# Stanovisko Evropského hospodářského a sociálního výboru k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 a návrhu směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů

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

(2021/C 286/28)

Zpravodaj: **Maurizio MENSI**



| | |
|---|---|
| Žádost o vypracování stanoviska | Evropský parlament, 21. 1. 2021 – 11. 2. 2021 |
| | Rada, 26. 1. 2021 – 19. 2. 2021 |
| Právní základ | Článek 114 Smlouvy o fungování Evropské unie |
| Odpovědná sekce | Doprava, energetika, infrastruktura a informační společnost |
| Přijato v sekci | 14. 4. 2021 |
| Přijato na plenárním zasedání | 27. 4. 2021 |
| Plenární zasedání č. | 560 |
| Výsledek hlasování | |
| (pro/proti/zdrželi se hlasování) | 243/0/5 |



## 1. **Závěry a doporučení**

1.1. EHSV vítá úsilí vynaložené Komisí za účelem zvýšení odolnosti veřejných a soukromých subjektů vůči hrozbám vyplývajícím z kybernetických a fyzických útoků a incidentů a souhlasí s tím, že je zapotřebí posílit průmysl a inovační kapacity EU způsobem podporujícím začlenění a v souladu se strategií založenou na těchto čtyřech pilířích: ochraně údajů, základních právech, bezpečnosti a kybernetické bezpečnosti.

1.2. EHSV však zdůrazňuje, že s ohledem na význam a citlivost cílů sledovaných oběma návrhy by bylo vhodnější zvolit jakožto nástroj spíše nařízení než směrnici. Není ostatně jasné, z jakých důvodů Komise nepovažovala za nutné ani to, aby tuto možnost zařadila mezi různé zvažované alternativy.

1.3. EHSV konstatuje, že některá ustanovení dotčených návrhů směrnic se překrývají, protože jsou úzce propojena a doplňují se, přičemž jeden z návrhů se zabývá především kybernetickou bezpečností a druhý fyzickou bezpečností. Proto žádá, aby byla zvážena možnost sloučit oba návrhy do jediného textu, a to za účelem zjednodušení a funkčního propojení.

1.4. EHSV souhlasí s navrhovaným přístupem spočívajícím ve zrušení rozdělení na provozovatele základních služeb a poskytovatele digitálních služeb stanovené původní směrnicí o bezpečnosti sítí a informací, avšak zdůrazňuje, že by bylo vhodné, s odkazem na oblast působnosti, poskytnout přesnější a jasnější pokyny pro stanovení subjektů, na které se směrnice vztahuje. Zejména by měla být přesněji definována kritéria pro rozlišení mezi „základními“ a „důležitými“ subjekty, jakož i požadavky, které je třeba splnit, aby se zabránilo situacím, kdy by nejednotné přístupy na vnitrostátní úrovni představovaly překážky pro hospodářskou soutěž a volný pohyb zboží a služeb, což by mohlo mít dopad na podniky a narušit obchodní výměnu.

1.5. Vzhledem k objektivní komplexnosti systému stanoveného dotčenými návrhy považuje EHSV za důležité, aby Komise přesně vyjasnila oblast působnosti obou předpisových rámců, zejména pokud jde o místa, kde se různá ustanovení sbíhají a vztahují se na stejné situace nebo na stejné subjekty.

1.6. EHSV zdůrazňuje, že jasnost každého ustanovení je klíčový cíl, stejně jako cíl snížit administrativní zátěž a roztříštěnost prostřednictvím zjednodušení postupů, bezpečnostních požadavků a povinností v oblasti oznamování incidentů. I za tímto účelem by mohlo být vhodné a pro občany i podniky prospěšné sloučit oba návrhy do jediného textu, a vyhnout se tak složitému výkladu a uplatňování.

1.7. EHSV uznává zásadní úlohu vedoucích orgánů „základních" a „důležitých" subjektů, jež je v návrhu směrnice zdůrazněna. Členové těchto orgánů jsou povinni pravidelně absolvovat zvláštní školení, aby získali dostatečné znalosti a dovednosti, a mohli tak rozpoznat a řídit různá kybernetická rizika a vyhodnotit jejich dopad. V tomto ohledu se domnívá, že v návrhu by měl být uveden minimální obsah těchto znalostí a dovedností s cílem poskytnout na evropské úrovni vodítko k tomu, jaké odborné dovednosti jsou považovány za odpovídající, a předejít tak tomu, že se obsah různých školicích kursů bude mezi jednotlivými zeměmi lišit.

1.8. EHSV souhlasí s tím, že agentura ENISA zastává významnou úlohu v komplexním institucionálním a provozním systému kybernetické bezpečnosti na evropské úrovni. Domnívá se v této souvislosti, že kromě zprávy o stavu kybernetické bezpečnosti v Unii vydávané jednou za dva roky by měla tato agentura zveřejňovat on-line pravidelné a aktualizované informace o kybernetických bezpečnostních incidentech a odvětvová oznámení s cílem poskytnout další užitečný informační nástroj, jenž subjektům, kterých se týká revidovaná směrnice o bezpečnosti sítí a informací, umožní lépe chránit své podniky.

1.9. EHSV souhlasí s návrhem pověřit agenturu ENISA vytvořením evropského registru zranitelností a domnívá se, že informování o zranitelnostech a nejvýznamnějších incidentech by mělo být povinné, a nikoli dobrovolné, a mohlo by se tak stát užitečným nástrojem i pro zadavatele v rámci postupů pro zadávání veřejných zakázek v EU, včetně produktů a technologií pro 5G.

## 2. **Obecné připomínky**

2.1. Dne 16. prosince 2020 byla představena nová strategie kybernetické bezpečnosti EU a současně byly předloženy dva legislativní návrhy: přezkum směrnice (EU) 2016/1148 ([1]) o bezpečnosti sítí a informačních systémů a nová směrnice o odolnosti kritických subjektů. Cílem zmíněné strategie, která je klíčovým prvkem sdělení „Formování digitální budoucnosti Evropy" ([2]), plánu na podporu oživení Evropy a strategie bezpečnostní unie EU, je posílit kolektivní odolnost Evropy proti kybernetickým hrozbám a pomoci zajistit, aby všichni občané i podniky mohli plně těžit z důvěryhodných a spolehlivých služeb a digitálních nástrojů.

2.2. Je potřeba aktualizovat stávající opatření na úrovni EU zaměřená na ochranu klíčových služeb a infrastruktur před kybernetickými i fyzickými riziky. Rizika v oblasti kybernetické bezpečnosti se s rostoucí digitalizací a propojeností nadále vyvíjejí. Proto je zapotřebí přezkoumat stávající právní rámec v duchu bezpečnostní strategie EU a překonat rozpor mezi on-line a off-line prostředím a přístup založený na striktním dělení do skupin.

2.3. Oba návrhy směrnic se týkají široké škály odvětví a řeší stávající a budoucí on-line i off-line rizika vyplývající z kybernetických a zločineckých útoků a z přírodních katastrof a dalších incidentů. Vycházejí rovněž ze zkušeností s probíhající pandemií, která ukázala, že společnosti a ekonomiky, jež jsou čím dál závislejší na digitálních řešeních, jsou zranitelné a vystavené kybernetickým hrozbám, které jsou na vzestupu a rychle se vyvíjejí, což se týká zejména skupin ohrožených sociálním vyloučením, jako jsou například zdravotně postižení. To EU vedlo k tomu, že navrhla opatření s cílem zajistit globální a otevřený kyberprostor, který je však založen na pevných bezpečnostních zárukách, technologické suverenitě a vedoucím postavení, dosažených prostřednictvím budování operačních kapacit pro prevenci případných hrozeb, odrazování od nich a reakci na ně, a to za respektování pravomocí v oblasti národní bezpečnosti, jež jsou svěřeny členským státům.

## 3. **Návrh přezkumu směrnice o bezpečnosti sítí a informačních systémů**

3.1. Směrnice (EU) 2016/1148 o bezpečnosti sítí a informačních systémů byla prvním „horizontálním" normativním nástrojem EU v oblasti kybernetické bezpečnosti a jejím cílem bylo posílit odolnost síťových a informačních systémů EU proti kybernetickým rizikům. Navzdory dobrým dosaženým výsledkům se ukázalo, že tato směrnice má určitá omezení v situaci, kdy digitální transformace společnosti, zintenzivněná krizí COVID-19, rozšířila spektrum hrozeb a zvýraznila zranitelnost našich společností, které jsou na sobě stále více závislé a čelí významným a neočekávaným rizikům. Vznikly

([1]) Úř. věst. L 194, 19.7.2016, s. 1.
([2]) COM(2020) 67 final.

nové výzvy, které vyžadují přiměřené a inovativní reakce. Výsledky rozsáhlé konzultace se zúčastněnými stranami odhalily nedostatečnou úroveň kybernetické bezpečnosti u evropských podniků, nejednotné uplatňování pravidel ze strany států v různých odvětvích a nedostatečné porozumění hlavním hrozbám a výzvám.

3.2. Návrh revidované směrnice o bezpečnosti sítí a informací úzce souvisí se dvěma iniciativami: s návrhem nařízení o digitální provozní odolnosti finančního sektoru (DORA) a s návrhem směrnice o posílení odolnosti kritických subjektů, která rozšiřuje působnost směrnice 2008/114/ES ([3]), jež se vztahuje pouze na energetiku a dopravu, také na další odvětví, například na odvětví zdravotní péče a na subjekty provádějící činnosti v oblasti výzkumu a vývoje léčivých přípravků. Směrnice o posílení odolnosti kritických subjektů, která se vztahuje na stejná odvětví, jako revidovaná směrnice o bezpečnosti sítí a informací pokud jde o základní subjekty (příloha I revidované směrnice o bezpečnosti sítí a informací) přesunuje zaměření od ochrany fyzických aktiv k odolnosti subjektů, které je provozují, a přechází od určování evropských kritických infrastruktur s přeshraničním rozměrem ke kritickým infrastrukturám na vnitrostátní úrovni. Revidovaná směrnice o bezpečnosti sítí a informací je rovněž v souladu se stávajícími normativními nástroji, jako je evropský kodex pro elektronické komunikace, obecné nařízení o ochraně osobních údajů a nařízení eIDAS o elektronické identifikaci a službách vytvářejících důvěru.

3.3. Návrh revidované směrnice o bezpečnosti sítí a informací si, v souladu s Programem pro účelnost a účinnost právních předpisů (REFIT), klade za cíl snížit regulační zátěž pro příslušné orgány a náklady na dodržování předpisů pro veřejné a soukromé subjekty a modernizovat referenční právní rámec. Kromě toho posiluje bezpečnostní požadavky kladené na podniky, řeší otázku bezpečnosti zásobovacích řetězců, racionalizuje povinnosti hlášení, zavádí přísnější kontrolní opatření pro vnitrostátní orgány a snaží se harmonizovat sankční režimy členských států.

3.4. Návrh revidované směrnice o bezpečnosti sítí a informací rovněž přispívá k posílení sdílení informací a spolupráce v oblasti řízení kybernetických krizí na vnitrostátní a evropské úrovni. Zrušuje rozdělení na provozovatele základních služeb a poskytovatele digitálních služeb, které stanoví směrnice o bezpečnosti sítí a informací. Její působnost zahrnuje velké a střední podniky působící v odvětvích vymezených na základě toho, že jsou kritická pro hospodářství a společnost. Tyto subjekty, veřejné nebo soukromé, jsou rozděleny na „základní“ a „důležité“ a platí pro ně různé režimy dohledu. Členským státům je však ponechána možnost zohlednit i menší subjekty, které jsou vysoce rizikové.

3.5. Návrh předpokládá vznik nové sítě bezpečnostních operačních středisek na úrovni EU řízených umělou inteligencí (UI), která budou sloužit jako skutečný „štít kybernetické bezpečnosti“, jenž zajistí včasnou detekci kybernetických útoků, a která umožní zasáhnout s dostatečným předstihem, ještě než vzniknou škody. Význam umělé inteligence pro kybernetickou bezpečnost je ostatně zdůrazněn i ve zprávě o umělé inteligenci, kterou 1. března 2021 zveřejnila americká Národní bezpečnostní komise pro umělou inteligenci (NSCAI). V důsledku toho budou mít členské státy a provozovatelé kritických infrastruktur přímý přístup k informacím o hrozbách v rámci evropské bezpečnostní sítě („Threat Intelligence“).

3.6. Komise se zabývá také problémem bezpečnosti dodavatelských řetězců a vztahů s dodavateli. Členské státy mohou ve spolupráci s Komisí a s agenturou ENISA provádět koordinovaná posouzení rizik kritických dodavatelských řetězců na základě přístupu, který byl úspěšně uplatněn v případě sítí 5G, stanoveného doporučením ze dne 26. března 2019 ([4]).

3.7. Návrh posiluje a racionalizuje požadavky v oblasti bezpečnosti a podávání zpráv pro podniky a prosazuje společný přístup k řízení rizik založený na minimálním seznamu bezpečnostních prvků, které musí být uplatňovány. Návrh předkládá přesnější ustanovení týkající se postupu oznamování incidentů, obsahu zpráv a lhůt. V této souvislosti návrh nastiňuje dvoufázový postup: podniky mají 24 hodin na předložení zkráceného počátečního oznámení a jeden měsíc na předložení podrobné konečné zprávy.

([3]) Úř. věst. L 345, 23.12.2008, s. 75.
([4]) Úř. věst. L 88, 29.3.2019, s. 42.

3.8. Je stanoveno, aby členské státy určily vnitrostátní orgány odpovědné za krizové řízení se zvláštními plány a aby byla zřízena nová síť pro operativní spolupráci, Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe). Posiluje se úloha skupiny pro spolupráci při definování strategických rozhodnutí a zavádí se registr zranitelností odhalených v EU, který má spravovat Agentura EU pro kybernetickou bezpečnost (ENISA). Dále se posiluje sdílení informací a spolupráce mezi orgány členských států, včetně operativní spolupráce v oblasti řešení kybernetických bezpečnostních krizí.

3.9. Návrh zavádí přísnější dohledová opatření pro vnitrostátní orgány a přísnější prováděcí požadavky a klade si za cíl harmonizovat sankční režimy členských států.

3.10. Navrhovaná směrnice v tomto ohledu stanoví seznam správních pokut pro případ porušování povinností v oblasti řízení kybernetických bezpečnostních rizik a komunikace. Obsahuje rovněž ustanovení o odpovědnosti fyzických osob, které mají manažerskou odpovědnost ve společnostech, na které se směrnice vztahuje, nebo tyto společnosti zastupují. Návrh tak zlepšuje schopnost EU předcházet rozsáhlým kybernetickým bezpečnostním incidentům a krizím, řídit je a reagovat na ně, a to prostřednictvím jasného vymezení odpovědnosti, odpovídajícího plánování a větší spolupráce na úrovni EU.

3.11. Členské státy by měly být schopny dohlížet na provádění norem EU a navzájem si pomáhat v případě přeshraničních problémů, navázat strukturovanější dialog se soukromým sektorem, koordinovat odhalování zranitelných míst softwaru a hardwaru uváděného na vnitřní trh a provádět koordinované posouzení bezpečnostních rizik a hrozeb souvisejících s novými technologiemi, jako tomu bylo v případě 5G.

## 4. **Návrh směrnice o odolnosti kritických subjektů**

4.1. EU v roce 2006 zavedla Evropský program na ochranu kritické infrastruktury (EPCIP) a v roce 2008 přijala směrnici o evropské kritické infrastruktuře (EKI), která se vztahuje na odvětví energetiky a dopravy. Jak strategie bezpečnostní unie EU pro období 2020–2025 ([5]), kterou přijala Evropská komise, tak nedávno přijatá agenda pro boj proti terorismu zdůrazňují, že je důležité zajistit odolnost kritických infrastruktur vůči fyzickým i digitálním rizikům. Hodnocení provádění směrnice o EKI provedené v roce 2019 i výsledky posouzení dopadů dotčeného návrhu ukázaly, že stávající evropská a vnitrostátní opatření nezaručují dostatečnou schopnost provozovatelů čelit stávajícím rizikům. Proto Rada a Parlament vyzývají Komisi k přezkoumání stávajícího přístupu k ochraně kritických infrastruktur.

4.2. Strategie bezpečnostní unie EU přijatá Komisí dne 24. července 2020 uznává, že fyzické a digitální infrastruktury jsou stále více vzájemně propojeny a vzájemně závislé, a zdůrazňuje, že je nezbytné přijmout soudržnější a jednotnější přístup, pokud jde o uplatňování směrnice o EKI a směrnice o bezpečnosti sítí a informací. V tomto smyslu návrh směrnice o odolnosti kritických subjektů, jehož objektivní referenční rámec je stejný jako referenční rámec revidované směrnice o bezpečnosti sítí a informací, pokud jde o základní subjekty, rozšiřuje původní působnost směrnice 2008/114/ES, která je omezena na odvětví energetiky a dopravy, o následující odvětví: bankovnictví, infrastruktura finančních trhů, zdraví, pitná voda, odpadní voda, digitální infrastruktura, veřejná správa a vesmír, a stanoví jasné povinnosti, odpovídající plánování a větší spolupráci. Je proto zapotřebí vytvořit referenční rámec pro všechna rizika a podporovat členské státy v jejich úsilí s cílem zajistit, aby kritické subjekty byly schopny předcházet důsledkům incidentů, odolávat jim a absorbovat je, a to nezávisle na tom, zda se jedná o rizika vyplývající z přírodních nebezpečí, incidentů, terorismu, vnitřní hrozby nebo mimořádné situace v oblasti veřejného zdraví, jako je ta současná.

4.3. Každý členský stát je povinen přijmout vnitrostátní strategii zaměřenou na zajištění odolnosti kritických subjektů, provádět pravidelná posouzení rizik a na jejich základě určit kritické subjekty. Kritické subjekty mají povinnost provádět posouzení rizik, zavést vhodná technická a organizační opatření k zajištění své odolnosti a hlásit incidenty vnitrostátním orgánům. Subjekty, které poskytují služby do více než jedné třetiny členských států nebo ve více než jedné třetině členských států podléhají zvláštnímu dozoru, který zahrnuje poradní mise organizované Komisí.

4.4. Návrh směrnice o odolnosti kritických subjektů předpokládá různé formy podpory členských států a kritických subjektů, přehled nebezpečí na úrovni EU, vypracování osvědčených postupů a metodiky a vzdělávací činnosti a cvičení sloužící k otestování odolnosti kritických subjektů. Systém přeshraniční spolupráce předpokládá také ad hoc expertní skupinu, skupinu pro posílení odolnosti kritických subjektů, fórum pro strategickou spolupráci a výměnu informací mezi členskými státy.

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

5. **Navrhované změny v předmětném legislativním návrhu**

5.1. EHSV vítá úsilí vynaložené Komisí na posílení odolnosti veřejných a soukromých subjektů vůči hrozbám vyplývajícím z kybernetických a fyzických útoků. Nabývá to zvláštního významu a důležitosti především s ohledem na rychlou digitální transformaci vyvolanou krizí COVID-19. Rovněž souhlasí s tím, že je zapotřebí, jak je uvedeno ve sdělení „Formování digitální budoucnosti Evropy“, aby Evropa těžila z výhod digitální éry a posílila svůj průmysl, zejména pokud jde o malé a střední podniky, a svou inovační kapacitu způsobem podporujícím začlenění, v souladu se strategií spočívající na čtyřech pilířích: ochraně údajů, základních právech, bezpečnosti a kybernetické bezpečnosti, které jsou základními předpoklady společnosti založené na síle dat.

5.2. Nicméně ve světle výsledků posouzení dopadů, které předcházelo návrhu revidované směrnice o bezpečnosti sítí a informací, a s ohledem na již několikrát zdůrazněný cíl vyvarovat se roztříštěnosti předpisů přijatých na vnitrostátní úrovni, vyjádřený rovněž ve sdělení ze dne 4. října 2017 o účinném provedení směrnice o bezpečnosti sítí a informačních systémů ([6]), EHSV zdůrazňuje, že nejsou patrné důvody, proč Komise nepovažovala za vhodné navrhnout přijetí nařízení, a nikoli směrnice, a to ani mezi zvažovanými možnostmi.

5.3. EHSV konstatuje, že některá ustanovení dotčených návrhů směrnic se překrývají, protože jsou úzce propojena a doplňují se, přičemž jeden z návrhů se zabývá především kybernetickou bezpečností a druhý fyzickou bezpečností. Zdůrazňuje také, že kritické subjekty uvedené ve směrnici o posílení odolnosti kritických subjektů jsou ve stejných odvětvích jako „základní“ subjekty uvedené v revidované směrnici o bezpečnosti sítí a informací ([7]), a shodují se tak s nimi. Kromě toho se na všechny kritické subjekty uvedené ve směrnici o posílení odolnosti kritických subjektů vztahují povinnosti v oblasti kybernetické bezpečnosti stanovené v revidované směrnici o bezpečnosti sítí a informací. Oba návrhy pak stanoví řadu překlenovacích ustanovení zajišťujících propojení: posílená spolupráce mezi orgány, výměna informací o kontrolních činnostech, hlášení orgánům podle revidované směrnice o bezpečnosti sítí a informací o kritických subjektech ve smyslu směrnice o odolnosti kritických subjektů nebo pravidelná zasedání příslušných skupin pro spolupráci nejméně jednou ročně. Oba návrhy mají také společný právní základ, článek 114 SFEU, zaměřený na fungování vnitřního trhu prostřednictvím opatření ke sbližování ustanovení právních a správních předpisů členských států, který Soudní dvůr Evropské unie vykládá mimo jiné v rozsudku C-58/08 – Vodafone a další. Proto EHSV žádá, aby byla zvážena možnost sloučit oba návrhy do jediného textu, za účelem zjednodušení a funkčního propojení.

5.4. EHSV souhlasí s navrhovaným přístupem spočívajícím ve zrušení rozdělení na provozovatele základních služeb a poskytovatele digitálních služeb stanovené původní směrnicí o bezpečnosti sítí a informací, avšak zdůrazňuje, že by bylo vhodné, s odkazem na oblast působnosti, poskytnout přesnější a jasnější pokyny pro stanovení subjektů, na které se směrnice vztahuje. Kromě odkazů uvedených v přílohách I a II totiž revidovaná směrnice o bezpečnosti sítí a informací uvádí řadu vzájemně nejednotných kritérií, která vyžadují citlivé kvalitativní a kvantitativní hodnocení, které by na vnitrostátní úrovni mohlo být prováděno různým způsobem, přičemž hrozí, že znovu dojde k roztříštěnosti, které měl stávající regulační zásah zamezit. Je totiž klíčové zabránit situacím, kdy by nejednotné přístupy na vnitrostátní úrovni představovaly překážky pro hospodářskou soutěž a volný pohyb zboží a služeb, což by mohlo mít dopad na podniky a narušit obchodní výměnu.

5.5. Revidovaná směrnice o bezpečnosti sítí a informací předpokládá, že klíčoví provozovatelé v odvětvích, která tento návrh považuje za základní, mají také obecnou povinnost posilovat svou odolnost, se zvláštním ohledem na nekybernetická rizika ve smyslu směrnice o odolnosti kritických subjektů. Tato směrnice však výslovně uvádí, že se nevztahuje na záležitosti, které upravuje revidovaná směrnice o bezpečnosti sítí a informací. Směrnice o odolnosti kritických subjektů totiž předpokládá, že vzhledem k tomu, že kybernetickou bezpečností se dostatečně zabývá revidovaná směrnice o bezpečnosti sítí a informací, by záležitosti, které upravuje, měly být vyloučeny z oblasti působnosti směrnice o odolnosti kritických subjektů, aniž by byl dotčen zvláštní režim pro subjekty v odvětví digitální infrastruktury. Dále tato směrnice zdůrazňuje, že subjekty v odvětví digitální infrastruktury jsou v zásadě založeny na síťových a informačních systémech a spadají do oblasti působnosti revidované směrnice o bezpečnosti sítí a informací, která v rámci jejich povinností týkajících se řízení rizik v oblasti kybernetické bezpečnosti a povinností hlásit incidenty řeší fyzickou bezpečnost těchto systémů. Směrnice o odolnosti kritických subjektů současně uvádí, že není vyloučeno, že pro některé subjekty v odvětví digitální infrastruktury budou její ustanovení platit.

5.6. V tomto komplexním rámci proto EHSV považuje za nezbytné, aby Komise přesně vyjasnila oblast působnosti obou předpisových rámců, zejména pokud jde o místa, kde se předpisy sbíhají a vztahují se na stejné situace nebo na stejné subjekty.

5.7. Jasnost každého ustanovení, zejména pokud se jedná o tak rozsáhlé a členité texty, jako jsou předmětné návrhy, je klíčový cíl, stejně jako cíl snížit administrativní zátěž a roztříštěnost prostřednictvím zjednodušení postupů, bezpečnostních požadavků a povinností v oblasti oznamování incidentů. Je třeba rovněž zajistit, aby velký počet orgánů zajišťujících

([6]) COM(2017) 476 final.
([7]) Příloha 1(Úř. věst. L 194, 19.7.2016, s. 1).

specifické úkoly nenarušil jasné stanovení jejich pravomocí, které by mohlo podkopávat sledované cíle. I z tohoto důvodu by mohlo být vhodné a pro občany i podniky prospěšné sloučit oba návrhy do jediného textu a vyhnout se tak složitému výkladu a uplatňování.

5.8. Revidovaná směrnice o bezpečnosti sítí a informací v několika případech odkazuje na jiné právní nástroje, např. na směrnici (EU) 2018/1972 ([8]), kterou se stanoví evropský kodex pro elektronické komunikace, jehož uplatňování se řídí zásadou speciality. Některá ustanovení směrnice (EU) 2018/1972 se zrušují (články 40 a 41), zatímco jiná budou muset být uplatňována v souladu s výše uvedenou zásadou, aniž by bylo objasněno proč. EHSV doufá, že všechny pochybnosti budou rozptýleny, aby se zabránilo problémům při výkladu. Pokud jde o systém sankcí, EHSV souhlasí s cílem Komise harmonizovat v rámci lepšího sdílení informací a spolupráce na úrovni EU jejich režim v případě nedodržení povinností v oblasti řízení rizik.

5.9. EHSV uznává zásadní úlohu vedoucích orgánů „základních" a „důležitých" subjektů ve strategii kybernetické bezpečnosti a při řízení rizik, jež je v návrhu směrnice zdůrazněna, jelikož jsou povinny schvalovat opatření týkající se řízení rizik, dohlížet na jejich provádění a reagovat na případné nedodržování povinností. V tomto ohledu se stanoví, že členové těchto orgánů musí pravidelně absolvovat zvláštní školení, aby získali dostatečné znalosti a dovednosti, a mohli tak rozpoznat a řídit různá kybernetická rizika a vyhodnotit jejich dopad. Domnívá se však, že v návrhu by měl být uveden obsah těchto znalostí a dovedností s cílem poskytnout na evropské úrovni vodítko k tomu, jaké odborné dovednosti jsou považovány za odpovídající požadavkům uvedeným v návrhu, a předejít tak tomu, že se požadavky a obsah různých školicích kursů budou mezi jednotlivými zeměmi lišit.

5.10. EHSV souhlasí s tím, že agentura ENISA zastává významnou úlohu v komplexním institucionálním a provozním systému kybernetické bezpečnosti na evropské úrovni. Domnívá se v této souvislosti, že kromě zprávy o stavu kybernetické bezpečnosti v Unii by měla tato agentura zveřejňovat on-line aktualizované informace o kybernetických bezpečnostních incidentech a odvětvová oznámení s cílem poskytnout užitečný informační nástroj, jenž subjektům, kterých se týká revidovaná směrnice o bezpečnosti sítí a informací, umožní lépe chránit své podniky.

5.11. EHSV souhlasí s tím, že přístup ke správným a včasným informacím o zranitelnostech dotýkajících se produktů a služeb IKT přispívá k lepšímu řízení kybernetických bezpečnostních rizik. V tomto ohledu jsou zdroje veřejně přístupných informací o zranitelnostech důležitým nástrojem pro příslušné vnitrostátní orgány, týmy CSIRT, podniky i uživatele. Z tohoto důvodu EHSV souhlasí s návrhem pověřit agenturu ENISA zřízením evropského registru zranitelností, do kterého mohou základní a důležité subjekty uvádět informace, jež uživatelům umožní přijímat vhodná opatření ke zmírnění dopadů. Domnívá se však, že informování o zranitelnostech a nejvýznamnějších incidentech by mělo být povinné, a nikoli dobrovolné, a mohlo by se tak stát užitečným nástrojem i pro zadavatele v rámci postupů pro zadávání veřejných zakázek v EU, včetně produktů a technologií pro 5G. Zmíněný registr by v tomto případě zahrnoval informace využitelné pro hodnocení nabídek, ověřování jejich kvality a pro účely hodnocení důvěryhodnosti evropských a mimoevropských smluvních partnerů, pokud jde o bezpečnost produktů a služeb, které jsou předmětem soutěže, v souladu s doporučením ke kybernetické bezpečnosti sítí 5G ze dne 26. března 2019. Registr by měl rovněž zajišťovat, aby v něm obsažené informace byly zpřístupněny takovým způsobem, aby se zamezilo jakékoli diskriminaci.

V Bruselu dne 27. dubna 2021.

*Předsedkyně*
*Evropského hospodářského a sociálního výboru*
Christa SCHWENG

([8]) Úř. věst. L 321, 17.12.2018, s. 36.