Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych"

[COM(2020) 823 final – 2020/0359 (COD) – COM(2020) 829 final – 2020/0365 (COD)]

(2021/C 286/28)

Sprawozdawca: **Maurizio MENSI**

Wniosek o konsultację	Parlament Europejski, 21.1.2021–11.2.2021
	Rada, 26.1.2021–19.2.2021
Podstawa prawna	Art. 114 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	14.4.2021
Data przyjęcia na sesji plenarnej	27.4.2021
Sesja plenarna nr	560
Wynik głosowania	
(za/przeciw/wstrzymało się)	243/0/5

1. **Wnioski i zalecenia**

1.1. EKES docenia wysiłki Komisji na rzecz zwiększenia odporności podmiotów publicznych i prywatnych na zagrożenia wynikające z incydentów i ataków cybernetycznych i fizycznych. Zgadza się z potrzebą wzmocnienia przemysłu UE i jej zdolności do innowacji w sposób inkluzywny, zgodnie ze strategią opartą na czterech filarach: ochronie danych, prawach podstawowych, bezpieczeństwie i cyberbezpieczeństwie.

1.2. EKES podkreśla jednak, że ze względu na istotny i wrażliwy charakter celów realizowanych w obu wnioskach bardziej wskazany od dyrektywy byłby instrument rozporządzenia. Niejasne są zresztą powody, dla których Komisja nie uznała za konieczne, by uwzględnić taką możliwość pośród różnych rozważanych wariantów.

1.3. EKES zauważa, że niektóre z przepisów obu wniosków dotyczących dyrektywy pokrywają się, ponieważ są ściśle ze sobą powiązane i komplementarne: jeden z nich dotyczy przede wszystkim profili cyberbezpieczeństwa, a drugi – bezpieczeństwa fizycznego. W związku z tym wzywa do zastanowienia się, czy mając na względzie uproszczenie i usprawnienie, tych dwóch wniosków nie należałoby połączyć w jeden dokument.

1.4. EKES zgadza się z proponowanym podejściem polegającym na wyeliminowaniu rozróżnienia między operatorami usług kluczowych a dostawcami usług cyfrowych, o którym mowa w pierwotnej dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS). Zwraca jednak uwagę, że w odniesieniu do jej zakresu stosowania należy zapewnić bardziej precyzyjne i jaśniejsze wskazówki co do tego, kto jest zobowiązany do przestrzegania jej przepisów. W szczególności należy dokładniej zdefiniować kryteria odróżniające podmioty „niezbędne" od „istotnych", a także obowiązujące je wymogi, aby nie dopuścić do tego, by rozbieżne podejścia na szczeblu krajowym powodowały przeszkody w konkurencji i swobodnym przepływie towarów i usług, co mogłoby działać na szkodę przedsiębiorstw i wymiany handlowej.

1.5. EKES uważa, że ze względu na obiektywną złożoność systemu przedstawionego w obu wnioskach ważne jest, by Komisja dokładnie wyjaśniła zakres stosowania tych dwóch zbiorów przepisów, zwłaszcza gdy różne przepisy przyczyniają się do uregulowania tego samego przypadku lub podmiotu.

1.6. EKES podkreśla, że nieodzownym celem jest jasność wszelkich przepisów prawnych, a także ograniczenie biurokracji i fragmentacji poprzez uproszczenie procesów oraz wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Również w tym celu, z korzyścią dla obywatelek i obywateli oraz przedsiębiorstw, wskazane mogłoby być połączenie w jeden tekst obu wniosków dotyczących dyrektywy, dzięki czemu uniknięto by skomplikowanego niekiedy procesu interpretacji i egzekwowania.

1.7. EKES uznaje podkreśloną we wniosku dotyczącym dyrektywy zasadniczą rolę organów zarządzających podmiotów niezbędnych i istotnych, których członkinie i członkowie muszą regularnie przechodzić specjalne szkolenia w celu zdobycia wiedzy i umiejętności wystarczających do poznania różnych zagrożeń cybernetycznych, zarządzania nimi i oceny ich skutków. W związku z tym uważa, że we wniosku należy wskazać minimalny zakres takiej wiedzy i umiejętności, tak by na szczeblu europejskim dostępne były wytyczne dotyczące tego, które kompetencje nabywane na szkoleniach uznaje się za stosowne, i by nie dopuścić do różnic w treści kursów szkoleniowych między poszczególnymi krajami.

1.8. EKES zgadza się co do istotnej roli ENISA w całościowej strukturze instytucjonalnej i operacyjnej cyberbezpieczeństwa na szczeblu europejskim. Uważa w tym względzie, że oprócz sporządzanego co dwa lata sprawozdania na temat stanu cyberbezpieczeństwa w Unii oraz zawiadomień dla poszczególnych sektorów organ ten powinien publikować w internecie okresowe i aktualne informacje na temat cyberincydentów. Powinno to być dla podmiotów, których dotyczy NIS 2, dodatkowe przydatne narzędzie informacyjne umożliwiające lepszą ochronę ich przedsiębiorstw.

1.9. EKES zgadza się z propozycją powierzenia ENISA zadania stworzenia europejskiego rejestru podatności i uważa, że zgłaszanie najpoważniejszych podatności i incydentów powinno być obowiązkowe, a nie dobrowolne i tym samym stać się pomocnym narzędziem również dla podmiotów zamawiających w postępowaniach o udzielenie zamówienia na szczeblu europejskim, w tym zamawiających produkty i technologie dla 5G.

2. **Uwagi ogólne**

2.1. Dnia 16 grudnia 2020 r. przedstawiono nową strategię UE w zakresie cyberbezpieczeństwa wraz z dwoma wnioskami ustawodawczymi: przeglądem dyrektywy (UE) 2016/1148 ([1]) w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS 2) oraz nową dyrektywą w sprawie odporności podmiotów krytycznych. Strategia ta, która jest kluczowym elementem komunikatu „Kształtowanie cyfrowej przyszłości Europy" ([2]), planu odbudowy dla Europy i strategii UE w zakresie unii bezpieczeństwa, ma na celu zwiększenie zbiorowej odporności Europy na zagrożenia dla cyberbezpieczeństwa oraz zagwarantowanie wszystkim obywatelkom i obywatelom oraz przedsiębiorstwom możliwości korzystania z niezawodnych i bezpiecznych usług i narzędzi cyfrowych.

2.2. Należy zaktualizować istniejące środki na szczeblu UE mające na celu ochronę usług krytycznych i infrastruktury krytycznej przed zagrożeniami sieciowymi i fizycznymi. Zagrożenia dla cyberbezpieczeństwa w dalszym ciągu ewoluują wraz ze wzrostem cyfryzacji i łączności. W związku z tym należy dokonać przeglądu obowiązujących ram regulacyjnych zgodnie z podejściem przyjętym w strategii bezpieczeństwa UE, odchodząc od podziału na świat wirtualny i realny oraz od schematycznego myślenia.

2.3. Oba wnioski dotyczące dyrektywy obejmują szeroki zakres sektorów i uwzględniają obecne i przyszłe zagrożenia, zarówno w internecie, jak i poza nim, wynikające z ataków cybernetycznych i przestępczych, klęsk żywiołowych i innych incydentów. Są one również oparte na wnioskach płynących z trwającej pandemii, która pokazała, że społeczeństwo i gospodarka są coraz bardziej zależne od rozwiązań cyfrowych i tym samym bardziej podatne i narażone na nasilające się i szybko zmieniające się zagrożenia dla cyberbezpieczeństwa, zwłaszcza w grupach zagrożonych wykluczeniem społecznym, takich jak osoby z niepełnosprawnościami. Skłoniło to UE do zaproponowania działań mających na celu ochronę globalnej i otwartej cyberprzestrzeni, opartych na solidnych gwarancjach bezpieczeństwa, suwerenności technologicznej i przywództwie poprzez rozwijanie zdolności operacyjnych ukierunkowanych na zapobieganie ewentualnym zagrożeniom, zniechęcanie do stwarzania tych zagrożeń i reagowanie na nie w drodze ściślejszej współpracy, z poszanowaniem prerogatyw państw członkowskich w zakresie bezpieczeństwa narodowego.

3. **Wniosek dotyczący zmiany dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych**

3.1. Dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych (UE) 2016/1148 – pierwszy unijny „horyzontalny" instrument regulacyjny w dziedzinie cyberbezpieczeństwa – miała na celu zwiększenie odporności systemów sieciowych i informatycznych w Unii na zagrożenia dla cyberbezpieczeństwa. Pomimo osiągnięcia dobrych wyników dyrektywa w sprawie bezpieczeństwa sieci i informacji miała też jednak pewne ograniczenia, gdyż transformacja cyfrowa społeczeństwa przybrała na sile wskutek kryzysu związanego z COVID-19 i poszerzyła zakres zagrożeń,

([1]) Dz.U. L 194 z 19.7.2016, s. 1.
([2]) COM(2020) 67 final.

zwiększając podatność coraz bardziej od siebie zależnych społeczeństw na istotne i nieprzewidziane ryzyko. Pojawiły się nowe wyzwania, wymagające odpowiednich i innowacyjnych rozwiązań. Wyniki szeroko zakrojonych konsultacji z zainteresowanymi stronami unaoczniły niewystarczający poziom cyberbezpieczeństwa europejskich przedsiębiorstw, niespójne stosowanie przepisów przez państwa w różnych sektorach oraz brak zrozumienia głównych zagrożeń i wyzwań.

3.2. Wniosek dotyczący NIS 2 jest ściśle powiązany z dwiema innymi inicjatywami: wnioskiem dotyczącym rozporządzenia w sprawie sektora finansów cyfrowych (Digital Operational Resilience Act, DORA) oraz wnioskiem dotyczącym dyrektywy w sprawie podmiotów krytycznych, który rozszerza zakres stosowania dyrektywy 2008/114/WE ([3]) dotyczącej energii i transportu na nowe sektory, skupiając się na przykład na sektorze opieki zdrowotnej i podmiotach prowadzących prace badawcze i rozwojowe w dziedzinie leków. Dyrektywa w sprawie podmiotów krytycznych, która ma taki sam zakres sektorowy jak NIS 2 w odniesieniu do podmiotów niezbędnych (załącznik 1 do NIS 2), przenosi swój punkt ciężkości z ochrony aktywów rzeczowych na odporność podmiotów nimi zarządzających i przechodzi od wskazania europejskiej infrastruktury krytycznej o wymiarze transgranicznym do określenia infrastruktury krytycznej na poziomie krajowym. NIS 2 jest ponadto spójna i komplementarna wobec innych obowiązujących instrumentów prawnych, takich jak Europejski kodeks łączności elektronicznej, ogólne rozporządzenie o ochronie danych oraz rozporządzenie eIDAS w sprawie identyfikacji elektronicznej i usług zaufania.

3.3. Zgodnie z programem sprawności i wydajności regulacyjnej (REFIT) wniosek dotyczący dyrektywy NIS 2 ma na celu zmniejszenie obciążeń regulacyjnych spoczywających na właściwych organach oraz kosztów przestrzegania przepisów przez podmioty publiczne i prywatne i aktualizuje odnośne ramy prawne. Ulepszono w nim ponadto wymogi w zakresie bezpieczeństwa nakładane na przedsiębiorstwa, poruszono kwestię bezpieczeństwa łańcuchów dostaw, zracjonalizowano wymogi sprawozdawcze, wprowadzono bardziej rygorystyczne środki nadzorcze dla organów krajowych i podjęto wysiłek harmonizacji systemów sankcji w państwach członkowskich.

3.4. NIS 2 przyczynia się również do rozwinięcia wymiany informacji i współpracy w zakresie zarządzania kryzysami cyberbezpieczeństwa na szczeblu krajowym i europejskim. Usunięto przewidziane w dyrektywie NIS rozróżnienie między operatorami usług kluczowych a dostawcami usług cyfrowych. Zakres stosowania wniosku obejmuje średnie lub duże przedsiębiorstwa w sektorach wskazanych na podstawie krytycznego znaczenia dla gospodarki i społeczeństwa. Podmioty te, publiczne lub prywatne, podzielono na „niezbędne" i „istotne", które podlegają różnym systemom nadzoru. Państwa członkowskie mają jednak możliwość uwzględnienia również mniejszych podmiotów o wysokim profilu ryzyka.

3.5. Przewiduje się nową ogólnounijną sieć centrów monitorowania bezpieczeństwa (SOC) opartych na sztucznej inteligencji, które będą zapewniać prawdziwą ochronę cyberbezpieczeństwa i będą zdolne do wykrywania sygnałów cyberataku z wystarczającym wyprzedzeniem, tak by można było interweniować przed wystąpieniem szkód. Znaczenie sztucznej inteligencji dla cyberbezpieczeństwa podkreślono również w przedstawionym w dniu 1 marca 2021 r. sprawozdaniu Narodowej Komisji Bezpieczeństwa (NSCAI) USA w sprawie sztucznej inteligencji (SI). W konsekwencji państwa członkowskie i operatorzy infrastruktury krytycznej będą mieli bezpośredni dostęp do informacji o zagrożeniach w ramach europejskiej sieci bezpieczeństwa „threat intelligence" (analiza zagrożeń).

3.6. Komisja porusza ponadto kwestię bezpieczeństwa łańcuchów dostaw i stosunków z dostawcami: państwa członkowskie we współpracy z Komisją i ENISA mogą przeprowadzać skoordynowane oceny ryzyka krytycznych łańcuchów dostaw w oparciu o przyjęte z powodzeniem podejście do sieci 5G, które zostało przewidziane w zaleceniu z dnia 26 marca 2019 r. ([4]).

3.7. Wniosek wzmacnia i optymalizuje obowiązki przedsiębiorstw w zakresie bezpieczeństwa i sprawozdawczości, wprowadzając wspólne podejście do zarządzania ryzykiem wraz z minimalnym wykazem podstawowych zabezpieczeń, które należy stosować. Ustanawia się bardziej precyzyjne przepisy dotyczące procesu zgłaszania incydentów, treści sprawozdań oraz terminów. W tym względzie nakreślono dwuetapowe podejście: przedsiębiorstwa mają 24 godziny na przedstawienie pierwszego sprawozdania podsumowującego, a następnie miesiąc – na szczegółowe sprawozdanie końcowe.

([3]) Dz.U. L 345 z 23.12.2008, s. 75.
([4]) Dz.U. L 88 z 29.3.2019, s. 42.

3.8. Przewiduje się, że państwa członkowskie wskażą organy krajowe odpowiedzialne za zarządzanie kryzysowe. W tym celu proponuje się szczegółowe plany i nową sieć współpracy operacyjnej – europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe). Wzmacnia się rolę Grupy Współpracy w podejmowaniu decyzji strategicznych oraz ustanawia zarządzany przez ENISA rejestr podatności wykrywanej w UE; rozwija się ponadto wymianę informacji i współpracę między organami państw członkowskich, w tym współpracę operacyjną w zakresie zarządzania cyberkryzysami.

3.9. Wprowadza się bardziej rygorystyczne środki nadzorcze dla organów krajowych oraz surowsze wymogi w zakresie egzekwowania przepisów i dąży się do harmonizacji systemów sankcji we wszystkich państwach członkowskich.

3.10. W tym względzie we wniosku dotyczącym dyrektywy ustanawia się wykaz sankcji administracyjnych za niespełnienie obowiązków w zakresie zarządzania ryzykiem dotyczącym bezpieczeństwa sieci informatycznych i komunikacji. Przewiduje się przepisy dotyczące odpowiedzialności osób fizycznych piastujących stanowiska reprezentacyjne lub kierownicze w spółkach, które wchodzą w zakres stosowania dyrektywy. W tym względzie wniosek usprawnia sposób, w jaki UE zapobiega incydentom i kryzysom związanym z cyberbezpieczeństwem na dużą skalę, zarządza nimi i reaguje na nie, wprowadzając jasne obowiązki, odpowiednie planowanie i wzmocnioną współpracę na szczeblu UE.

3.11. Umożliwia się państwom członkowskim wspólny nadzór nad wdrażaniem przepisów UE i wzajemną pomoc w przypadku problemów transgranicznych, ustanawia się bardziej zorganizowany dialog z sektorem prywatnym, koordynuje się ujawnianie podatności w oprogramowaniu i sprzęcie wprowadzanym do obrotu na rynku wewnętrznym, ocenia się zagrożenia dla bezpieczeństwa i zagrożenia związane z nowymi technologiami w skoordynowany sposób, jak miało to miejsce w przypadku sieci 5G.

4. **Wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych**

4.1. W 2006 r. UE ustanowiła europejski program ochrony infrastruktury krytycznej (EPCIP), a w 2008 r. przyjęła dyrektywę w sprawie europejskiej infrastruktury krytycznej (EIK), która ma zastosowanie do sektorów energii i transportu. Znaczenie zagwarantowania odporności infrastruktury krytycznej na zagrożenia fizyczne i cyfrowe podkreślono tak w strategii UE w zakresie unii bezpieczeństwa na lata 2020–2025 ([5]) przyjętej przez Komisję Europejską, jak i w niedawno przyjętym programie zwalczania terroryzmu. Jednak zarówno przeprowadzona w 2019 r. ocena wdrożenia dyrektywy w sprawie EIK, jak i wyniki oceny skutków omawianego wniosku wykazały, że obowiązujące środki europejskie i krajowe nie gwarantują w wystarczającym stopniu, że operatorzy potrafią stawić czoła obecnym zagrożeniom. Z tego wynikają apele Rady i Parlamentu zaadresowane do Komisji, by dokonała przeglądu obecnego podejścia do ochrony infrastruktury krytycznej.

4.2. W strategii UE w zakresie unii bezpieczeństwa przyjętej przez Komisję w dniu 24 lipca 2020 r. dostrzeżono rosnące wzajemne połączenia i współzależność infrastruktury fizycznej i cyfrowej, podkreślając potrzebę przyjęcia bardziej spójnego i ujednoliconego podejścia między dyrektywą w sprawie EIK a dyrektywą w sprawie bezpieczeństwa sieci i informacji. W związku z tym wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych, którego obiektywny zakres stosowania pokrywa się z dyrektywą NIS 2 odnośnie do podmiotów niezbędnych, rozszerza pierwotny zakres stosowania dyrektywy 2008/114/WE, ograniczony do energii i transportu, na następujące sektory: bankowość, infrastruktura rynków finansowych, zdrowie, woda pitna, ścieki, infrastruktura cyfrowa, administracja publiczna i przestrzeń kosmiczna, przewidując również jasne obowiązki, odpowiednie planowanie i wzmocnioną współpracę. Należy w tym celu ustanowić ramy odniesienia dla wszystkich rodzajów ryzyka i wspierać państwa członkowskie w wysiłkach na rzecz zapewnienia, aby podmioty krytyczne były w stanie zapobiegać konsekwencjom incydentów, być na nie odporne i je amortyzować, niezależnie od tego, czy ryzyko wynika z zagrożeń naturalnych, incydentów, terroryzmu, zagrożeń wewnętrznych czy stanów zagrożenia zdrowia publicznego takich jak obecny.

4.3. Każde państwo członkowskie ma obowiązek przyjąć krajową strategię w celu zagwarantowania odporności podmiotów krytycznych, przeprowadzać regularne oceny ryzyka i na tej podstawie identyfikować podmioty krytyczne. Podmioty krytyczne są z kolei zobowiązane do dokonywania ocen ryzyka, przedsięwzięcia odpowiednich środków technicznych i organizacyjnych w celu zwiększenia odporności i do zgłaszania incydentów organom krajowym. Podmioty świadczące usługi na rzecz co najmniej jednej trzeciej państw członkowskich lub w co najmniej jednej trzeciej z nich podlegają szczególnemu nadzorowi, który obejmuje specjalne misje pomocowe organizowane dla nich przez Komisję.

4.4. Proponowana dyrektywa w sprawie odporności podmiotów krytycznych przewiduje różne formy wsparcia dla państw członkowskich i podmiotów krytycznych, przegląd zagrożeń na szczeblu UE, najlepsze praktyki i metodyki, a także szkolenia i ćwiczenia w celu sprawdzenia odporności podmiotów krytycznych. System współpracy transgranicznej obejmuje również grupę ekspertów ad hoc: Grupę ds. Odporności Podmiotów Krytycznych, która jest forum strategicznej współpracy i wymiany informacji między państwami członkowskimi.

([5]) COM(2020) 605 final.

5. **Proponowane zmiany do omawianego wniosku ustawodawczego**

5.1. EKES docenia wysiłki Komisji na rzecz zwiększenia odporności podmiotów publicznych i prywatnych na zagrożenia wynikające z ataków cybernetycznych i fizycznych. Nabiera to szczególnego znaczenia zwłaszcza w świetle szybkiej transformacji cyfrowej spowodowanej kryzysem związanym z COVID-19. EKES zgadza się ponadto, że – tak jak stwierdzono w komunikacie „Kształtowanie cyfrowej przyszłości Europy" – Europa musi czerpać korzyści z ery cyfrowej i wzmacniać przemysł, ze szczególnym uwzględnieniem małych i średnich przedsiębiorstw, oraz jego potencjał innowacyjny w sposób inkluzywny, zgodnie ze strategią opartą na czterech filarach: ochronie danych, prawach podstawowych, bezpieczeństwie i cyberbezpieczeństwie jako podstawowych warunkach funkcjonowania społeczeństwa opartego na potędze danych.

5.2. Niemniej w świetle wyników oceny skutków i konsultacji poprzedzających opracowanie wniosku dotyczącego NIS 2 EKES – biorąc pod uwagę wielokrotnie podkreślany cel, którym jest uniknięcie fragmentacji przepisów przyjętych na szczeblu krajowym, o co apelowano również w komunikacie z dnia 4 października 2017 r. w sprawie wdrożenia dyrektywy NIS ([6]) – zauważa, że niejasne są powody, dla których Komisja nie zdecydowała się zaproponować przyjęcia rozporządzenia zamiast dyrektywy. Możliwość ta nie została nawet uwzględniona wśród rozważanych wariantów.

5.3. EKES zauważa, że niektóre z przepisów obu wniosków dotyczących dyrektywy pokrywają się, ponieważ są ściśle ze sobą powiązane i komplementarne: jeden z nich dotyczy przede wszystkim profili cyberbezpieczeństwa, a drugi – bezpieczeństwa fizycznego. Podkreśla ponadto, że podmioty krytyczne, o których mowa w dyrektywie w sprawie odporności podmiotów krytycznych, dotyczą tych samych sektorów i pokrywają się z niezbędnymi podmiotami, o których mowa w NIS 2 ([7]). Co więcej, wszystkie podmioty krytyczne, o których mowa dyrektywie w sprawie odporności podmiotów krytycznych, podlegają obowiązkom w zakresie cyberbezpieczeństwa przewidzianym w NIS 2. Oba wnioski przewidują zatem szereg klauzul pomostowych w celu ich powiązania: przepisy dotyczące wzmocnionej współpracy między organami, wymiany informacji w sprawie działań nadzorczych, powiadamiania organów NIS 2 o identyfikacji podmiotów krytycznych w rozumieniu dyrektywy w sprawie odporności podmiotów krytycznych, a także regularnych spotkań Grup Współpracy, co najmniej raz w roku. Oba wnioski mają również tę samą podstawę prawną, tj. art. 114 TFUE, ukierunkowany na funkcjonowanie rynku wewnętrznego poprzez zbliżenie przepisów krajowych, zgodnie między innymi z wykładnią dokonaną przez Trybunał Sprawiedliwości w wyroku w sprawie C-58/08 Vodafone i in. W związku z tym Komitet wzywa do zastanowienia się, czy mając na względzie uproszczenie i usprawnienie, tych dwóch wniosków nie należałoby połączyć w jeden dokument.

5.4. EKES zgadza się z proponowanym podejściem polegającym na wyeliminowaniu rozróżnienia między operatorami usług kluczowych a dostawcami usług cyfrowych, o którym mowa w pierwotnej dyrektywie NIS. Zwraca jednak uwagę, że w odniesieniu do jej zakresu stosowania należy zapewnić bardziej precyzyjne i jaśniejsze wskazówki co do tego, kto jest zobowiązany do przestrzegania jej przepisów. Oprócz odniesień zawartych w załącznikach I i II – NIS 2 przywołuje szereg rozbieżnych ze sobą kryteriów, wymagających dokonania delikatnych ocen jakościowych i ilościowych, które mogą być przeprowadzane w różny sposób na szczeblu krajowym. Grozi to ponownie fragmentarycznością, której miała zapobiec omawiana interwencja legislacyjna. Istotne jest bowiem, by niedopasowane podejścia na szczeblu krajowym nie powodowały przeszkód w konkurencji i swobodnym przepływie towarów i usług, co mogłoby działać na szkodę przedsiębiorstw i wymiany handlowej.

5.5. NIS 2 przewiduje, że krytyczni operatorzy w sektorach uznanych w omawianym wniosku za „niezbędne" również podlegają ogólnym obowiązkom budowania odporności, ze szczególnym uwzględnieniem zagrożeń innych niż cybernetyczne w rozumieniu dyrektywy w sprawie odporności podmiotów krytycznych. Jednakże we wniosku tym stwierdza się wyraźnie, że nie ma on zastosowania do kwestii poruszonych w NIS 2. W istocie dyrektywa w sprawie odporności podmiotów krytycznych przewiduje, że, ponieważ bezpieczeństwo systemów informatycznych zostało już wystarczająco omówione w dyrektywie NIS 2, dziedziny przez nią regulowane powinny być wyłączone z zakresu stosowania tej dyrektywy, z wyjątkiem szczególnego systemu dla podmiotów w sektorze infrastruktury cyfrowej. Następnie odnotowuje się w niej, że podmioty należące do sektora infrastruktury cyfrowej opierają się zasadniczo na systemach sieciowych i informatycznych i są objęte zakresem stosowania dyrektywy NIS 2, która dotyczy również fizycznego bezpieczeństwa takich systemów jako elementu ich obowiązków w zakresie zarządzania ryzykiem dla bezpieczeństwa systemów informatycznych i sprawozdawczości. Jednocześnie w dyrektywie tej wskazuje się, że nie jest wykluczone, że mogą do nich mieć zastosowanie konkretne jej przepisy.

5.6. W tym złożonym kontekście EKES uważa zatem, że niezbędne jest, by Komisja dokładnie wyjaśniła zakres stosowania tych dwóch zbiorów przepisów, zwłaszcza gdy różne przepisy przyczyniają się do uregulowania tego samego przypadku lub podmiotu.

5.7. Na wszystkich szczeblach nieodzownym celem musi być jasność wszystkich przepisów prawnych, tym bardziej takich, które są zawarte w obszernych i skomplikowanych aktach prawnych jak te omawiane, a także ograniczenie biurokracji i fragmentacji poprzez uproszczenie procesów, wymogów bezpieczeństwa i obowiązków powiadamiania o incydentach. Należy również zadbać o to, by mnożenie organów odpowiedzialnych za konkretne zadania nie podważało

([6]) COM(2017) 476 final.
([7]) Załącznik 1 (Dz.U. L 194 z 19.7.2016, s. 1).

jasnego podziału ich kompetencji, niwecząc wytyczone cele. Również z tego powodu, z korzyścią dla obywatelek i obywateli oraz przedsiębiorstw, wskazane mogłoby być połączenie w jeden tekst obu wniosków dotyczących dyrektywy, dzięki czemu uniknięto by skomplikowanego niekiedy procesu interpretacji i egzekwowania.

5.8. W różnych przypadkach w NIS 2 przywołane zostały przepisy zawarte w innych instrumentach prawnych, takich jak dyrektywa (UE) 2018/1972 ([8]) ustanawiająca Europejski kodeks łączności elektronicznej, którego stosowanie reguluje kryterium szczególności. Niektóre przepisy tej dyrektywy zostały wyraźnie uchylone (art. 40 i 41), podczas gdy inne muszą być stosowane zgodnie z powyższą zasadą, bez żadnego wyjaśnienia w tym względzie. EKES ma w związku z tym nadzieję, że wszelkie wątpliwości zostaną rozwiane, aby uniknąć problemów interpretacyjnych. Jeśli chodzi o system sankcji, EKES popiera ponadto dążenie Komisji do jego harmonizacji na wypadek nieprzestrzegania zasad zarządzania ryzykiem, w ramach lepszej wymiany informacji oraz lepszej współpracy na szczeblu UE.

5.9. EKES uznaje podkreśloną we wniosku dotyczącym dyrektywy zasadniczą rolę organów zarządzających podmiotów niezbędnych i istotnych w strategii cyberbezpieczeństwa i zarządzaniu ryzykiem, ponieważ są one zobowiązane do zatwierdzania środków zarządzania ryzykiem, nadzorowania ich stosowania oraz reagowania na wszelkie przypadki nieprzestrzegania przepisów. W związku z tym przewiduje się, że członkinie i członkowie tych organów powinni regularnie odbywać specjalne szkolenia w celu zdobycia wiedzy i umiejętności wystarczających do poznania różnych zagrożeń cybernetycznych, zarządzania nimi i oceny ich skutków. Niemniej EKES uważa, że we wniosku należy wskazać zakres takiej wiedzy i umiejętności. Na szczeblu europejskim powinny być dostępne wytyczne na temat tego, które kompetencje nabywane na szkoleniach odpowiadają wymogom określonym we wniosku, i należy unikać różnic w wymogach i treści kursów szkoleniowych między poszczególnymi krajami.

5.10. EKES zgadza się co do istotnej roli ENISA w całościowej strukturze instytucjonalnej i operacyjnej cyberbezpieczeństwa na szczeblu europejskim. W związku z tym sądzi, że oprócz sprawozdania na temat stanu cyberbezpieczeństwa w Unii organ ten powinien publikować w internecie aktualne informacje na temat cyberincydentów i zawiadomienia dla poszczególnych sektorów, aby zapewnić podmiotom, których dotyczy NIS 2, przydatne narzędzie informacyjne umożliwiające lepszą ochronę ich przedsiębiorstw.

5.11. EKES zgadza się, że dostęp do prawidłowych i udzielanych w odpowiednim czasie informacji na temat podatności produktów i usług ICT na zagrożenia przyczynia się do lepszego zarządzania ryzykiem związanym z bezpieczeństwem systemów informatycznych. Pod tym względem publicznie dostępne źródła informacji na temat podatności są ważnym narzędziem dla właściwych organów krajowych, zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), przedsiębiorstw i użytkowników. Dlatego też EKES popiera propozycję powierzenia ENISA zadania ustanowienia europejskiego rejestru podatności, do którego niezbędne i istotne podmioty oraz ich dostawcy mogą przekazywać informacje, tak aby użytkownicy mogli przedsięwziąć odpowiednie środki łagodzące. Uważa jednak, że jeśli chodzi o najpoważniejsze podatności i incydenty, przekazywanie takich informacji powinno być obowiązkowe, a nie dobrowolne, tak aby był to przydatny instrument również dla podmiotów zamawiających w ramach różnych postępowań o udzielenie zamówienia na szczeblu europejskim, w tym zamówień na produkty i technologie 5G. Taki rejestr zawierałby wówczas elementy przydatne podczas oceny ofert – do celów weryfikacji ich jakości oraz wiarygodności wykonawców europejskich i pozaeuropejskich – w zakresie bezpieczeństwa produktów i usług będących przedmiotem przetargu, zgodnie z zaleceniem w sprawie cyberbezpieczeństwa sieci 5G z 26 marca 2019 r. Rejestr powinien również gwarantować, że zawarte w nim informacje będą udostępniane w sposób pozwalający uniknąć jakiejkolwiek dyskryminacji.

Bruksela, dnia 27 kwietnia 2021 r.

Christa SCHWENG
Przewodnicząca
Europejskiego Komitetu Ekonomiczno-Społecznego

([8]) Dz.U. L 321 z 17.12.2018, s. 36.