Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 ir Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl ypatingos svarbos subjektų atsparumo

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

(2021/C 286/28)

Pranešėjas **Maurizio MENSI**

Prašymas pateikti nuomonę	Europos Parlamentas, 2021 1 21–2021 2 11
	Taryba, 2021 1 26–2021 2 19
Teisinis pagrindas	Sutarties dėl Europos Sąjungos veikimo 114 straipsnis
Atsakingas skyrius	Transporto, energetikos, infrastruktūros ir informacinės visuomenės skyrius
Priimta skyriuje	2021 4 14
Priimta plenarinėje sesijoje	2021 4 27
Plenarinės sesijos Nr.	560
Balsavimo rezultatai	
(už / prieš / susilaikė)	243 / 0/ 5

1. **Išvados ir rekomendacijos**

1.1. EESRK palankiai vertina Komisijos pastangas didinti viešųjų ir privačiųjų subjektų atsparumą incidentų, kibernetinių ir fizinių išpuolių keliamoms grėsmėms ir pritaria, kad reikia įtraukiu būdu stiprinti ES pramonės ir inovacijų pajėgumus laikantis strategijos, grindžiamos keturiais ramsčiais: duomenų apsauga, pagrindinės teisės, sauga ir kibernetinis saugumas.

1.2. Vis dėlto EESRK pabrėžia, kad atsižvelgiant į abiem pasiūlymais siekiamų tikslų svarbą ir ypatingumą reglamentas būtų tinkamesnė priemonė nei direktyva. Be to, Komisija nenurodė priežasčių, kodėl tarp visų svarstytų galimybių pasiūlymas dėl reglamento net nebuvo paminėtas.

1.3. EESRK pažymi, kad kai kurios šių dviejų pasiūlymų dėl direktyvos nuostatos sutampa, nes jos yra glaudžiai susijusios ir viena kitą papildo, vienoje jų daugiausia dėmesio skiriama kibernetiniam saugumui, o kitoje – fiziniam saugumui. Todėl ragina apsvarstyti galimybę abu pasiūlymus sujungti į vieną tekstą supaprastinimo ir racionalizavimo sumetimais.

1.4. EESRK pritaria pasiūlymui panaikinti skirtumą tarp esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų, kaip nurodyta pirminėje Kibernetinio saugumo direktyvoje (TIS direktyva), tačiau atkreipia dėmesį į tai, kad, kalbant apie taikymo sritį, reikėtų pateikti tikslesnes ir aiškesnes nuorodas, kaip nustatyti, kokiems subjektams direktyva yra taikoma. Visų pirma reikėtų tiksliau apibrėžti „esminių“ ir „svarbių“ subjektų atskyrimo kriterijus, taip pat reikalavimus, kurių turi būti laikomasi, kad nacionaliniu lygmeniu būtų išvengta skirtingų veiksmų, dėl kurių kiltų kliūčių konkurencijai ir laisvam prekių ir paslaugų judėjimui ir kurie galėtų turėti poveikio įmonėms ir pakenkti prekybai.

1.5. EESRK mano, kad, atsižvelgiant į objektyvų abiejuose pasiūlymuose nustatytos sistemos sudėtingumą, svarbu, kad Komisija tiksliai paaiškintų abiejų teisės aktų taikymo sritį, visų pirma tais atvejais, kai skirtingomis nuostatomis siekiama reguliuoti tuos pačius atvejus arba subjektus.

1.6. EESRK atkreipia dėmesį į tai, kad visų teisės aktų nuostatų aiškumas yra esminis tikslas, kaip ir biurokratizmo ir susiskaidymo mažinimas supaprastinant procesus, saugos ir pranešimo apie incidentus reikalavimus. Taigi ir šiuo tikslu bei siekiant naudos piliečiams ir įmonėms galėtų būti tikslinga du pasiūlymus dėl direktyvos sujungti į vieną tekstą ir taip išvengti kartais sudėtingo aiškinimo ir taikymo.

1.7. EESRK pripažįsta, kad esminis vaidmuo, kaip pabrėžiama pasiūlyme dėl direktyvos, tenka „esminių“ ir „svarbių“ subjektų valdymo organams, kurių nariai turi reguliariai dalyvauti specialiuose mokymuose, kad galėtų įgyti pakankamai žinių ir įgūdžių, kurie leistų suprasti ir valdyti kibernetinio saugumo riziką ir įvertinti jos poveikį. Atsižvelgdamas į tai, Komitetas mano, kad pasiūlyme turėtų būti nurodytas būtiniausias tokių žinių ir įgūdžių turinys, kad Europos lygmeniu būtų galima pateikti gaires, kokių įgūdžių turi būti mokoma, ir taip išvengti, kad įvairių mokymų turinio skirtumų šalyse.

1.8. EESRK pritaria svarbiam ENISA vaidmeniui bendroje Europos institucinėje ir operatyvinėje kibernetinio saugumo sistemoje. Atsižvelgdamas į tai, mano, kad be kas dvejus metus rengiamos kibernetinio saugumo Sąjungoje būklės ataskaitos, ši agentūra turėtų reguliariai skelbti naujausią informaciją apie kompiuterių saugumo incidentus, taip pat konkretiems sektoriams skirtus pranešimus; taip suinteresuotosioms šalims, kurioms taikoma TIS 2 direktyva, būtų suteikiama papildomos naudingos informacijos ir jie galėtų geriau apsaugoti savo įmones.

1.9. EESRK pritaria pasiūlymui pavesti ENISA sukurti Europos pažeidžiamumo registrą ir mano, kad pranešimas apie pažeidžiamumą ir didelius incidentus turi būti privalomas, o ne savanoriškas, kad tai taptų naudinga priemone perkančioms organizacijoms, dalyvaujančioms viešųjų pirkimų procedūrose Europos lygmeniu, įskaitant 5G produktus ir technologijas.

2. **Bendrosios pastabos**

2.1. 2020 m. gruodžio 16 d. buvo pateikta nauja ES saugumo strategija kartu su dviem teisėkūros pasiūlymais: persvarstyti Direktyvą (ES) 2016/1148 ([1]) dėl tinklų ir informacinių sistemų saugumo (toliau – TIS 2 direktyva) ir pateikti naują direktyvą dėl ypatingos svarbos subjektų atsparumo (toliau – CER direktyva). Strategija, kuri yra vienas iš pagrindinių komunikato „Europos skaitmeninės ateities formavimas“ ([2]), Europos ekonomikos gaivinimo plano ir ES saugumo sąjungos strategijos elementų, siekiama stiprinti bendrą Europos atsparumą kibernetinėms grėsmėms ir užtikrinti visiems piliečiams ir įmonėms galimybę naudotis patikimomis ir saugiomis skaitmeninėmis paslaugomis ir priemonėmis.

2.2. Reikia atnaujinti esamas ES lygmens priemones, skirtas apsaugoti ypatingos svarbos paslaugas ir infrastruktūrą nuo kibernetinių ir fizinių grėsmių. Didėjant skaitmeninimui ir tarpusavio junglumui, toliau didėja kibernetinio saugumo grėsmės. Todėl reikia peržiūrėti galiojančią reglamentavimo sistemą laikantis ES saugumo strategijos principų, panaikinti interneto ir ne interneto pasaulio atskyrimą ir atsisakyti griežtu suskirstymu grindžiamo požiūrio.

2.3. Šie du pasiūlymai dėl direktyvos apima daug sektorių ir jais siekiama šalinti dabartines ir būsimas grėsmes internete ir realiame gyvenime, kylančias dėl kibernetinių ir nusikalstamų išpuolių, gaivalinių nelaimių ir kitų incidentų, taip pat atsižvelgti į patirtį, įgytą per tebesitęsiančią pandemiją, kuri parodė, kad visuomenė – visų pirma grupės, kurioms gresia socialinė atskirtis, pavyzdžiui, žmonės su negalia – ir ekonomika vis labiau priklauso nuo skaitmeninių technologijų ir yra pažeidžiamos ir susiduria su sparčiai didėjančiomis ir kintančiomis kibernetinėmis grėsmėmis. Todėl ES pasiūlė veiksmų, kuriais būtų apsaugota pasaulinė ir atvira kibernetinė erdvė, tačiau kuri būtų grindžiama tvirtomis saugumo garantijomis, technologiniu suverenumu ir lyderyste, plėtojant operatyvinius reagavimo į krizes pajėgumus, kad būtų užkirstas kelias galimoms grėsmėms, nuo jų atgrasyta ir į jas būtų labiau reaguojama, atsižvelgiant į valstybių narių nacionalinio saugumo prerogatyvas.

3. **Pasiūlymas dėl Tinklų ir informacinių sistemų saugumo direktyvos peržiūros**

3.1. TIS direktyva (ES) 2016/1148 – pirmąja horizontaliąja ES kibernetinio saugumo reguliavimo priemone – siekta padidinti Sąjungos tinklų ir informacinių sistemų atsparumą kibernetinei rizikai. Vis dėlto, nepaisant gerų rezultatų, pastebėtas tam tikras TIS direktyvos ribotumas, kai dėl visuomenės skaitmeninės transformacijos, suintensyvėjusios dėl COVID-19 krizės, padidėjo grėsmių įvairovė ir išryškėjo vis labiau tarpusavyje susijusių mūsų visuomenių pažeidžiamumas

([1]) OL L 194, 2016 7 19, p. 1.
([2]) COM(2020) 67 *final*.

kilus didelei ir nenumatytai rizikai. Atsirado naujų iššūkių, kuriems spręsti reikia tinkamų ir novatoriškų sprendimų. Plataus masto konsultacijų su suinteresuotaisiais subjektais rezultatai parodė, kad Europos įmonėse kibernetinio saugumo lygis yra nepakankamas, valstybės narės nenuosekliai taiko taisykles įvairiuose sektoriuose ir nepakankamai supranta pagrindines grėsmes ir problemas.

3.2. Pasiūlymas dėl TIS 2 direktyvos yra glaudžiai susijęs su kitomis dviem iniciatyvomis: pasiūlymu dėl reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA reglamentas) ir pasiūlymu dėl direktyvos dėl ypatingos svarbos subjektų atsparumo (CER direktyva), kuriuo išplečiama daugiausia energetikos ir transporto sektoriams taikomos Direktyvos 2008/114/EB ([3]) aprėptis į ją įtraukiant naujus sektorius, daugiau dėmesio skiriant, pavyzdžiui, sveikatos sektoriui ir vaistų mokslinių tyrimų ir plėtros veiklą vykdantiems subjektams. CER direktyvoje, kurios sektorinė taikymo sritis ypatingos svarbos subjektų požiūriu yra tokia pati kaip ir TIS 2 direktyvos (TIS 2 direktyvos 1 priedas), dėmesys sutelkiamas nebe į fizinio turto apsaugą, bet į juos valdančių subjektų atsparumą ir pereinama nuo Europos ypatingos svarbos ir tarpvalstybinė reikšmę turinčių infrastruktūros objektų nustatymo prie ypatingos svarbos infrastruktūros objektų nustatymo nacionaliniu lygmeniu. TIS 2 direktyva taip pat dera su kitais galiojančiais teisės aktais, pavyzdžiui, Europos elektroninių ryšių kodeksu, Bendruoju duomenų apsaugos reglamentu ir eIDAS reglamentu dėl elektroninės atpažinties ir patikimumo užtikrinimo paslaugų, ir juos papildo.

3.3. Pagal Reglamentavimo kokybės ir rezultatų programą (REFIT) pasiūlymu dėl TIS 2 direktyvos siekiama sumažinti kompetentingoms institucijoms tenkančią reguliavimo naštą ir reikalavimų laikymosi išlaidas viešiesiems ir privatiesiems subjektams bei modernizuoti teisinę sistemą. Pasiūlymu taip pat sustiprinami įmonėms taikomi saugumo reikalavimai, sprendžiami tiekimo grandinių saugumo klausimai, supaprastinami ataskaitų teikimo reikalavimai, nustatomos griežtesnės priežiūros priemonės nacionalinėms valdžios institucijoms ir siekiama suderinti sankcijų taikymo tvarką valstybėse narėse.

3.4. TIS 2 direktyva taip pat sustiprinamas dalijimasis informacija ir bendradarbiavimas kibernetinių krizių valdymo srityje nacionaliniu ir Europos lygmenimis. Panaikinamas esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų atskyrimas, numatytas TIS direktyvoje. Į jos taikymo sritį patenka vidutinės ir didelės įmonės, priklausančios sektoriams, kurie suskirstyti pagal jų svarbą ekonomikai ir visuomenei. Šie viešieji ir privatieji subjektai skirstomi į „esminius subjektus“ ir „svarbius subjektus“, kuriems taikoma skirtinga priežiūros tvarka. Tačiau valstybėms narėms paliekama teisė įtraukti mažesnius, tačiau didelės rizikos subjektus.

3.5. Bus sukurtas naujas ES masto dirbtiniu intelektu grindžiamų saugumo operacijų centrų tinklas, kuris taps visaverčių kibernetinio saugumo skydu, galinčiu pakankamai iš anksto aptikti kibernetinio išpuolio signalus, kad būtų galima įsikišti, kol dar nepadaryta žala. Dirbtinio intelekto svarba kibernetiniam saugumui be kita ko pabrėžiama ir 2021 m. kovo 1 d. pateiktoje JAV Nacionalinės saugumo komisijos (NSCAI) ataskaitoje dėl dirbtinio intelekto. Taip valstybės narės ir ypatingos svarbos infrastruktūros objektų operatoriai turės tiesioginę prieigą prie informacijos apie grėsmę Europos saugumo tinkle, kuris vykdys „grėsmių žvalgybą“.

3.6. Komisija taip pat sprendžia tiekimo grandinių saugumo ir santykių su tiekėjais klausimą: valstybės narės, bendradarbiaudamos su Komisija ir ENISA, gali atlikti koordinuotą ypatingos svarbos tiekimo grandinių rizikos vertinimą, remdamosi sėkmingai 5G tinklams taikytu metodu, nustatytu 2019 m. kovo 26 d. rekomendacijoje ([4]).

3.7. Pasiūlymu sugriežtinami ir suderinami įmonių saugumo ir ataskaitų teikimo reikalavimai nustatant bendrą rizikos valdymo metodą ir būtiną pagrindinių taikytinų apsaugos priemonių sąrašą. Tiksliau apibrėžiamos nuostatos dėl pranešimų apie incidentus teikimo tvarkos, ataskaitų turinio ir terminų. Pasiūlyme apibrėžiamas dviejų etapų metodas: įmonės per 24 valandas nuo incidento pateikia pradinį pranešimą, o vėliau per vieną mėnesį pateikia išsamią galutinę ataskaitą.

([3]) OL L 345, 2008 12 23, p. 75.
([4]) OL L 88, 2019 3 29, p. 42.

3.8. Numatyta, kad valstybės narės nustatyto už krizių valdymą atsakingas nacionalines institucijas, parengia konkrečius planus ir sukuria naują operatyvinio bendradarbiavimo tinklą „Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas“ (EU-CyCLONe). Stiprinamas Bendradarbiavimo grupės vaidmuo priimant strateginius sprendimus ir sukuriamas ENISA valdomas ES pažeidžiamumų registras; taip pat sustiprinamas dalijimasis informacija ir bendradarbiavimas tarp valstybių narių institucijų, įskaitant operatyvinį bendradarbiavimą kibernetinių krizių valdymo srityje.

3.9. Nacionalinėms valdžios institucijoms nustatytos griežtesnės priežiūros priemonės, griežtesni vykdymo užtikrinimo reikalavimai ir siekiama suderinti sankcijų taikymo tvarką visose valstybėse narėse.

3.10. Pasiūlyme dėl direktyvos nustatomas administracinių sankcijų už kibernetinio saugumo rizikos valdymo ir pranešimo pareigų pažeidimą sąrašas. Apibrėžiamos nuostatos dėl fizinių asmenų, einančių atstovavimo arba vadovaujamas pareigas įmonėse, kurioms taikoma direktyva, atsakomybės. Pasiūlymu patobulinamas būdas, kuriuo ES užkerta kelią didelio masto kibernetinio saugumo incidentams ir krizėms, juos valdo ir į juos reaguoja, nustatydama aiškią atsakomybę, tinkamą planavimą ir tvirtesnį bendradarbiavimą ES lygmeniu.

3.11. Valstybės narės gali bendrai stebėti, kaip įgyvendinamos ES taisyklės, ir padėti viena kitai kilus tarpvalstybinėms problemoms, užmegzti labiau struktūrizuotą dialogą su privačiuoju sektoriumi, suderintai atskleisti informaciją apie vidaus rinkoje parduodamos programinės ir aparatinės įrangos pažeidžiamumą, atlikti suderintus saugumo rizikos ir su naujomis technologijomis susijusios grėsmės vertinimus, kaip tai buvo daroma 5G atveju.

4. **Pasiūlymas dėl direktyvos dėl ypatingos svarbos subjektų atsparumo**

4.1. 2006 m. ES parengė Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos (EPCIP), o 2008 m. priėmė Europos direktyvą dėl ypatingos svarbos infrastruktūros objektų (ECI direktyva), kuri taikoma energetikos ir transporto sektoriams. Europos Komisijos priimtoje 2020–2025 m. ES saugumo sąjungos strategijoje ([5]) ir neseniai priimtoje Kovos su terorizmu darbotvarkėje pabrėžiama, kad svarbu užtikrinti ypatingos svarbos infrastruktūros atsparumą fizinėms ir skaitmeninėms grėsmėms. Tačiau tiek 2019 m. atliktas direktyvos dėl ypatingos svarbos infrastruktūros objektų įgyvendinimo vertinimas, tiek nagrinėjamo pasiūlymo poveikio vertinimo išvados parodė, kad esamų Europos ir nacionalinių priemonių nepakanka, kad veiklos vykdytojai galėtų spręsti su dabartinėmis grėsmėmis susijusias problemas. Todėl Taryba ir Parlamentas paragino Komisiją persvarstyti dabartinę ypatingos svarbos infrastruktūros objektų apsaugos strategiją.

4.2. 2020 m. liepos 24 d. Komisija priėmė ES saugumo sąjungos strategiją, kurioje pripažino didėjantį fizinės ir skaitmeninės infrastruktūros objektų tarpusavio junglumą ir priklausomybę ir pabrėžė, kad reikalingas išsamesnis ir nuoseklesnis požiūris į ESI ir TIS direktyvas. Todėl pasiūlymu dėl CER direktyvos, kurios esminių subjektų požiūriu taikymo sritis yra tokia pati, kaip ir TIS 2 direktyvos, išplečiama pirminė Direktyvos 2008/114/EB taikymo sritis, apimanti tik energetikos ir transporto sektorius, į ją įtraukiant kitus sektorius: bankų, finansų rinkos infrastruktūros, sveikatos infrastruktūros objektai, geriamojo vandens ir nuotekų, skaitmeninės infrastruktūros, viešojo administravimo ir kosmoso, numatant, be kita ko, aiškią atsakomybę, tinkamą planavimą ir tvirtesnį bendradarbiavimą. Turėtų būti sukurtas visų rūšių rizikos orientacinis pagrindas ir remiamos valstybių narių pastangos užtikrinti, kad ypatingos svarbos subjektai galėtų užkirsti kelią incidentams, atlaikyti juos ir sušvelninti jų pasekmes, nepriklausomai nuo to, ar rizika susijusi su gaivalinėmis nelaimėmis, incidentais, terorizmu, vidaus grėsmėmis ar visuomenės sveikatos ekstremaliosiomis situacijomis, panašiomis į dabartinę.

4.3. Kiekviena valstybė narė turi priimti nacionalinę ypatingos svarbos subjektų atsparumo užtikrinimo strategiją, reguliariai atlikti rizikos vertinimus ir tuo remdamasi nustatyti „ypatingos svarbos subjektus“. Taip pat reikalaujama, kad ypatingos svarbos subjektai atliktų rizikos vertinimus, imtųsi tinkamų techninių ir organizacinių priemonių atsparumui didinti ir praneštų apie incidentus nacionalinėms valdžios institucijoms. Subjektams, teikiantiems esmines paslaugas bent trečdaliui valstybių narių arba bent trečdalyje valstybių narių, taikoma konkreti priežiūra, įskaitant specialias Komisijos organizuojamas patariamąsias misijas.

4.4. Pasiūlyme dėl direktyvos CER numatyta įvairių formų parama valstybėms narėms ir ypatingos svarbos subjektams, rizikos apžvalga ES lygmeniu, geriausia praktika ir metodika, taip pat mokymai ir pratybos, skirti apmokyti patikrinti ypatingos svarbos subjektų atsparumą. Tarpvalstybinio bendradarbiavimo sistemoje taip pat numatyta sudaryti specialią ekspertų grupę „Ypatingos svarbos subjektų atsparumo klausimų grupę“, kuri taptų valstybių narių strateginio bendradarbiavimo ir keitimosi informacija forumu.

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

5. **Rekomenduojami pakeitimai nagrinėjamam teisėkūros pasiūlymui**

5.1. EESRK teigiamai vertina Komisijos pastangas didinti viešųjų ir privačiųjų subjektų atsparumą kibernetinėms ir fizinėms grėsmėms. Tai labai svarbu ir aktualu visų pirma dėl sparčios skaitmeninės transformacijos, kurią paskatino COVID-19 protrūkis. Komitetas taip pat pritaria komunikato „Europos skaitmeninės ateities kūrimas“ teiginiui, kad Europai labai svarbu pasinaudoti visais skaitmeninio amžiaus privalumais ir įtraukiu būdu sustiprinti savo pramonę, ypatingą dėmesį skiriant MVĮ, ir inovacijų pajėgumus laikantis strategijos, grindžiamos keturiais ramsčiais: duomenų apsauga, pagrindinės teisės, sauga ir kibernetinis saugumas, kurie yra būtinos sąlygos kuriant duomenų visuomenę.

5.2. Vis dėlto, atsižvelgdamas į poveikio vertinimo ir konsultacijų, surengtų prieš pateikiant pasiūlymą dėl TIS 2 direktyvos, rezultatus, taip pat į ne kartą skelbtą ir 2017 m. spalio 4 d. Komunikate dėl TIS direktyvos įgyvendinimo ([6]) patvirtintą tikslą – išvengti nacionaliniu lygmeniu priimtų taisyklių susiskaidymo, EESRK atkreipia dėmesį į tai, kad neaišku, kodėl Komisija pasiūlė priimti direktyvą, o ne reglamentą ir tokia galimybė net nebuvo svarstoma.

5.3. EESRK pažymi, kad kai kurios šių dviejų pasiūlymų dėl direktyvos nuostatos sutampa, nes jos yra glaudžiai susijusios ir viena kitą papildo, vienoje jų daugiausia dėmesio skiriama kibernetiniam saugumui, o kitoje – fiziniam saugumui. Taip pat reikėtų atkreipti dėmesį, kad CER direktyvoje nurodyti ypatingos svarbos subjektai priklauso tiems patiems sektoriams ir sutampa su ypatingos svarbos subjektais, kurie nurodyti TIS 2 direktyvoje ([7]). Be to, visiems ypatingos svarbos subjektams, kuriems taikoma CER direktyva, taikomi TIS 2 direktyvoje nustatyti kibernetinio saugumo reikalavimai. Siekiant susieti abu pasiūlymus abiejuose pateikiama keletas nuostatų dėl pereigos: nuostatos dėl sustiprinto institucijų bendradarbiavimo, dėl informacijos apie priežiūros veiklą keitimosi, dėl pranešimų teikimo TIS 2 direktyvoje nustatytoms institucijoms apie ypatingos svarbos subjektų pagal CER direktyvą nustatymą, taip pat dėl reguliarių, bent kartą per metus rengiamų, atitinkamų bendradarbiavimo grupių posėdžių. Abu pasiūlymai taip pat grindžiami tuo pačiu teisiniu pagrindu – SESV 114 straipsniu, kuriuo siekiama užtikrinti vidaus rinkos veikimą suderinant nacionalines taisykles, kaip ES Teisingumo Teismas ex multis aiškino savo sprendime byloje C-58/08, *Vodafone ir kt.* Todėl Komitetas ragina apsvarstyti galimybę abu pasiūlymus sujungti į vieną tekstą supaprastinimo ir racionalizavimo sumetimais.

5.4. EESRK pritaria skirtumo tarp esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų panaikinimui, kaip nurodyta pirminėje Kibernetinio saugumo direktyvoje (TIS direktyva), tačiau atkreipia dėmesį į tai, kad, kalbant apie taikymo sritį, reikėtų pateikti tikslesnes ir aiškesnes nuorodas, kaip nustatyti, kokiems subjektams direktyva yra taikoma. Be nuorodų I ir II prieduose, TIS 2 direktyvoje pateikiami įvairūs su opiais kokybiniais ir kiekybiniais vertinimais susiję, tačiau tarpusavyje nesuderinti kriterijai, todėl vertinimai nacionaliniu lygmeniu gali būti atliekami skirtingai, dėl ko kyla susiskaidymo, kurio buvo siekiama išvengti imantis atitinkamų teisės aktų, pavojus. Svarbu, kad nacionaliniu lygmeniu nebūtų taikomi skirtingi veiksmai, dėl kurių atsirastų kliūčių konkurencijai ir laisvam prekių ir paslaugų judėjimui, kiltų pavojus, kad bus pakenkta įmonėms ir daromas poveikis prekybai.

5.5. TIS 2 direktyvoje numatyta, kad šių sektorių ypatingos svarbos operatoriai, kurie pagal šį pasiūlymą laikomi „esminiais“, taip pat būtų įpareigoti laikytis bendresnio pobūdžio atsparumą didinančių įpareigojimų visų pirma atsižvelgiant į nekibernetinę riziką pagal CER direktyvą. Tačiau pastarojoje direktyvoje aiškiai nurodoma, kad jis netaikomas TIS 2 direktyvoje aptariamiems klausimams. Iš tiesų CER direktyvoje teigiama, kad, kadangi TIS 2 direktyvoje kibernetinio saugumo klausimas pakankamai aptartas, joje nagrinėjami klausimai neturėtų būti kartojami CER direktyvoje, kurioje nustatomas režimas, taikomas skaitmeninės infrastruktūros sektoriaus subjektams. Toliau CER direktyvoje pabrėžiama, kad su skaitmeninės infrastruktūros sektoriumi susiję subjektai savo veiklą iš esmės grindžia tinklų ir informacinėmis sistemomis ir patenka į TIS 2 direktyvos taikymo sritį, kurioje sprendžiami tokių sistemų fizinio saugumo klausimai atsižvelgiant į jų kibernetinio saugumo rizikos valdymą ir pareigas pranešti. Be to, CER direktyvoje nurodoma, kad neatmetama galimybė, jog šiems subjektams gali būti taikomos specialiosios šios direktyvos nuostatos.

5.6. Sistema sudėtinga, todėl EESRK nuomone svarbu, kad Komisija tiksliai paaiškintų abiejų teisės aktų taikymo sritį, visų pirma tais atvejais, kai skirtingomis nuostatomis siekiama reguliuoti tuos pačius atvejus arba subjektus.

5.7. EESRK atkreipia dėmesį į tai, kad visų teisės nuostatų aiškumas, ypač kai jos įtraukiamos į tokius plačius ir sudėtingus dokumentus, kaip nagrinėjami šioje nuomonėje, yra esminis tikslas, kaip ir biurokratizmo ir susiskaidymo mažinimas supaprastinant procesus, saugos reikalavimus ir pranešimo apie incidentus reikalavimus. Taip pat reikia siekti,

([6]) COM(2017) 476 *final*.
([7]) 1 priedas (OL L 194, 2016 7 19 p. 1).

kad daugėjant konkrečioms užduotims vykdyti paskirtų įstaigų netaptų sunkiau aiškiai nustatyti jų kompetenciją, nes tai trukdytų įgyvendinti siekiamus tikslus. Todėl šiuo tikslu ir siekiant naudos piliečiams ir įmonėms, galėtų būti tikslinga du pasiūlymus dėl direktyvos sujungti į vieną tekstą ir taip išvengti kartais sudėtingo aiškinimo ir taikymo.

5.8. Įvairiose TIS 2 direktyvos vietose nurodomos kitų teisės aktų nuostatos, pavyzdžiui, Direktyvos (ES) 2018/1972 ([8]), kuria nustatomas Europos elektroninių ryšių kodeksas ir kurios taikymas grindžiamas konkretumo principu. Kai kurios minėtos direktyvos nuostatos yra aiškiai panaikintos (40 ir 41 straipsniai), o kitos turi būti taikomos laikantis nurodyto principo, nepateikiant jokių paaiškinimų šiuo klausimu. Šiuo klausimu EESRK tikisi, kad visos abejonės bus išsklaidytos siekiant išvengti aiškinimo problemų. EESRK taip pat pritaria Komisijos tikslui suderinti sankcijų sistemą ir jų taikymo tvarką tais atvejais, kai nesilaikoma rizikos valdymo reikalavimų, šiuo tikslu geriau keičiantis informacija ir bendradarbiaujant ES lygmeniu.

5.9. EESRK pripažįsta, kad, kaip pabrėžiama pasiūlyme dėl direktyvos, kibernetinio saugumo strategijoje ir rizikos valdyme labai svarbus vaidmuo tenka „esminių“ ir „svarbių“ subjektų valdymo organams, nes jie turi patvirtinti rizikos valdymo priemones, prižiūrėti jų įgyvendinimą ir reaguoti į bet kokius neatitikimus. Todėl šių organų nariai turėtų reguliariai dalyvauti specialiuose mokymuose, kad galėtų įgyti pakankamai žinių ir įgūdžių, kurie leistų suprasti ir valdyti kibernetinio saugumo riziką ir įvertinti jos poveikį. Vis dėlto EESRK mano, kad pasiūlyme turėtų būti nurodytas tokių žinių ir įgūdžių turinys, kad Europos lygmeniu būtų galima pateikti gaires, kokių įgūdžių turi būti mokoma, kad jie atitiktų pasiūlyme nustatytus reikalavimus, ir taip išvengti skirtingo šalyse vykdomų mokymų turinio.

5.10. EESRK pritaria svarbiam ENISA vaidmeniui bendroje Europos institucinėje ir operatyvinėje kibernetinio saugumo sistemoje. Atsižvelgdamas į tai mano, kad be kibernetinio saugumo Sąjungoje būklės ataskaitos, ši agentūra turėtų skelbti naujausią informaciją apie kompiuterių saugumo incidentus ir konkretiems sektoriams skirtus pranešimus; taip suinteresuotosioms šalims, kurioms taikoma TIS 2 direktyva, būtų suteikiama naudingos informacijos ir jie galėtų geriau apsaugoti savo įmones.

5.11. EESRK sutinka, kad prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Šiuo požiūriu viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi priemonė nacionalinėms kompetentingoms institucijoms, CSIRT, įmonėms ir naudotojams. Todėl EESRK pritaria pasiūlymui pavesti ENISA sukurti Europos pažeidžiamumo registrą, kuriame pagrindiniai ir svarbūs subjektai ir jų tiekėjai galėtų pateikti informaciją, kuri sudarytų sąlygas naudotojams imtis atitinkamų rizikos mažinimo priemonių. Vis dėlto mano, kad pranešimas apie pažeidžiamumą ir didelius incidentus turi būti privalomas, o ne savanoriškas, kad tai taptų naudinga priemone perkančioms organizacijoms, dalyvaujančioms įvairiose viešųjų pirkimų procedūrose Europos lygmeniu, įskaitant 5G produktus ir technologijas. Tokiame registre būtų pateikiama informacija, kuria būtų galima pasinaudoti vertinant pasiūlymus ir patikrinti pasiūlymų kokybę ir Europos bei ne Europos rangovų patikimumą pagal produktų ir paslaugų, dėl kurių skelbiamas konkursas, saugumą, vadovaujantis 2019 m. kovo 26 d. 5G tinklų kibernetinio saugumo rekomendacija. Registras taip pat turėtų užtikrinti, kad jame pateikiama informacija būtų prieinama vengiant bet kokios diskriminacijos.

Briuselis, 2021 m. balandžio 27 d.

Europos ekonomikos ir socialinių reikalų komiteto pirmininkė
Christa SCHWENG

([8]) OL L 321, 2018 12 17, p. 36.