Rada
Unii Europejskiej

Bruksela, 11 lipca 2023 r.
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	10 lipca 2023 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2023) 363 final
Dotyczy:	SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY zawierające ocenę zakresu, w jakim państwa członkowskie podjęły niezbędne działania w celu zapewnienia zgodności z dyrektywą (UE) 2019/713 w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępującą decyzję ramową Rady 2001/413/WSiSW

Delegacje otrzymują w załączeniu dokument COM(2023) 363 final.

Zał.: COM(2023) 363 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 10.7.2023 r.
COM(2023) 363 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

zawierające ocenę zakresu, w jakim państwa członkowskie podjęły niezbędne działania w celu zapewnienia zgodności z dyrektywą (UE) 2019/713 w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępującą decyzję ramową Rady 2001/413/WSiSW

1. Wprowadzenie

Fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi takimi jak karty kredytowe lub płatnicze stanowią ważne źródło dochodów dla przestępczości zorganizowanej i umożliwiają prowadzenie innej działalności przestępczej, takiej jak terroryzm, nielegalny obrót środkami odurzającymi i handel ludźmi. Przestępstwa te powodują znaczne straty: całkowita wartość transakcji przeprowadzanych w celu dokonania oszustwa z wykorzystaniem kart wydanych na jednolitym obszarze płatności w euro wyniosła w 2019 r. 1,87 mld EUR[1]. Zdecydowana większość transakcji przeprowadzanych w celu dokonania oszustwa związana jest z oszustwami dotyczącymi płatności bez fizycznej obecności karty: w 2019 r. 80 % wartości oszustw z wykorzystaniem kart wynikało z transakcji dotyczących płatności bez fizycznej obecności karty, tj. płatności w internecie, za pośrednictwem poczty lub telefonu[2]. W 2019 r. straty z tytułu oszustw dotyczących płatności bez fizycznej obecności karty wyniosły 1,50 mld EUR, co stanowi wzrost o 4,3 % w porównaniu z rokiem poprzednim[3].

Problem ten ma wyraźny wymiar transgraniczny: ponad połowa całkowitej wartości oszustw w 2019 r. była związana z transakcjami transgranicznymi w ramach jednolitego obszaru płatności w euro. Pod względem geograficznym transakcje krajowe stanowiły 89 % wartości wszystkich transakcji realizowanych w oparciu o kartę w 2019 r., ale tylko 35 % transakcji przeprowadzonych w celu dokonania oszustwa. Transakcje transgraniczne w ramach jednolitego obszaru płatności w euro stanowiły 9 % wszystkich transakcji realizowanych w oparciu o kartę pod względem wartości, ale 51 % zgłoszonych oszustw[4].

Aby skutecznie zwalczać tego rodzaju przestępstwa, państwa członkowskie muszą wspólnie określić, jakiego rodzaju czyny powinny być uznawane za fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi. Państwa członkowskie powinny również nakładać zbliżone kary i stosować podobne środki operacyjne w kontekście składania powiadomień o popełnieniu przestępstwa i wymiany informacji między organami. W związku z tym 17 kwietnia 2019 r. Parlament Europejski i Rada przyjęły dyrektywę (UE) 2019/713 („dyrektywa") w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępującą decyzję ramową Rady 2001/413/WSiSW[5]. Niniejsze sprawozdanie sporządzono w celu spełnienia wymogu określonego w art. 21 dyrektywy.

1.1. Cel i zakres dyrektywy

Celem dyrektywy jest zbliżenie prawa karnego państw członkowskich[6] w dziedzinie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz

---

[1] Europejski Bank Centralny, Siódme sprawozdanie na temat oszustw z wykorzystaniem kart, dostępne pod adresem: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html

[2] Ibidem.

[3] Ibidem.

[4] Ibidem.

[5] https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32019L0713

[6] Od tego momentu i o ile wprost nie stwierdzono inaczej, termin „państwa członkowskie" lub „wszystkie państwa członkowskie" odnosi się do państw członkowskich związanych dyrektywą, tj. do wszystkich państw członkowskich UE z wyjątkiem Danii i Irlandii, które nie brały udziału w procesie przyjmowania dyrektywy odpowiednio zgodnie z Protokołem w sprawie stanowiska Danii załączonym do Traktatu o Unii Europejskiej

usprawnienie współpracy między właściwymi organami. W tym celu w dyrektywie ustanowiono normy minimalne dotyczące definicji przestępstw oraz sankcji.Zakres dyrektywy jest szeroki i obejmuje dowolne „niematerialne lub materialne chronione urządzenie, przedmiot lub zapis, lub ich kombinację, inny niż prawny środek płatniczy, który – samodzielnie lub w połączeniu z określoną procedurą lub zestawem procedur – umożliwia posiadaczowi lub użytkownikowi dokonanie przekazu środków pieniężnych lub wartości pieniężnych, w tym przy użyciu cyfrowych środków wymiany", art. 2 lit. a)[7]. Zakresem tej definicji objęta byłaby na przykład aplikacja do płatności mobilnych w połączeniu z procedurą autoryzacji (np. PIN). Obejmuje ona również waluty wirtualne, art. 2 lit. d) i art. 6.

W dyrektywie zdefiniowano konkretne przestępstwa, a mianowicie:

- użycie bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa (art. 3);
- przestępstwa związane z użyciem materialnych bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa (art. 4);
- przestępstwa związane z użyciem niematerialnych bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa (art. 5);
- oszustwa związane z systemami informatycznymi (art. 6);
- niezgodne z prawem dostarczanie narzędzi do popełniania wymienionych powyżej przestępstw (art. 7).

Ponadto w dyrektywie **rozszerzono zakres odpowiedzialności karnej** o podżeganie przez osoby fizyczne lub prawne do popełniania wymienionych powyżej przestępstw, pomocnictwo przy ich popełnianiu i usiłowanie ich popełnienia (art. 8).

W art. 9 określono minimalne poziomy maksymalnego wymiaru **kary** z tytułu popełnienia przestępstw, o których mowa w dyrektywie.

W kolejnych artykułach określono minimalne wymogi dotyczące **odpowiedzialności osób prawnych** (art. 10) i sankcje obejmujące grzywny nałożone na podstawie przepisów prawa karnego lub na podstawie innych przepisów oraz przedstawiono przykładowy wykaz innych sankcji, jakie można nałożyć na te osoby (art. 11).

Celem art. 12 jest zapewnienie, aby sprawcy, o których mowa w dyrektywie, byli ścigani w odniesieniu do przestępstw określonych w art. 3–8 dyrektywy. Należy ustalić **jurysdykcję** państwa członkowskiego w przypadku, gdy a) przestępstwo zostało popełnione w całości lub części na jego terytorium lub gdy b) sprawca jest jego obywatelem. Innymi słowy, w art. 12 ust. 1 lit. a) dyrektywy określono zasadę terytorialności, podczas gdy lit. b) prowadzi do zasady czynnego obywatelstwa.

Art. 13 ust. 1 dyrektywy stanowi, że **narzędzia dochodzeniowo-śledcze** służące do prowadzenia postępowań przygotowawczych i ścigania przestępstw, o których mowa w art. 3–8, powinny być skuteczne, proporcjonalne i dostępne dla odpowiedzialnych osób, jednostek i służb. Zgodnie z art. 13 ust. 2 dyrektywy informacje dotyczące przestępstw,

---

i Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) i z Protokołem 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii.

[7] O ile nie stwierdzono inaczej, wszystkie odesłania do artykułów należy traktować jako odesłania do artykułów dyrektywy.

o których mowa w art. 3–8, powinny docierać bez zbędnej zwłoki do organów prowadzących postępowania przygotowawcze w sprawie tych przestępstw lub je ścigających.

W odniesieniu do wymiany informacji zgodnie z art. 13 ust. 14 państwa członkowskie są zobowiązane do zapewnienia istnienia operacyjnych krajowych **punktów kontaktowych** dostępnych 24 godziny na dobę, przez siedem dni w tygodniu, aby mogły reagować na wszelkiego rodzaju pilne wnioski w ciągu ośmiu godzin od ich otrzymania.

Ponadto w art. 15 ust. 1 dyrektywy zobowiązuje się państwa członkowskie do ustanowienia odpowiednich kanałów **powiadamiania** bez zbędnej zwłoki organów publicznych **o przestępstwach**, o których mowa w art. 3–8. W szczególności zachęca się instytucje finansowe, aby zgłaszały podejrzenia o popełnieniu oszustwa organom ścigania i organom sądowym (art. 15 ust. 2). Zgłoszenia prowadzą często do wszczęcia postępowań przygotowawczych (motyw 27).

Ponadto art. 16 i 17 dyrektywy dotyczą odpowiednio **pomocy i wsparcia dla ofiar** oraz **zapobiegania**.

1.2. Cel i metodyka sprawozdania

Zgodnie z art. 20 dyrektywy państwa członkowskie są zobowiązane do wprowadzenia w życie przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania dyrektywy w terminie do 31 maja 2021 r. i powiadomienia Komisji o tych przepisach.

Niniejsze sprawozdanie sporządzono zgodnie z wymogiem ustanowionym w art. 21 dyrektywy nakładającym na Komisję obowiązek przedłożenia Parlamentowi Europejskiemu i Radzie sprawozdania, w którym oceni, w jakim zakresie państwa członkowskie wprowadziły środki niezbędne do wykonania tej dyrektywy. Niniejsze sprawozdanie – które jest pierwszym sprawozdaniem na podstawie art. 21 – zawiera przegląd najistotniejszych środków transpozycji wprowadzonych przez państwa członkowskie.

Transpozycja przepisów przez państwo członkowskie wiązała się z koniecznością zgromadzenia informacji na temat stosownych przepisów i środków administracyjnych, przeprowadzenia ich analizy, opracowania nowych przepisów lub – w większości przypadków – wprowadzenia zmian w istniejących aktach prawnych, zapewnienia ich przyjęcia oraz – ostatecznie – przekazania odpowiedniego sprawozdania Komisji.

Dziewięć państw członkowskich powiadomiło Komisję o pełnym zakończeniu transpozycji dyrektywy przed upływem terminu transpozycji (31 maja 2021 r.) oraz zgłosiło podjęte przez siebie środki transpozycji. W lipcu 2021 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego z tytułu nieprzekazania informacji o krajowych środkach transpozycji przeciwko pozostałym 16 państwom członkowskim: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO i SI[8]. Chociaż od tego czasu 15 państw członkowskich zgłosiło wprowadzone przez siebie środki transpozycji, według stanu na 30 kwietnia 2023 r. postępowanie w sprawie uchybienia zobowiązaniom państwa

[8] Nazwy państw członkowskich w niniejszym dokumencie skrócono zgodnie z zasadami przedstawionymi na stronie internetowej: http://publications.europa.eu/code/pl/pl-5000600.htm

członkowskiego z tytułu nieprzekazania informacji o krajowych środkach transpozycji wszczęte przeciwko BG było jeszcze w toku[9].

Podstawą poniższego opisu i analizy w niniejszym sprawozdaniu są informacje o krajowych środkach transpozycji przekazane przez państwa członkowskie do 31 stycznia 2023 r. Powiadomienia otrzymane po tym terminie nie zostały uwzględnione. Pod uwagę wzięto wszystkie zgłoszone środki dotyczące przepisów krajowych, jak również orzeczenia sądów oraz – w stosownych przypadkach – powszechnie uznawaną teorię prawną. Ponadto w toku analizy Komisja kontaktowała się bezpośrednio z państwami członkowskimi w przypadkach, w których było to właściwe do celów uzyskania dodatkowych informacji lub wyjaśnień. Na potrzeby analizy uwzględniono wszystkie zgromadzone informacje.

Nie można wykluczyć, że poza kwestiami, na które zwrócono uwagę w niniejszym sprawozdaniu, istnieją również inne wyzwania związane z transpozycją dyrektywy oraz inne przepisy lub planowane zmiany o charakterze prawnym i pozaprawnym, które nie zostały zgłoszone Komisji. Z tego względu publikacja niniejszego sprawozdania nie uniemożliwia Komisji dalszego oceniania niektórych przepisów ani udzielania państwom członkowskim dalszego wsparcia przy transpozycji i wdrażaniu przepisów dyrektywy.

[9] Informacje na temat decyzji Komisji dotyczących postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego można uzyskać pod adresem: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=pl

2. Środki transpozycji

2.1 Definicje legalne

Art. 2 zawiera definicje głównych pojęć stosowanych w dyrektywie, mianowicie: bezgotówkowego instrumentu płatniczego; chronionego urządzenia, przedmiotu lub zapisu; cyfrowego środka wymiany; waluty wirtualnej; systemu informatycznego; danych komputerowych; osoby prawnej.

Państwa członkowskie zasadniczo transponowały te definicje, opierając się na przepisach obowiązujących przed wejściem w życie dyrektywy lub przyjętych po jej wejściu w życie. W niektórych przypadkach – mimo że brak jest przepisów, w których wyraźnie określono definicje – transpozycji przestępstw dokonuje się za pośrednictwem przepisów ogólnych kodeksu karnego, które mają szerszy zakres, np. przepisów dotyczące kradzieży. W związku z tym nieprzekazanie informacji o dosłownej transpozycji definicji niekoniecznie oznacza niekompletność lub niezgodność.

Ponadto kilka definicji zawiera odniesienia do definicji zawartych w innych dyrektywach.

a) Bezgotówkowe instrumenty płatnicze

W ramach oceny wykazano co najmniej jeden przypadek niepełnej transpozycji, ponieważ definicja określona w decyzji ramowej Rady 2001/413/WSiSW nie została zaktualizowana. W związku z tym odnosi się ona wyłącznie do materialnych instrumentów płatniczych i nie obejmuje „chronionego urządzenia, przedmiotu lub zapisu, lub ich kombinacji", o których mowa w definicji zawartej w dyrektywie.

b) Chronione urządzenie, przedmiot lub zapis

Szereg państw członkowskich nie transponowało tej definicji (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Niekoniecznie uważa się to za przypadek niezgodności, ponieważ zazwyczaj znaczenie jest oczywiste lub można je wywnioskować z brzmienia definicji bezgotówkowego instrumentu płatniczego. W niektórych państwach pojęcie to wyjaśniono w ramach prac przygotowawczych.

c) Cyfrowe środki płatnicze i waluta wirtualna

Te dwie definicje mają kluczowe znaczenie dla dyrektywy 2019/713, której głównym celem było odniesienie się do faktu, że decyzja ramowa 2001/413/WSiSW nie odzwierciedlała już obecnych realiów i w niewystarczającym stopniu uwzględniała nowe wyzwania i zmiany technologiczne, takie jak waluty wirtualne i płatności mobilne, które należało uwzględnić, aby zapewnić kompleksową odpowiedź na to zjawisko i usunąć niezamierzone luki w kryminalizacji.

Głównym problemem napotkanym podczas transpozycji jest zakres waluty wirtualnej zdefiniowanej w art. 2 lit. d) dyrektywy. Chociaż we wszystkich państwach członkowskich określono definicję pieniądza elektronicznego, często w wyniku transpozycji dyrektywy w sprawie pieniądza elektronicznego[10] określenie definicji i zakresu waluty wirtualnej nie zawsze jest proste.

[10] Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz.U. L 267 z 10.10.2009.

W HU walutę wirtualną uznaje się za mienie i dane elektroniczne, które może podlegać konfiskacie mienia i zajęciu. Podobnie w PL w przepisach nie zdefiniowano waluty wirtualnej i istnieje pewien poziom niepewności co do tego, czy wchodziłaby ona w zakres poszczególnych przestępstw istotnych dla transpozycji dyrektywy, chociaż niektórzy z autorów uważają, że waluta wirtualna mogłaby podlegać przepisom kodeksu karnego regulującym przestępstwa związane z informacjami, nośnikami danych lub danymi informacyjnymi.

Wiele państw członkowskich transponowało te definicje za pośrednictwem przepisów finansowych, a nie do prawa karnego (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Jednak nie we wszystkich tych przypadkach istnieje odniesienie do odpowiednich przepisów w ustawodawstwie krajowym określającym przestępstwa. Ponadto w trzech państwach członkowskich (IT, MT, RO) obie definicje transponowano do kodeksu karnego.

d) System informatyczny

W art. 2 lit. e) zdefiniowano „system informatyczny", odsyłając do art. 2 lit. a) dyrektywy 2013/40/UE. Wszystkie państwa członkowskie transponowały tę definicję zgodnie z dyrektywą.

e) Dane komputerowe

Dane komputerowe zdefiniowano w art. 2 lit. f) przez odesłanie do art. 2 lit. b) dyrektywy 2013/40/UE. Wszystkie państwa członkowskie transponowały art. 2 lit. f) zgodnie z dyrektywą.

f) Osoba prawna

Ponadto w art. 2 lit. g) uwzględniono definicję „osoby prawnej". Niemal wszystkie państwa członkowskie dokonały transpozycji tego pojęcia do swoich przepisów. Jedynym wyjątkiem jest SE, która nie definiuje „osoby prawnej". Najbliższym pojęciem użytym w transpozycji jest „przedsiębiorstwo". Pojęcia tego nie zdefiniowano w żadnym tekście prawnym ani w doktrynie czy orzecznictwie.

2.2 Konkretne przestępstwa

a) Użycie bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa

Art. 3 lit. a) dyrektywy zobowiązuje państwa członkowskie do wprowadzenia środków niezbędnych do zapewnienia, aby użycie w celu dokonania oszustwa skradzionego lub przywłaszczonego bądź uzyskanego w inny bezprawny sposób bezgotówkowego instrumentu płatniczego, jeżeli zostało popełnione umyślnie, było karalne jako przestępstwo.

25 państw członkowskich transponowało art. 3 lit. a) dyrektywy. Spośród 25 państw 14 dokonało transpozycji dyrektywy za pośrednictwem przepisu dotyczącego konkretnie użycia bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). Pozostałe państwa członkowskie odniosły się do bardziej ogólnych przestępstw, takich jak oszustwa i fałszerstwa komputerowe lub oszustwa związane ze środkami płatniczymi, nie ograniczając się do bezgotówkowych instrumentów płatniczych (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

Prawo HR nie odnosi się do korzystania ze skradzionych lub w inny sposób bezprawnie przywłaszczonych instrumentów płatniczych; przepis transponujący w HU odnosi się wyłącznie do elektronicznych bezgotówkowych instrumentów płatniczych.

Zgodnie z art. 3 lit. b) dyrektywy państwa członkowskie przyjmują środki niezbędne do zapewnienia, aby użycie w celu dokonania oszustwa podrobionego lub sfałszowanego bezgotówkowego instrumentu płatniczego podlegało karze jako przestępstwo, jeżeli popełniono je umyślnie.

Art. 3 lit. b) został zasadniczo transponowany w sposób kompletny.

W celu transpozycji dyrektywy 15 państw członkowskich odwołuje się do przepisów krajowych dotyczących bezgotówkowych instrumentów płatniczych (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), podczas gdy krajowe przepisy transponujące w 10 państwach członkowskich obejmują bardziej ogólne przestępstwa, takie jak kradzież lub oszustwo, lub przestępstwa związane z instrumentami płatniczymi, ale nie konkretnie z instrumentami bezgotówkowymi (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Przestępstwa związane z użyciem materialnych bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa

Art. 4 dyrektywy zobowiązuje państwa członkowskie do wprowadzania środków niezbędnych do zapewnienia, aby popełnione umyślnie czyny wymienione w literach tego artykułu były karalne jako przestępstwo. Brzmienie liter jest następujące: a) kradzież lub innego rodzaju przywłaszczenie materialnego bezgotówkowego instrumentu płatniczego; b) podrobienie lub sfałszowanie materialnego bezgotówkowego instrumentu płatniczego do użycia go w celu dokonania oszustwa; c) posiadanie skradzionego lub przywłaszczonego, podrobionego lub sfałszowanego materialnego bezgotówkowego instrumentu płatniczego do użycia go w celu dokonania oszustwa; d) pozyskiwanie dla siebie lub dla osoby trzeciej, w tym otrzymanie, przywłaszczenie, nabycie, transfer, przywóz, wywóz, sprzedaż, transport lub dystrybucja skradzionego, podrobionego lub sfałszowanego materialnego bezgotówkowego instrumentu płatniczego do użycia go w celu dokonania oszustwa.

Chociaż wydaje się, że art. 4 został transponowany w mniej lub bardziej dosłowny sposób, w kilku przypadkach transpozycja krajowa budzi wątpliwości dotyczące konkretnego działania polegającego na nabyciu dla siebie lub innej osoby skradzionego, podrobionego lub sfałszowanego materialnego bezgotówkowego instrumentu płatniczego w celu dokonania oszustwa.

c) Przestępstwa związane z użyciem niematerialnych bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa

W art. 5 dyrektywy za przestępstwo uznaje się czyny związane z użyciem niematerialnych bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa. W analizie wykazano, że artykuł ten najwyraźniej nie stwarza wyzwań w zakresie transpozycji. W większości przypadków przepis krajowy ma zastosowanie zarówno do materialnych, jak i niematerialnych bezgotówkowych instrumentów płatniczych. Około połowa państw członkowskich dokonała transpozycji art. 5 dyrektywy za pośrednictwem bardziej ogólnych przepisów (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), a ponad połowa dokonała transpozycji za pośrednictwem przepisu odnoszącego się konkretnie do użycia bezgotówkowych instrumentów płatniczych w celu dokonania oszustwa (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Oszustwa związane z systemami informatycznymi

W art. 6 dyrektywy zobowiązano państwa członkowskie do zapewnienia, aby dokonanie lub spowodowanie dokonania przekazu środków pieniężnych, wartości pieniężnych lub waluty wirtualnej i tym samym spowodowanie bezprawnego pozbawienia innej osoby jej własności w celu uzyskania bezprawnej korzyści przez sprawcę lub osobę trzecią były karalne jako przestępstwo, jeżeli czyny te zostały popełnione umyślnie poprzez nieuprawnione zakłócanie funkcjonowania systemu informatycznego lub ingerowanie w jego funkcjonowanie (art. 6 lit. a)); lub nieuprawnione wprowadzanie, zmienianie, usuwanie, przekazywanie lub eliminowanie danych komputerowych (art. 6 lit. b)). Wszystkie państwa członkowskie dokonały transpozycji art. 6.

e) Narzędzia wykorzystywane do popełniania przestępstw

W art. 7 dyrektywy wymaga się od państw członkowskich wprowadzenia środków niezbędnych do zapewnienia, aby wytwarzanie, pozyskiwanie dla siebie lub dla innej osoby, w tym przywóz, wywóz, sprzedaż, transportowanie lub dystrybucja, lub udostępnianie urządzenia lub instrumentu, danych komputerowych lub innych środków zasadniczo przeznaczonych lub specjalnie przystosowanych w celu popełnienia dowolnego z przestępstw, o których mowa w art. 4 lit. a) i b), art. 5 lit. a) i b) lub w art. 6, przynajmniej jeżeli czyn został popełniony z zamiarem użycia tych środków, były karalne jako przestępstwo.

Zdecydowana większość państw członkowskich dokonała transpozycji art. 7 dyrektywy (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Sześć państw dokonało transpozycji art. 7 dyrektywy za pośrednictwem przepisów, które odsyłają do szerszych przepisów dotyczących ogólnych przestępstw, takich jak kradzież, albo dotyczących instrumentów finansowych i środków płatniczych (BG, FI, FR, LV, SE, SK). 17 państw dokonało jego transpozycji za pośrednictwem przepisu szczegółowego dotyczącego narzędzi wykorzystywanych do popełniania poszczególnych przestępstw określonych w dyrektywie związanych z materialnymi lub niematerialnymi bezgotówkowymi instrumentami płatniczymi (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Wydaje się, że pięć państw członkowskich stanęło w obliczu wyzwań związanych z transpozycją (BE, BG, HU, PL, PT).

2.3. Przepisy ogólne dotyczące omawianych przestępstw

a) Podżeganie i pomocnictwo; usiłowanie

Zgodnie z art. 8 ust. 1 dyrektywy państwa członkowskie muszą zapewnić, aby podżeganie do popełnienia przestępstw, o których mowa w art. 3–7, lub pomocnictwo w jego popełnieniu było karalne jako przestępstwo.

Wszystkie państwa członkowskie dokonały transpozycji tego przepisu. Zdecydowana większość państw członkowskich dokonała transpozycji dyrektywy za pośrednictwem istniejącego już artykułu dotyczącego podżegania i pomocnictwa (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Dwa państwa członkowskie zdecydowały się jednak na wprowadzenie nowego przepisu, który ma zastosowanie wyłącznie w kontekście przestępstw określonych w dyrektywie (CY, MT).

Zgodnie z art. 8 ust. 2 zdanie pierwsze dyrektywy państwa członkowskie są zobowiązane do zapewnienia, aby usiłowanie popełnienia przestępstw, o których mowa w art. 3, art. 4 lit. a), b) lub d), art. 5 lit. a) lub b) lub art. 6, było karalne jako przestępstwo. Wydaje się, że wszystkie państwa członkowskie dokonały pełnej transpozycji tego przepisu, z wyjątkiem BE, LU i SI.

Również w tym przypadku większość państw członkowskich dokonała transpozycji dyrektywy za pośrednictwem istniejącego już przepisu mającego ogólne zastosowanie do usiłowania (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Pozostałe państwa uwzględniły to w specjalnym środku transpozycji (CY, DE, FI, MT, RO).

Państwa członkowskie muszą również zapewnić, aby przynajmniej usiłowanie nabycia bezprawnie uzyskanego, podrobionego lub sfałszowanego niematerialnego bezgotówkowego instrumentu płatniczego dla siebie lub innej osoby w celu dokonania oszustwa (art. 5 lit. d)) podlegało karze jako przestępstwo, art. 8 ust. 2 zdanie drugie.

W ocenie wykazano, że kryminalizacja usiłowania może podlegać ograniczeniom nieprzewidzianym w dyrektywie w dwóch państwach członkowskich (HR, SI).

Wszystkie pozostałe państwa członkowskie transponowały odpowiednie przepisy dyrektywy. Uczyniły to za pośrednictwem artykułu dotyczącego ogólnie usiłowania (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK) albo za pośrednictwem specjalnego środka transpozycji (CY, DE, FI, MT, RO).

b) Kary

Art. 9 stanowi, że przestępstwa, o których mowa w art. 3–8, podlegają skutecznym, proporcjonalnym i odstraszającym sankcjom karnym; określono w nim maksymalny wymiar kary pozbawienia wolności za poszczególne przestępstwa.

Chociaż państwa członkowskie zasadniczo dokonały transpozycji art. 9 dyrektywy, w ocenie stwierdzono możliwe problemy związane z zakresem definicji w odniesieniu do art. 9 ust. 2 w HR i art. 9 ust. 6 w BE, CZ, HR i HU.

Porównanie ustanowionych przez państwa członkowskie sankcji za poszczególne przestępstwa jest skomplikowane, ponieważ przestępstwa są objęte zarówno przepisami ogólnymi, jak i szczegółowymi. Dokonując transpozycji dyrektywy za pośrednictwem przepisów dotyczących przestępstw ogólnych, państwa członkowskie oparły się na kilku przepisach krajowych w celu uznania jednego z czynów zabronionych przez dyrektywę za przestępstwo. Prowadzi to do szeregu maksymalnych kar mających zastosowanie do tego konkretnego przestępstwa i oznacza, że rzeczywista maksymalna kara będzie zależeć od poszczególnych konkretnych przypadków, od podejścia stosowanego przez sądy i od przepisów krajowych dotyczących kumulacji sankcji. Przykładowo w PL obowiązuje zasada, że jeden czyn może stanowić tylko jedno przestępstwo. W przypadku gdy czyn ma znamiona, o których mowa w co najmniej dwóch przepisach prawa karnego, sąd musi wybrać jedno konkretne przestępstwo. Przeciwna sytuacja ma miejsce w BG, gdzie w przypadkach, w których część szczegółowa kodeksu karnego przewiduje nałożenie co najmniej dwóch kar jednocześnie za określone przestępstwo, sąd określa wymiar każdej kary w taki sposób, aby suma ta była zgodna z ogólnymi celami kary.

Ponadto przepisy mogą zawierać okoliczności obciążające, które mogą podnieść pułap i prowadzić do zaostrzenia sankcji. Maksymalna kara zależy zatem od sposobu popełnienia przestępstwa. Na przykład w ogólnym przepisie dotyczącym sprzeniewierzenia w HR przewidziano maksymalną karę pięciu lat pozbawienia wolności. Jeśli jednak sprawca użyje siły, maksymalna kara wynosi 10 lat, a jeśli działanie to przyniosło znaczną korzyść majątkową, sprawcy grozi do 12 lat pozbawienia wolności. W DE za fałszowanie bezgotówkowych instrumentów płatniczych grozi do pięciu lat pozbawienia wolności. Jeśli jednak sprawca działał w celu komercyjnym, kara wyniesie maksymalnie 10 lat.

W ocenie wykazano również, że w większości przypadków progi przewidziane w przepisach krajowych są bardziej rygorystyczne niż progi określone w dyrektywie. Różnica może być znacząca: fałszowanie pieniędzy podlega karze do 15 lat w BG i LU oraz do 25 lat w PL. Tylko dwa państwa członkowskie przewidują maksymalne kary takie same jak te określone w dyrektywie lub bardzo do nich zbliżone (AT, MT).

c) Odpowiedzialność osób prawnych

W ocenie wykazano, że 16 państw członkowskich dokonało transpozycji art. 10 dyrektywy za pośrednictwem już istniejącego ogólnego przepisu w swoich kodeksach karnych (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), podczas gdy dziewięć państw członkowskich dokonało transpozycji za pośrednictwem ustawy dotyczącej konkretnie odpowiedzialności osób prawnych w kontekście dyrektywy (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sankcje wobec osób prawnych

W art. 11 dyrektywy ustanowiono wymóg zobowiązujący państwa członkowskie do przewidzenia skutecznych, proporcjonalnych i odstraszających sankcji również dla osób prawnych w postaci grzywien nałożonych na podstawie przepisów prawa karnego lub na podstawie innych przepisów. Wszystkie państwa członkowskie ustanowiły takie sankcje.

W art. 11 przewidziano możliwość włączenia przez państwa członkowskie różnych szczególnych sankcji dla osób prawnych, takich jak wykluczenie z prawa do świadczeń publicznych lub likwidacja sądowa. Sześć państw członkowskich w ogóle nie skorzystało z wariantu określonego w art. 11 dyrektywy (AT, BG, EE, FI, NL, SE). Pozostałe 19 państw dokonało transpozycji całego art. 11 albo jego części (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Jurysdykcja

Artykuł ten, zobowiązujący państwa członkowskie do ustanowienia jurysdykcji w odniesieniu do przestępstw popełnionych na ich terytorium lub przez ich obywatela, został transponowany do przepisów ogólnych krajowego kodeksu karnego lub kodeksu postępowania karnego we wszystkich państwach członkowskich. W związku z tym zasada terytorialności i zasada czynnego obywatelstwa mają zastosowanie ogólne i nie są właściwe dla przestępstw regulowanych niniejszą dyrektywą. Ponadto art. 12 został również transponowany przez CY w krajowej ustawie o zwalczaniu fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz przez PT w ustawie o cyberprzestępczości.

Wszystkie państwa członkowskie dokonały transpozycji art. 12 ust. 1 lit. a) i b).

W art. 12 ust. 3 zezwala się państwom członkowskim na ustanowienie jurysdykcji w odniesieniu do dowolnego z przestępstw, o których mowa w art. 3–8 dyrektywy, popełnionego poza jego terytorium, jeżeli m.in.: a) przestępstwo zostało popełnione przez osobę, której miejsce zwykłego pobytu znajduje się na jego terytorium; b) przestępstwo zostaje popełnione na korzyść osoby prawnej ustanowionej na jego terytorium; lub c) przestępstwo zostało popełnione wobec obywatela tego państwa lub wobec osoby mającej miejsce zwykłego pobytu na jego terytorium. 14 państw członkowskich (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) skorzystało z wariantu określonego w art. 12 ust. 3 lit. a). 12 państw członkowskich (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) dokonało transpozycji art. 12 ust. 3 lit. b); a 16 państw członkowskich (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) rozszerzyło swoją jurysdykcję zgodnie z art. 12 ust. 3 lit. c). Jeśli chodzi o art. 12 ust. 3 lit. c), w BG, DE, EE, HU, RO i SI ustanowiono jurysdykcję w odniesieniu do przestępstwa popełnionego poza ich terytorium, jeżeli zostało ono popełnione (tylko) przeciwko jednemu z ich obywateli – pomijając w ten sposób osoby mające tam miejsce zwykłego pobytu. AT przewiduje ściganie przez austriacki system sądownictwa karnego przestępstw popełnionych za granicą, jeśli sprawca i ofiara są Austriakami. CY, CZ, EL, FI, LV i MT skorzystały ze wszystkich trzech przepisów fakultatywnych określonych w art. 12 ust. 3.

2.4 Kwestie operacyjne

a) Skuteczne prowadzenie postępowań przygotowawczych i współpraca

We wszystkich państwach członkowskich narzędzia dochodzeniowo-śledcze służące do prowadzenia postępowań przygotowawczych i ścigania przestępstw, o których mowa w art. 3–8, nie są wyraźnie zawarte w przepisach transponujących dyrektywę, ale raczej w przepisach o bardziej ogólnym charakterze, takich jak kodeksy postępowania karnego. Zazwyczaj możliwość wykorzystania narzędzia dochodzeniowo-śledczego w danej sprawie jest związana z sankcją za dane przestępstwo; w związku z tym, jak już wskazano w przepisie dyrektywy, narzędzia dochodzeniowo-śledcze stosowane w zwalczaniu przestępczości zorganizowanej lub w innych sprawach dotyczących poważnej przestępczości będą również dostępne do prowadzenia postępowań przygotowawczych i ścigania przestępstw określonych w przedmiotowej dyrektywie. O wyjątkowości niektórych narzędzi dochodzeniowo-śledczych i potrzebie proporcjonalności do przestępstwa najczęściej jest mowa w odpowiednich przepisach prawnych lub w Konstytucji.

Zgodnie z art. 13 ust. 2 dyrektywy informacje dotyczące przestępstw, o których mowa w art. 3–8, powinny docierać bez zbędnej zwłoki do organów prowadzących postępowania przygotowawcze w sprawie tych przestępstw lub je ścigających. Innymi słowy, organy ścigania i inne właściwe organy powinny mieć odpowiednio wcześnie dostęp do odpowiednich informacji, aby móc prowadzić postępowania przygotowawcze w sprawie przestępstw określonych w przedmiotowej dyrektywie (motyw 22). Kodeks postępowania karnego często przewiduje różne systemy zgłaszania, aby przestępstwa (w rozumieniu art. 3–8 dyrektywy) mogły być zgłaszane skutecznie i szybko. Te systemy zgłaszania obejmują: obowiązek organów i władz publicznych w zakresie zgłaszania; system sygnalizowania nieprawidłowości; procedurę dotyczącą skarg; obowiązek zgłaszania przez dostawców usług płatniczych poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem; oraz prawo osób prywatnych do zgłaszania incydentów. Ponadto niektóre bardziej szczegółowe przepisy mogą zapewnić, aby zgłoszenia incydentów związanych z bezpieczeństwem (w tym zgłoszenia poważnych przestępstw, takich jak nieuprawnione nabycie, fałszerstwo i modyfikacja środków płatniczych) były zgłaszane odpowiednim organom tak szybko, jak to możliwe. Takie przepisy zgłosiły następujące państwa: AT, CZ, LT, FI, MT i PT.

Warunek, zgodnie z którym przekazane informacje powinny „dotrzeć do odpowiednich organów bez zbędnej zwłoki", najczęściej nie jest transponowany w sposób wyraźny.

b) Wymiana informacji

Wymianę informacji między krajowymi organami ścigania do celów prowadzenia postępowań przygotowawczych i ścigania przestępstw, w tym tych, o których mowa w art. 3–8 dyrektywy, można ułatwić dzięki operacyjnym punktom kontaktowym (motyw 26). W art. 14 ust. 1 zdanie pierwsze dyrektywy zagwarantowano, aby państwa członkowskie rzeczywiście ustanowiły te punkty kontaktowe i aby były one dostępne całodobowo. Ponadto w zdaniu drugim zobowiązano państwa członkowskie do wprowadzenia procedur umożliwiających szybkie rozpatrywanie pilnych wniosków o pomoc i przekazywanie w ciągu ośmiu godzin od otrzymania wniosku informacji co najmniej o tym, czy na wniosek zostanie udzielona odpowiedź oraz jaka będzie jej forma i przewidywany termin jej udzielenia.

Następujące państwa członkowskie postanowiły wykorzystać istniejący operacyjny punkt kontaktowy do celów opisanych w przedmiotowej dyrektywie: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Tabela 1 zawiera przegląd ustanowionych punktów kontaktowych. Nie wskazano żadnych punktów kontaktowych w BG, CZ, LU, SI, HR.

Tabela 1 Operacyjne punkty kontaktowe

Państwo członkowskie	Punkt kontaktowy	Państwo członkowskie	Punkt kontaktowy
AT	Federalna Policja Kryminalna	**EE**	Ministerstwo Sprawiedliwości
BE	Dyrekcja ds. Operacyjnych Informacji Policyjnych	**FI**	Krajowe Biuro Śledcze
BG	Nie dotyczy	**FR**	Wydział ds. Stosunków Międzynarodowych Centralnej Dyrekcji Policji Sądowej
CY	Policja cypryjska	**HR**	Nie dotyczy
CZ	Nie dotyczy	**HU**	Międzynarodowe Centrum Współpracy Kryminalnej (NEBEK)
DE	16 Biur Policji Kryminalnej Krajów Związkowych i jedno Federalne Biuro Policji Kryminalnej – Centralne Punkty Kontaktowe ds. Cyberprzestępczości	**MT**	Policja maltańska
EL	Policja grecka (Wydział Międzynarodowej Współpracy Policyjnej)	**ES**	Komórka ds. Koordynacji Kryzysowej
IT	Międzynarodowe Centrum Dowodzenia Służby Międzynarodowej Współpracy Policyjnej	**NL**	Krajowe Centrum Międzynarodowej Pomocy Prawnej (LIRC)
LT	2. Wydział Zarządu Sił Departamentu Policji podlegający Ministerstwu Spraw Wewnętrznych Republiki Litewskiej oraz Rada ds. Stosunków Międzynarodowych Litewskiego Biura Policji Kryminalnej	**PL**	Komenda Główna Policji
LV	Policja krajowa	**PT**	Policja kryminalna
RO	Sekcja Ścigania i Postępowań Przygotowawczych Prokuratury Generalnej	**SE**	Organ policji
SI	Nie dotyczy	**SK**	Biuro Policji Kryminalnej Prezydium Sił Policyjnych Republiki Słowackiej

Art. 14 ust. 1 zdanie drugie dyrektywy praktycznie wdrożono w kilku państwach członkowskich. Nie można było znaleźć informacji na temat procedur mających zastosowanie do pilnych wniosków w BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Zgłaszanie przestępstw

Państwa członkowskie są również zobowiązane do zapewnienia dostępności odpowiednich kanałów zgłoszeniowych. Takie kanały zgłaszania podejrzeń o popełnieniu oszustwa lub, bardziej ogólnie, zgłaszania wszelkich możliwych przestępstw, można określić w aktach ustawodawczych. W wielu przypadkach państwa członkowskie ustanowiły obowiązek zgłaszania przestępstw w odniesieniu do niektórych kategorii osób (fizycznych i prawnych) (zgodnie z art. 15 ust. 2), podczas gdy ofiary i inne osoby postronne mają możliwość (ale nie obowiązek) zgłaszania przestępstw. Te przepisy prawne są zwykle uzupełniane o praktyczne wdrożenia.

We wszystkich państwach członkowskich zgłoszenia w formie pisemnej lub ustnej można kierować do policji lub wymiaru sprawiedliwości. Ponadto niektóre państwa członkowskie zapewniły dodatkowe kanały zgłoszeniowe:

w prawie federalnym AT przewidziano różne systemy zgłaszania, aby przestępstwa w rozumieniu art. 3–8 dyrektywy mogły być zgłaszane skutecznie i szybko: 1) obowiązek organów i władz publicznych w zakresie zgłaszania; 2) system sygnalizowania nieprawidłowości Biura Prokuratora do Spraw Gospodarczych i Korupcji; 3) system sygnalizowania nieprawidłowości Urzędu ds. Rynku Finansowego; oraz 4) obowiązek zgłaszania przez dostawców usług płatniczych poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem. W Federalnym Biurze Policji Kryminalnej utworzono specjalne biuro ds. zgłaszania cyberprzestępstw. Ponadto Federalne Ministerstwo Spraw Wewnętrznych współpracuje z Federalną Izbą Gospodarczą. W rezultacie prowadzone są różne akcje mailingowe i kampanie, w ramach których motywuje się i zachęca społeczeństwo do zgłaszania istotnych naruszeń prawa.

W BE Ministerstwo Gospodarki zarządza pojedynczym punktem kontaktowym dla ofiar nadużyć finansowych, scamu, podstępu i oszustw. Ponadto Urząd ds. Usług i Rynków Finansowych prawnie ustanowił oraz udostępnił kanał sygnalizowania nieprawidłowości dla wszystkich skarg związanych z produktami i usługami kredytowymi lub inwestycyjnymi.

Na CY policja cypryjska, wraz z Centralnym Bankiem Cypru i krajowym organem ds. bezpieczeństwa sieci i systemów informatycznych, zostały formalnie wyznaczone za pośrednictwem środka legislacyjnego jako właściwe organy krajowe odpowiedzialne za ustanowienie odpowiednich kanałów zgłaszania i komunikacji.

Prawo karne CZ zobowiązuje organy państwowe do zgłaszania.

W DE podmioty zobowiązane mają obowiązek bez zbędnej zwłoki zgłaszać podejrzane transakcje. Ponadto na szczeblu federalnym przyjęto środki o charakterze nielegislacyjnym takie jak zinstytucjonalizowane partnerstwo publiczno-prywatne w celu wykrywania lub ścigania przestępstw, o których mowa w art. 3–8 dyrektywy, zapobiegania im, prowadzenia dochodzeń w ich sprawie oraz platforma wymiany informacji.

W EL, oprócz ogólnych kanałów zgłaszania, grecki rząd utworzył państwową usługę online, w ramach której obywatele mogą bezpośrednio składać skargi dotyczące przestępstw popełnionych w internecie. Ponadto instytucje kredytowe i inni dostawcy usług płatniczych muszą zgłaszać Bankowi Grecji (który ma kompetencje w zakresie takich skarg) wszelkie przypadki oszustw natychmiast po ich napotkaniu.

W Hiszpanii, oprócz ogólnych kanałów zgłaszania przestępstw, Bank Hiszpanii zapewnia kanał zgłaszania we współpracy z Krajowym Instytutem Cyberbezpieczeństwa.

Włoskie przepisy zapewniają terminowe przekazywanie prokuratorowi przez policję sądową informacji o przestępstwie uzyskanych z własnej inicjatywy lub w wyniku skargi lub pozwu. Zachęca się również do wymiany informacji za pośrednictwem platform cyfrowych.

LT dysponuje wieloma kanałami zgłaszania przestępstw, o których mowa w art. 3–8 dyrektywy – za pośrednictwem strony internetowej (portal e-policja), ogólnego numeru alarmowego 112, osobiście, pocztą elektroniczną, SMS-em i za pośrednictwem aplikacji mobilnej e-policji oraz innych środków automatycznych. Dostawcy usług płatniczych, instytucje finansowe i inne podmioty zobowiązane, Bank Litwy i Służba Śledcza ds. Przestępczości Finansowej są zobowiązane do powiadamiania właściwych organów ścigania o uzasadnionych podejrzeniach dotyczących przestępstw lub innych działań niezgodnych z prawem.

W LU dostępna jest strona internetowa, na której można znaleźć instrukcje, jak zgłaszać oszustwa. Komisja Kontroli Sektora Finansowego określiła wytyczne dotyczące wykrywania oszustw finansowych, ale także wymaga, aby wszystkie instytucje podlegające jej nadzorowi jak najszybciej zgłaszały wszelkie oszustwa i wszelkie incydenty spowodowane zewnętrznymi atakami komputerowymi.

W RO istnieje obowiązek zgłaszania przez urzędników państwowych i osoby zajmujące stanowiska kierownicze w organach publicznych, osoby świadczące usługi w interesie publicznym oraz osoby działające w organach kontroli i nadzoru.

W SI istnieje obowiązek zgłaszania przestępstw przez wszystkie organy państwowe i organizacje posiadające uprawnienia organów publicznych.

Platforma Perceval we Francji, ustanowiona aktem prawnym, umożliwia ofiarom zgłaszanie oszustw związanych z kartami bankowymi i przypadków ich fałszowania. Istnieje podobna platforma do zgłaszania cyberprzestępczości. Ponadto sankcje mają zastosowanie do każdej osoby (fizycznej lub prawnej), która nie zapobiega przestępstwu poprzez swoje natychmiastowe działanie, co prowadzi do ogólnego obowiązku zgłaszania.

W HU obowiązek złożenia zawiadomienia o popełnieniu przestępstwa dotyczy wyłącznie członków władz, funkcjonariuszy publicznych i ustawowych samorządów zawodowych. Węgierski Bank Narodowy zachęca na swojej stronie internetowej instytucje finansowe – w formie opinii – do zgłaszania podejrzeń o popełnieniu oszustwa.

W MT krajowy punkt kontaktowy zachęca do zgłaszania, w szczególności przez instytucje finansowe, podejrzeń fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi.

Oprócz prawnie ustanowionego kanału sygnalizowania nieprawidłowości w PT dostępny jest system zgłaszania cyberprzestępstw „za jednym kliknięciem”, w którym można kliknąć link, który natychmiast otwiera wiadomość e-mail skierowaną do właściwych organów.

W SE niektóre rodzaje przestępstw, takie jak oszustwa związane z kartami kredytowymi, można również zgłaszać za pośrednictwem e-usługi Organu Policji. Ponadto podmioty prowadzące działalność bankową i finansową są zobowiązane do zgłaszania Organowi Policji podejrzanych działań związanych z potencjalnymi przypadkami prania pieniędzy lub finansowania terroryzmu, lub mienia, które w inny sposób pochodzi z przestępstwa. Ponadto prowadzony jest stały dialog między operacjami bankowymi i finansowymi a Krajowym Centrum ds. Oszustw w ramach Organu Policji.

W przepisach prawnych w SK określono wymóg (i procedury) organów publicznych i innych osób prawnych w zakresie niezwłocznego zgłaszania przestępstw organom ścigania. Istnieją również obowiązki w zakresie zgłaszania spoczywające na osobach zobowiązanych, w szczególności bankach, związane z praniem pieniędzy.

Jako rozwiązanie alternatywne w NL i PL przeprowadzono działania o charakterze nieustawodawczym wdrażające art. 15 dyrektywy. Infolinie policyjne i strona internetowa policji niderlandzkiej stanowią odpowiedni kanał do zgłaszania władzom oszustw związanych z bezgotówkowymi środkami płatniczymi. Ponadto rząd niderlandzki zobowiązał się do zachęcania instytucji finansowych i innych osób prawnych do zgłaszania wszelkich podejrzeń popełnienia oszustwa. Wysiłki te są widoczne na przykładzie istnienia biura ds. oszustw finansowych, które jest powoływane w ramach wszystkich jednostek policji w Niderlandach. Ponadto cztery główne banki i wystawca kart ICS Cards podpisali porozumienie z policją w celu wspólnego zwalczania oszustw (bankowych) i phishingu. W PL zgłoszenia przestępstw przyjmowane są całodobowo przez wszystkie jednostki policji. Dodatkowo, z uwagi na charakter przestępstw popełnianych z wykorzystaniem technologii komputerowych, istnieje możliwość bezpośredniego kontaktu z wyspecjalizowaną komórką organizacyjną Komendy Głównej Policji. Ponadto w celu zapewnienia jak najszybszej współpracy z sektorem bankowym utworzono kanał współpracy pomiędzy Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji a Bankowym Centrum Bezpieczeństwa Związku Banków Polskich.

Art. 15 ust. 2 dyrektywy nie transponowano w BG, EE, HR.

2.5 Wsparcie dla ofiar i zapobieganie

a) Pomoc i wsparcie dla pokrzywdzonych

Pomoc i wsparcie dla osób fizycznych i prawnych, których dane osobowe zostały niewłaściwie wykorzystane, zapewnia art. 16 ust. 1 dyrektywy. Środki powinny obejmować: a) oferowanie szczegółowych informacji i porad dotyczących sposobów ochrony przed niekorzystnymi skutkami takich przestępstw oraz b) udostępnianie wykazu właściwych instytucji zajmujących się różnymi aspektami przestępstw związanych z kradzieżą tożsamości i wsparciem dla ofiar.

W tym samym duchu osoby prawne będące ofiarami przestępstw, o których mowa w art. 3–8 niniejszej dyrektywy, powinny mieć dostęp do informacji o a) procedurach składania skargi, b) prawie do uzyskania informacji o danej sprawie, c) dostępnych procedurach składania skarg, jeżeli właściwy organ nie przestrzega uprawnień ofiary w toku postępowania karnego, oraz d) danych kontaktowych na potrzeby przekazywania informacji o sprawie, która ich dotyczy (art. 16 ust. 3 dyrektywy).

Kodeks postępowania karnego większości państw członkowskich zawiera przepisy dotyczące ofiar i ich praw, w tym niektóre przepisy szczegółowe dotyczące praw ofiar do informacji i pomocy w trakcie postępowania, prawa do doradztwa i prawa do złożenia skargi. Konkretna ustawa transponująca dyrektywę często uzupełnia to, co zostało już określone w kodeksie postępowania karnego. Osób prawnych zazwyczaj dotyczą odrębne przepisy prawne w ramach kodeksu postępowania karnego lub w innych aktach prawnych. Ponadto dostępne są różne kampanie informacyjne, ulotki, specjalne strony internetowe, okólniki itp. mające na celu pomoc i wsparcie dla ofiar przestępstw, o których mowa w art. 3–8 dyrektywy. Tak jest w przypadku AT, BE (w odniesieniu do art. 16 ust. 1), CY, CZ, DE, IT, LT, LU (w odniesieniu do art. 16 ust. 1), LV (w odniesieniu do art. 16 ust. 3), RO, SI (w odniesieniu do art. 16 ust. 3), EE, FI (w odniesieniu do art. 16 ust. 1), FR (w odniesieniu do art. 16 ust. 1), HR, HU, NL, PL (w odniesieniu do art. 16 ust. 3), PT, SE i SK. Art. 16 ust. 1 lub art. 16 ust. 3 dyrektywy nie zostały nigdzie dosłownie lub prawie dosłownie transponowane, z wyjątkiem MT.

Wykaz akredytowanych ośrodków doradczych świadczących pomoc ofiarom, o której mowa w art. 16 ust. 1 lit. b) dyrektywy, jest zwykle dostępny online, a zatem jest wdrażany w praktyce.

b) Zapobieganie

Art. 17 dotyczący zapobiegania wymaga od państw członkowskich podjęcia odpowiednich działań, np. kampanii informacyjnych i uświadamiających, programów badawczych i edukacyjnych. Niniejsza sekcja opiera się na ocenie informacji zgłoszonych Komisji przez państwa członkowskie, a także na badaniach internetowych przeprowadzonych w celu zbadania istnienia środków zapobiegawczych. Jak opisano w tabeli 2 poniżej, w przypadkach w których zidentyfikowano działania zapobiegawcze, odnoszą się one głównie do cyberprzestępczości i oszustw internetowych. Jednak w niektórych państwach również zapewnia się informacje na temat zapobiegania oszustwom, zazwyczaj za pośrednictwem policji.

Tabela 2 Działania zapobiegawcze

Państwo członkowskie	Działania
AT	Policja Federalna regularnie udostępnia na swojej stronie internetowej i w sieciach społecznościowych informacje na temat sposobów ochrony przed oszustwami. Współpraca z zainteresowanymi stronami, takimi jak Izba Handlowa, jest wspierana i realizowana w ramach projektów w zakresie handlu elektronicznego.
BE	Różne strony internetowe z poradami/materiałami służącymi podnoszeniu świadomości, takie jak te prowadzone przez Belgijskie Centrum Cyberbezpieczeństwa (CCB). Możliwe było zidentyfikowanie pewnej współpracy z zainteresowanymi stronami poprzez wyszukiwanie w internecie, np. organizacja reprezentująca sektor finansowy współpracowała z brukselską prokuraturą (*parquet*) w celu opracowania materiałów służących podnoszeniu świadomości.
BG	W 2021 r. w Bułgarii rozpoczęła się kampania mająca na celu walkę z tzw. „słupami", prowadzona przez Stowarzyszenie Banków wspólnie z Generalną Dyrekcją ds. Zwalczania Przestępczości Zorganizowanej i prokuraturą. Generalna Dyrekcja rozpoczęła również kampanię dotyczącą phishingu.
CY	Poddział Policji ds. Cyberprzestępczości udostępnia na swojej stronie internetowej informacje i porady dotyczące kwestii takich jak oszustwa cyfrowe, a także informacje o nadchodzących wydarzeniach, np. kampaniach służących podnoszeniu świadomości. Jednym z przykładów jest kampania informacyjna na temat bezpieczeństwa informacji prowadzona przez policję, banki centralne, Związek Banków i Urząd Bezpieczeństwa Cyfrowego.
DE	Policja Federalna (BKA) udostępnia na swojej stronie internetowej przegląd środków ukierunkowanych na zinstytucjonalizowane partnerstwo publiczno-prywatne w celu wykrywania lub ścigania przestępstw objętych dyrektywą, zapobiegania im lub prowadzenia

	dochodzeń w ich sprawie, np. partnerstwo między Federalnym Urzędem Policji Kryminalnej (BKA), Federalnym Urzędem ds. Bezpieczeństwa Informacji (BSI) i „Niemieckim Centrum Kompetencji przeciwko Cyberprzestępczości e.V." (G4C), stowarzyszeniem instytucji finansowych i przedsiębiorstw z sektora bezpieczeństwa informatycznego. BKA zainicjowało również konferencję poświęconą cyberprzestępczości C³ oraz uruchomiło platformę wymiany między przedstawicielami władzy, biznesu, nauki i polityki. G4C przygotowuje również broszury informacyjne i szkolenia. Ponadto BKA uczestniczy również w działaniach zapobiegawczych w obszarze cyberprzestępczości na szczeblu krajów związkowych, a na szczeblu krajowym BKA współpracuje również z innymi organami i organizacjami policyjnymi i niepolicyjnymi (zainteresowanymi stronami) oraz zacieśnia współpracę, zwłaszcza w zakresie trendów.
FR	Ministerstwo Spraw Wewnętrznych publikuje informacje na temat zapobiegania cyberprzestępczości. Platformy dostępne do zgłaszania cyberprzestępstw obejmują również komunikaty prewencyjne, a także Krajową Policyjną Służbę Informacyjno-Komunikacyjną (SICoP). Inne przykłady obejmują wytyczne wydane przez Bank Francji lub przewodnik dotyczący zapobiegania oszustwom opublikowany przez Krajową Grupę Zadaniową ds. walki z oszustwami, która skupia różne organy administracji i egzekwowania prawa.
EL	Biuro ds. Walki z Cyberprzestępczością i Komenda Główna Policji są bardzo aktywne w informowaniu społeczeństwa, podnoszeniu świadomości i zmniejszaniu ryzyka stania się ofiarą oszustwa, za pośrednictwem kampanii telewizyjnych, pogadanek i informacji dostępnych w internecie.
ES	Hiszpański Narodowy Instytut Cyberbezpieczeństwa i Urząd Skarbowy udostępniają na swoich stronach internetowych istotne informacje dotyczące zapobiegania phishingowi, oprogramowaniu szantażującemu itp. w środowiskach biznesowych.
HR	Ministerstwo Spraw Wewnętrznych zapewnia informacje online na temat oszustw internetowych i prowadzi kanał Youtube poświęcony „Oszustwom i bezpieczeństwu komputerowemu", zawierający filmy o scamie.
IT	Departament Skarbu, którego zadaniem jest zapobieganie oszustwom związanym ze środkami płatniczymi, już teraz promuje szereg inicjatyw na szczeblu lokalnym, we współpracy z lokalnymi organami administracji i systemem uniwersyteckim, organizując seminaria i warsztaty skierowane do kategorii osób zaangażowanych w fałszowanie walut, w tym obywateli.
LT	Informacje na temat zapobiegania można znaleźć na stronie internetowej Urzędu Regulacji Łączności w odniesieniu do oszustw internetowych oraz na stronie internetowej Policji dotyczącej najczęstszych rodzajów cyberoszustw. Ponadto jednym z celów Krajowej Strategii w zakresie Cyberprzestępczości jest wzmocnienie zapobiegania cyberprzestępczości i jej kontroli, w szczególności przez rozwijanie skutecznej współpracy między organami ścigania i innymi zainteresowanymi stronami.
LV	Komisja Rynku Finansowego i Kapitałowego opracowała różne narzędzia internetowe w celu dostarczania informacji i wytycznych na temat bezpieczeństwa finansowego i kwestii związanych z oszustwami. Ponadto zorganizowano różne kampanie we współpracy z Policją Państwową i Centrum Ochrony Praw Konsumentów.
NL	Istnieją środki, takie jak „Fraudehelpdesk" (infolinia na temat oszustw), która jest organizacją dotowaną przez rząd niderlandzki. Fraudehelpdesk jest częścią fundacji SAFECIN (Fundacja na Rzecz Zwalczania Przestępczości Finansowej i Gospodarczej w Niderlandach (SAFECIN)), w którą zaangażowany jest rząd i która umożliwia zgłaszanie działań podejmowanych w celu dokonania oszustwa.
SE	Prowadzony jest stały dialog między operacjami bankowymi i finansowymi a Krajowym Centrum ds. Oszustw w ramach Organu Policji, NBC. Ponadto NBC współpracuje, również w celu zapobiegania przestępczości, np. z podmiotami działającymi w obszarze handlu elektronicznego. W kontaktach tych podkreśla się znaczenie zgłaszania policji oszustw.

W przypadku 10 państw członkowskich (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK) nie znaleziono informacji na temat odpowiednich działań zapobiegawczych i ich praktycznego wdrożenia, chociaż w MT i RO przepisy odzwierciedlają ten obowiązek, ściśle przestrzegając brzmienia dyrektywy.

3. Wnioski i kolejne działania

Dyrektywa przyczyniła się do osiągnięcia istotnych postępów w procesie zapewniania zbliżonego poziomu kryminalizacji fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi we wszystkich państwach członkowskich, co sprzyja współpracy transgranicznej między organami ścigania prowadzącymi dochodzenia w sprawie tego rodzaju przestępstw. Państwa członkowskie wprowadziły zmiany w swoich kodeksach karnych i w innych stosownych przepisach, uprościły stosowane przez siebie procedury i ustanowiły lub udoskonaliły swoje mechanizmy współpracy. Komisja docenia znaczne wysiłki podjęte przez państwa członkowskie na rzecz transpozycji dyrektywy.

Potencjał dyrektywy nie został jeszcze jednak w pełni wykorzystany – zakres jej oddziaływania mógłby zostać zwiększony, gdyby państwa członkowskie w pełni wdrożyły wszystkie jej przepisy. Wyniki przeprowadzonych do tej pory analiz wskazują, że usprawnienia, których państwa członkowskie mogłyby dokonać, obejmują art. 2 lit. d), który zawiera definicję waluty wirtualnej; art. 7 dotyczący przestępstw związanych z narzędziami wykorzystywanymi do popełnienia przestępstw oraz art. 8 ust. 2 dotyczący usiłowania; art. 9 ust. 6 dotyczący kar w przypadku osób fizycznych, gdy przestępstwo zostało popełnione w ramach organizacji przestępczej; art. 14 dotyczący wymiany informacji i art. 16 dotyczący pomocy i wsparcia dla ofiar.

Komisja będzie nadal wspierała państwa członkowskie w ich wysiłkach na rzecz wdrożenia dyrektywy. W szczególności w 2023 r. zostanie opublikowane szczegółowe zaproszenie do składania wniosków.

Komisja zobowiązuje się do zapewnienia pomyślnego zakończenia transpozycji dyrektywy w całej UE oraz prawidłowego wdrożenia jej przepisów. W tym celu Komisja zamierza m.in. monitorować zgodność środków krajowych z odpowiednimi przepisami dyrektywy. W stosownych przypadkach Komisja zamierza korzystać z uprawnień w zakresie egzekwowania prawa przysługujących jej na mocy Traktatów, wszczynając postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.