Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020“

(COM(2022) 454 final – 2022/0272 (COD))

(2023/C 100/15)

Raportöör: **Maurizio MENSI**

Kaasraportöör: **Marinel Dănuț MUREȘAN**

Konsulteerimistaotlus	Euroopa Parlament, 9.11.2022
	Euroopa Liidu Nõukogu, 28.10.2022
Õiguslik alus	Euroopa Liidu toimimise lepingu artikkel 114
Vastutav sektsioon	ühtse turu, tootmise ja tarbimise sektsioon
Vastuvõtmine sektsioonis	10.11.2022
Vastuvõtmine täiskogus	14.12.2022
Täiskogu istungjärk nr	574
Hääletuse tulemus	
(poolt/vastu/erapooletuid)	177/0/0

1. **Järeldused ja soovitused**

1.1. Euroopa Majandus- ja Sotsiaalkomitee väljendab heameelt komisjoni ettepaneku üle võtta vastu küberkerksuse õigusakt, millega kehtestatakse kõrgemad küberturvalisuse standardid, et luua usaldusväärne süsteem ettevõtjatele ja tagada ELi kodanikele, et turul pakutavaid tooteid on ohutu kasutada. See algatus on osa Euroopa andmestrateegiast, millega tugevdatakse andmete, sealhulgas isikuandmete turvalisust ja põhiõigusi, mis on meie digiühiskonna olulised eeltingimused.

1.2. Komitee peab hädavajalikuks tugevdada ühist reageerimist küberrünnetele ning konsolideerida küberturvalisuse ühtlustamise protsessi riigi tasandil tegevuseeskirjade ja -vahendite osas, et vältida olukorda, kus riikide erinevad lähenemisviisid võivad tekitada õiguslikku ebakindlust ja õigustakistusi.

1.3. Komitee väljendab heameelt komisjoni algatuse üle, mis mitte ainult ei saa aidata vähendada ettevõtjatele küberrünnakutest tulenevaid märkimisväärseid kulusid, vaid võimaldab ka kodanikel/tarbijatel saada kasu oma põhiõiguste, näiteks eraelu puutumatuse paremast kaitsest. Eelkõige näitab komisjon, et sertifitseerimisasutuste osutatavate teenuste puhul võetakse arvesse VKEde erivajadusi. Komitee juhib siiski tähelepanu vajadusele selgitada kohaldatavaid kriteeriume.

1.4. Komitee peab oluliseks rõhutada, et kuigi on tervitatav, et küberkerksuse õigusaktiga on hõlmatud praktiliselt kõik digitaalsed tooted, võivad selle praktilisel rakendamisel tekkida probleemid, arvestades sellega kaasnevat märkimisväärset ja keerukat analüüsi- ja kontrollitegevust. Seetõttu on vaja tugevdada järelevalve- ja kontrollivahendeid.

1.5. Komitee juhib tähelepanu vajadusele määrata täpselt kindlaks küberkerksuse õigusakti sisuline kohaldamisala, pöörates erilist tähelepanu digielemente sisaldavatele toodetele ja tarkvarale.

1.6. Komitee märgib, et tootjad on kohustatud teatama ühelt poolt toodete nõrkustest ja teiselt poolt kõigist turvaintsidentidest, teavitades nendest Euroopa Liidu Küberturvalisuse Ametit (ENISA). Sellega seoses on oluline, et ENISA käsutusse antaks vajalikud vahendid, et amet saaks täita õigeaegselt ja tõhusalt talle usaldatud olulisi ja tundlikke ülesandeid.

1.7. Tõlgendamisest tuleneva ebaselguse vältimiseks soovitab komitee komisjonil koostada suunised, et suunata tootjaid ja tarbijaid konkreetsete kohaldatavate eeskirjade ja menetluste osas, kuna näib, et mitmete ettepaneku kohaldamisalasse kuuluvate toodete suhtes kohaldatakse ka muid küberturvalisust käsitlevaid õigusnorme. Sellega seoses oleks samuti oluline, et iseäranis VKEdel ja mikroettevõtjatel on juurdepääs kvalifitseeritud ekspertide abile, kes suudavad pakkuda spetsiaalseid professionaalseid teenuseid.

1.8. Komitee märgib, et suhted küberkerksuse õigusakti tähenduses sertifitseerimisasutuste ja muude asutuste vahel, kes on teiste õigusnormide alusel volitatud küberturvalisuse sertifitseerimiseks, ei ole täiesti selged. Sama tegevuse koordineerimise probleem võib tekkida ka siin vaadeldavas ettepanekus ette nähtud järelevalveasutuste ja samade toodete suhtes kohaldatavate teiste õigusnormide alusel juba tegutsevate järelevalveasutuste vahel.

1.9. Komitee märgib, et ettepanekus nähakse sertifitseerimisasutustele ette märkimisväärne hulk tegevusi ja kohustusi, mis tuleb praktikas tagada. See on vajalik ka selleks, et küberkerksuse õigusakt ei tooks kaasa halduskoormuse suurenemist, mis karistaks tootjaid, kes peavad turul tegutsemise jätkamiseks täitma rea täiendavaid sertifitseerimisnõudeid.

2. **Ettepaneku analüüs**

2.1. Küberkerksuse õigusakti ettepanekuga kavatseb komisjon põhjalikult ja horisontaalselt ratsionaliseerida ja ümber kujundada kehtivad küberturvalisust käsitlevad õigusnormid, samal ajal ajakohastades neid tehnoloogiliste uuenduste valguses.

2.2. Küberkerksuse õigusaktiga taotletakse peamiselt nelja eesmärki: tagada, et tootjad parandavad digielemente sisaldavate toodete turvalisust alates projekteerimis- ja arendamisetapist ning kogu elutsükli jooksul; tagada sidus küberturvalisuse raamistik, mis hõlbustab riist- ja tarkvaratootjatel nõuete täitmist; suurendada digielemente sisaldavate toodete turvaomaduste läbipaistvust ning võimaldada ettevõtjatel ja tarbijatel selliseid tooteid turvaliselt kasutada. Sisuliselt kehtestatakse ettepanekuga küberturvalisuse CE-märgis, mis tuleb kinnitada kõigile küberkerksuse õigusaktiga hõlmatud toodetele.

2.3. Tegemist on horisontaalse meetmega, mille abil komisjon kavatseb kogu temaatikat põhjalikult reguleerida, kuna sellega on hõlmatud peaaegu kõik digielemente sisaldavad tooted. Välja on jäetud meditsiinilised tooted, tsiviillennundusega seotud tooted, sõidukid ja sõjaliseks otstarbeks mõeldud tooted. Lisaks ei hõlma ettepanek selliseid teenuseid nagu teenusena pakutav tarkvara (SaaS – pilvteenus), välja arvatud juhul, kui neid kasutatakse digielemente sisalduvate toodete valmistamiseks.

2.4. Mõiste „digielemente sisaldavad tooted“ on väga lai ja hõlmab mis tahes tarkvaralisi või riistvaralisi tooteid, samuti tarkvara või riistvara, mida ei ole tootes kasutatud, kuid mis lastakse turule eraldi.

2.5. Õigusaktiga kehtestatakse kohustuslikud küberturvalisuse nõuded toodetele, mis sisaldavad digielemente. Need nõuded kehtivad kogu elutsükli jooksul, kuid ei asendata juba kehtestatud nõudeid. Pigem loetakse uue määruse kohaselt normidele vastavaks ka tooteid, mis on juba sertifitseeritud vastavalt olemasolevatele ELi standarditele.

2.6. Üldpõhimõte on, et Euroopas viiakse turule ainult turvalisi tooteid, mille tootjad tagavad, et need tooted jäävad turvaliseks kogu nende elutsükli jooksul.

2.7. Toode loetakse turvaliseks, kui see on projekteeritud ja valmistatud nii, et selle turvalisuse tase vastab selle kasutamisega kaasnevatele küberriskidele, sellel ei ole müügihetkel teadaolevaid nõrkusi, sellel on turvaline vaikimisi konfiguratsioon, see on kaitstud ebaseaduslike ühenduste eest, see kaitseb andmeid, mida kogub, ning tagab, et kogutavad andmed piirduvad toote toimimiseks vajalike andmetega.

2.8. Tootja loetakse sobivaks oma tooteid turustama, kui ta teeb kättesaadavaks oma toodete erinevate tarkvarakomponentide loetelu, pakub viivitamata tasuta parandusmeetmeid uute nõrkuste korral, avalikustab ja selgitab üksikasjalikult nõrkusi, mida ta avastab ja lahendab, ning kontrollib korrapäraselt tema turustatavate toodete töökindlust. Neid ja muid küberkerksuse õigusaktiga kehtestatud tegevusi tuleb teha toote kogu elutsükli jooksul või vähemalt viis aastat pärast toote turule laskmist. Tootja peab tagama, et turvanõrkused kõrvaldatakse korrapäraste tarkvarauuenduste abil.

2.9. Eri sektorites kohaldatava üldpõhimõtte kohaselt lasuvad need kohustused ka importijatel ja turustajatel.

2.10. Küberkerksuse õigusaktis on sätestatud nn tavapäraste toodete ja tarkvara makrokategooria, mille puhul võib tugineda tootja enesehindamisele, nagu juba tehakse muud liiki CE-märgisele vastavuse sertifitseerimise puhul. Komisjoni sõnul kuulub 90 % turul olevatest toodetest sellesse kategooriasse.

2.11. Asjaomased tooted võib turule lasta pärast seda, kui tootja, kes esitab õigusakti suunistes sätestatud asjakohased dokumendid, on toodete küberturvalisust ise hinnanud. Sama tootja peab toote muutmise korral viima läbi uue hindamise.

2.12. Ülejäänud 10 % toodetest on jagatud veel kahte kategooriasse: I klass (väiksema riskiga) ja II klass (suurema riskiga), mis nõuab suuremat tähelepanu toodete turuleviimisel. Nende puhul on tegu nn digielemente sisaldavate kriitilise tähtsusega toodetega, mille puudused võivad kaasa tuua muid ohtlikke ja laiemaid turvarikkumisi.

2.13. Kõnealustesse kahte klassi kuuluvate toodete puhul on põhiline enesehindamine lubatud ainult juhul, kui tootja tõendab, et ta on järginud konkreetseid turustusstandardeid ja turvaspetsifikaate või läbinud ELi poolt juba ette nähtud küberturvalisuse sertifitseerimise. Vastasel juhul võib ta saada tootesertifikaadi akrediteeritud sertifitseerimisasutuselt. See sertifitseerimine on II klassi toodete puhul kohustuslik.

2.14. Toodete riskikategooriatesse liigitamise süsteem sisaldub ka tehisintellekti käsitleva määruse ettepanekus. Selleks et vältida kahtlusi kohaldatavate sätete suhtes, hõlmatakse küberkerksuse õigusaktiga digielemente sisaldavad tooted, mis on tehisintellekti käsitleva ettepaneku kohaselt samaaegselt liigitatud suure riskiga tehisintellektisüsteemideks. Sellised tooted peavad üldiselt vastama tehisintellekti määruses sätestatud vastavushindamismenetlusele, välja arvatud digielemente sisaldavad kriitilise tähtsusega tooted, mille suhtes kohaldatakse lisaks küberkerksuse õigusakti küberturvalisuse olulistele nõuetele ka küberkerksuse õigusakti vastavushindamise eeskirju.

2.15. Selleks et tagada küberkerksuse õigusakti järgimine, usaldab iga liikmesriik järelevalvetegevuse konkreetsele riigi ametiasutusele. Kui riigi ametiasutus leiab kooskõlas muude toodete ohutust käsitlevate õigusaktidega, et toote küberturvalisuse omadused ei ole enam piisavad, võib selle turustamise asjaomases riigis peatada. Euroopa Liidu Küberturvalisuse Amet on pädev üksikasjalikult hindama teatatud toodet ja kui tuvastatakse toote puudulik ohutus, võivad ameti hinnangud viia toote turustamise peatamiseni ELis.

2.16. Küberkerksuse õigusakti karistussüsteem sisaldab rida rikkumiste raskusele vastavaid karistusi, mis võivad toodete oluliste küberturvalisuse nõuete rikkumise korral ulatuda kuni 15 miljoni euroni või 2,5 %-ni eelmise maksuaasta käibest.

3. **Märkused**

3.1. Komitee väljendab heameelt komisjoni algatuse üle, mille eesmärk on lisada küberturvalisuse reguleerimise laiemasse võrgustikku üks põhielement. Seda tehakse kooskõlastatult küberturvalisuse direktiiviga ([1]) ja täiendades küberkerksuse õigusakti ([2]). Kõrgetel küberturvalisuse standarditel on oluline roll kõigi ettevõtjate jaoks tugeva ELi küberturvalisuse süsteemi loomisel, mis aitab tagada, et ELi kodanikud kasutavad kõiki turul pakutavaid tooteid ohutult, ja suurendada nende usaldust digimaailma vastu.

3.2. Määruses käsitletakse seega kahte probleemi: paljude toodete madal kübeturvalisuse tase ja eelkõige asjaolu, et paljud tootjad ei paku uuendusi kübeturvalisuse nõrkuste parandamiseks. Kuigi digielemente sisaldavate toodete tootjad kannavad mõnikord mainekahju, kui nende tooted ei ole turvalised, jäävad nõrkustega seotud kulud peamiselt professionaalsete kasutajate ja tarbijate kanda. See piirab tootjate stiimuleid investeerida turvaliste toodete projekteerimisse ja arendamisse ning pakkuda turvauuendusi. Lisaks puudub ettevõtjatel ja tarbijatel sageli piisav ja täpne teave turvaliste

([1]) Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

([2]) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

toodete valimiseks ning sageli ei tea nad, kuidas tagada, et nende ostetavad tooted on turvaliselt konfigureeritud. Uutes eeskirjades käsitletakse neid kahte aspekti, tegeledes turvauuenduste ja klientidele ajakohastatud teabe esitamise küsimusega. Komitee arvates võib nõuetekohase kohaldamise korral kavandatavast määrusest saada rahvusvaheline küberturvalisuse võrdlusalus ja mudel.

3.3. Komitee peab tervitatavaks ettepanekut kehtestada digielemente sisaldavatele toodetele küberturvalisuse nõuded. Siiski on oluline vältida kattuvust teiste seda küsimust käsitlevate kehtivate õigusaktidega, nagu uus küberturvalisuse 2. direktiiv ([3]) ja tehisintellekti käsitlev määrus.

3.4. Komitee peab oluliseks rõhutada, et kuigi on tervitatav, et küberkerksuse õigusaktiga on hõlmatud praktiliselt kõik digitaalsed tooted, võivad selle praktilisel rakendamisel tekkida probleemid, arvestades sellega kaasnevat märkimisväärset analüüsi- ja kontrollitegevust.

3.5. Küberkerksuse õigusakti sisuline kohaldamisala on lai ja hõlmab kõiki digielemente sisaldavaid tooteid. Kavandatud määratluse kohaselt on hõlmatud kõik tarkvaralised ja riistvaralised tooted ning nendega seotud andmetöötlustoimingud. Komitee soovitab komisjonil selgitada, kas kogu tarkvara kuulub määruse ettepaneku kohaldamisalasse.

3.6. Tootjaid kohustatakse teatama aktiivselt ärakasutatavatest nõrkustest ja turvaintsidentidest. Nad peavad teavitama Euroopa Liidu Küberturvalisuse Ametit (ENISA) kõigist tootes sisalduvatest aktiivselt ärakasutatavatest nõrkustest ja (eraldi) mis tahes intsidendist, mis mõjutab toote turvalisust, igal juhul 24 tunni jooksul pärast intsidendist teada saamist. Sellega seoses märgib komitee, et ENISA käsutusse tuleb anda piisavad vahendid nii arvulises mõttes kui ka ametialase ettevalmistuse poolest, et amet saaks tõhusalt täita talle määruse alusel usaldatavaid asjakohaseid ja tundlikke ülesandeid.

3.7. Asjaolu, et mitmete ettepaneku kohaldamisalasse kuuluvate toodete suhtes kohaldatakse ka muid küberturvalisuse alaseid õigusnorme, võib tekitada ebakindlust selle suhtes, milliseid õigusnorme kohaldada. Kuigi küberkerksuse õigusakti eesmärk on kooskõla kehtiva ELi tooteid reguleeriva õigusraamistikuga ja muude praegu ELi digistrateegia raames ettevalmistamisel olevate ettepanekutega, kattuvad näiteks kõrge riskiteguriga tehisintellekti tooteid käsitlevad eeskirjad isikuandmete töötlemist käsitleva määruse eeskirjadega. Sellega seoses teeb komitee ettepaneku, et komisjon koostaks tootjatele ja tarbijatele suunised õigusakti õige kohaldamise kohta.

3.8. Komitee märgib, et suhted küberkerksuse õigusakti tähenduses sertifitseerimisasutuste ja muude asutuste vahel, kes on teiste võrdselt kohaldatavate eeskirjade alusel volitatud küberturvalisuse sertifitseerimiseks, ei näi olevat täiesti selged.

3.9. Märkimisväärne tegevus- ja vastutuskoormus langeb siis sertifitseerimisasutustele endile, kelle konkreetset tegutsemisvõimet tuleb kontrollida ja see tagada, et vältida olukorda, kus küberkerksuse õigusakt suurendaks tootjatele juba praegu turul tegutsemiseks pandud halduskoormust. Sellega seoses oleks samuti oluline, et iseäranis VKEdel ja mikroettevõtjatel on juurdepääs kvalifitseeritud ekspertide abile, kes suudavad pakkuda spetsiaalseid professionaalseid teenuseid.

3.10. Küberkerksuse õigusaktiga nähakse ette, et sertifitseerimisasutused võtavad endi osutatavate teenuste puhul arvesse VKEde erivajadusi. Komitee juhib siiski tähelepanu vajadusele selgitada kohaldatavaid kriteeriume.

3.11. Koordineerimise probleem võib tekkida ka siin vaadeldavas määruses ette nähtud järelevalveasutuste ja samade toodete suhtes kohaldatavate teiste eeskirjade alusel juba tegutsevate järelevalveasutuste vahel. Seepärast soovitab komitee, et komisjon kutsuks liikmesriike üles seda aspekti jälgima ja võtma vajaduse korral meetmeid olukorra parandamiseks.

Brüssel, 14. detsember 2022

Euroopa Majandus- ja Sotsiaalkomitee
president
Christa SCHWENG

([3]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).