O2] SN, uchwała składu siedmiu sędziów z 24.06.2015 r., I KZP 5/15

<https://www.sn.pl/pl/sprawy/zagadnienia-prawne/i-kzp-5-15>

[O3] SN, wyrok z 05.03.2015 r., III KK 407/14 – pełna treść w SAOS / odtworzenie treści SN

<https://www.saos.org.pl/search?referencedCourtCaseId=100779>

[O4] SN, wyrok z 20.05.2013 r., III KK 455/12

<https://www.saos.org.pl/judgments/101849>

[UE1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673, zwłaszcza art. 3

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1673>

[UE2] Rozporządzenie (UE) 2024/1624 (AMLR), zasadnicze stosowanie od 10.07.2027 r.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624>

[UE3] Dyrektywa (UE) 2024/1640, etapowe terminy transpozycji

<https://eur-lex.europa.eu/eli/dir/2024/1640/oj>

[UE4] Rozporządzenie (UE) 2023/1113 o informacji przy transferach środków pieniężnych i określonych kryptoaktywów

<https://eur-lex.europa.eu/eli/reg/2023/1113/oj>

[UE5] TSUE, wyrok z 26.06.2007 r., C-305/05, *Ordre des barreaux francophones et germanophone i in.*, ECLI:EU:C:2007:383

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62005CJ0305>

[UE6] ETPC, *Michaud przeciwko Francji*, skarga nr 12323/11, wyrok z 6.12.2012 r.

https://ks.echr.coe.int/documents/d/echr-ks/reports_recueil_2012-vi

[I1] Ministerstwo Finansów / GIIF, Publikacje i wytyczne dla instytucji obowiązanych

<https://www.gov.pl/web/finanse/-publikacje-i-wytyczne-giif-dla-instytucji-obowiazanych>

[I2] GIIF, komunikat nr 113 o Travel Rule i zawiadomieniach AML

<https://www.gov.pl/web/finanse/komunikat-nr-113-sprawie-stosowania-wytycznych-eba-dotyczacych-wymogow-informacyjnych-towarzyszacych-transferom-srodkow-pienieznych-i-niektorych-kryptoaktywow-tzw-travel-rule-oraz-zasad-raportowania-do-giif>

[F1] FATF, Recommendations – standard podejścia opartego na ryzyku

<https://www.fatf-gafi.org/en/topics/fatf-recommendations.html>

[F2] FATF, Guidance on Beneficial Ownership of Legal Persons (2023)

<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>

30. Granice opracowania i rekomendacja dla sprawy indywidualnej

Poradnik odtwarza zasady prawne i kierunki argumentacji, ale nie zastępuje opinii wydanej po wglądzie w kompletny materiał. Rozstrzygające mogą być: relacja chronologiczna między czynem bazowym a transakcją, techniczny sposób autoryzacji, przepisy w dacie czynu, znaczenie przestępstwa skarbowego jako źródła wartości, skala i źródło korzyści, realne zachowania osoby obciążonej, a także dowody odciążające, których nie badała jeszcze prokuratura.

Za profesjonalny rezultat analizy konkretnych akt należy uznać nie tylko tezę o braku znamion, lecz także: (a) mapę dowodową z lukami; (b) alternatywną rekonstrukcję przepływów; (c) matrycę ryzyka ustaleń procesowych; (d) plan pozyskania dokumentów; (e) plan działań wobec blokady/zabezpieczenia; (f) precyzyjne, uzasadnione wnioski dowodowe i środki zaskarżenia.

W sytuacji realnego ryzyka zarzutu nie należy podejmować samodzielnie działań na majątku objętym zainteresowaniem organów, niszczyć lub „porządkować” dokumentów w sposób zmieniający ich treść, instruować świadków ani ujawniać poufnych zawiadomień AML. Należy natychmiast niezwłocznie uzyskać profesjonalną pomoc i zachować nienaruszoną dokumentację.