Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady" w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi oraz zastępującej decyzję ramową Rady 2001/413/WSiSW

[COM(2017) 489 final – 2017/0226 (COD)]

(2018/C 197/04)

Sprawozdawca **Victor ALISTAR**

Wniosek o konsultację	Parlament Europejski, 2.10.2017
	Rada, 25.10.2017
Podstawa prawna	Art. 83 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	18.12.2017
Data przyjęcia na sesji plenarnej	18.1.2018
Sesja plenarna nr	531
Wynik głosowania (za/przeciw/wstrzymało się)	129/0/1

1. **Wnioski i zalecenia**

1.1. EKES pochwala inicjatywę Komisji w kwestii nadania priorytetu walce z cyberprzestępczością będącą zjawiskiem wpływającym negatywnie na elektroniczne instrumenty płatnicze, choć należało wystąpić z nią dużo wcześniej. Korzyściom płynącym z digitalizacji powinny towarzyszyć mechanizmy reagowania na wyzwania z nią związane, tak aby gospodarka europejska i obywatele europejscy mogli w pełni korzystać z oferty społeczeństwa informacyjnego. EKES z zadowoleniem przyjmuje wniosek Komisji w zakresie, w jakim jego celem jest ochrona obywateli i przedsiębiorstw przed sieciami cyberprzestępców i w jakim przewidziano w nim środki, które mogą wzmocnić zaufanie do elektronicznych instrumentów płatniczych.

1.2. W ramach analizy wniosku dotyczącego dyrektywy EKES dostrzegł kilka niedociągnięć, które wymagają uwagi i skorygowania:

1.2.1. Aby uniknąć sporu kompetencyjnego pozytywnego, w art. 11 dotyczącym ustalania jurysdykcji w dziedzinie dochodzeń należy uściślić, czy podstawowym kryterium jest przebywanie sprawcy przestępstwa na danym terytorium, czy fakt, że na tym terytorium znajdują się systemy informatyczne użyte do popełnienia przestępstwa. W tym względzie EKES zwraca się o dodanie do artykułu nowego ustępu dotyczącego rozwiązywania konfliktów jurysdykcji zgodnie z jedną z dwóch metod zaproponowanych w niniejszej opinii.

1.2.2. We wniosku dotyczącym dyrektywy nie omówiono również w sposób skuteczny sytuacji, w której w sprawę zaangażowane są też inne jurysdykcje spoza UE, ani zasad odsyłania do innych prawnych instrumentów międzynarodowej współpracy sądowej, tak aby nieuchronne było wdrożenie przewidywalnych i określonych ram proceduralnych.

1.2.3. W art. 16 dotyczącym zapobiegania należy dodać specjalne środki, narzucone w przepisach transponujących państw członkowskich, w odniesieniu do obowiązku informacji, który spoczywałby albo na operatorach, którzy emitują elektroniczne produkty płatnicze, albo na krajowych organach regulacyjnych, lub też na organach odpowiedzialnych za edukację finansową.

1.2.4. Jeżeli chodzi o art. 12 i 13, należy również przewidzieć wymianę dobrych praktyk w dziedzinie wykrywania, prowadzenia dochodzeń i działań zaradczych w odniesieniu do cyberprzestępczości w obszarze oszustw związanych z elektronicznymi środkami płatniczymi.

1.3. Chociaż przedmiotowa dziedzina regulacyjna dotyczy współpracy w dziedzinie dochodzeń i współpracy sądowej w sprawach dotyczących oszustw informatycznych, należy również wprowadzić – za pomocą kampanii informacyjnych prowadzonych przez organy ścigania państw członkowskich – mechanizmy zniechęcające i mechanizmy informowania opinii publicznej odnośnie do sposobów działania przestępców.

1.4. W celu zagwarantowania skuteczności środków ochrony osób i osiągnięcia celów przedmiotowej inicjatywy, tj. poprawy zaufania do elektronicznych i cyfrowych instrumentów płatniczych, a także wyższego poziomu zgodności i prewencji, należy przewidzieć, tytułem uzupełnienia przepisów art. 15, wprowadzenie na mocy przepisów krajowych ubezpieczenia finansowego od oszustw, polegającego na obowiązku wypłacenia ofiarom odszkodowania pokrywającego 100 % szkody w przypadku oszustw informatycznych wobec posiadaczy elektronicznych instrumentów płatniczych. Takie odszkodowanie byłoby pobierane w ramach dochodzenia prowadzonego przez podmiot emitujący jako zainteresowaną stronę cywilną.

1.5. Aby zagwarantować skuteczność i efektywność polityki zwalczania fałszowania elektronicznych instrumentów płatniczych należy przewidzieć w dyrektywie obowiązek zgłaszania incydentów związanych z fałszywymi elektronicznymi instrumentami płatniczymi, na wzór obowiązku deklaracji w ramach polityki zwalczania prania pieniędzy lub rozporządzenia w sprawie ochrony danych osobowych.

1.6. EKES podkreśla konieczność wzmocnienia zdolności umożliwiających zrozumienie zjawiska oszustwa związanego z elektronicznymi i cyfrowymi środkami płatniczymi i zapobieganie mu poprzez wprowadzenie mechanizmu gromadzenia danych statystycznych w celu wzmocnienia strategii zapobiegania skutkom takich oszustw i korygowania tych skutków. Podobnie należy kontynuować ocenę wpływu środków transpozycji na szczeblu państw członkowskich oraz przewidzieć coroczne sprawozdania ilościowe wraz z przeprowadzaną co dwa lub trzy lata oceną jakościową skutków, aby umożliwić ocenę skuteczności tej polityki i określenie niezbędnych dostosowań.

1.7. Aby w perspektywie średnioterminowej zwiększyć skuteczność walki z oszustwami informatycznymi i fałszowaniem środków płatniczych, należy wzmocnić przepis art. 16 i jasno sprecyzować, że państwa członkowskie mają obowiązek rozwinąć specjalizację w tej dziedzinie przez waloryzację wiedzy specjalistycznej nabytej w obszarze dochodzeń oraz na podstawie wymiany doświadczeń, aby poprawić kompetencje ogólne absolwentów (w ramach kursów fakultatywnych) oraz ekspertów i śledczych (dzięki specjalistycznemu kształceniu ustawicznemu).

1.8. Ponadto Komitet uważa, że współpraca w terenie jest bezwzględnie konieczna i powinno się ją wspierać. Dotyczy to zarówno współpracy krajowej jak i transgranicznej w celu zwalczania tego typu przestępczości, a także jej zapobiegania. Wszystkie zainteresowane podmioty, zarówno z sektora publicznego, jak i prywatnego, powinny zostać włączone w te działania.

1.9. Proponuje się zastąpić w tytule dyrektywy termin „bezgotówkowe środki płatnicze" terminem „elektroniczne i cyfrowe środki płatnicze" w celu uniknięcia wszelkich nieścisłości co do przedmiotu dyrektywy.

2. **Wniosek Komisji**

2.1. Celem dyrektywy jest zapewnienie harmonizacji instrumentów i wzmocnienie zdolności państw członkowskich w dziedzinie prowadzenia dochodzeń w sprawie oszustw popełnionych za pomocą elektronicznych lub cyfrowych środków płatniczych. Wniosek dotyczący uregulowań ma sprzyjać współpracy transgranicznej między organami odpowiedzialnymi za dochodzenia oraz wprowadzeniu szeregu środków dotyczących tej współpracy, a także minimalnych norm wspólnych w dziedzinie prewencji, pomocy ofiarom i odpowiedzialności emitentów tych instrumentów. W związku z tym przyjęte podejście polega na zdefiniowaniu zakresu stosowania instrumentu, co ma zapewnić neutralną pod względem technologicznym perspektywę.

2.2. W kontekście postępu technologicznego i dywersyfikacji sposobów działania w dziedzinie przestępstw informatycznych, w tym strategii stosowanych przez grupy przestępcze, Komisja uznaje w „Strategii jednolitego rynku cyfrowego dla Europy" ([1]), że decyzja ramowa nie jest wystarczająca, aby stawić czoło nowym wyzwaniom i postępom technologicznym takim jak waluty wirtualne i płatności mobilne.

2.3. W zakresie, w jakim karty stanowią najważniejszy bezgotówkowy sposób płatności w UE pod względem liczby transakcji, oszustwa związane z kartami wystawionymi w strefie euro osiągnęły w 2013 r. poziom 1,44 mld EUR według danych Europejskiego Banku Centralnego i wciąż przybierają na sile ([2]). 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]).

2.4. Z analizy Komisji wynika, że jeden z profilów najbardziej narażonych na przestępstwo związany jest z korzystaniem z płatności elektronicznych do opłacenia kosztów podróży – biletów kolejowych i samolotowych, noclegów i innych powiązanych operacji wykraczających poza te wymienione.

([1]) COM(2015) 192 final.

([2]) Europejski Bank Centralny, *Fourth report on card fraud* [Czwarte sprawozdanie na temat oszustw popełnianych za pomocą kart płatniczych], lipiec 2015 r. (ostatnie dostępne dane).

([3]) Zob. przypis 2.

2.5. Jeżeli chodzi o zakres regulacyjny, wniosek Komisji ma zapewnić solidne i neutralne technologicznie ramy, wyeliminować przeszkody operacyjne i wzmocnić zapobieganie oszustwom związanym z bezgotówkowymi środkami płatniczymi.

2.6. Aby zagwarantować dostęp do skutecznych środków walki z przestępstwami związanymi z elektronicznymi instrumentami płatniczymi i przestępczością informatyczną, wniosek dotyczący dyrektywy wprowadza wspólne zasady w przepisach krajowych dotyczące: przestępstw przewidzianych w prawie karnym w dziedzinie oszustw informatycznych związanych ze środkami płatniczymi; udziału w przestępstwach i polityki karnej w dziedzinie kar; odpowiedzialności prawnej osób prawnych i wprowadzenia jednolitych kar o charakterze zniechęcającym. EKES zwraca uwagę na nowatorski aspekt wniosku, który zawiera pierwsze przepisy dotyczące elektronicznych walut wirtualnych w prawie Unii Europejskiej. Definicja przestępstw obejmuje zachowania, które – mimo że nie są bezpośrednio oszustwami sensu stricto – zostały popełnione z myślą o oszustwie (kradzież i fałszowanie, ale również sprzedaż i sam fakt posiadania skradzionych instrumentów płatniczych).

2.7. Aby poprawić skuteczność współpracy europejskiej w dziedzinie walki z przestępczością informatyczną i oszustwami związanymi z elektronicznymi instrumentami płatniczymi, w dyrektywie przewidziano wprowadzenie konkretnych i odpowiednich przepisów dotyczących mechanizmów instytucjonalnych i kompetencji w dziedzinie dochodzeń na szczeblu państw członkowskich, a także przepisów dotyczących europejskiego mechanizmu wymiany informacji między organami krajowymi.

2.8. Bardzo ważnym elementem wniosku jest ustanowienie obowiązku wprowadzenia skutecznych środków obrony interesów ofiar, które zagwarantują im dostęp do skutecznego środka prawnego.

2.9. Wniosek Komisji wpisuje się w całej rozciągłości w zakres kompetencji regulacyjnych Unii Europejskiej zdefiniowanych w art. 83 Traktatu o funkcjonowaniu Unii Europejskiej i wprowadza wymóg minimalnej harmonizacji na szczeblu państw członkowskich w ramach 24-miesięcznego okresu transpozycji.

3. **Uwagi ogólne**

3.1. Wybrana opcja regulacyjna jest o wiele bardziej dostosowana, mając na uwadze, że w dyrektywie można wprowadzić ramy prawnie obowiązujące na szczeblu wszystkich jurysdykcji krajowych (z wyjątkiem Danii, jeżeli to państwo nie zechce ich przyjąć), co wykracza poza ujednolicenie praktyk przewidziane w decyzji ramowej 2001/413/WSiSW, bez uszczerbku dla treści.

3.2. EKES stwierdza, że projekt dyrektywy tworzy synergię z innymi instrumentami regulacyjnymi, w których uczestniczą państwa członkowskie, i uzupełnia inne strategie polityczne Unii, takie jak paneuropejskie mechanizmy współpracy w sprawach karnych, a także akty prawne mające na celu zwalczanie oszustw informatycznych i prania pieniędzy. W tym kontekście należy również podkreślić konieczność zapewnienia korelacji między badanym problemem a środkami ochrony danych osobowych posiadanych przez instytucje finansowe, a także środków z zakresu cyberbezpieczeństwa.

3.3. Po pierwsze, na szczeblu Unii Europejskiej istnieje szereg instrumentów prawnych, które określają zasady niezbędne na poziomie rynków finansowych i usług finansowych i ustanawiają obowiązki w zakresie należytej staranności w związku z wydawaniem instrumentów płatniczych, zarządzaniem nimi i ich zabezpieczaniem, lecz wniosek dotyczący dyrektywy zawiera niezbędne rozwiązania w dziedzinie wzmocnienia infrastruktury prawnej w zakresie sprawozdań, dochodzeń i kar w odniesieniu do oszustw informatycznych dotyczących środków płatniczych.

3.4. EKES podkreśla konieczność wzmocnienia zdolności umożliwiających zrozumienie zjawiska oszustwa związanego z elektronicznymi i cyfrowymi środkami płatniczymi oraz zapobieganie mu poprzez wprowadzenie mechanizmu gromadzenia danych statystycznych w celu wzmocnienia strategii zapobiegania skutkom takich oszustw i korygowania tych skutków. Podobnie należy kontynuować ocenę wpływu środków transpozycji na szczeblu państw członkowskich oraz przewidzieć coroczne sprawozdania ilościowe wraz z przeprowadzaną co dwa lub trzy lata oceną jakościową skutków, aby umożliwić ocenę skuteczności tej polityki i określenie niezbędnych dostosowań.

3.5. Ponadto w zakresie, w jakim zostaną wdrożone elementy odpowiedzialności prawnej osób prawnych oraz kary w ramach solidniejszego mechanizmu gwarancji środków prawnych, należy przypomnieć o konieczności wprowadzenia instrumentów wsparcia podmiotów, które dostarczają produkty do płatności elektronicznych lub korzystają z platform płatności internetowych, aby umożliwić im dostosowanie się do uregulowań sektorowych ([4]).

([4]) Dz.U. L 267 z 10.10.2009, s. 7.

3.6. Jeżeli chodzi o mechanizm wymiany informacji na temat dochodzeń w sprawie oszustw związanych z instrumentami płatniczymi w kontekście cyberprzestępczości, o którym mowa w art. 13 i 14 wniosku dotyczącego dyrektywy, należy przewidzieć przekazanie uprawnień Komisji w celu wprowadzenia uregulowań w formie aktów delegowanych zarówno w kwestii matrycy wymiany informacji, jak i znormalizowanych danych do sprawozdań w sprawach będących przedmiotem dochodzeń.

3.7. Jeżeli chodzi o prewencję, jeżeli Komisja wprowadza w komunikacie odniesienie do podobnego mechanizmu przyjętego na podstawie dyrektywy 2011/93/UE, to EKES uważa, że należałoby, po pierwsze, zwiększyć przejrzystość w kwestii obowiązków przewidzianych w odniesieniu do środków zapobiegania, a po drugie, wprowadzić szereg obowiązków w dziedzinie informowania opinii publicznej o przyczynach, ryzyku i indywidualnych sposobach prewencji, aby unikać oszustw związanych z finansowymi instrumentami płatniczymi, popełnionych przez sieci cyberprzestępców z użyciem pułapek.

3.8. Należy opracować specjalizacje w tej dziedzinie przez waloryzację wiedzy specjalistycznej w zakresie prowadzenia dochodzeń, na podstawie wymiany doświadczeń, aby, po pierwsze, poprawić ogólne kompetencje absolwentów nauczania ogólnego w ramach kursów fakultatywnych, a po drugie, opracować ramy kompetencji dla ekspertów i śledczych za pomocą specjalnych programów szkoleń.

3.9. Ważne jest zapewnienie skutecznej współpracy w terenie w celu zwalczania takich przestępstw. Współpraca ta powinna odbywać się w różnych dziedzinach i, o ile to możliwe, muszą być w nią zaangażowane wszystkie zainteresowane strony. Powinno to pozwolić nie tylko na zwalczanie tej poważnej formy przestępczości, lecz także na zapobieganie jej zarówno na poziomie krajowym jak i transgranicznym.

3.10. We wniosku dotyczącym dyrektywy nie omówiono również w sposób skuteczny sytuacji, w której w sprawę zaangażowane są też inne jurysdykcje spoza UE, ani zasad odsyłania do innych prawnych instrumentów międzynarodowej współpracy sądowej, tak aby nieuchronne było wdrożenie przewidywalnych i określonych ram proceduralnych.

3.11. Chociaż przedmiotowa dziedzina regulacyjna dotyczy współpracy w dziedzinie dochodzeń i współpracy sądowej w sprawach dotyczących oszustw informatycznych, należy również wprowadzić – za pomocą kampanii informacyjnych prowadzonych przez organy ścigania państw członkowskich – mechanizmy zniechęcające i mechanizmy informowania opinii publicznej odnośnie do sposobów działania przestępców. W związku z tym w przepisach końcowych wniosku należy wprowadzić odniesienie do międzynarodowych instrumentów współpracy sądowej w sprawach karnych, o których będzie mowa w sytuacjach związanych z eksterytorialnością i ze sposobami prowadzenia dochodzeń z użyciem tych mechanizmów. W kwestii proceduralnej chodzi o przydatny instrument regulacyjny mający wartość uściślającą.

4. **Konkretne propozycje**

4.1. W art. 11 dotyczącym ustalania jurysdykcji w dziedzinie dochodzeń należy uściślić, czy podstawowym kryterium jest przebywanie sprawcy przestępstwa na danym terytorium, czy fakt, że na tym terytorium znajdują się systemy informatyczne użyte do popełnienia przestępstwa, aby uniknąć sporu kompetencyjnego pozytywnego między sytuacją, o której mowa w art. 11 ust. 2 lit. a), odnoszącą się do fizycznej obecności sprawcy, a sytuacją, o której mowa w art. 11 ust. 2 lit. b), w przypadku gdy sprawca popełnił przestępstwo na terytorium danego państwa członkowskiego, lecz przy użyciu mechanizmu z dostępem zdalnym (ang. remote shell). Wówczas jurysdykcję mogą mieć dwa państwa członkowskie Unii, których ta sytuacja dotyczy. W art. 11 należy wprowadzić nowy ustęp dotyczący rozwiązywania sporów kompetencyjnych, tj. albo przez wyznaczenie podmiotu, któremu zostanie powierzone takie zadanie (np. Eurojust), albo przez odesłanie do podobnego mechanizmu rozwiązywania sporów (np. do decyzji ramowej 2009/948/WSiSW ([5])).

4.2. W art. 16 dotyczącym zapobiegania należy dodać specjalne środki, narzucone w przepisach transponujących państw członkowskich, w odniesieniu do obowiązku informacji, który spoczywałby albo na operatorach, którzy emitują elektroniczne produkty płatnicze, albo na krajowych organach regulacyjnych lub też na organach odpowiedzialnych za edukację finansową.

4.3. Jeżeli chodzi o obowiązek stworzenia mechanizmu wymiany informacji na temat dochodzeń dotyczących oszustw, o którym mowa w art. 13 wniosku dotyczącego dyrektywy, należy utworzyć pojedynczy punkt kontaktowy na wzór tego, który istnieje w dziedzinie walki z praniem pieniędzy czy w dziedzinie bezpieczeństwa żywnościowego, aby zagwarantować spójność na szczeblu europejskim. Pojedynczym punktem kontaktowym może być albo ministerstwo sprawiedliwości, albo podmiot posiadający kompetencje w odniesieniu do większości jurysdykcji UE. EKES uważa, że określenie „odpowiednie kanały służące do składania zawiadomień" mogłoby częściowo zaspokajać potrzebę skuteczności, lecz nie harmonizacji.

([5]) Dz.U. L 328 z 15.12.2009, s. 42.

4.4. Jeżeli chodzi o art. 12 i 13, należy również przewidzieć wymianę dobrych praktyk w dziedzinie wykrywania, prowadzenia dochodzeń i działań zaradczych w odniesieniu do przypadków cyberprzestępczości opartych na oszustwach związanych z elektronicznymi środkami płatniczymi.

4.5. W celu zagwarantowania skuteczności środków ochrony osób i osiągnięcia celów przedmiotowej inicjatywy, tj. poprawy zaufania do elektronicznych instrumentów płatniczych, a także wyższego poziomu zgodności i prewencji, należy przewidzieć, tytułem uzupełnienia przepisów art. 15, wprowadzenie na mocy przepisów krajowych ubezpieczenia finansowego od oszustw polegającego na obowiązku wypłacenia ofiarom odszkodowania pokrywającego 100 % szkody w przypadku oszustw informatycznych wobec posiadaczy elektronicznych instrumentów płatniczych. Takie odszkodowanie byłoby pobierane w ramach dochodzenia prowadzonego przez podmiot emitujący jako zainteresowaną stronę cywilną. Takie gwarancje powinny obejmować również szkody poniesione przez specjalistów reprezentowanych przez MŚP w przypadku braku uregulowania kwot do rozsądnego pułapu wyznaczonego na szczeblu państw członkowskich.

4.6. Aby zagwarantować skuteczność i efektywność polityki zwalczania fałszowania elektronicznych instrumentów płatniczych należy przewidzieć w dyrektywie obowiązek zgłaszania incydentów związanych z fałszywymi elektronicznymi instrumentami płatniczymi, na wzór obowiązku deklaracji w ramach polityki zwalczania prania pieniędzy lub rozporządzenia w sprawie ochrony danych osobowych.

Bruksela, dnia 18 stycznia 2018 r.

Georges DASSIS
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego