KOMISJA
EUROPEJSKA

Bruksela, dnia 13.9.2017 r.
COM(2017) 489 final

2017/0226 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz zastępująca decyzję ramową Rady 2001/413/WSiSW

{SWD(2017) 298 final}
{SWD(2017) 299 final}

SPIS TREŚCI

UZASADNIENIE

1. KONTEKST WNIOSKU

1.1. Przyczyny i cele wniosku

Obecnie obowiązujące przepisy unijne, które określają wspólne normy minimalne w celu uznania za przestępstwo oszustw związanych z płatnościami bezgotówkowymi, są zawarte w decyzji ramowej Rady 2001/413/WSiSW w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi[1].

W Europejskiej agendzie bezpieczeństwa[2] potwierdzono, że decyzja ramowa nie odpowiada już obecnym realiom i w niewystarczającym stopniu uwzględnia nowe wyzwania i zmiany technologiczne, takie jak waluty wirtualne czy płatności mobilne.

W 2013 r. skala oszustw przy użyciu kart wydanych w obrębie jednolitego obszaru płatności w euro (SEPA) wyniosła 1,44 mld EUR, co stanowi wzrost o 8 proc. w stosunku do poprzedniego roku. Dostępne są wprawdzie tylko dane dotyczące oszustw związanych z płatnościami kartowymi, ale karty stanowią najważniejszy w UE bezgotówkowy instrument płatniczy pod względem liczby transakcji[3].

Skuteczne przeciwdziałanie oszustwom związanym z płatnościami bezgotówkowymi ma duże znaczenie, gdyż przestępstwa te zagrażają bezpieczeństwu publicznemu. Oszustwa związane z płatnościami bezgotówkowymi stanowią źródło dochodów dla przestępczości zorganizowanej i umożliwiają finansowanie innych rodzajów działalności przestępczej, takich jak terroryzm, obrót środkami odurzającymi i handel ludźmi. Według Europolu dochody z oszustw związanych z płatnościami bezgotówkowymi są wykorzystywane do finansowania w szczególności:

- podróży:
  - lotów: doświadczenia zebrane podczas cyklicznych operacji Global Airline Action Day[4] w latach 2014–2016 wskazują, że istnieje wyraźny związek między oszustwami związanymi z płatnościami bezgotówkowymi a oszustwami związanymi z biletami lotniczymi oraz inną poważną i zorganizowaną przestępczością, w tym terroryzmem. O niektórych osobach podróżujących na podstawie oszukańczo uzyskanych biletów lotniczych wiadomo, że są sprawcami innych przestępstw lub podejrzanymi;
  - inne oszustwa związane z podróżami (tj. sprzedaż oszukańczo uzyskanego biletu i podróżowanie na podstawie takiego biletu). Głównym sposobem zakupu oszukańczych biletów było użycie karty kredytowej, której zabezpieczenia zostały naruszone. Inne metody obejmowały nieuprawnione wykorzystanie kont, na których są gromadzone punkty lojalnościowe, wyłudzanie informacji przez fałszywe biura podróży i oszustwa związane z voucherami. Z oszukańczo uzyskanych biletów korzystali przestępcy, ale na

[1] Dziennik Urzędowy L 149 z 2.6.2001 s.1.
[2] Komunikat Komisji *Strategia jednolitego rynku cyfrowego dla Europy*, COM(2015) 192 final.
[3] Europejski Bank Centralny „*Czwarte sprawozdanie w sprawie oszustw związanych z kartami płatniczymi*", lipiec 2015 r. (najnowsze dostępne dane).
[4] Więcej informacji można znaleźć tutaj.

ich podstawie były przemieszczane także ofiary handlu ludźmi i osoby pełniące rolę tzw. słupa[5].

- zakwaterowania: z doniesień organów ścigania wynika też, że oszustwa związane z płatnościami bezgotówkowymi pomagają w popełnianiu innych przestępstw, które wymagają czasowego zakwaterowania, takich jak handel ludźmi, nielegalna imigracja i nielegalny obrót środkami odurzającymi.

Europol donosi również, że działający w UE rynek przestępczy oszustw związanych z kartami płatniczymi jest zdominowany przez zorganizowane grupy przestępcze posiadające rozwinięte struktury i prowadzące działalność w skali światowej[6].

Oszustwa związane z płatnościami bezgotówkowymi utrudniają ponadto rozwój jednolitego rynku cyfrowego; dzieje się to na dwa sposoby:

- powodują on znaczne bezpośrednie straty gospodarcze, o czym świadczy szacowana na 1,44 mld EUR skala oszustw związanych z kartami, o czym wspomniano wcześniej. Na przykład linie lotnicze tracą wskutek oszustw kartowych około 1 mld USD rocznie na całym świecie[7];
- oszustwa tego typu osłabiają zaufanie konsumentów, co może prowadzić do zmniejszenia dynamiki działalności gospodarczej i ograniczonego zaangażowania w budowę jednolitego rynku cyfrowego. Zgodnie z najnowszym badaniem Eurobarometr dotyczącym bezpieczeństwa cybernetycznego[8], zdecydowana większość użytkowników internetu (85 proc.) uważa, że ryzyko stania się ofiarą cyberprzestępczości wzrasta. Ponadto 42 proc. użytkowników ma obawy związane z bezpieczeństwem płatności online. Kwestie bezpieczeństwa zniechęcają 12 proc. użytkowników do korzystania z transakcji cyfrowych takich jak bankowość internetowa.

Podczas oceny obecnych ram prawnych UE[9] stwierdzono występowanie trzech czynników stanowiących źródło obecnych problemów dotyczących oszustw związanych z płatnościami bezgotówkowymi w UE:

1. W przypadku niektórych przestępstw **skuteczne prowadzenie dochodzeń i ściganie** jest niemożliwe ze względu na obowiązujące ramy prawne.
2. W przypadku innych przestępstw **skuteczne prowadzenie dochodzeń i ściganie** jest niemożliwe ze względu na **przeszkody operacyjne**.
3. Przestępcy popełniają oszustwa, wykorzystując luki w zakresie **zapobiegania** tego typu przestępczości.

---

5 Pojęcie „osoba działająca jako słup" oznacza osobę, która dokonuje przekazów środków pieniężnych stanowiących dochody z przestępstwa między różnymi krajami. Środki pieniężne wpływają najpierw na rachunek bankowy słupa; następnie słup otrzymuje instrukcję wycofania środków i przesłania ich na inny rachunek, często za granicą, po potrąceniu pewnej kwoty dla siebie.

6 Europol, *Sprawozdanie dotyczące sytuacji: Oszustwa związane z kartami płatniczymi w Unii Europejskiej*, 2012 r.

7 IATA, 2015 r.

8 Komisja Europejska, *specjalne badanie Eurobarometr 423* dotyczące cyberbezpieczeństwa, luty 2015 r.

9 Dokument roboczy służb Komisji – ocena skutków towarzysząca wnioskowi w sprawie dyrektywy w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, SWD(2017)298.

Niniejszy wniosek ma trzy szczegółowe cele, których osiągnięcie pozwoli rozwiązać zidentyfikowane problemy:

1. Zapewnienie jasnych, solidnych i **neutralnych pod względem technologicznym** zasad polityki i ram prawnych.
2. Wyeliminowanie **przeszkód operacyjnych**, które utrudniają prowadzenie dochodzeń i ściganie.
3. Lepsze zapobieganie.

1.2. Potrzeba wdrożenia odpowiednich międzynarodowych standardów i zobowiązań oraz skutecznego przeciwdziałania fałszowaniu i oszustwom związanym z bezgotówkowymi środkami płatniczymi

Tytuł 2 Konwencji Rady Europy o cyberprzestępczości (konwencji budapesztańskiej)[10] dotyczący przestępstw komputerowych zobowiązuje strony konwencji do uznania za przestępstwa w ich prawie wewnętrznym fałszerstwa komputerowego (art. 7) i oszustwa komputerowego (art. 8). Obecnie obowiązująca decyzja ramowa jest zgodna z tymi postanowieniami. Zmiana obecnych przepisów poprawi jeszcze bardziej współpracę między organami policyjnymi i sądowymi oraz między organami ścigania a podmiotami sektora prywatnego, dzięki czemu przyczyni się do osiągnięcia ogólnych celów konwencji; zmienione przepisy będą w dalszym ciągu zgodne z odpowiednimi przepisami konwencji.

1.3. Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Cele niniejszego wniosku są spójne z następującymi zasadami polityki i z przepisami obowiązującymi w dziedzinie prawa karnego:

1. paneuropejskie **mechanizmy współpracy w sprawach karnych**, które ułatwiają koordynację prowadzenie dochodzeń i ściganie (prawo karne procesowe):
    - decyzja ramowa Rady 2002/584/WSiSW w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi[11];
    - konwencja o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej[12];
    - dyrektywa 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych[13];
    - decyzja ramowa Rady 2005/214/WSiSW w sprawie stosowania zasady wzajemnego uznawania do kar o charakterze pieniężnym[14];

---

10 Konwencja Rady Europy o cyberprzestępczości (ETS nr 185).

11 Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi.

12 Akt Rady z dnia 29 maja 2000 r. ustanawiający, zgodnie z art. 34 Traktatu o Unii Europejskiej, Konwencję o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej.

13 Dyrektywa 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych

14 Decyzja ramowa Rady 2005/214/WSiSW z dnia 24 lutego 2005 r. w sprawie stosowania zasady wzajemnego uznawania do kar o charakterze pieniężnym.

- decyzja ramowa Rady 2009/948/WSiSW w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów[15];
- decyzja ramowa Rady 2009/315/WSiSW w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji[16];
- dyrektywa 2012/29/UE ustanawiająca normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw[17];
- rozporządzenie (UE) 2016/794 w sprawie Europolu[18];
- decyzja Rady 2002/187/WSiSW ustanawiająca Eurojust[19];
- konkluzje Rady o usprawnieniu wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni[20].

Co do zasady, niniejszy wniosek nie wprowadza przepisów odnoszących się konkretnie do oszustw związanych z płatnościami bezgotówkowymi, które różniłyby się od wspomnianych szerszych instrumentów, aby zapobiec fragmentacji prawa, która mogłaby utrudnić transpozycję i wdrażanie przez państwa członkowskie. Jedynym wyjątkiem jest dyrektywa 2012/29/UE dotycząca praw, wsparcia i ochrony ofiar przestępstw, którą niniejszy wniosek uzupełnia.

2. Akty prawne **uznające za przestępstwa czyny** w zakresie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (prawo karne materialne):

- dyrektywa 2013/40/UE dotycząca ataków na systemy informatyczne[21]:
  - niniejszy wniosek uzupełnia dyrektywę 2013/40, ustanawiając przepisy dotyczące innych aspektów cyberprzestępczości[22]. Te dwa instrumenty prawne

---

15 Decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów.

16 Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji.

17 Dyrektywa Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiająca normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępująca decyzję ramową Rady 2001/220/WSiSW.

18 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW

19 Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością.

20 Konkluzje Rady z dnia 6 czerwca 2016 r. o usprawnieniu wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni.

21 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

22 W strategii bezpieczeństwa cybernetycznego Unii Europejskiej wskazano, co następuje: „cyberprzestępczość ogólnie odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Cyberprzestępczość obejmuje tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy

odpowiadają różnym postanowieniom Konwencji Rady Europy o cyberprzestępczości[23] stanowiącej międzynarodowe prawne ramy odniesienia dla UE[24];

- niniejszy wniosek jest również spójny z dyrektywą 2013/40, ponieważ przyjęto w nim podobne podejście w odniesieniu do szczegółowych kwestii, takich jak jurysdykcja czy też określenie dolnego progu maksymalnego wymiaru kary.

- dyrektywa 2014/62/UE w sprawie prawnokarnych środków ochrony euro i innych walut przed fałszowaniem[25]:
  - niniejszy wniosek uzupełnia dyrektywę 2014/62/UE, ponieważ dotyczy fałszowania bezgotówkowych instrumentów płatniczych, podczas gdy dyrektywa 2014/62/UE dotyczy fałszowania pieniądza;
  - jest on również spójny z dyrektywą 2014/62/UE, ponieważ przyjęto w nim to samo podejście w odniesieniu do niektórych kwestii, takich jak środki dochodzeniowe.
- dyrektywa 2017/541/UE w sprawie zwalczania terroryzmu:
  - niniejszy wniosek uzupełnia dyrektywę 2017/541/UE, ponieważ jego celem jest ograniczenie wysokości środków czerpanych z oszustw dotyczących płatności bezgotówkowych – większość tych kwot trafia do zorganizowanych grup przestępczych i finansuje poważną przestępczość, w tym terroryzm.
- wniosek dotyczący dyrektywy w sprawie przeciwdziałania praniu pieniędzy z wykorzystaniem prawa karnego:
  - niniejszy wniosek i wniosek dotyczący dyrektywy w sprawie przeciwdziałania praniu pieniędzy z wykorzystaniem prawa karnego uzupełniają się, ponieważ ten drugi ustanawia ramy prawne niezbędne do zapobiegania praniu pieniędzy pochodzących z oszustw związanych z płatnościami bezgotówkowymi (przez tzw. słupy) jako przestępstwa źródłowego.

1.4. Spójność z innymi politykami UE

Niniejszy wniosek jest spójny z unijną agendą bezpieczeństwa i strategią bezpieczeństwa cybernetycznego UE, które stawiają sobie za główny cel poprawę bezpieczeństwa.

Wniosek jest także spójny ze strategią jednolitego rynku cyfrowego, która zmierza do zwiększenia zaufania użytkowników do rynku cyfrowego – ta poprawa zaufania stanowi kolejny główny cel wniosku. W kontekście strategii jednolitego rynku cyfrowego powstał szereg instrumentów prawnych, które ułatwiają bezpieczne płatności w obrębie UE; niniejszy wniosek jest spójny również z tymi instrumentami:

---

informatyczne, w tym ataki prowadzące do zablokowania usług/systemów, oraz złośliwe oprogramowanie)".

23 Konwencja Rady Europy o cyberprzestępczości (ETS nr 185). Przepisy dyrektywy 2013/40 odpowiadają art. 2–6 konwencji, a nowy akt prawny odpowiadałby art. 7 i 8 konwencji.

24 Komisja oraz Wysoki Przedstawiciel Unii Europejskiej do Spraw Zagranicznych i Polityki Bezpieczeństwa – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń.

25 Dyrektywa Parlamentu Europejskiego i Rady 2014/62/UE z dnia 15 maja 2014 r. w sprawie prawnokarnych środków ochrony euro i innych walut przed fałszowaniem, zastępująca decyzję ramową Rady 2000/383/WSiSW.

- Zmieniona dyrektywa w sprawie usług płatniczych (druga dyrektywa w sprawie usług płatniczych)[26] zawiera szereg środków, które zaostrzą wymogi dotyczące bezpieczeństwa płatności elektronicznych i zapewnią ramy prawne i nadzorcze, którym będą podlegać podmioty rozwijające działalność na rynku płatności.
- Dyrektywa 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu[27] (czwarta dyrektywa w sprawie przeciwdziałania praniu pieniędzy) obejmuje przypadki, w których przestępcy wykorzystują niezgodnie z prawem bezgotówkowe instrumenty płatnicze, aby ukryć swoje działania. Niniejszy wniosek uzupełnia tę dyrektywę, wprowadzając przepisy dotyczące przypadków, gdy bezgotówkowe instrumenty płatnicze zostały, na przykład, przywłaszczone, podrobione lub sfałszowane przez przestępców w nielegalny sposób.
- Wniosek Komisji dotyczący dyrektywy zmieniającej dyrektywę 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu[28], z którego na potrzeby niniejszego wniosku przejęto definicję walut wirtualnych. Jeżeli brzmienie tej definicji zostanie zmienione w toku procedury przyjmowania powyższego wniosku, należy odpowiednio dostosować także definicję w niniejszym wniosku.
- Inne ważne akty prawne to rozporządzenie (UE) 2015/847 w sprawie informacji towarzyszących transferom środków pieniężnych[29]; rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[30]; rozporządzenie (UE) 2012/260 ustanawiające wymogi techniczne i handlowe w odniesieniu do poleceń przelewu i poleceń zapłaty w euro[31]; i dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[32].

Wskazane powyżej akty prawne przyczyniają się generalnie do ustanowienia skuteczniejszych środków zapobiegawczych. Niniejszy wniosek uzupełnia je,

---

26 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

27 Dyrektywa 2015/849/UE z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

28 Wniosek Komisji dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu i zmieniającej dyrektywę 2009/101/WE.

29 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006.

30 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

31 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 260/2012 z dnia 14 marca 2012 r. ustanawiające wymogi techniczne i handlowe w odniesieniu do poleceń przelewu i poleceń zapłaty w euro oraz zmieniające rozporządzenie (WE) nr 924/2009.

32 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

wprowadzając dodatkowe środki w celu karania działalności przestępczej i umożliwienia ścigania przestępstw w sytuacji, gdy nie udało się im zapobiec.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

2.1. Podstawa prawna

Podstawą prawną działania UE jest art. 83 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, w którym wyraźnie wymieniono **fałszowanie środków płatniczych, przestępczość komputerową i przestępczość zorganizowaną** jako dziedziny szczególnie poważnej przestępczości o wymiarze transgranicznym:

Parlament Europejski i Rada, stanowiąc w drodze dyrektyw zgodnie ze zwykłą procedurą ustawodawczą, mogą ustanowić normy minimalne odnoszące się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości ***o wymiarze transgranicznym****, wynikające z rodzaju lub skutków tych przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania.*

Powyższe dziedziny przestępczości są następujące: terroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, ***fałszowanie środków płatniczych, przestępczość komputerowa i przestępczość zorganizowana****.*

2.2. Europa o zmiennej geometrii

Decyzja ramowa 2001/413/WSiSW w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi stosuje się do wszystkich państw członkowskich.

Zgodnie z Protokołem nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonym do Traktatów, Zjednoczone Królestwo i Irlandia mogą zdecydować o uczestnictwie w przyjęciu niniejszego wniosku. Mogą one również skorzystać z tej możliwości po przyjęciu wniosku.

Ponieważ w dniu 29 marca 2017 r. Zjednoczone Królestwo notyfikowało swój zamiar wystąpienia z Unii, zgodnie z art. 50 Traktatu o Unii Europejskiej (TUE) Traktaty przestają mieć zastosowanie do Zjednoczonego Królestwa od dnia wejścia w życie umowy o wystąpieniu lub, w przypadku jej braku, dwa lata po notyfikacji, chyba że Rada Europejska w porozumieniu ze Zjednoczonym Królestwem podejmie decyzję o przedłużeniu tego okresu. Nie naruszając jakichkolwiek postanowień umowy o wystąpieniu, wspomniany opis uczestnictwa Zjednoczonego Królestwa w niniejszym wniosku ma w związku z powyższym zastosowanie tylko do momentu, gdy Zjednoczone Królestwo przestanie być państwem członkowskim.

Zgodnie z Protokołem nr 22 w sprawie stanowiska Danii Dania nie uczestniczy w przyjęciu przez Radę środków na podstawie tytułu V TFUE (z wyjątkiem środków odnoszących się do polityki wizowej). W związku z tym na mocy obecnie obowiązujących procedur Dania nie uczestniczy w przyjęciu niniejszego wniosku i nie będzie nim związana.

2.3. Pomocniczość

Oszustwa związane z płatnościami bezgotówkowymi mają bardzo istotny wymiar transgraniczny, zarówno w obrębie UE, jak i poza jej terytorium. Typowy sposób postępowania oszustów może obejmować przechwycenie czy też skopiowanie (ang. *skimming*) danych karty w jednym z państw UE, stworzenie fałszywej karty przy użyciu tych danych oraz wypłatę gotówki ze sfałszowanej karty poza terytorium UE, aby obejść wysokie

standardy bezpieczeństwa obowiązujące w Unii. Tego rodzaju przestępstwa mają obecnie miejsce niemal wyłącznie w internecie.

W związku z tym cel, jakim jest skuteczne zwalczanie tego typu przestępstw, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie działające indywidualnie lub w sposób nieskoordynowany:

- okoliczności tych przestępstw mogą spowodować, że ofiara, sprawca i dowody podlegają różnym krajowym porządkom prawnym w UE i poza jej granicami. W konsekwencji skuteczne przeciwdziałanie tym działaniom przestępczym przez pojedyncze kraje może być bardzo czasochłonne i trudne, jeżeli nie będą istniały wspólne normy minimalne;
- konieczność podjęcia działania na szczeblu UE została już stwierdzona przez sam fakt ustanowienia obecnych unijnych przepisów dotyczących zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi („decyzja ramowa”);
- potrzeba interwencji UE znajduje również odzwierciedlenie w bieżących inicjatywach mających na celu koordynowanie działań państw członkowskich w tej dziedzinie na szczeblu UE, takich jak wyspecjalizowany zespół Europolu zajmujący się oszustwami płatniczymi[33] oraz priorytetowe traktowanie współpracy operacyjnej w zakresie zwalczania oszustw związanych z płatnościami bezgotówkowymi przy realizacji Cyklu Polityki Bezpieczeństwa w ramach projektów EMPACT[34]. Podczas konsultacji z interesariuszami podczas przygotowywania niniejszego wniosku, w szczególności podczas spotkań z ekspertami, podkreślano wielokrotnie wartość dodaną wnoszoną przez wspomniane inicjatywy, które rzeczywiście pomagają państwom członkowskim zwalczać ten rodzaj przestępczości.

Inną wartością dodaną działania na szczeblu UE jest ułatwienie współpracy z państwami spoza UE; jest to ważne, ponieważ oszustwa związane z płatnościami bezgotówkowymi mają wymiar międzynarodowy i są często popełniane poza granicami UE. Wprowadzenie w UE minimalnych wspólnych norm może także dać impuls do powstania skutecznych rozwiązań ustawodawczych w krajach nienależących do UE, co ułatwiłoby współpracę transgraniczną w wymiarze globalnym.

2.4. Proporcjonalność

Zgodnie z zasadą proporcjonalności, określoną w art. 5 ust. 4 TUE, proponowana nowa dyrektywa ogranicza się do tego, co jest konieczne i proporcjonalne, aby wdrożyć normy międzynarodowe i zaktualizować istniejące przepisy mające zastosowanie do przestępstw w tym obszarze, aby uwzględniały nowe zagrożenia. Działania dotyczące korzystania ze środków dochodzeniowych i wymiany informacji zostały uwzględnione tylko w zakresie potrzebnym do zapewnienia skutecznego funkcjonowania proponowanych ram prawnokarnych.

We wniosku określono zakres przestępstw w ten sposób, że obejmuje on wszystkie odpowiednie czyny, ograniczając się jednak do tego, co jest konieczne i proporcjonalne.

---

33 Zob. strona Europolu.

34 Więcej informacji na ten temat można uzyskać tutaj.

2.5. Wybór instrumentu

Zgodnie z art. 83 ust. 1 TFUE normy minimalne odnoszące się do określania przestępstw oraz kar w dziedzinie poważnej przestępczości o wymiarze transgranicznym, w tym fałszowania środków płatniczych i przestępczości komputerowej, mogą być ustanawiane wyłącznie w drodze dyrektywy Parlamentu Europejskiego i Rady przyjętej zgodnie ze zwykłą procedurą ustawodawczą.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

3.1. Oceny *ex post*/kontrole sprawności obowiązującego prawodawstwa

Komisja dokonała oceny[35] obowiązujących ram ustawodawczych UE i przygotowała jedocześnie ocenę skutków dołączoną do niniejszego wniosku (więcej informacji można znaleźć w odnośnym dokumencie roboczym służb Komisji).

W ocenie stwierdzono występowanie trzech czynników stanowiących źródła problemów. Każdy z tych czynników obejmuje pewną liczbę elementów składowych:

[35] Dokument roboczy służb Komisji – ocena skutków towarzysząca wnioskowi w sprawie dyrektywy w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, SWD(2017)298.

Czynniki	Elementy składowe
1. W przypadku niektórych przestępstw **skuteczne prowadzenie dochodzeń i ściganie** jest niemożliwe ze względu na obowiązujące **ramy prawne**.	a. Niektóre przestępstwa nie mogą być skutecznie ścigane, ponieważ pomiędzy państwami członkowskimi występują różnice w zakresie kryminalizacji czynów popełnionych przy użyciu niektórych instrumentów płatniczych (zwłaszcza **niematerialnych**); w niektórych państwach nie są one nawet uznawane za przestępstwa. b. **Działania przygotowujące** oszustwa związane z płatnościami bezgotówkowymi nie mogą być skutecznie ścigane, ponieważ pomiędzy państwami członkowskimi występują różnice w zakresie ich kryminalizacji, a w niektórych państwach nie są one nawet uznawane za przestępstwa. c. Dochodzenia transgraniczne może być utrudnione, ponieważ **wymiar kary** za te same przestępstwa jest różny w poszczególnych państwach członkowskich. d. Luki dotyczące określania **jurysdykcji** mogą utrudniać skuteczne prowadzenie transgranicznych dochodzeń i transgraniczne ściganie niektórych przestępstw.
2. W przypadku innych przestępstw **skuteczne prowadzenie dochodzeń i ściganie** jest niemożliwe ze względu na **przeszkody operacyjne**.	a. Przekazywanie informacji w odpowiedzi na wnioski dotyczące **współpracy transgranicznej** może trwać zbyt długo, utrudniając prowadzenie dochodzeń i ściganie. b. Skuteczne prowadzenie dochodzeń i ściganie przestępstw utrudnia niska zgłaszalność organom ścigania wynikająca z niedostatecznej **współpracy między sektorami publicznym i prywatnym (współpracy publiczno-prywatnej)**.
3. Przestępcy popełniają oszustwa, wykorzystując luki w zakresie **zapobiegania** tego typu przestępczości.	a. Niedostateczna **wymiana informacji** w ramach **współpracy publiczno-prywatnej** utrudnia natomiast zapobieganie przestępczości. b. Przestępcy wykorzystują **brak świadomości zagrożeń** po stronie ofiar.

Na podstawie analizy czynników stanowiących źródło problemów można stwierdzić, że chodzi tu przede wszystkim o **niedociągnięcia regulacyjne**, ponieważ obowiązujące ramy prawne UE (decyzja ramowa) stały się częściowo nieaktualne, przede wszystkim ze względu na **zmiany technologiczne**. W ocenie wykazano, że ta luka regulacyjna nie została w wystarczającym stopniu uzupełniona o nowsze akty prawne.

3.2. Konsultacje z zainteresowanymi stronami

Konsultacje

Przeprowadzono trzy rodzaje konsultacji: otwarte konsultacje publiczne, ukierunkowane konsultacje zorganizowane przez Komisję Europejską i ukierunkowane konsultacje zorganizowane przez wykonawcę na zlecenie.

1. Otwarte konsultacje publiczne

W dniu 1 marca 2017 r. Komisja Europejska rozpoczęła otwarte konsultacje publiczne w celu zasięgnięcia opinii ogółu społeczeństwa w kwestii określenia problemów, adekwatności i skuteczności obecnych ram prawnych dotyczących oszustw związanych z płatnościami bezgotówkowymi oraz możliwych rozwiązań obecnych problemów i potencjalnych skutków tych rozwiązań. Konsultacje zamknięto po 12 tygodniach, w dniu 24 maja 2017 r.

Kwestionariusze otwartych konsultacji wypełniło 33 specjalistów i 21 osób prywatnych. Czterech specjalistów przedstawiło dodatkowe informacje w formie pisemnej. Respondenci będący specjalistami to:

- przedsiębiorstwa prywatne (sektor prywatny);
- międzynarodowe lub krajowe organy publiczne (organy ścigania, organy wymiaru sprawiedliwości oraz instytucje i organy UE);
- stowarzyszenia przedsiębiorców, branżowe i zawodowe (np. krajowe federacje bankowe);
- organizacje, platformy lub sieci pozarządowe;
- firmy konsultingowe, kancelarie prawne, konsultanci pracujący na własny rachunek.

2. Ukierunkowane konsultacje zorganizowane przez Komisję Europejską:

- spotkania z dużymi grupami ekspertów, w których skład wchodzili przedstawiciele organów policyjnych i sądowych ze wszystkich krajów UE (wybrani przez państwa członkowskie) oraz specjaliści reprezentujący sektor prywatny (instytucje finansowe, dostawców usług płatniczych, akceptantów, systemy kart płatniczych);
- różnego rodzaju spotkania z ekspertami i interesariuszami ze środowisk akademickich, organów ścigania i sektorów walut wirtualnych oraz przedstawicielami organizacji konsumenckich, prywatnych instytucji finansowych i organów regulujących rynek finansowy.

3. Ukierunkowane konsultacje zorganizowane przez wykonawcę na zlecenie:

Wykonawca przeprowadził ukierunkowane konsultacje, które obejmowały ankiety internetowe i wywiady. Wstępne wyniki zostały przedstawione do walidacji grupie dyskusyjnej, która przekazała informacje zwrotne i zweryfikowała wyniki konsultacji.

W konsultacjach uczestniczyło w sumie 125 interesariuszy z 25 państw członkowskich.

<u>Główne wyniki</u>

- Skala przestępstw:

  Koszty oszustw związanych z bezgotówkowymi płatnościami są generalnie postrzegane jako wysokie i przewiduje się, że w nadchodzących latach jeszcze wzrosną. Uczestnicy konsultacji reprezentowali wszystkie grupy interesariuszy, ale pomimo tego szerokiego przekroju sektorowego mieli trudności z ilościowym określeniem skali tego rodzaju przestępstw. Danych statystycznych dotyczących tej dziedziny jest niewiele i nie zawsze można uzyskać do nich dostęp. Pewne dane dostarczają jednak konkretnych dowodów świadczących o znacznej skali niektórych rodzajów oszustw związanych z płatnościami bezgotówkowymi.

- Ramy prawnokarne:

  Większość interesariuszy stwierdziła, że obecne ramy prawne UE tylko częściowo odpowiadają aktualnym potrzebom w zakresie bezpieczeństwa, w szczególności jeżeli chodzi o definicję instrumentów płatniczych i przestępstw. Niektórzy respondenci potwierdzili konieczność zmiany krajowych ram prawnych.

- Prawo karne procesowe:

  Pomimo faktu, że już istnieją odpowiednie przepisy prawa, obecny poziom współpracy między państwami członkowskimi w zakresie prowadzenia dochodzeń i ścigania jest postrzegany jako tylko częściowo zadowalający. Powszechnie potwierdzono, że Europol jest faktycznie pomocny we współpracy transgranicznej.

- Zgłaszanie przestępstw organom ścigania:

  Opinie na temat zgłaszania przestępstw organom ścigania różniły się: niektórzy respondenci byli zadowoleni z obecnego poziomu zgłaszalności, podczas gdy inni uważali, że należy go zwiększyć. Wszystkie grupy interesariuszy zgadzały się co do tego, że przyszłe rozwiązania polityczne w zakresie zgłaszalności powinny odpowiadać rzeczywistym zdolnościom operacyjnym organów ścigania.

- Współpraca publiczno-prywatna:

  W odczuciu interesariuszy współpraca między podmiotami publicznymi a prywatnymi przynosi generalnie korzyści; byli oni zgodni, że należy zachęcać do szukania lepszych rozwiązań problemu oszustw związanych z płatnościami bezgotówkowymi, zwłaszcza w zakresie zapobiegania.

  Większość interesariuszy uznała, że aby móc zwalczać oszustwa związane z płatnościami bezgotówkowymi, należy poprawić współpracę publiczno-prywatną. Najbardziej niezadowoleni ze stanu współpracy wydawali się przedstawiciele sektora prywatnego. Ich zdaniem głównymi przeszkodami utrudniającymi współpracę są np. ograniczenia dotyczące możliwości dzielenia się informacjami z organami ścigania i narzędzi używanych do celów takiej wymiany informacji.

  Zdecydowana większość interesariuszy zgodziła się, że w celach prowadzenia dochodzeń i ścigania przestępców należy uprawnić instytucje finansowe do przekazywania policji krajowej lub policji innego państwa UE, z własnej inicjatywy, niektórych danych osobowych ofiary przestępstwa (np. imienia i nazwiska albo nazwy firmy, adresu, numeru rachunku bankowego itp.).

  Wymieniając przeszkody utrudniające walkę z oszustwami związanymi z płatnościami bezgotówkowymi, pewna liczba interesariuszy wskazała również słabą współpracę między sektorem prywatnym a organami publicznymi.

  Zdaniem przedsiębiorstw prywatnych, organów publicznych oraz stowarzyszeń przedsiębiorców, branżowych i zawodowych skuteczną współpracę między organami publicznym a podmiotami prywatnymi z różnych państw UE utrudniają niedoskonałe przepisy prawa, różne priorytety i brak zaufania, w połączeniu z problemami praktycznymi i organizacyjnymi. Brak

odpowiedniej technologii (np. kanału komunikacji) został wskazany jako przeszkoda zarówno przez przedsiębiorstwa prywatne, jak i organy publiczne.

- Prawa ofiar przestępstwa:

  Zainteresowane strony podkreślały, jak ważne jest chronienie ofiar oszustw. Niektórzy respondenci uważali, że poziom tej ochrony nie jest wystarczający, chociaż doceniali inicjatywy podejmowane w tym zakresie na poziomie państw członkowskich. Stowarzyszenia ofiar oszustw wypracowały dobre mechanizmy współpracy z organami ścigania. Kilka zainteresowanych stron zwróciło uwagę na konieczność lepszej ochrony ofiar przed kradzieżą tożsamości; ich zdaniem przestępstwem tym są zagrożone zarówno osoby fizyczne, jak i prawne. Ofiary przestępstw należy zatem chronić niezależnie od tego, czy są osobami fizycznymi czy prawnymi.

3.3. Ocena skutków

Zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa[36] Komisja przeprowadziła ocenę skutków[37], aby ocenić potrzebę przedstawienia wniosku ustawodawczego.

Ocenę skutków przedstawiono i omówiono na posiedzeniu Rady ds. Kontroli Regulacyjnej w dniu 12 lipca 2017 r. Rada doceniła prace mające na celu ilościowe określenie kosztów i korzyści. Wydała ona opinię pozytywną[38], z zaleceniem, aby poprawiono sprawozdanie w odniesieniu do następujących aspektów:

1. W sprawozdaniu nie wyjaśniono odpowiednio kontekstu politycznego, w tym powiązań pomiędzy istniejącymi i planowanymi mechanizmami współpracy sądowej i współpracy ogólnoeuropejskiej, ani komplementarności tych mechanizmów.
2. Cel inicjatywy w zakresie wzrostu gospodarczego wydaje się zawyżony.

Sprawozdanie z oceny skutków zostało zmienione, aby uwzględnić zalecenia dołączone do pozytywnej opinii Rady ds. Kontroli Regulacyjnej.

Po zidentyfikowaniu środków z zakresu polityki, które można potencjalnie wykorzystać w celu rozwiązania poszczególnych problemów wskazanych w ocenie, dokonano ich selekcji i następnie zgrupowano je, tworząc pewną liczbę wariantów strategicznych. Każdy wariant strategiczny został opracowany w taki sposób, że stanowi rozwiązanie wszystkich zidentyfikowanych problemów. Rozważane warianty strategiczne miały charakter kumulatywny, tzn. każdy kolejny wariant przewidywał większą liczbę działań ustawodawczych na poziomie UE. Biorąc pod uwagę fakt, że analizowany problem dotyczył generalnie **niedociągnięć regulacyjnych**, należało rozważyć pełny zakres narzędzi regulacyjnych, aby ustalić, które z nich będzie stanowić najbardziej proporcjonalną odpowiedź UE.

Rozważono następujące warianty:

- **wariant A**: poprawa wdrażania prawa UE i ułatwienie samoregulacji współpracy publiczno-prywatnej;

---

36 Więcej informacji na temat wytycznych dotyczących lepszego stanowienia prawa można znaleźć tutaj.

37 Dokument roboczy służb Komisji – ocena skutków towarzysząca wnioskowi w sprawie dyrektywy w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, SWD(2017)298.

38 Komisja Europejska, Rada ds. Kontroli Regulacyjnej – Opinia w sprawie oceny skutków – Zwalczanie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, SEC(2017)390.

- **wariant B:** wprowadzenie nowych ram prawnych i ułatwienie samoregulacji współpracy publiczno-prywatnej;
- **wariant C:** wariant B uzupełniony o przepisy zachęcające do zgłaszania przestępstw w ramach współpracy publiczno-prywatnej (zamiast samoregulacji) oraz o nowe przepisy dotyczące zwiększania świadomości zagrożeń;
- **wariant D:** wariant C uzupełniony o dodatkowe przepisy dotyczące jurysdykcji, uzupełniające przepisy w sprawie europejskiego nakazu dochodzeniowego i nakazów sądowych.

Wariantem preferowanym był wariant C, zarówno pod względem jakościowym, jak i z punktu widzenia kosztów i korzyści.

Jeżeli chodzi o związane z nim korzyści, preferowany wariant zapewnia spójniejsze stosowanie przepisów w całej UE, skuteczniejszą współpracę transgraniczną, pogłębioną współpracę publiczno-prywatną oraz usprawnioną wymianę informacji i dzięki temu utoruje drogę skuteczniejszym i wydajniejszym działaniom organów ścigania przeciwko oszustwom związanym z płatnościami bezgotówkowymi. Dzięki zwiększeniu bezpieczeństwa inicjatywa zwiększy też zaufanie do jednolitego rynku cyfrowego.

Jeżeli chodzi o koszty związane z preferowanym wariantem, szacuje się, że koszty opracowania nowej inicjatywy i wdrożenia jej po stronie państw członkowskich wyniosą około 561 000 EUR (są to koszty jednorazowe). Szacuje się, że państwa członkowskie będą ponosić stałe koszty wdrażania i stosowania nowych przepisów w wysokości około 2 285 140 EUR rocznie (łącznie).

We wniosku nie przewidziano imperatywnych przepisów w sprawie zgłaszania przestępstw, nie powinien więc on wiązać się z dodatkowymi kosztami dla przedsiębiorstw, w tym MŚP. Pozostałe przepisy zawarte we wniosku również nie mają wpływu na MŚP.

Przewiduje się, że ogólny łączny wpływ proponowanych środków na koszty administracyjne i finansowe będzie wyższy niż obecnie – liczba dochodzeń będzie obciążeniem dla organów ścigania zajmujących się tą dziedziną i zasoby tych organów trzeba będzie zwiększyć. Wynika to przede wszystkim z następujących czynników:

- szersza definicja środków płatniczych i poszerzony zakres przestępstw, które będą wymagały działań odpowiednich organów (akty przygotowawcze), najprawdopodobniej spowodują wzrost liczby spraw wchodzących w zakres odpowiedzialności policji i organów wymiaru sprawiedliwości;
- niezbędne będą dodatkowe zasoby w celu intensyfikacji współpracy transgranicznej;
- dodatkowym obciążeniem administracyjnym dla państw członkowskich będzie obowiązek gromadzenia danych statystycznych.

Z drugiej strony, ustanowienie jasnych ram prawnych umożliwiających walkę z przestępstwami umożliwiającymi popełnianie oszustw związanych z płatnościami bezgotówkowymi pozwoli jednak wykrywać i ścigać te przestępstwa przygotowawcze oraz karać za nie na wcześniejszym etapie. Co więcej, mimo że zacieśnienie współpracy publiczno-prywatnej wymaga nakładów, to zwrot z tej inwestycji pod względem skuteczności i efektywności egzekwowania prawa jest natychmiastowy.

3.4. Sprawność regulacyjna i uproszczenie

W ujęciu jakościowym niniejszy wniosek może uprościć przepisy w kilku obszarach, np.:

- większe ujednolicenie krajowych przepisów prawnokarnych (np. przez wprowadzenie wspólnych definicji i wspólnego dolnego progu maksymalnego wymiaru kar) uprościłoby i ułatwiło współpracę między krajowymi organami ścigania prowadzącymi dochodzenia i postępowania karne w sprawach transgranicznych;
- w szczególności, jaśniejsze przepisy dotyczące jurysdykcji, wzmocniona rola krajowych punktów kontaktowych oraz wymiana danych i informacji pomiędzy krajowymi organami policyjnymi a Europolem mogłyby doprowadzić do większego uproszczenia procedur i praktyk w zakresie współpracy.

Ilościowe określenie potencjalnych uproszczeń nie jest możliwe ze względu na brak danych (a w niektórych przypadkach ze względu na brak możliwości wyizolowania skutków decyzji ramowej).

Generalnie potencjał niniejszej inicjatywy w zakresie sprawności regulacyjnej jest bardzo ograniczony.

1. Po pierwsze, już sama decyzja ramowa z 2001 r. była stosunkowo prostym aktem prawnym, który trudno byłoby jeszcze bardziej uprościć.
2. Po drugie, niniejsza inicjatywa ma na celu zwiększenie bezpieczeństwa przez wyeliminowanie istniejących luk prawnych. W normalnych okolicznościach jej wprowadzenie doprowadzi do zwiększenia kosztów administracyjnych związanych z prowadzeniem dochodzeń i ściganiem przestępstw, które nie są obecnie objęte przepisami, a nie do znaczących oszczędności wskutek uproszczenia współpracy transgranicznej.
3. Po trzecie inicjatywa nie ma na celu nakładania dodatkowych obowiązków prawnych na przedsiębiorstwa i obywateli. Wzywa się w niej państwa członkowskie, aby zachęcały do składania zawiadomień o przestępstwach odpowiednimi kanałami i ułatwiały takie zgłoszenia (nie wprowadzając jednak obowiązku zgłaszania tego rodzaju przestępstw), analogicznie jak w przypadku innych instrumentów unijnych, takich jak dyrektywa 2011/93 w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (art. 16 ust. 2).

3.5. Prawa podstawowe

Wniosek zawiera przepisy mające na celu dostosowanie ram prawnych dotyczących walki z fałszowaniem i oszustwami związanymi z bezgotówkowymi środkami płatniczymi do nowych i pojawiających się zagrożeń oraz ustanowienie regulacji dotyczących tych rodzajów oszustw związanych z płatnościami bezgotówkowymi, które nie są obecnie objęte przepisami.

Ostatecznym celem tych środków jest ochrona praw ofiar i potencjalnych ofiar. Ustanowienie jasnych ram prawnych umożliwiających organom ścigania i organom sądowym reagowanie na działania przestępcze mające bezpośredni wpływ na dane osobowe ofiar, w tym uznanie za przestępstwa działań przygotowawczych, może w szczególności wywrzeć pozytywny wpływ na ochronę praw ofiar i potencjalnych ofiar do prywatności i ochrony danych osobowych.

Wszystkie środki przewidziane w niniejszym wniosku zapewniają także respektowanie podstawowych praw i wolności uznanych w Karcie praw podstawowych Unii Europejskiej, i muszą być wdrożone z ich poszanowaniem. Wszelkie ograniczenia w korzystaniu z tych podstawowych praw i wolności podlegają warunkom określonym w art. 52 ust. 1 Karty: ograniczenia te muszą być proporcjonalne i rzeczywiście odpowiadać uzasadnionym celom

interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Ograniczenia muszą być przewidziane ustawą i szanować istotę praw i wolności określonych w Karcie.

W tym kontekście wzięto pod uwagę szereg podstawowych praw i wolności zapisanych w Karcie, w tym: prawo do wolności i bezpieczeństwa osobistego; prawo do poszanowania życia prywatnego i rodzinnego; wolność wyboru zawodu i prawo do podejmowania pracy; wolność prowadzenia działalności gospodarczej; prawo własności; prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu; domniemanie niewinności i prawo do obrony; zasady legalności oraz proporcjonalności kar do czynów zabronionych pod groźbą kary, a także zakaz ponownego sądzenia lub karania w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary.

W szczególności, niniejszy wniosek jest zgodny z zasadą, że przestępstwa i kary muszą być określone w przepisach prawa i mieć proporcjonalny charakter. Wniosek obejmuje tylko taki zakres przestępstw, jaki jest niezbędny do zapewnienia skutecznego ścigania czynów stanowiących szczególne zagrożenie dla bezpieczeństwa, oraz wprowadza normy minimalne dotyczące poziomu sankcji zgodnie z zasadą proporcjonalności, uwzględniając charakter przestępstwa.

Niniejszy wniosek służy również zapewnieniu, aby dane osób podejrzanych o popełnienie przestępstw wymienionych w niniejszej dyrektywie były przetwarzane z poszanowaniem podstawowego prawa do ochrony danych osobowych i przepisów prawa obowiązujących w tym zakresie, także w ramach współpracy publiczno-prywatnej.

4. WPŁYW NA BUDŻET

Wniosek nie ma bezpośredniego wpływu na budżet UE.

5. ELEMENTY FAKULTATYWNE

5.1. Plany wdrożenia i monitorowanie, ocena i sprawozdania

Komisja będzie monitorować wdrażanie dyrektywy na podstawie informacji dostarczonych przez państwa członkowskie na temat środków przyjętych w celu wprowadzenia w życie przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania dyrektywy.

Po dwóch latach od terminu wdrożenia niniejszej dyrektywy do prawa krajowego Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym oceni, w jakim zakresie państwa członkowskie wprowadziły środki niezbędne do zastosowania się do przepisów niniejszej dyrektywy.

Oprócz tego Komisja oceni skutki niniejszej dyrektywy sześć lat po terminie jej wdrożenia, aby mieć pewność, że upłynął wystarczająco długi czas od pełnego wdrożenia dyrektywy we wszystkich państwach członkowskich, pozwalający na ocenę jej wyników.

5.2. Dokumenty wyjaśniające

Uważa się, że nie są konieczne żadne dokumenty wyjaśniające dotyczące transpozycji.

6. ASPEKTY PRAWNE WNIOSKU

6.1. Krótki opis proponowanych działań

Niniejszy wniosek uchyla decyzję ramową 2001/413/WSiSW i aktualizuje większość obowiązujących obecnie przepisów tej decyzji; wniosek jest także zgodny z wynikami analizy i oceny skutków (np. w odniesieniu do preferowanego wariantu).

Poniższa tabela przedstawia związki pomiędzy niniejszym wnioskiem a decyzją ramową oraz wskazuje, które artykuły są nowe, a które zostały zaktualizowane w stosunku do decyzji ramowej:

	DYREKTYWA		DECYZJA RAMOWA		Uwagi
	Artykuł	**Motyw**	**Artykuł**	**Motyw**	
I. Przedmiot i definicje	1. Przedmiot	1-6	Brak	1-7	Nowe
	2. Definicje	7-8	1. Definicje	10	Zaktualizowane
II. Przestępstwa	3. Oszukańcze użycie instrumentów płatniczych	9	2. Przestępstwa odnoszące się do instrumentów płatniczych	8-10	
	4. Przygotowanie do oszukańczego użycia instrumentów płatniczych				
	5. Przestępstwa związane z systemami informatycznymi		3. Przestępstwa odnoszące się do stosowania rozwiązań informatycznych		
	6. Narzędzia do popełniania przestępstw		4. Przestępstwa odnoszące się do urządzeń specjalnie dostosowanych		
	7. Podżeganie, pomocnictwo oraz usiłowanie		5. Uczestnictwo, podżeganie oraz usiłowanie		
	8. Kary w przypadku osób fizycznych	10-11	6. Kary	9	
	9. Odpowiedzialność osób prawnych	Brak	7. Odpowiedzialność osób prawnych	Brak	
	10. Kary w przypadku osób prawnych		8. Sankcje dla osób prawnych		
III. Jurysdykcja i prowadzenie dochodzeń	11. Jurysdykcja	12-14	9. Jurysdykcja; 10. Ekstradycja i ściganie	11	
	12. Skuteczne dochodzenia	15	Brak	Brak	Nowe
IV. Wymiana informacji i składanie zawiadomień o przestępstwach	13. Wymiana informacji	16-18	11. Współpraca pomiędzy Państwami Członkowskimi; 12. Wymiana informacji	11	Zaktualizowane
	14. Składanie zawiadomień o przestępstwach	19	Brak	Brak	Nowe
V. Pomoc i wsparcie dla ofiar przestępstw oraz zapobieganie	15. Pomoc i wsparcie dla ofiar przestępstw	20-22	Brak		
	16. Zapobieganie	23	Brak		
VI. Przepisy końcowe	17. Monitorowanie i statystyki	24	Brak		
	18. Zastąpienie decyzji ramowej	25	Brak		
	19. Transpozycja	Brak	14. Wdrożenie [art. 14 ust. 1]		Zaktualizowane
	20. Ocena i sprawozdawczość		14. Wdrożenie [art. 14 ust. 2]		
	21. Wejście w życie		15. Wejście w życie		

	Brak	26-29	13. Zasięg terytorialny		Usunięto

W szczególności, niniejszy wniosek:

- wprowadza szerszą i bezpieczniejszą definicję instrumentów płatniczych, która obejmuje również niematerialne instrumenty płatnicze, a także cyfrowe środki wymiany;
- stanowi, że następujące czyny stanowią samodzielne przestępstwo, odrębne od wykorzystywania takich instrumentów: posiadanie, sprzedaż, pozyskiwanie z zamiarem wykorzystania, przywóz, dystrybucja lub inne udostępnianie skradzionego albo przywłaszczonego w inny nielegalny sposób podrobionego lub sfałszowanego instrumentu płatniczego;
- rozszerza zakres przestępstw związanych z systemami informatycznymi, aby obejmował on wszystkie transakcje płatnicze, w tym transakcje dokonywane za pomocą cyfrowych środków wymiany;
- wprowadza przepisy dotyczące wysokości kar, w szczególności dolny próg maksymalnego wymiaru kar;
- obejmuje kwalifikowany typ przestępstwa w następujących przypadkach:
- sytuacje, gdy przestępstwa zostały popełnione w ramach organizacji przestępczej, w rozumieniu decyzji ramowej 2008/841/WSiSW, niezależnie od tego, jaki wymiar kary w niej przewidziano;
- sytuacje, gdy przestępstwo wyrządziło ogółem znaczną szkodę lub przyniosło sprawcom znaczne korzyści ekonomiczne. Przepisy te zostały przygotowane z myślą o przestępstwach, które powodują dużą liczbę szkód o niskiej indywidualnej wysokości, zwłaszcza takich jak oszustwa związane z płatnościami bez fizycznej obecności karty.
- precyzuje zakres jurysdykcji w odniesieniu do przestępstw będących przedmiotem niniejszego wniosku przez zapewnienie, aby państwo członkowskie miało jurysdykcję w przypadkach, gdy przestępstwo zostało popełnione za pomocą systemu informatycznego zlokalizowanego na terytorium tego państwa członkowskiego, chociaż sprawca może się znajdować w innym państwie, lub w przypadkach, w których sprawca znajduje się na terytorium danego państwa członkowskiego, ale system informatyczny może być zlokalizowany w innym państwie;
- precyzuje zakres jurysdykcji w odniesieniu do skutków przestępstwa przez zapewnienie, aby państwa członkowskie mogły wykonywać swoją jurysdykcję, gdy przestępstwo wyrządziło szkodę na ich terytorium, w tym szkodę wynikającą z kradzieży tożsamości osoby;
- wprowadza środki mające poprawić unijną współpracę wymiarów sprawiedliwości w sprawach karnych poprzez wzmocnienie obecnej struktury i wykorzystywanie operacyjnych punktów kontaktowych;
- poprawia warunki dotyczące składania zawiadomień o przestępstwach przez ofiary i osoby prywatne;
- stanowi odpowiedź na potrzebę pozyskania danych statystycznych dotyczących fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, ponieważ nakłada na państwa członkowskie obowiązek zapewnienia istnienia odpowiedniego systemu umożliwiającego rejestrowanie,

produkcję i udostępnianie danych statystycznych o przestępstwach, o których mowa w proponowanej dyrektywie;

- zapewnia ofiarom dostęp do informacji o przysługujących im prawach oraz o dostępnej pomocy i wsparciu, także w przypadkach, gdy mieszkają w innym państwie niż państwo, w którym przebywa sprawca oszustwa lub w którym jest prowadzone dochodzenie.

6.2. Szczegółowe objaśnienia poszczególnych przepisów wniosku

Artykuł 1: Przedmiot – artykuł ten określa zakres i cel wniosku.

Artykuł 2: Definicje – artykuł ten zawiera definicje, które są stosowane w całym akcie. Art. 2 zawiera tę samą definicję waluty wirtualnej, jak wskazana we wniosku Komisji dotyczącym dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu i zmieniającej dyrektywę 2009/101/WE[39]. Jeżeli brzmienie tej definicji zostanie zmienione w toku procedury przyjmowania powyższego wniosku, należy odpowiednio dostosować także definicję walut wirtualnych w tym artykule.

Artykuł 3: Oszukańcze użycie instrumentów płatniczych – artykuł ten zawiera wykaz przestępstw związanych z czynami zabronionymi, które stanowią bezpośrednio oszustwo, tj. oszukańcze użycie instrumentów płatniczych, w tym skradzionych i podrobionych. Za przestępstwa uznaje się czyny popełniane przy użyciu wszystkich rodzajów instrumentów płatniczych, zarówno materialnych, jak i niematerialnych, w związku z czym obejmują one również oszustwa polegające na wykorzystaniu skradzionych lub sfałszowanych danych uwierzytelniających płatności albo innych zapisów umożliwiających zainicjowanie lub użytych do zainicjowania zlecenia płatniczego lub innego przekazu środków pieniężnych, w tym przekazu waluty wirtualnej.

Artykuł 4: Przygotowanie do oszukańczego użycia instrumentów płatniczych – artykuł ten określa przestępstwa związane z czynami zabronionymi, które – chociaż nie stanowią bezpośrednio oszustwa prowadzącego do utraty własności – są popełniane w celu przygotowania takiego oszustwa. Przygotowanie stanowią m.in. kradzież lub sfałszowanie instrumentu płatniczego oraz różnego rodzaju czyny związane z nielegalnym obrotem skradzionymi lub sfałszowanymi instrumentami. Obejmuje ono posiadanie, dystrybucję lub udostępnianie do wykorzystania w celu oszukańczego użycia, w tym przypadki, gdy sprawca ma świadomość, że może dojść do oszukańczego użycia (*dolus eventualis*). Podobnie jak art. 3, artykuł ten obejmuje wszystkie przestępstwa związane z instrumentami płatniczymi, zarówno materialnymi, jak i niematerialnymi, a zatem ma również zastosowanie do zachowań takich jak handel skradzionymi danymi uwierzytelniającymi (ang. *carding*) i wyłudzanie informacji[40].

Artykuł 5: Przestępstwa związane z systemami informatycznymi – artykuł ten określa czyny związane z systemami informatycznymi, które powinny zostać uznane za przestępstwa przez państwa członkowskie. Wykaz tych przestępstw zawiera elementy, które odróżniają je od niezgodnej z prawem ingerencji w system albo niezgodnej z prawem ingerencji w dane

---

39 COM(2016) 450 final.

40 Wyłudzanie informacji (ang. *phishing*) to metoda stosowana przez oszustów w celu uzyskania dostępu do cennych danych osobowych, takich jak nazwa użytkownika i hasło. Najczęstszą metodą działania jest masowe rozsyłanie wiadomości mailowej, która wygląda jakby pochodziła od dobrze znanej firmy, która cieszy się dużym zaufaniem. Wiadomość mailowa może zawierać link kierujący odbiorcę do fałszywej strony internetowej, na której zostanie on poproszony o podanie danych osobowych.

w rozumieniu dyrektywy 2013/40/UE, takiej jak dokonanie przekazu wartości pieniężnych w celu uzyskania bezprawnej korzyści. Artykuł ten został dodany, aby zapewnić uznawanie za przestępstwo czynów takich jak włamanie do komputera lub innego urządzenia ofiary przestępstwa w celu przekierowania ruchu na sfałszowaną stronę internetową banku i doprowadzenia w ten sposób do nieświadomego dokonania wpłaty na rachunek bankowy kontrolowany przez sprawcę (lub tzw. słupa)[41]. Obejmuje ona także inne formy działalności przestępczej, takie jak *pharming*[42], polegające na wykorzystywaniu systemów informatycznych w celu uzyskania bezprawnej korzyści dla sprawcy lub innej osoby.

Artykuł 6: Narzędzia do popełniania przestępstw – artykuł ten określa czyny związane z narzędziami wykorzystywanymi do popełniania przestępstw, o których mowa w art. 4 lit. a) i b) oraz w art. 5, które to czyny państwa członkowskie powinny uznać za przestępstwa. Ma on na celu uznanie za przestępstwo umyślnego produkowania, sprzedaży, pozyskiwania z zamiarem wykorzystania, przywozu, dystrybucji lub innego udostępniania np. urządzeń służących do przechwytywania danych uwierzytelniających (tzw. skimmerów), a także złośliwego oprogramowania i fałszywych stron internetowych służących do wyłudzania informacji. Artykuł ten opiera się w dużej mierze na art. 4 decyzji ramowej 2001/413/WSiSW i na art. 3 lit. d) ppkt (i) dyrektywy 2014/62/UE w sprawie prawnokarnych środków ochrony euro i innych walut przed fałszowaniem.

Artykuł 7: Podżeganie, pomocnictwo oraz usiłowanie – artykuł ten dotyczy czynów związanych z przestępstwami, o których mowa w art. 3–6, i zobowiązuje państwa członkowskie do kryminalizacji wszystkich form przygotowywania tych przestępstw i udziału w nich. Wprowadzona zostaje odpowiedzialność karna za usiłowanie przestępstw, o których mowa w art. 3–6.

Artykuł 8: Kary w przypadku osób fizycznych – aby móc skutecznie zwalczać fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi, kary muszą mieć odstraszający charakter we wszystkich państwach członkowskich. Analogicznie jak w przypadku innych instrumentów UE zbliżających wymiar sankcji karnych w państwach członkowskich, artykuł ten stanowi, że maksymalnym wymiarem kary przewidzianym w prawie krajowym powinny być co najmniej trzy lata pozbawienia wolności, z wyjątkiem przestępstw wskazanych w art. 6, w przypadku których maksymalny wymiary kary powinien wynosić co najmniej dwa lata. W artykule tym ustanawia się surowsze kary za przestępstwa kwalifikowane – maksymalny wymiar kary za tego typu przestępstwa ma wynosić co najmniej pięć lat, gdy przestępstwo zostało popełnione przez organizację przestępczą w rozumieniu decyzji ramowej Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej[43] lub gdy przestępstwo jest dokonywane na dużą skalę, przez co wyrządza ogółem rozległą lub znaczącą szkodę; dotyczy to zwłaszcza przypadków, gdy indywidualna szkoda jest niewielka, ale łączny poziom szkód – wysoki, lub gdy przestępstwo wiąże się z uzyskaniem przez sprawcę łącznej korzyści wynoszącej co najmniej 20 000 EUR.

---

41 Pojęcie „osoba działająca jako słup” oznacza osobę, która dokonuje przekazów środków pieniężnych stanowiących dochody z przestępstwa między różnymi krajami. Środki pieniężne wpływają najpierw na rachunek bankowy słupa; następnie słup otrzymuje instrukcję wycofania środków i przesłania ich na inny rachunek, często zagraniczny, po potrąceniu pewnej kwoty dla siebie (ActionFraudUK, 2017 r.). Czasami osoby te wiedzą, że środki finansowe stanowią dochody z przestępstw, a czasami są wprowadzane w błąd i działają w przekonaniu, że fundusze te pochodzą z legalnego źródła.

42 *Pharming* stanowi formę oszustwa polegającą na zainstalowaniu na komputerze osobistym lub serwerze złośliwego oprogramowania, które przekierowuje użytkowników na fałszywe strony internetowe bez ich wiedzy i zgody.

43 Dz.U. L 300 z 11.11.2008, s. 42.

Wydaje się, że w większości państw członkowskich, dla których dane te były dostępne, przestępstwa wymienione w art. 2–5 decyzji ramowej 2001/413/WSiSW są penalizowane za pomocą szczególnych kar. Generalnie nie nastąpiło jednak zbliżenie przepisów: we wszystkich państwach członkowskich obowiązują wprawdzie kary pozbawienia wolności (przynajmniej w odniesieniu do poważnych przestępstw), ale wymiar kar za ten sam czyn jest bardzo różny. W rezultacie efekt odstraszający tych kar jest mniejszy w niektórych państwach członkowskich.

Różnice w poziomie sankcji mogą również utrudniać współpracę sądową. Jeżeli w kodeksie karnym danego państwa członkowskiego przewidziany jest niski minimalny wymiar kary, może to powodować, że organy ścigania i organy sądowe nie będą traktować odpowiednio priorytetowo prowadzenia dochodzeń i postępowań karnych w sprawie oszustw związanych z płatnościami bez fizycznej obecności karty (ang. *card-not-present*). To z kolei może utrudnić współpracę transgraniczną – wystosowane przez inne państwa członkowskie wnioski o pomoc mogą być rozpatrywane z opóźnieniem. Największe korzyści z różnic w poziomie sankcji odniosą prawdopodobnie sprawcy najpoważniejszych przestępstw, tzn. transgraniczne zorganizowane grupy przestępcze, które posiadają bazy operacyjne w kilku państwach członkowskich.

Artykuły 9 i 10: Odpowiedzialność i kary w przypadku osób prawnych artykuły te mają zastosowanie do wszystkich przestępstw, o których mowa w art. 3–7. Nakładają one na państwa członkowskie obowiązek zapewnienia ponoszenia odpowiedzialności przez osoby prawne, bez wykluczania odpowiedzialności osób fizycznych, oraz stosowania skutecznych, proporcjonalnych i odstraszających sankcji wobec osób prawnych. W art. 10 znajduje się wykaz przykładowych kar.

Artykuł 11: Jurysdykcja – artykuł ten opiera się na zasadach terytorialności oraz narodowości podmiotowej i określa przypadki, w których państwa członkowskie muszą ustanowić swoją jurysdykcję w sprawach przestępstw, o których mowa w art. 3–7.

Włączono do niego pewne sformułowania z art. 12 dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne. Jeżeli fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi mają miejsce w internecie, zasięg tych przestępstw obejmuje najprawdopodobniej wiele krajów: są one często popełniane przy użyciu systemów informatycznych zlokalizowanych poza terytorium, na którym znajduje się fizycznie sprawca, i mają skutki w jeszcze innym państwie, w którym mogą się też znajdować dowody. Przepisy art. 11 mają zatem na celu zapewnienie, aby właściwość miejscowa obejmowała sytuacje, w których sprawca znajduje się w innym państwie niż system informatyczny użyty przez niego w celu popełnienia przestępstwa.

Do artykułu tego włączono nowy element w związku z potrzebą, aby państwa członkowskie mogły stwierdzić swoją jurysdykcję w sytuacji, gdy przestępstwo wyrządza szkodę w innym państwie niż państwo, w którym zostało popełnione, w tym szkodę wynikającą z kradzieży tożsamości osoby. Zmiana ta ma na celu uwzględnienie przypadków, które nie zostały wymienione w dyrektywie 2013/40/UE dotyczącej ataków na systemy informatyczne, a które są charakterystyczne dla przestępstw polegających na oszustwach związanych z płatnościami bezgotówkowymi. Są to m.in. sytuacje, w których żaden z czynów powiązanych z odnośnym przestępstwem (np. kradzież danych uwierzytelniających, sklonowanie karty, bezprawna wypłata z bankomatu) nie został popełniony w państwie członkowskim, w którym została wyrządzona szkoda (np. w państwie, gdzie ofiara przestępstwa ma rachunek bankowy, z którego skradziono pieniądze). W takich przypadkach ofiara najprawdopodobniej zgłosi przestępstwo organom państwa członkowskiego, w którym stwierdzono stratę ekonomiczną. Dane państwo członkowskie powinno mieć możliwość wykonywania jurysdykcji, aby

zapewnić skuteczne prowadzenie dochodzeń i postępowań karnych; będzie ono wówczas stanowić punkt, w którym rozpoczną się ewentualne dochodzenia z udziałem wielu różnych państw członkowskich i państw trzecich.

Artykuł 12: Skuteczne dochodzenia – artykuł ten ma na celu zapewnienie możliwości stosowania w odniesieniu do fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (a przynajmniej w odniesieniu do poważnych przestępstw tego typu) środków dochodzeniowych przewidzianych w prawie krajowym do walki z przestępczością zorganizowaną i innymi poważnymi przestępstwami. Artykuł ten ma też zapewnić bezzwłoczne przekazywanie informacji właściwym organom po wydaniu nakazu sądowego.

Artykuł 13: Wymiana informacji – przepisy tego artykułu mają na celu zachęcenie do częstszego korzystania z operacyjnych krajowych punktów kontaktowych.

Artykuł 14: Składanie zawiadomień o przestępstwach – artykuł ten odpowiada na zidentyfikowaną w ocenie skutków potrzebę zwiększenia zgłaszalności i ułatwienia składania zawiadomień o przestępstwach. Ma on na celu zapewnienie dostępności odpowiednich kanałów umożliwiających ofiarom i podmiotom prywatnym składanie zawiadomień o przestępstwach i zachęcanie do ich zgłaszania bez zbędnej zwłoki, analogicznie jak w przypadku podobnych przepisów art. 16 ust. 2 dyrektywy 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej. Przykłady działań, które zostaną podjęte, są przedstawione w motywie 19.

Artykuł 15: Pomoc i wsparcie dla ofiar przestępstw – artykuł ten zobowiązuje państwa członkowskie do zapewnienia, by ofiary oszustw związanych z płatnościami bezgotówkowymi otrzymywały dostęp do informacji i kanałów umożliwiających im zgłoszenie przestępstwa oraz do porad dotyczących sposobów ochrony przed niekorzystnymi skutkami oszustwa i uszczerbkiem dla reputacji wynikłym z tego oszustwa.

Artykuł ten stosuje się zarówno do osób fizycznych, jak i prawnych, które również są dotknięte skutkami przestępstw objętych niniejszym wnioskiem. Wprowadza on również przepisy rozszerzające na osoby prawne kilka szczególnych praw, które dyrektywa 2012/29/UE ustanowiła na rzecz osób fizycznych.

Artykuł 16: Zapobieganie – artykuł ten odpowiada na potrzebę podniesienia świadomości obywateli i zmniejszenia w ten sposób ryzyka stania się ofiarą oszustwa; środkami do tego celu są kampanie informacyjne i uświadamiające, a także programy badawcze i edukacyjne. W ocenie skutków stwierdzono, że elementem stanowiącym źródło problemów jest występowanie luk w zapobieganiu oszustwom związanym z płatnościami bezgotówkowymi. W artykule tym przyjęto podobne podejście jak w przypadku art. 23 (Zapobieganie) dyrektywy 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej.

Artykuł 17: Monitorowanie i statystyki – artykuł ten odpowiada na potrzebę pozyskania danych statystycznych dotyczących fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, ponieważ nakłada na państwa członkowskie obowiązek zapewnienia istnienia odpowiedniego systemu umożliwiającego rejestrowanie, produkcję i udostępnianie danych statystycznych o przestępstwach, o których mowa w proponowanej dyrektywie, oraz o monitorowaniu skuteczności ich systemów (w tym wszystkich etapów postępowań sadowych) służących zwalczaniu oszustw związanych z płatnościami bezgotówkowymi. W artykule tym przyjęto podobne podejście jak w przypadku art. 14 (Monitorowanie i statystyki) dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne oraz art. 44 dyrektywy (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego

do prania pieniędzy lub finansowania terroryzmu (czwarta dyrektywa w sprawie przeciwdziałania praniu pieniędzy). Wniosek ma się również przyczynić do rozwiązania obecnego problemu polegającego na ograniczonej dostępności danych na temat takich oszustw; większa liczba danych będzie pomocna w ocenie skuteczności systemów krajowych w zwalczaniu oszustw związanych z płatnościami bezgotówkowymi.

Artykuł 18: Zastąpienie decyzji ramowej Rady 2001/413/WSiSW – artykuł ten zastępuje obecnie obowiązujące przepisy w dziedzinie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi w odniesieniu do państw członkowskich uczestniczących w niniejszej dyrektywie.

Artykuły 19, 20 i 21 – artykuły te zawierają dalsze przepisy dotyczące transpozycji przez państwa członkowskie, oceny przez Komisję i składania przez nią sprawozdań oraz wejścia w życie dyrektywy.

2017/0226 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz zastępująca decyzję ramową Rady 2001/413/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 83 ust. 1,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi stanowią zagrożenie dla bezpieczeństwa, ponieważ są źródłem dochodów dla przestępczości zorganizowanej i umożliwiają finansowanie innych rodzajów działalności przestępczej, takich jak terroryzm, obrót środkami odurzającymi i handel ludźmi.

(2) Fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi utrudniają również funkcjonowanie jednolitego rynku cyfrowego, ponieważ osłabiają zaufanie konsumentów i powodują bezpośrednie straty ekonomiczne.

(3) Należy zaktualizować decyzję ramową Rady 2001/413/WSiSW[44] i uzupełnić ją o dodatkowe przepisy dotyczące przestępstw, kar oraz współpracy transgranicznej.

(4) Poważne luki i różnice w przepisach państw członkowskich w dziedzinie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi mogą hamować walkę z tego rodzaju przestępstwami, jak również z inną poważną i zorganizowaną przestępczością, która jest z powiązana z fałszowaniem i oszustwami związanymi z bezgotówkowymi środkami płatniczymi i finansowana z dochodów z tych przestępstw, oraz utrudniać skuteczną współpracę policyjną i sądową w tej dziedzinie.

(5) Fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi mają znaczący wymiar transgraniczny, o czym świadczy rosnąca rola płatności cyfrowych, w związku z czym konieczne jest podejmowanie dalszych działań w celu zbliżenia przepisów prawnokarnych w tej dziedzinie.

(6) W ostatnich latach byliśmy świadkami nie tylko wykładniczego wzrostu gospodarki cyfrowej, ale także ekspansji innowacji w wielu obszarach, w tym w dziedzinie technologii płatniczych. Nowe technologie płatnicze wiążą się z wykorzystaniem nowych rodzajów instrumentów płatniczych, które otwierają wprawdzie nowe

[44] Decyzja ramowa Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (Dz.U. L 149 z 2.6.2001, s. 1).

możliwości dla konsumentów i przedsiębiorstw, ale jednocześnie dają też pole do oszustw. W świetle tych zmian technologicznych konieczne jest dbanie o adekwatność i aktualność przepisów prawa.

(7) Wspólne definicje w tej dziedzinie mają istotne znaczenie dla zapewnienia przyjęcia przez państwa członkowskie spójnego podejścia w zakresie stosowania niniejszej dyrektywy. Definicje powinny uwzględniać nowe rodzaje instrumentów płatniczych, takie jak pieniądz elektroniczny i waluty wirtualne.

(8) Intencją udzielenia ochrony prawnokarnej przede wszystkim tym instrumentom płatniczym, które są wyposażone w specjalną formę ochrony przed imitacjami lub nadużyciami, jest zachęcenie podmiotów gospodarczych do zapewniania emitowanym przez nie instrumentom płatniczym tego rodzaju specjalnych form ochrony, a w ten sposób do wprowadzenia do nich dodatkowego elementu zapobiegającego oszustwom.

(9) Skuteczne i efektywne środki prawnokarne są niezbędne do ochrony bezgotówkowych środków płatniczych przed oszustwami i fałszowaniem. Konieczne jest zwłaszcza przyjęcie wspólnego podejścia karnoprawnego w odniesieniu do znamion zachowania przestępczego, które stanowi wkład w oszukańcze wykorzystanie środków płatniczych lub je przygotowuje. Zachowania takie jak gromadzenie i posiadanie instrumentów płatniczych z zamiarem popełnienia oszustwa, na przykład poprzez *phishing* czy *skimming*, oraz ich dystrybucja, na przykład poprzez sprzedaż w internecie danych karty kredytowej, powinny być zatem uznawane za odrębne przestępstwa, nawet gdy nie wiążą się bezpośrednio z faktycznym oszukańczym wykorzystaniem środków płatniczych. W związku z tym za zachowanie przestępcze należy również uznawać przypadki, w których posiadanie, pozyskiwanie lub dystrybucja instrumentów płatniczych nie prowadzą rzeczywiście do ich oszukańczego wykorzystania, o ile sprawca jest świadomy, że może dojść do takiego oszukańczego wykorzystania (*dolus eventualis*). Niniejsza dyrektywa nie wprowadza kar za korzystanie z instrumentu płatniczego w sposób zgodny z prawem, w tym w ramach świadczenia innowacyjnych usług płatniczych, takich jak usługi oferowane typowo przez przedsiębiorstwa z branży technologii finansowych (ang. *FinTech*).

(10) Sankcje i kary za fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi powinny być skuteczne, proporcjonalne i odstraszające na terytorium całej Unii.

(11) Należy przewidzieć surowsze kary w przypadkach, gdy przestępstwo zostało popełnione przez organizację przestępczą w rozumieniu decyzji ramowej Rady 2008/841/WSiSW[45] lub gdy przestępstwo jest dokonywane na dużą skalę, przez co wyrządza ofiarom rozległe lub znaczące szkody, albo gdy przynosi sprawcy łączną korzyść wynoszącą co najmniej 20 000 EUR.

(12) Przepisy odnoszące się do jurysdykcji powinny zapewniać skuteczne ściganie przestępstw określonych w niniejszej dyrektywie. Z reguły przestępstwo jest w stanie ścigać najskuteczniej system sądownictwa karnego państwa, w którym zostało ono popełnione. Państwa członkowskie powinny zatem określić swoją jurysdykcję w odniesieniu do przestępstw popełnionych na ich terytorium, przestępstw popełnionych przez ich obywateli i przestępstw wyrządzających szkodę na ich terytorium.

---

[45] Decyzja ramowa Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej (Dz.U. L 300 z 11.11.2008, s. 42).

(13) Systemy informatyczne stanowią wyzwanie dla tradycyjnej koncepcji terytorialności, ponieważ można z nich korzystać i sterować nimi zdalnie, w zasadzie z dowolnego miejsca na świecie. Jeżeli państwa członkowskie stwierdzają swoją jurysdykcję na tej podstawie, że przestępstwo zostało popełnione na ich terytorium, właściwe wydaje się dokonanie oceny zakresu jurysdykcji również w odniesieniu do przestępstw popełnionych przy użyciu systemów informatycznych. Zakres jurysdykcji powinien wówczas obejmować przypadki, w których system informatyczny jest zlokalizowany na terytorium państwa członkowskiego, chociaż sprawca może się znajdować w innym państwie, oraz przypadki, w których sprawca znajduje się na terytorium państwa członkowskiego, chociaż system informatyczny może być zlokalizowany w innym państwie.

(14) Należy uprościć złożony proces stwierdzenia jurysdykcji w sytuacji, gdy przestępstwo ma skutki w innym państwie niż to, w którym zostało faktycznie popełnione. O stwierdzeniu właściwości powinny zatem rozstrzygać szkody wyrządzone przez przestępstwo na terytorium danego państwa członkowskiego, niezależnie od narodowości sprawcy i jego fizycznej obecności na tym terytorium.

(15) Ze względu na konieczność posiadania specjalnych środków umożliwiających skuteczne prowadzenie dochodzeń w sprawie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz znaczenie tych środków dla skutecznej współpracy międzynarodowej między organami krajowymi, na potrzeby prowadzenia dochodzeń w sprawie takich przestępstw właściwe organy wszystkich państw członkowskich powinny mieć dostęp do środków dochodzeniowych zwykle stosowanych w przypadku spraw związanych z przestępczością zorganizowaną i innymi poważnymi przestępstwami. Z uwagi na zasadę proporcjonalności wykorzystywanie takich narzędzi zgodnie z prawem krajowym powinno być współmierne do charakteru i wagi przestępstwa będącego przedmiotem dochodzenia. Oprócz tego organy ścigania i inne właściwe organy powinny mieć odpowiednio wcześnie dostęp do ważnych informacji, aby móc prowadzić dochodzenia i ścigać przestępstwa określone w niniejszej dyrektywie.

(16) U źródeł incydentów, które podlegają obowiązkowi zgłoszenia właściwym organom krajowym na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[46], leżą często działania przestępcze. W przypadku takich incydentów można domniemywać, że mają one charakter przestępczy, nawet jeżeli na samym początku nie istnieją wystarczające dowody jednoznacznie wskazujące na przestępstwo. W związku z tym należy zachęcać odpowiednich operatorów usług kluczowych i dostawców usług cyfrowych do przekazywania do wiadomości organów ścigania sprawozdań, które mają oni obowiązek przedstawiać na mocy dyrektywy (UE) 2016/1148. Przekazane sprawozdania umożliwią organom ścigania skuteczne i kompleksowe działania, a także ułatwią podział zadań i pociąganie sprawców do odpowiedzialności za ich czyny. Działania na rzecz bezpiecznego, chronionego i bardziej odpornego na zagrożenia środowiska wymagają w szczególności systematycznego zgłaszania organom ścigania incydentów, co do których domniemywa się, że mają charakter poważnego przestępstwa. W stosownych przypadkach w dochodzeniach prowadzonych przez organy ścigania powinny uczestniczyć także zespoły reagowania na incydenty bezpieczeństwa komputerowego

[46] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

wyznaczone zgodnie z art. 9 dyrektywy (UE) 2016/1148; zespoły te powinny przekazywać informacje, stosownie do ustaleń na poziomie krajowym, oraz zapewniać specjalistyczne doradztwo w dziedzinie systemów informatycznych.

(17) Poważne incydenty związane z bezpieczeństwem określone w art. 96 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366[47] mogą być wynikiem działań przestępczych. W stosownych przypadkach dostawcy usług płatniczych powinni być zachęcani do przekazywania do wiadomości organów ścigania sprawozdań, które mają obowiązek przedstawiać właściwym organom w swoim państwie członkowskim pochodzenia na mocy dyrektywy (UE) 2015/2366.

(18) Na szczeblu Unii istnieją pewne instrumenty i mechanizmy, które umożliwiają wymianę informacji pomiędzy krajowymi organami ścigania do celów prowadzenia dochodzeń i ścigania przestępstw. W celu ułatwienia i przyspieszenia współpracy między krajowymi organami ścigania oraz upewnienia się, że instrumenty i mechanizmy tej współpracy są wykorzystywane w pełnym zakresie, niniejsza dyrektywa powinna zwiększyć znaczenie operacyjnych punktów kontaktowych, które zostały wprowadzone na mocy decyzji ramowej Rady 2001/413/WSiSW. Państwa członkowskie mogą podjąć decyzję o wykorzystywaniu już istniejących sieci operacyjnych punktów kontaktowych, takich jak sieci ustanowione dyrektywą Parlamentu Europejskiego i Rady 2013/40/UE[48]. Powinny one udzielać skutecznej pomocy, na przykład przez ułatwianie wymiany istotnych informacji oraz udzielanie porad technicznych lub informacji prawnych. Aby zapewnić sprawne funkcjonowanie sieci, każdy punkt kontaktowy powinien być w stanie szybko nawiązać łączność z podobnym punktem w innym państwie członkowskim. Biorąc pod uwagę fakt, że ten rodzaj przestępczości ma w dużym stopniu transgraniczny charakter, a dowody elektroniczne mogą szybko zniknąć, państwa członkowskie powinny być w stanie szybko rozpatrywać pilne wnioski otrzymywane w ramach sieci punktów kontaktowych i przekazywać informacje zwrotne w ciągu ośmiu godzin.

(19) Szybkie zgłaszanie przestępstw organom publicznym ma ogromne znaczenie dla walki z fałszowaniem i oszustwami związanymi z bezgotówkowymi środkami płatniczymi, ponieważ takie zgłoszenia prowadzą często do wszczęcia dochodzeń. Należy wprowadzić środki zachęcające osoby fizyczne i prawne, a w szczególności instytucje finansowe, do zgłaszania przestępstw organom ścigania i organom sądowym. Środki te mogą opierać się na różnego rodzajach działaniach, w tym ustawodawczych, takich jak obowiązek zgłaszania domniemanych oszustw, lub innych niż ustawodawcze, takich jak powoływanie lub wspieranie organizacji lub mechanizmów poprawiających wymianę informacji lub podnoszących świadomość zagrożeń. Wszelkie środki, które wiążą się z przetwarzaniem danych osobowych osób fizycznych, powinny być wdrażane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[49]. W szczególności przekazywanie informacji dotyczących zapobiegania

---

47 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

48 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

49 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego

przestępstwom polegającym na fałszowaniu i oszustwach związanych z bezgotówkowymi środkami płatniczymi oraz zwalczania takich przestępstw powinno odbywać się z poszanowaniem wymogów określonych w rozporządzeniu (UE) 2016/679, przede wszystkim wymogu posiadania ważnej podstawy prawnej przetwarzania.

(20) Fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi narażają ofiary tego rodzaju przestępstw na poważne szkody ekonomiczne i nieekonomiczne. W przypadku gdy takie oszustwo wiąże się z kradzieżą tożsamości, jego skutki są często jeszcze groźniejsze, ponieważ pociągają za sobą uszczerbek dla reputacji i poważny uraz emocjonalny. W celu złagodzenia tych skutków państwa członkowskie powinny wprowadzić środki niosące wsparcie i pomoc ofiarom oraz chroniące je.

(21) Osobom fizycznym będącym ofiarami oszustwa związanego z bezgotówkowymi środkami płatniczymi przysługują pewne prawa na mocy dyrektywy Parlamentu Europejskiego i Rady 2012/29/UE[50]. Państwa członkowskie powinny wdrożyć działania niosące pomoc i wsparcie tym ofiarom, opierając się na środkach wymaganych na mocy dyrektywy 2012/29/UE, ale działania te powinny odpowiadać bardziej bezpośrednio na szczególne potrzeby osób, które padły ofiarą oszustw wiążących się z kradzieżą tożsamości. Działania te powinny obejmować w szczególności specjalistyczne wsparcie psychologiczne i doradztwo w kwestiach finansowych, praktycznych i prawnych, a także pomoc w uzyskaniu dostępnych odszkodowań. Szczegółowe informacje i porady dotyczące sposobów ochrony przed niekorzystnymi skutkami takich przestępstw powinny być oferowane również osobom prawnym.

(22) Niniejsza dyrektywa powinna przyznać osobom prawnym prawo dostępu do informacji na temat procedury dotyczącej zawiadomienia o popełnieniu przestępstwa. To prawo do informacji jest konieczne zwłaszcza w przypadku małych i średnich przedsiębiorstw[51] – powinno ono przyczynić się do stworzenia bardziej przyjaznego otoczenia biznesowego dla tego rodzaju przedsiębiorstw. Osoby fizyczne korzystają już z tego prawa na mocy dyrektywy 2012/29/UE.

(23) Państwa członkowskie powinny ustanowić lub wzmocnić polityki zapobiegające fałszowaniu i oszustwom związanym z bezgotówkowymi środkami płatniczymi oraz środki zmniejszające ryzyko stania się ofiarą tego przestępstwa poprzez organizowanie kampanii informacyjnych i uświadamiających i prowadzenie programów badawczych i edukacyjnych.

(24) Istnieje potrzeba gromadzenia porównywalnych danych o przestępstwach określonych w niniejszej dyrektywie. Dane należy udostępniać właściwym wyspecjalizowanym agencjom i organom Unii, takim jak Europol, stosownie do ich zadań i potrzeb informacyjnych. Celem powinno być uzyskanie bardziej kompletnego obrazu problemu fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz kwestii związanych z bezpieczeństwem płatności na poziomie Unii, a tym samym przyczynienie się do opracowania skuteczniejszych mechanizmów

---

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[50] Dyrektywa Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiająca normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępująca decyzję ramową Rady 2001/220/WSiSW (Dz.U. L 315 z 14.11.2012, s. 57).

[51] Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

reagowania. Państwa członkowskie powinny wykorzystywać w pełni mandat i zdolności Europolu w zakresie udzielania pomocy i wsparcia w dochodzeniach, przekazując temu urzędowi informacje o metodach działania stosowanych przez przestępców, by mógł on dokonywać strategicznych analiz i ocen zagrożeń dotyczących fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794[52]. Przekazywanie tych informacji może przyczynić się do lepszego zrozumienia obecnych i przyszłych zagrożeń oraz pomóc Radzie i Komisji w określaniu priorytetów strategicznych i operacyjnych Unii w zakresie zwalczania przestępczości, a także we wdrażaniu tych priorytetów.

(25) Niniejsza dyrektywa służy zmianie i rozszerzeniu przepisów decyzji ramowej Rady 2001/413/WSiSW. Ponieważ proponowane zmiany są liczne i mają istotny charakter, dla zachowania przejrzystości należy zastąpić w całości decyzję ramową 2001/413/WSiSW w odniesieniu do państw członkowskich związanych niniejszą dyrektywą.

(26) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, te dwa państwa członkowskie powiadomiły o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.

ALBO

(26) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Zjednoczone Królestwo powiadomiło [, pismem z dnia ... r.,] o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.

ALBO

(26) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Irlandia powiadomiła [, pismem z dnia ... r.,] o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.

LUB

(26) Zgodnie z art. 1 i 2 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, te państwa członkowskie nie uczestniczą w przyjęciu niniejszej dyrektywy i nie są nią związane ani jej nie stosują.

ALBO

(26) Zgodnie z art. 1 i 2 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości,

[52] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana ani jej nie stosuje.

ALBO

(26) Zgodnie z art. 1 i 2 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, Zjednoczone Królestwo nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związane ani jej nie stosuje.

(27) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana ani jej nie stosuje.

(28) Ponieważ cele niniejszej dyrektywy, mianowicie zapewnienie, by fałszowanie i oszustwa związane z bezgotówkowymi środkami płatniczymi podlegały we wszystkich państwach członkowskich skutecznym, proporcjonalnym i odstraszającym sankcjom karnym, oraz poprawa transgranicznej współpracy między właściwymi organami, a także między osobami fizycznymi i prawnymi a właściwymi organami, jak również propagowanie tej współpracy, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na ich rozmiary i skutki możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(29) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, w tym z prawem do wolności i bezpieczeństwa, zasadą poszanowania życia prywatnego i rodzinnego, ochroną danych osobowych, wolnością prowadzenia działalności gospodarczej, prawem własności, prawem do skutecznego środka prawnego i dostępu do bezstronnego sądu, zasadą domniemania niewinności i prawem do obrony, zasadami legalności oraz proporcjonalności kar do czynów zabronionych pod groźbą kary, jak również zakazem ponownego sądzenia lub karania w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary. Niniejsza dyrektywa służy zapewnieniu pełnego poszanowania tych praw oraz zasad i musi być odpowiednio wdrażana,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

TYTUŁ I: PRZEDMIOT I DEFINICJE

Artykuł 1
Przedmiot

W niniejszej dyrektywie określa się normy minimalne odnoszące się do definicji przestępstw i określania kar w dziedzinie fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi.

Artykuł 2
Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

a) „instrument płatniczy” oznacza chronione urządzenia, przedmioty lub zapisy, inne niż prawny środek płatniczy, które – samodzielnie albo po zastosowaniu pewnej procedury lub szeregu procedur – umożliwiają posiadaczowi lub użytkownikowi dokonanie przekazu środków pieniężnych lub wartości pieniężnych albo zainicjowanie zlecenia płatniczego, w tym przy użyciu cyfrowych środków wymiany;

b) „chronione urządzenia, przedmioty lub zapisy” oznaczają urządzenie, przedmiot lub zapis zabezpieczone przed ich imitowaniem lub oszukańczym użyciem, na przykład przez sposób konstrukcji, kodowanie lub podpis;

c) „zlecenie płatnicze” oznacza zlecenie płatnicze zdefiniowane w art. 4 pkt 13 dyrektywy (UE) 2015/2366;

d) „cyfrowy środek wymiany” oznacza pieniądz elektroniczny zdefiniowany w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE[53] oraz waluty wirtualne;

e) „waluty wirtualne” oznaczają cyfrowe wyznaczniki wartości, które nie są emitowane przez bank centralny ani organ publiczny, nie muszą być powiązane z walutą fiducjarną, lecz są przyjmowane przez osoby fizyczne lub prawne jako środek płatniczy i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną;

f) „usługa płatnicza” oznacza usługę płatniczą zdefiniowaną w art. 4 pkt 3 dyrektywy (UE) 2015/2366;

g) „użytkownik usług płatniczych” oznacza użytkownika usług płatniczych zdefiniowanego w art. 4 pkt 10 dyrektywy (UE) 2015/2366;

h) „rachunek płatniczy” oznacza rachunek płatniczy zdefiniowany w art. 4 pkt 12 dyrektywy (UE) 2015/2366;

i) „transakcja płatnicza” oznacza transakcję płatniczą zdefiniowaną w art. 4 pkt 5 dyrektywy (UE) 2015/2366;

j) „płatnik” oznacza osobę fizyczną lub prawną, która jest posiadaczem rachunku płatniczego i zezwala na wykonanie zlecenia płatniczego z tego rachunku płatniczego, lub – w przypadku gdy rachunek płatniczy nie istnieje – osobę fizyczną lub prawną, która składa zlecenie płatnicze lub dokonuje przekazu waluty wirtualnej;

k) „odbiorca” oznacza odbiorcę zdefiniowanego w art. 4 pkt 9 dyrektywy (UE) 2015/2366;

l) „system informatyczny” oznacza system informatyczny zdefiniowany w art. 2 lit. a) dyrektywy 2013/40/UE;

---

[53] 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, s. 7).

m) „dane komputerowe” oznaczają dane komputerowe zdefiniowane w art. 2 lit. b) dyrektywy 2013/40/UE.

TYTUŁ II: PRZESTĘPSTWA

Artykuł 3
Oszukańcze użycie instrumentów płatniczych

Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby następujące czyny, gdy są popełniane umyślnie, były karalne jako przestępstwo:

a) oszukańcze użycie skradzionego lub przywłaszczonego w inny nielegalny sposób instrumentu płatniczego;

b) oszukańcze użycie podrobionego lub sfałszowanego instrumentu płatniczego.

Artykuł 4
Przygotowanie do oszukańczego użycia instrumentów płatniczych

Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby następujące czyny, gdy są popełniane umyślnie, były karalne jako przestępstwo:

a) kradzież lub innego rodzaju bezprawne przywłaszczenie instrumentu płatniczego;

b) podrabianie lub fałszowanie instrumentu płatniczego w celu użycia go w sposób oszukańczy;

c) posiadanie, pozyskiwanie z zamiarem wykorzystania, przywóz, wywóz, sprzedaż, transportowanie, dystrybucja lub inne udostępnianie skradzionego albo przywłaszczonego w inny nielegalny sposób instrumentu płatniczego lub podrobionego albo sfałszowanego instrumentu płatniczego z zamiarem oszukańczego wykorzystania.

Artykuł 5
Przestępstwa związane z systemami informatycznymi

Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by dokonanie lub spowodowanie dokonania przekazu środków pieniężnych, wartości pieniężnych lub walut wirtualnych z zamiarem uzyskania bezprawnej korzyści dla sprawcy lub osoby trzeciej były karalne jako przestępstwo, jeżeli czyny te są popełniane umyślnie poprzez:

a) zakłócanie funkcjonowania systemu informatycznego lub naruszenie jego integralności;

b) wprowadzanie, zmienianie, wykasowywanie, przekazywanie lub usuwanie danych komputerowych.

Artykuł 6
Narzędzia do popełniania przestępstw

Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby – w przypadku umyślnego działania z oszukańczym zamiarem – produkcja, pozyskiwanie z zamiarem wykorzystania, przywóz, wywóz, sprzedaż, transportowanie, dystrybucja lub inne udostępnianie urządzenia lub instrumentu, danych komputerowych lub innych środków

specjalnie przeznaczonych lub przystosowanych do celów popełnienia któregokolwiek z przestępstw, o których mowa w art. 4 lit. a) i b) lub w art. 5, były karalne jako przestępstwo.

Artykuł 7
Podżeganie, pomocnictwo oraz usiłowanie

1. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby wspomniane w art. 3–6 czyny polegające na podżeganiu do przestępstw lub pomocnictwu w nich były karalne jako przestępstwo.

2. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby wspomniane w art. 3–6 czyny polegające na usiłowaniu popełnienia przestępstwa były karalne jako przestępstwo.

Artykuł 8
Kary w przypadku osób fizycznych

1. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by przestępstwa, o których mowa w art. 3–7, podlegały skutecznym, proporcjonalnym i odstraszającym sankcjom karnym.

2. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by przestępstwa, o których mowa w art. 3, 4 i 5, podlegały karze pozbawienia wolności w maksymalnym wymiarze co najmniej trzech lat.

3. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by przestępstwa, o których mowa w art. 6, podlegały karze pozbawienia wolności w maksymalnym wymiarze co najmniej dwóch lat.

4. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by przestępstwa, o których mowa w art. 3, 4 i 5, podlegały karze pozbawienia wolności w maksymalnym wymiarze co najmniej pięciu lat, jeżeli:

   a) zostały popełnione w ramach organizacji przestępczej, w rozumieniu decyzji ramowej 2008/841/WSiSW, niezależnie od tego, jaki wymiar kary przewidziano w tej decyzji;

   b) wiązały się z rozległymi lub znaczącymi szkodami albo przyniosły sprawcy łączną korzyść wynoszącą co najmniej 20 000 EUR.

Artykuł 9
Odpowiedzialność osób prawnych

1. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by osoby prawne mogły zostać pociągnięte do odpowiedzialności za przestępstwa, o których mowa w art. 3–7, popełnione na ich korzyść przez jakąkolwiek osobę działającą indywidualnie albo jako członek organu osoby prawnej i pełniącą funkcje kierownicze w tej osobie prawnej, w oparciu o jedną z poniższych podstaw:

   a) prawo reprezentowania osoby prawnej;

   b) uprawnienie do podejmowania decyzji w imieniu osoby prawnej;

   c) uprawnienia kontrolne w danej osobie prawnej.

2. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by osoby prawne mogły zostać pociągnięte do odpowiedzialności w przypadku, gdy brak

nadzoru lub kontroli ze strony osoby, o której mowa w ust. 1, umożliwił popełnienie przez osobę jej podwładną, któregokolwiek z przestępstw, o których mowa w art. 3–7, na korzyść tej osoby prawnej.

3. Odpowiedzialność osoby prawnej na podstawie ust. 1 i 2 nie wyklucza postępowania karnego przeciw osobom fizycznym będącym sprawcami przestępstw określonych w art. 3–7, osobami podżegającymi do popełnienia tych przestępstw lub pomocnikami w tych przestępstwach.

Artykuł 10
Kary w przypadku osób prawnych

Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, by osoba prawna pociągnięta do odpowiedzialności na podstawie art. 9 ust. 1 podlegała skutecznym, proporcjonalnym i odstraszającym karom, obejmującym grzywny karne i grzywny niemające charakteru karnego i mogącym obejmować także inne sankcje, takie jak:

a) pozbawienie prawa do korzystania ze świadczeń publicznych lub pomocy publicznej;

b) czasowy lub stały zakaz prowadzenia działalności handlowej;

c) objęcie nadzorem sądowym;

d) sądowy nakaz likwidacji;

e) czasowe lub stałe zamknięcie zakładów wykorzystywanych do popełnienia przestępstwa.

TYTUŁ III: JURYSDYKCJA I PROWADZENIE DOCHODZEŃ

Artykuł 11
Jurysdykcja

1. Każde państwo członkowskie wprowadza środki niezbędne do ustanowienia swojej jurysdykcji w odniesieniu do przestępstw, o których mowa w art. 3–7, w przypadku gdy:

   a) przestępstwo zostało popełnione w całości albo w części na jego terytorium;

   b) sprawca jest jego obywatelem;

   c) przestępstwo wyrządziło szkodę na jego terytorium, w tym szkodę wynikającą z kradzieży tożsamości osoby.

2. Określając zakres swojej jurysdykcji zgodnie z ust. 1 lit. a), dane państwo członkowskie zapewnia, aby obejmowała ona przypadki, w których:

   a) sprawca popełnił przestępstwo, przebywając fizycznie na jego terytorium, niezależnie od tego, czy przestępstwo zostało popełnione przy użyciu komputerów lub systemów informatycznych znajdujących się na jego terytorium;

   b) przestępstwo zostało popełnione przy użyciu komputerów lub systemów informatycznych znajdujących się na jego terytorium, niezależnie od tego, czy sprawca popełnił przestępstwo, przebywając fizycznie na jego terytorium.

3. Państwo członkowskie informuje Komisję, jeżeli podejmie decyzję o ustanowieniu jurysdykcji w odniesieniu do jednego z przestępstw, o których mowa w art. 3–7, popełnionego poza jego terytorium, w tym również, jeżeli:

a) miejsce zwykłego pobytu sprawcy znajduje się na jego terytorium;

b) przestępstwo zostało popełnione na korzyść osoby prawnej mającej siedzibę na jego terytorium;

c) przestępstwo zostało popełnione wobec obywatela tego państwa albo wobec osoby mającej miejsce zwykłego pobytu na jego terytorium.

Artykuł 12
Skuteczne dochodzenia

1. Państwa członkowskie podejmują działania niezbędne do zapewnienia osobom, jednostkom lub służbom odpowiedzialnym za prowadzenie dochodzeń w sprawie przestępstw, o których mowa w art. 3–7, lub za ich ściganie, dostępu do skutecznych środków dochodzeniowych, takich jak narzędzia wykorzystywane w sprawach związanych z przestępczością zorganizowaną lub innymi poważnymi przestępstwami.

2. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia, aby w przypadku, gdy prawo krajowe nakłada na osoby fizyczne i prawne obowiązek przekazywania informacji dotyczących przestępstw, o których mowa w art. 3–7, informacje takie docierały bez zbędnej zwłoki do organów prowadzących dochodzenia w sprawie tych przestępstw lub zajmujących się ich ściganiem.

TYTUŁ IV: WYMIANA INFORMACJI I SKŁADANIE ZAWIADOMIEŃ O PRZESTĘPSTWACH

Artykuł 13
Wymiana informacji

1. Do celów wymiany informacji odnoszących się do przestępstw, o których mowa w art. 3–7, państwa członkowskie zapewniają istnienie operacyjnego krajowego punktu kontaktowego dostępnego 24 godziny na dobę oraz przez siedem dni w tygodniu. Państwa członkowskie zapewniają również istnienie procedur zapewniających szybkie rozpatrywanie pilnych wniosków o pomoc i wysyłanie przez właściwy organ, w ciągu ośmiu godzin od otrzymania wniosku, informacji co najmniej o tym, czy na wniosek zostanie udzielona odpowiedź oraz jaka będzie jej forma i termin przekazania. Państwa członkowskie mogą podjąć decyzję o wykorzystywaniu już istniejących sieci operacyjnych punktów kontaktowych.

2. Państwa członkowskie informują Komisję, Europol i Eurojust o swoich wyznaczonych punktach kontaktowych, o których mowa w ust. 1. Komisja przekazuje te informacje pozostałym państwom członkowskim.

Artykuł 14
Składanie zawiadomień o przestępstwach

1. Państwa członkowskie wprowadzają środki niezbędne do zapewnienia dostępności odpowiednich kanałów służących do składania zawiadomień w celu ułatwienia

niezwłocznego informowania właściwych organów ścigania i innych właściwych organów krajowych o przestępstwach, o których mowa w art. 3–7.

2. Państwa członkowskie wprowadzają środki niezbędne do zachęcenia instytucji finansowych i innych osób prawnych działających na ich terytorium do niezwłocznego zgłaszania domniemanych oszustw organom ścigania i innych właściwym organom, aby umożliwić im wykrywanie przestępstw, o których mowa w art. 3–7, i zapobieganie im, a także prowadzenie dochodzeń w sprawie tych przestępstw i ich ściganie.

TYTUŁ V: UDZIELANIE POMOCY OFIAROM PRZESTĘPSTW I ZAPOBIEGANIE

Artykuł 15
Pomoc i wsparcie dla ofiar przestępstw

1. Państwa członkowskie zapewniają, aby osobom fizycznym i prawnym, które doznały szkody w wyniku przestępstwa, o którym mowa w art. 3–7, popełnionego przez nadużycie danych osobowych, zaoferowano szczegółowe informacje i porady dotyczące sposobów ochrony przed niekorzystnymi skutkami przestępstwa, takimi jak uszczerbek dla reputacji.

2. Państwa członkowskie zapewniają, aby osobom prawnym będącym ofiarami przestępstw, o których mowa w art. 3–7 niniejszej dyrektywy, oferowano od momentu pierwszego kontaktu z właściwym organem i bez zbędnej zwłoki:

   a) informacje o procedurach dotyczących zawiadomienia o popełnieniu przestępstwa oraz roli ofiary w takich procedurach;

   b) informacje o dostępnych procedurach złożenia skargi w przypadku braku poszanowania praw ofiary przez właściwy organ w ramach postępowania karnego;

   c) dane kontaktowe na potrzeby przekazywania informacji o sprawie, która dotyczy ofiary.

Artykuł 16
Zapobieganie

Państwa członkowskie podejmują odpowiednie działania, w tym realizowane w internecie, takie jak kampanie informacyjne i uświadamiające, programy badawcze i edukacyjne, prowadzone w stosownych przypadkach we współpracy z zainteresowanymi stronami, aby zmniejszyć skalę oszustw, zwiększyć świadomość zagrożeń i ograniczyć ryzyko stania się ofiarą tego przestępstwa.

TYTUŁ VI: PRZEPISY KOŃCOWE

Artykuł 17
Monitorowanie i statystyki

1. Najpóźniej do dnia [3 miesiące po dniu wejścia w życie niniejszej dyrektywy] Komisja ustanowi szczegółowy program monitorowania produktów, rezultatów

i skutków niniejszej dyrektywy. Program monitorowania określa środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich będą one gromadzone. Wskazane są w nim również działania podejmowane przez Komisję i przez państwa członkowskie w celu gromadzenia, przekazywania i analizowania danych oraz innych dowodów.

2. Państwa członkowskie zapewniają istnienie systemu umożliwiającego rejestrowanie, produkcję i udostępnianie danych statystycznych mierzących zgłaszalność przestępstw, o których mowa w art. 3–7, a także prowadzenie dochodzeń i postępowań sądowych w ich sprawie.

3. Dane statystyczne, o których mowa w ust. 2, obejmują co najmniej liczbę przestępstw, o których mowa w art. 3–7, zgłoszonych państwom członkowskim, liczbę dochodzeń, liczbę osób oskarżonych o popełnienie przestępstw, o których mowa w art. 3–7, i osób skazanych za ich popełnienie oraz dane dotyczące zgłaszalności tych przestępstw oraz prowadzenia dochodzeń i postępowań sądowych w ich sprawie.

4. Państwa członkowskie przekazują corocznie Komisji dane zgromadzone zgodnie z ust. 1, 2 i 3. Komisja zapewnia opublikowanie raz w roku skonsolidowanego przeglądu tych sprawozdań statystycznych oraz przekazanie go właściwym wyspecjalizowanym agencjom i organom Unii.

Artykuł 18
Zastąpienie decyzji ramowej 2001/413/WSiSW

Zastępuje się decyzję ramową 2001/413/WSiSW w odniesieniu do państw członkowskich związanych niniejszą dyrektywą, bez uszczerbku dla zobowiązań tych państw członkowskich dotyczących terminu transpozycji tej decyzji ramowej do prawa krajowego.

W przypadku państw członkowskich związanych niniejszą dyrektywą odesłania do decyzji ramowej 2001/413/WSiSW traktuje się jako odesłania do niniejszej dyrektywy.

Artykuł 19
Transpozycja

1. Państwa członkowskie wprowadzają w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy do dnia [24 miesiące po jej wejściu w życie] r. Niezwłocznie informują o tym Komisję.

2. Środki przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

3. Państwa członkowskie przekazują Komisji tekst środków przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 20
Ocena i sprawozdawczość

1. Do dnia [48 miesięcy od dnia wejścia w życie] Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym ocenia, w jakim zakresie państwa członkowskie wprowadziły środki niezbędne do wykonania niniejszej dyrektywy. Państwa członkowskie dostarczają Komisji informacje niezbędne do przygotowania tego sprawozdania.

2. Do dnia [96 miesięcy od dnia wejścia w życie] Komisja dokonuje oceny niniejszej dyrektywy w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz przedkłada sprawozdanie Parlamentowi Europejskiemu i Radzie.

Artykuł 21
Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Niniejsza dyrektywa skierowana jest do państw członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia r.

W imieniu Parlamentu Europejskiego
Przewodniczący

W imieniu Rady
Przewodniczący