Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Droša 5G ieviešana ES – ES rīkkopas īstenošana""

(COM(2020) 50 final)

(2020/C 429/37)

Ziņotājs: ***Alberto MAZZOLA***

Līdzziņotājs: ***Dumitru FORNEA***

Lietu nodošana	Eiropas Komisija, 9.3.2020.
Juridiskais pamats	Līguma par Eiropas Savienības darbību 304. pants
Atbildīgā specializētā nodaļa	Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa
Pieņemts specializētās nodaļas sanāksmē	3.9.2020.
Pieņemts plenārsesijā	16.9.2020.
Plenārsesija Nr.	554
Balsojuma rezultāts	217/0/2
(par/pret/atturas)	

1. **Secinājumi un ieteikumi**

1.1. EESK atzinīgi vērtē dalībvalstu un Eiropas Komisijas (EK) iniciatīvu pārbaudīt, vai dalībvalstis īsteno to pasākumu kopumu, kuri ieteikti stratēģisko un tehnisko 5G ekosistēmas drošas ieviešanas pasākumu ES rīkkopas secinājumos.

1.2. EESK uzskata, ka, ņemot vērā 5G lietojumu pieaugošo sarežģītību un daudzveidību (Komisija 2025. gadam ir noteikusi šādus savienojamības mērķus: skolām, universitātēm, pētniecības centriem, slimnīcām, galvenajiem sabiedrisko pakalpojumu sniedzējiem un uzņēmumiem ar augstu digitālās intensitātes rādītāju internetā vajadzētu būt pieejamam viena gigabita datu lejupielādes/augšupielādes ātrumam sekundē; pilsētu un lauku mājsaimniecībām vajadzētu būt pieejamiem savienojumiem ar lejupielādes ātrumu vismaz 100 megabiti sekundē; pilsētu teritorijām, galvenajiem autoceļiem un dzelzceļiem vajadzētu būt nepārtrauktam 5G pārklājumam), šādai 5G ekosistēmas pārskatīšanai un Komisijas pasākumiem, kas vērsti uz 5G tīklu kiberdrošību un daudzveidīgu 5G vērtību ķēdi, tehnisko standartizāciju un sertificēšanu, ārvalstu tiešajiem ieguldījumiem un tirdzniecības un konkurences aizsardzību, sabiedrisko pakalpojumu pienākumiem, iepirkumu un kiberdiplomātiju būt jāaptver ģeopolitiskā drošība, infrastruktūra un datu drošība, kā arī veselības drošība, turklāt saskaņā ar LESD 168. panta 1. punktu.

1.3. Pēc EESK domām ir svarīgi, lai Eiropas 5G ekosistēma nodrošinātu integritāti, konfidencialitāti, atbildību par vadību un darbību, drošību, piegādes vienkāršību, aparatūras un programmatūras komponentu savietojamību, kopējus tehniskos un normatīvos standartus, pakalpojumu nepārtrauktību, plūsmas uzticamību un datu aizsardzību, pārklājumu visās teritorijās, pat mazapdzīvotajās, skaidrību par saziņu ar lietotāju kā aktīvu subjektu digitālajā tirgū, dinamisku *ICNIRP* norādījumu ievērošanu nolūkā aizsargāt iedzīvotāju veselību. *ICNIRP* attiecīgi 1998. gada pamatnostādnēs ir atjauninājusi to daļu, kas attiecas uz radiofrekvenču elektromagnētisko lauku (EML). Šajā dokumentā ir izklāstītas minētās pārskatītās pamatnostādnes, kas nodrošina cilvēku aizsardzību pret elektromagnētiskā lauka iedarbību diapazonā no 100 kHz līdz 300 GHz. *Health Phys.* 118(5):483–524; 2020- 2020. GADA MARTS *ICNIRP* (2020) ir ieviesusi virkni izmaiņu, lai nodrošinātu, ka jaunas tehnoloģijas, tādas kā 5G, nespēj radīt kaitējumu neatkarīgi no mūsu pašreizējiem pieņēmumiem.

1.4. EESK aicina EK stingri uzraudzīt virzību 5G ieviešanā un reālā izmantošanā un aicina dalībvalstis vēl vairāk paātrināt šo procesu un nodrošināt atbildīgu īstenošanu, ņemot vērā visus drošības un drošuma aspektus, tostarp tos, kas saistīti ar 5G tehnoloģiju ietekmi uz iedzīvotāju veselību un dzīvām ekosistēmām, sociālekonomisko un konkurences ietekmi, izglītības un apmācības ietekmi, kā arī garantējot pamattiesību ievērošanu.

1.5. EESK aicina ES kļūt par pasaules līderi nākamās paaudzes 5G mobilajās tehnoloģijās ar drošu digitālo infrastruktūru, kas ir būtisks Eiropas jaunās mūsdienīgās rūpniecības stratēģijas pamats, krasi mainot mobilo savienojamību un izmantojot milzīgu dinamisko potenciālu palielināt produktivitāti un attīstīt ekonomiku un pakalpojumus iedzīvotājiem.

1.6. EESK jo īpaši uzskata, ka ir būtiski novērtēt piegādātāju riska profilu un piemērot attiecīgus ierobežojumus iespējamajiem paaugstināta riska piegādātājiem – tostarp izņēmumus, kas vajadzīgi, lai efektīvi mazinātu riskus un definētu atbildību –, to attiecinot uz nozīmīgākajiem aktīviem, kas koordinētajā riska novērtējumā ES līmenī atzīti par būtiskiem un jūtīgiem.

1.7. EESK uzskata, ka Eiropai ir ļoti svarīgi vidējā termiņā koncentrēties uz autonomiju un pašpietiekamību šajā jomā, stingri atbalstot pētniecību un Eiropas uzņēmumu daudzveidību. EESK uzskata, ka ir svarīgi palielināt Kopienas līdzekļus digitālajai pētniecībai un inovācijai, kā arī atbalstīt operatoru un piegādātāju ieguldījumus jaunos tehniskās drošības elementos – šādiem ieguldījumiem jāspēj iet roku rokā ar tirgus spēju atzīt un atlīdzināt visas tās iniciatīvas, kuru mērķis ir palielināt sistēmu drošību un noturību.

1.8. Ir svarīgi garantēt drošību visām dalībvalstīm, arī uzturot pētniecības centrus dažādās ES teritorijās. EESK atbalsta arī ierosinājumu katrai valstij izmantot vismaz divus piegādātājus, tostarp vienu no Eiropas, kurš var garantēt datu politisko drošību un veselības ierobežojumu ievērošanu.

1.9. EESK uzskata, ka lielāks uzsvars būtu jāliek uz tādiem rīkiem, kuri paredzēti lietotājiem, iedzīvotājiem un attiecīgajām pilsoniskās sabiedrības organizācijām un kuri ir ierobežoti un neefektīvi – papildus pareizam uzsvaram uz atbilstošajiem pasākumiem, kas attiecas uz valstu regulatoru pilnvarām un telesakaru operatoru lomu –, ar mērķi veicināt patērētāju iespējas un stiprināt patērētāju spēju, lai tiem dotu iespējas kļūt par proaktīviem tirgus dalībniekiem.

1.10. Eiropas Komisijai, Eiropas Parlamentam, Padomei un dalībvalstu valdībām un parlamentiem ir jānodrošina demokrātiska apspriešanās sistēma, kurā sabiedrību var iepazīstināt ar zinātniskiem vai tehnoloģiskiem tematiem, juridiskām garantijām un kompetento iestāžu atbildēm uz pilsoniskās sabiedrības jautājumiem.

1.11. EESK iesaka stiprināt Eiropas tehnoloģisko diplomātiju Eiropas Savienībā, lai nodrošinātu līdzsvarotākus un savstarpīgākus nosacījumus tirdzniecībai un ieguldījumiem, jo īpaši attiecībā uz uzņēmumu piekļuvi tirgum, subsīdijām, publisko iepirkumu, tehnoloģiju nodošanu, rūpniecisko īpašumu, kā arī sociālajiem un vides standartiem.

2. **Ievads**

2.1. 5G tīklu drošība ir stratēģiski svarīgs jautājums attiecībā uz visu ES vienoto tirgu un tehnoloģisko suverenitāti. Jau 2013. gadā Komisija uzsāka ES pamatiniciatīvu, nodibinot publiskā un privātā sektora partnerību 5G jautājumos (5G PPP), lai paātrinātu pētniecību un inovācijas 5G tehnoloģijas jomā.

2.2. Ir aplēsts, ka 2025. gadā visā pasaulē no 5G tīkliem tiks gūti ieņēmumi vairāk nekā 100 miljardu EUR apmērā, tādējādi 5G ir būtisks līdzeklis, kas ļaus Eiropai konkurēt pasaules tirgū, un tīklu kiberdrošība ir īpaši svarīga Savienības stratēģiskās autonomijas nodrošināšanā.

2.3. 5G tīklu pamatā ir pašreizējās 4. paaudzes (4G) tīkla tehnoloģijas un optiskās šķiedras infrastruktūra, nodrošinot jaunas pakalpojumu iespējas un kļūstot par Savienības ekonomikas lielas daļas galveno infrastruktūru un virzītājspēku, lai veidotu pamatu plašam pakalpojumu klāstam, kas ir būtiski iekšējā tirgus darbībai un būtisku ekonomisko un sociālo funkciju uzturēšanai un pārvaldībai, piemēram, enerģētikas, transporta, banku un veselības aprūpes pakalpojumu, kā arī lauksaimniecības un rūpnieciskās ražošanas, izplatīšanas un patēriņa sistēmu jomā.

2.4. Ņemot vērā 5G tīklu svarīgo nozīmi ES ekonomikas un sabiedrības digitālās pārveides īstenošanā un ņemot vērā digitālās ekosistēmas pamatinfrastruktūras savstarpēji saistīto un starptautisko būtību un attiecīgo apdraudējumu pārrobežu raksturu, jebkura ievērojama neaizsargātība un/vai kiberdrošības starpgadījumi, kas saistīti ar 5G tīkliem un kas notiek kādā dalībvalstī, ietekmētu Savienību kopumā. Tādēļ būtu lietderīgi paredzēt pasākumus 5G tīklu augstāka kopējā kiberdrošības līmeņa atbalstam.

2.5. EK 2016. gadā kā daļu no iniciatīvu kopuma – sākot no paziņojuma par gigabaitu savienojamību konkurētspējīgam digitālajam vienotajam tirgum ([1]) ([2]) un ietverot pasākumus, ar kuriem pārskata elektronisko sakaru tiesisko regulējumu ([3]) un Eiropas Elektronisko sakaru regulatoru iestādes (*BEREC*) funkcijas ([4]), prioritātes IKT standartizācijā digitālajā vienotajā tirgū ([5]), kā arī pasākumus interneta savienojamības veicināšanai vietējās kopienās ([6]) –, pieņēma ES rīcības plānu attiecībā uz 5G ([7]) (par kuru EESK ir izteikusies atzinīgi ([8])), lai pastiprinātu ES centienus izvērst 5G infrastruktūru un pakalpojumus digitālajā vienotajā tirgū, kā arī pieņēma ceļvedi valsts un privātajiem ieguldījumiem 5G infrastruktūrā Eiropas Savienībā un mērķi līdz 2020. gadam ieviest 5G tirdzniecības tīklus.

2.6. Saskaņā ar definīciju EK ieteikumā ([9]) "5G tīkli nozīmē visu attiecīgo tīkla infrastruktūras elementu kopumu mobilo un bezvadu sakaru tehnoloģijai, ko izmanto savienojamības un pievienotās vērtības pakalpojumiem, ar uzlabotiem veiktspējas parametriem, piemēram, ļoti lielu datu pārraides ātrumu un jaudu, zema latentuma sakariem, ārkārtīgi augstu uzticamību vai atbalstu lielam skaitam savienotu ierīču".

2.7. Ieteikumā ir norādīts, ka EK atbalstīs ES pieejas 5G kiberdrošībai ieviešanu un pēc dalībvalstu pieprasījuma strādās, lai nodrošinātu 5G infrastruktūras un piegādes ķēdes drošību, vajadzības gadījumā izmantojot visus tās rīcībā esošos rīkus:

— telesakaru, multivides un kiberdrošības noteikumus,

— standartizācijas un sertifikācijas koordinēšanu ES līmenī,

— pamatsistēmu tiešo ārvalstu ieguldījumu kontrolei, lai aizsargātu Eiropas 5G piegādes ķēdi,

— tirdzniecības aizsardzības instrumentus,

— konkurences noteikumus,

— publisko iepirkumu, nodrošinot, ka tiek pienācīgi ņemti vērā drošības aspekti,

— ES finansēšanas programmas, nodrošinot, ka saņēmēji ievēro attiecīgās drošības prasības.

2.8. Dalībvalstis 2019. gada jūlijā izklāstīja savu valstu riska novērtējumu rezultātus sadarbības grupai, ko paredz TID direktīva ([10]) (grupā ir katras dalībvalsts pārstāvji), Eiropas Komisijai un *ENISA*, informējot par galvenajām darbībām, apdraudējumiem un neaizsargātību saskaņā ar ISO/IEC 27005 standartu, kas attiecas uz 5G infrastruktūru un galvenajiem riska scenārijiem, aprakstot iespējamos veidus, kā apdraudējuma dalībnieki varētu izmantot konkrētas darbības neaizsargātību: šie valstu novērtējumi bija pamats turpmākam saskaņotam novērtējumam un kopējai iespējamo riska mazināšanas pasākumu rīkkopai.

2.9. TID sadarbības grupa 2019. gada oktobrī ar EK un ENISA atbalstu iesniedza ziņojumu par piektās paaudzes (5G) tīklu kiberdrošības risku ES mērogā saskaņotu novērtējumu, kurā tika apzinātas vairākas svarīgas problēmas attiecībā uz drošību, kas saistītas ar galvenajām programmatūras, lietojumprogrammu un pakalpojumu tehnoloģiskajām inovācijām, kā arī ar piegādātāju nozīmi 5G tīklu izveidē un izmantošanā un atkarības pakāpi no atsevišķiem piegādātājiem:

— palielināta neaizsargātība pret uzbrukumiem un lielāks iespējamo piekļuves punktu skaits šādu uzbrukumu veicējiem,

— paaugstināta jutība pret jauno 5G tīklu struktūru un funkcionalitātes īpašībām,

— riski, kas saistīti ar mobilo sakaru tīkla operatoru atkarību no piegādātājiem, palielinoties uzbrukumu kanālu skaitam, kurus izmanto apdraudējuma īstenotāji,

---

([1]) LESD 168. panta 1. punkts "Savienības rīcība papildina dalībvalstu politiku …".
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) OV C 125, 21.4.2017., 74. lpp.
([9]) Ieteikums (ES) 2019/534 (2019. gada 26. marts) par 5G tīklu kiberdrošību (OV L 88, 29.3.2019., 42. lpp.).
([10]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

— atsevišķu piegādātāju riska profila atbilstība iespējamiem iejaukšanās gadījumiem ārpus ES,

— palielināti riski, ko rada spēcīga atkarība no piegādātājiem saistībā ar iespējamiem piegādes pārtraukumiem, kurus izraisa tirdzniecības vai cita spriedze,

— apdraudējumi tīklu pieejamībai un integritātei drošības, konfidencialitātes un privātuma aizsardzības jautājumos.

2.10. Visas šīs problēmas rada jaunu drošības paradigmu, kas paredz vajadzību pārskatīt pašreizējo nozarei un tās ekosistēmai piemērojamo politisko un drošības sistēmu, un prasa dalībvalstīm veikt vajadzīgos seku mazināšanas pasākumus.

2.11. *ENISA* 2019. gada 21. novembrī publicēja ziņojumu par tematu "*Threat landscape for 5G Networks* (5G tīklu apdraudējumu panorāma)", kurā tika novērtēti apdraudējumi, kas saistīti ar piektās paaudzes mobilo telesakaru tīkliem, un kurā tika iekļauts ES dalībvalstu ziņojums.

2.12. TID sadarbības grupa 2020. gada 29. janvārī publicēja dokumentu par tematu "5G tīklu kiberdrošība – ES riska mazināšanas pasākumu kopums" ([11]), kurā iekļauts iespējams kopīgu pasākumu kopums, kas spēj mazināt 5G tīklu galvenos kiberdrošības riskus un sniedz norādījumus to pasākumu atlasei, kuriem būtu jāpiešķir prioritāte riska mazināšanas plānos valstu un ES līmenī. Tajā pašā dienā Komisija pieņēma paziņojumu par atbalstu rīkkopai ([12]), kas ir šā atzinuma temats.

2.13. 5G tīkla infrastruktūrā galvenās ieinteresētās personas ir:

— iedzīvotāji, patērētāji un 5G tiešie lietotāji,

— mobilo tīklu operatori – uzņēmumi, kas lietotājiem nodrošina mobilo tīklu pakalpojumus, pārvaldot savu tīklu ar trešo personu palīdzību,

— mobilo tīklu operatoru piegādātāji – uzņēmumi, kas nodrošina pakalpojumus vai infrastruktūru mobilo tīklu operatoriem savu tīklu izveidei un/vai pārvaldībai. Šajā kategorijā ietilpst telesakaru iekārtu ražotāji, citi trešo pušu pakalpojumu sniedzēji, piemēram, mākoņu infrastruktūras nodrošinātāji, sistēmu integrētāji, drošības un tehniskās apkopes darbuzņēmēji, pārraides iekārtu ražotāji,

— savienoto ierīču ražotāji un saistītie pakalpojumu sniedzēji – uzņēmumi, kas nodrošina objektus vai pakalpojumus, kuri izveido savienojumu ar 5G tīkliem (piemēram, viedtālruņi, satīkloti transportlīdzekļi, e-veselība), un saistītos pakalpojumu komponentus, kas tiek iekļauti 5G vadības plānā, kā to paredz uz pakalpojumiem balstīta struktūra vai mobilā perifērdatošana (*Mobile Edge Computing*),

— citas ieinteresētās personas, tostarp pakalpojumu un satura sniedzēji.

Visas šīs ieinteresētās personas ir nozīmīgas ieinteresētās personas drošības jautājumos, gan sniedzot ieguldījumu 5G tīklu kiberdrošībā, gan kā iespējamie uzbrukumu veikšanas punkti vai pārvirzītāji. Tāpēc ir svarīgi novērtēt riskus, kas saistīti ar viņu stāvokli 5G ekosistēmā.

2.14. Galvenās ierastās apdraudējumu kategorijas ir saistītas ar konfidencialitātes, integritātes un pieejamības kompromitēšanu. Proti, tika konstatēts, ka vairāki uz 5G tīkliem vērstu apdraudējumu scenāriji jo īpaši attiecas uz:

— vietējā vai globālā 5G tīkla traucējumiem (pieejamība),

— datu plūsmas spiegošanu 5G tīkla infrastruktūrā (konfidencialitāte),

— datu plūsmas izmainīšana vai maršrutēšanas maiņa 5G tīkla infrastruktūrā (integritāte un/vai konfidencialitāte),

— citu digitālo infrastruktūru vai informācijas sistēmu iznīcināšana vai pārveidošana, izmantojot 5G tīklus (integritāte un/vai pieejamība).

2.15. Valstu vai to atbalstīto dalībnieku radītie apdraudējumi tiek uztverti kā ārkārtīgi svarīgi – tie būtībā ir visnopietnākie un iespējamākie apdraudējumu īstenotāji, jo tiem var būt motivācija, nodomi un, jo īpaši, spēja veikt pastāvīgus un sarežģītus uzbrukumus 5G tīklu drošībai.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures

([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission

Lai arī daudzi no šiem neaizsargātības aspektiem nav raksturīgi tikai 5G tīkliem, to skaits un nozīmīgums, iespējams, palielināsies līdz ar 5G ieviešanu, ņemot vērā augstāku tehnoloģiju sarežģītības pakāpi, kā arī ekonomikas un sabiedrības lielāku paļaušanos uz šo infrastruktūru nākotnē.

2.16. Tā kā 5G tīkli galvenokārt balstīsies uz programmatūru, galvenie drošības trūkumi, piemēram, tādi, kas rodas no sliktiem programmatūras izstrādes procesiem aprīkojuma piegādātāju starpā, varētu dalībniekiem atvieglot apzinātas slepenpiekļuves (backdoor) tīšu izveidi produktos un padarīt tās vēl grūtāk atklājamas. Tas var palielināt iespēju, ka to izmantošanai ir īpaši nopietna un plaši izplatīta nelabvēlīga ietekme. Tā kā vēl nav pilnībā atrisināti ar 4G saistīti kiberdrošības jautājumi, ar 5G saistītas problēmas varētu eksponenciāli pieaugt.

2.17. Jāņem vērā arī procesa vai konfigurācijas neaizsargātības aspekti:

— tāda personāla trūkums, kurš ir specializēts un apmācīts aizsargāt, uzraudzīt un uzturēt 5G tīklus,

— nepilnības pienācīgā iekšējā drošības kontrolē, uzraudzības praksē, drošības pārvaldības sistēmās un neatbilstības riska pārvaldības praksē,

— drošības vai darbības uzturēšanas procedūru neatbilstība, piemēram, programmatūras un ielāpu pārvaldības atjaunināšana 5G tīklos,

— neatbilstība 3GPP standartiem vai nepareiza standartu ieviešana,

— tīkla plānošanas vai struktūras trūkumi, tostarp efektīvu avārijas un nepārtrauktības mehānismu trūkums, neatbilstoša vai nepareiza konfigurācija, piemēram, virtualizācijā vai administrēšanas vai piekļuves tiesībās,

— nepietiekami kritēriji attiecībā uz vietējo un attālināto piekļuvi tīkla komponentiem,

— drošības prasību nepietiekamība iepirkuma procedūrā: šī neaizsargātība var izpausties kā nepiemērotas piegādātāju izvēles stratēģijas vai drošības prioritāšu trūkums attiecībā pret citiem aspektiem.

2.18. Atsevišķu piegādātāju riska profili jānovērtē, pamatojoties uz vairākiem aspektiem joīpaši: iespēju, ka piegādātājs var iejaukties no trešās valsts, ko veicina ciešas saites starp piegādātāju un konkrētas trešās valsts valdību; trešo valstu tiesību aktiem, jo īpaši gadījumos, kad nav likumdošanas vai demokrātisku pārbaužu un līdzsvara un kad ES strādājošās uzņēmuma meitsabiedrības tā rezultātā var atturēties pildīt ES tiesību aktus vai ja starp ES un konkrēto trešo valsti nav noslēgti drošības vai datu aizsardzības nolīgumi; piegādātāja korporatīvā īpašuma raksturojumu; trešās valsts spēju izdarīt jebkāda veida spiedienu, arī attiecībā uz iekārtu ražošanas vietu; vispārējo produktu kvalitāti un piegādātāja kiberdrošības praksi, ieskaitot piegādes ķēdes kontroles līmeni un atbilstīgas drošības prakses prioritātes.

2.19. Dalībvalstis ir vienojušās nodrošināt, ka tiek veikti pasākumi, lai atbilstīgi un samērīgi reaģētu uz jau konstatētajiem riskiem un iespējamiem nākotnes riskiem. Dalībvalstis jo īpaši ir vienojušās nodrošināt, ka, ņemot vērā uz risku orientētu pieeju, tās varēs ierobežot, aizliegt un/vai noteikt īpašas prasības un nosacījumus attiecībā uz 5G tīkla iekārtu piegādi, izplatīšanu un darbību.

2.20. Ņemot to vērā, dalībvalstīm būtu jānodrošina:

— mobilo tīklu operatoriem izvirzīto drošības prasību nostiprināšana, piemēram, jānosaka stingra piekļuves kontrole, jāparedz noteikumi par drošu ekspluatāciju un uzraudzību, jāierobežo konkrētu funkciju nodošana ārpakalpojumu sniedzējiem,

— piegādātāju riska profila novērtējumi, pamatojoties uz objektīviem un skaidriem kritērijiem; līdz ar to, pamatojoties uz proporcionalitātes un juridiskās noteiktības principiem, jāpiemēro attiecīgi ierobežojumi iespējamajiem paaugstināta riska piegādātājiem – tostarp izņēmumi, kas vajadzīgi, lai efektīvi mazinātu riskus –, to attiecinot uz nozīmīgākajiem aktīviem, kas koordinētajā riska novērtējumā ES līmenī atzīti par būtiskiem un jūtīgiem,

— vispārēji atzītu un īstenojamu un uz vienprātību balstītu drošības standartu un paraugprakses ieviešana,

— katram operatoram pieejama vairāku pārdevēju stratēģija, kas paredzēta tam, lai novērstu vai ierobežotu jebkādu būtisku atkarību no viena piegādātāja vai piegādātājiem ar līdzīgu riska profilu,

— stingra piekļuves kontrole un droša tīkla pārvaldība, darbība un uzraudzība, izmantojot 5G tīkla komponentu un/vai procesu sertifikāciju. Šīs stratēģijas pamatā jābūt riska analīzei, ko veic dalībvalstis un operatori, lai vairāku pakalpojumu sniedzēju stratēģijas izvēle nepaaugstinātu operatora tīkla riska līmeni,

— pienācīgs piegādātāju līdzsvars valsts līmenī un novērsta atkarība no piegādātājiem, kurus uzskata par paaugstināta riska piegādātājiem, arī veicinot iekārtu labāku savietojamību,

— daudzveidīgas un ilgtspējīgas 5G piegādes ķēdes uzturēšana, lai novērstu ilgtermiņa atkarību, pilnībā izmantojot ES rīkus ārvalstu tiešo ieguldījumu kontrolei, tirdzniecības aizsardzības rīkus, konkurences noteikumus, ES iepirkuma noteikumus,

— ES iekšējo spēju stiprināšana 5G un tai sekojošajās tehnoloģijās, izmantojot attiecīgās ES programmas un finansējumu, standartizācijas saskaņošanu starp dalībvalstīm, stiprinot testēšanas un revīzijas spējas, lai sasniegtu konkrētus drošības mērķus un izstrādātu atbilstīgas ES sertifikācijas sistēmas saskaņā ar IT drošības tiesību aktiem un veicinātu sadarbspēju.

2.21. Kā EK ir vairākkārt uzsvērusi, Eiropas iekšējais tirgus ir un paliek atvērts tiem, kuri vēlas sākt darbību Eiropā, ja vien visi ievēro skaidrus un stingrus noteikumus, kuru pamatā ir objektīvi kritēriji.

2.22. Padome 2020. gada 6. jūnijā uzsvēra, ka ir būtiski stiprināt digitālo suverenitāti un sadarbību Eiropas Savienībā, kā arī radīt sinerģiju, izmantojot ES programmas, piemēram, Eiropas infrastruktūras savienošanas instrumentu un programmu "Digitālā Eiropa", digitālo prasmju attīstīšanu, datu ekonomikas attīstību, mākslīgā intelekta un IT drošības nozīmi ar aktīvu digitālo lomu zaļā kursa mērķu sasniegšanā.

3. **Komisijas paziņojums**

3.1. Reaģējot uz TID sadarbības grupas paziņojumu par 5G drošības rīkkopu, Eiropas Komisija:

— pēc dalībvalstu pieprasījuma strādā, lai nodrošinātu 5G infrastruktūras un piegādes ķēdes drošību, vajadzības gadījumā izmantojot visus tās rīcībā esošos rīkus,

— aicina dalībvalstis un iestādes nodrošināt efektīvu riska mazināšanas stratēģiju īstenošanu, ES līmenī pieņemt turpmākus koordinācijas pasākumus, lai izveidotu saskaņotu pieeju attiecībā uz 5G kiberdrošību,

— aicina dalībvalstis turpināt īstenot pasākumu kopumu, kas ieteikts rīkkopas secinājumos, un sagatavot kopīgu ziņojumu par to īstenošanu, kamēr NIS sadarbības grupa turpina strādāt, lai veicinātu rīkkopas īstenošanu,

— savas kompetences jomās paredz darbības, lai nodrošinātu 5G tīklu kiberdrošību un daudzveidīgu 5G vērtību ķēdi, tehnisko standartizāciju un sertifikāciju, ārvalstu tiešos ieguldījumus, tirdzniecības un konkurences aizsardzību, publiskos iepirkumus un IT diplomātiju, kā arī savas programmas un fondus, īpaši pētniecības un inovācijas, kohēzijas un izstrādes jomā.

4. **Vispārīgas piezīmes**

4.1. EESK pauž pārliecību par to, ka jaunās 5G tehnoloģijas var pārveidot to, kā mēs mijiedarbojamies ar pasauli, piedāvājot jaunas lietojumprogrammas, darījumdarbības modeļus, jaunu dzīvesveidu, viedas rūpnīcas, lielāku produktivitāti un jaunus kvalitatīvus pakalpojumus iedzīvotājiem, iespējams, paverot durvis revolucionārām tehnoloģijām, piemēram, automatizētiem automobiļiem un progresīvām ražošanas un izplatīšanas sistēmām, kā arī nodrošinot daudzus tūkstošus savstarpēji savienotu ierīču, kurām vajadzētu ienākt mūsu ikdienā kā lietu interneta (IoT) daļai. Tomēr EESK sagaida, ka EK veiks pamatīgākus 5G ietekmes novērtējumus un priekšizpēti, kā arī izmaksu un ieguvumu analīzi un to salīdzinās ar 4G tehnoloģijas vai optisko šķiedru telekomunikāciju izmantošanu. EESK uzskata, ka ir būtiski 5G orientēt uz to, lai panāktu resursu labāku izmantošanu atbilstoši aprites principam un samazinātu apjomīgo oglekļa pēdu, kas saistīta ar enerģiju. EESK uzsver, ka ir svarīgi risināt sociālās strukturālās pārmaiņas, veicinot taisnīgu un vienmērīgu pāreju un novēršot prasmju trūkumu, lai veidotu labāk apmaksātas, elastīgas un augsti kvalificētas darbvietas.

4.2. Trīskāršie riski – nekontrolētas pandēmijas, nepietiekams ekonomikas politikas pasākumu arsenāls, ģeopolitikas "melnais gulbis" – varētu izraisīt pasaules ekonomikas ilgstošu depresiju un finanšu tirgus sabrukumu un bēgšanu no tā, lai gan visas Eiropas sabiedrības grupas arvien vairāk apzinās, ka ilgtspējīgai ekonomikas attīstībai **un notiekošajai digitālajai revolūcijai, kurā 5G ir viens no galvenajiem rīkiem**, ir vajadzīgi pasākumi, kas vienlaikus skar tehnoloģisko aspektu, produktivitātes palielināšanu un resursu efektīvāku izmantošanu, kā arī atbilstošs tiesiskais un regulatīvais ekonomikas un finanšu satvars.

4.3. EESK mudina ES iestādes un dalībvalstis pabeigt digitālā vienotā tirgus izveidi, iekļaujot spēju veidošanu 5G pakalpojumu integrēšanai un izmantošanai, lai aizsargātu un uzlabotu Eiropas rūpniecības konkurētspēju; aicina EK stingri uzraudzīt virzību 5G ieviešanā un reālā izmantošanā un aicina dalībvalstis vēl vairāk paātrināt šo procesu, ņemot vērā visus drošības un drošuma aspektus, tostarp tos, kas saistīti ar 5G tehnoloģiju ietekmi uz iedzīvotāju veselību un dzīvām ekosistēmām, sociālekonomisko un konkurences ietekmi, izglītības un apmācības ietekmi, kā arī garantētu pamattiesību ievērošanu, piemēram, tiesības uz īpašumu vai tiesības uz privātumu un personas datu drošību.

4.4. EESK aicina ES kļūt par pasaules līderi nākamās paaudzes 5G mobilajās tehnoloģijās ar drošu digitālo infrastruktūru, kas ir būtisks Eiropas jaunās mūsdienīgās rūpniecības stratēģijas pamats, krasi mainot mobilo savienojamību un izmantojot milzīgu dinamisko potenciālu palielināt produktivitāti un attīstīt ekonomiku un pakalpojumus iedzīvotājiem, veicināt viņu labklājību, kā arī klimata un vides aizsardzību, izvirzot Eiropas Savienību 5G revolūcijas priekšplānā.

4.5. Tā kā kiberdrošība un nacionālā drošība ir divi nesaraujami saistīti aspekti, EESK uzskata, ka jebkurš lēmums par ES dalībvalsts nacionālo drošību ir jāpieņem ES kontekstā, un netehniskie novērtējumi objektīvi jāpiemēro, pamatojoties uz Eiropas līmenī noteiktiem riska novērtēšanas kritērijiem, kas vajadzīgi, lai visā Eiropā nodrošinātu paredzamu un saskaņotu normatīvo vidi, kura garantē pilnīgu savietojamību.

4.6. EESK uzskata, ka informācijas kvalitāte un tās nodošanas metodes – tā dēvētais strukturēšanas efekts vai raksturiezīmju uzsvēršana – būtiski ietekmē saņēmēju attieksmi. Tāpēc mērķis veicināt patērētāju iespēju palielināšanu nozīmē tādu rīku noteikšanu, kuru mērķis ir izglītot patērētājus un nostiprināt viņu prasmes, padarot viņus par aktīviem digitālā tirgus dalībniekiem. EESK atzīst vajadzību sniegt iedzīvotājiem aktuālu un precīzu informāciju par 5G priekšrocībām un riskiem, pamatojoties uz zinātnisko aprindu vairākuma vienprātību un norādot uz aspektiem, kuros šī vienprātība nav skaidra.

4.7. EESK ir pārliecināta, ka jebkuram uzņēmumam joprojām ir jābūt brīvai, nediskriminētai piekļuvei Eiropas digitālajam tirgum, taču ievērojot stingru un skaidru noteikumu, standartu un novērtēšanas un drošības kritēriju Eiropas sistēmu, kura Eiropas stratēģijas uzmanības centrā izvirza tai piemītošās Eiropas tehnoloģiskās suverenitātes atgūšanu un atjaunošanu.

4.8. Lai arī piecu galveno infrastruktūras piegādātāju vidū ir divi Eiropas, divi Ķīnas un viens Korejas pakalpojumu sniedzējs ([13]), neviens no lielākajiem Eiropas uzņēmumiem nav to uzņēmumu priekšgalā, kuri ražo 5G ierīces un mikroshēmojumus; EESK ir pārliecināta, ka ir jānodrošina pakalpojumu sniedzēju uzņēmumu daudzveidība, no kuriem vismaz vienam ir jāpieder īpašniekiem Eiropā, un ka ir jādrošina aparatūras un programmatūras komponentu savietojamības un pilnīgas aizstājamības sistēma, kā arī jānodrošina pilnīga Eiropas tehnoloģiskā suverenitāte spēcīgas starptautiskās sadarbības un tirgus atvērtības, piekļuves un darbības pilnīgas savstarpības apstākļos. Šādu diversifikāciju var piemērot, ja vien ir iespējama pakalpojumu sadarbspēja un daudzveidība nepalielina kiberdrošības riskus.

4.9. EESK uzskata, ka Eiropai ir ļoti svarīgi vidējā termiņā koncentrēties uz autonomiju un pašpietiekamību šajā jomā, stingri atbalstot pētniecību un Eiropas uzņēmumu daudzveidību. EESK atzinīgi vērtē pasākumu kopumu, par kuru vienojušās dalībvalstis, lai novērstu drošības un drošuma riskus, kas saistīti ar 5G tehnoloģijas ieviešanu un jau norādīti Eiropas novērtējumā. Tomēr Komiteja uzskata, ka stingri un droši elektromagnētisko lauku iedarbības ierobežojumi, kas ieteikti ES līmenī un balstīti uz atjauninātajām Starptautiskās komisijas aizsardzībai pret nejonizējošo starojumu (*ICNIRP*) norādēm, kuras atzinusi Pasaules Veselības organizācija (PVO), ir jāpiemēro visām 5G paredzētajām frekvenču joslām ([14]): *ICNIRP* ierobežojumu pamatā ir piesardzības princips, jo tie ir 50 reižu zemāki par sabiedrības veselības ietekmes līmeņiem, kas noteikti, pamatojoties uz pieejamiem zinātniskiem pierādījumiem.

([13]) Pieci pasaules mēroga piegādātāji pašreiz ir *Ericcson*, *Nokia*, *Huawei*, *ZTE* un *Samsung*.
([14]) EP – E-003040/2019. Atbilde, ko Eiropas Komisijas vārdā sniedza *Kyriakides* kdze (17.1.2020.).

4.10. Tomēr EESK norāda, ka ne visas kopienas atzīst *ICNIRP* pamatnostādnes, jo daži zinātnieki saskaņā ar *ALARA* principu atbalsta daudz stingrākas robežvērtības attiecībā uz iedzīvotāju ekspozīciju. Risinājumi, kurus varētu ierosināt 5G komunikāciju infrastruktūras papildināšanai, ietver fiksētu datu savienojumu izmantošanu ar esošajām, ar radiosakariem neaprīkotām, tehnoloģijām (*Ethernet* kabeļi, optiskās šķiedras kabeļi u. c.) situācijās, kad lietojums ir fiksēts (piemēram, bankomātos, banku POS terminālos, rūpniecības robotos, tālvadības medicīnas robotos utt.) un tur, kur darbojas lielo datu pārraides lietotāji (digitālā pakalpojuma sniedzēji, uzņēmumi utt.); lietu internets fiksētās, nemobilās vietās (viedais mājoklis, viedā pilsēta, sensori sabiedrisko pakalpojumu sniedzēju aprīkojumā utt.).

4.11. Eiropas Komisijai, Eiropas Parlamentam, Padomei un dalībvalstu valdībām un parlamentiem ir jānodrošina demokrātiska apspriešanās sistēma, kurā sabiedrību var iepazīstināt ar zinātniskiem vai tehnoloģiskiem tematiem, juridiskām garantijām un kompetento iestāžu atbildēm uz pilsoniskās sabiedrības jautājumiem.

4.12. EESK uzskata, ka lielāks uzsvars būtu jāliek uz tādiem rīkiem, kuri paredzēti lietotājiem, iedzīvotājiem un attiecīgajām pilsoniskās sabiedrības organizācijām un kuri ir ierobežoti un neefektīvi, papildus pareizam uzsvaram uz atbilstošajiem pasākumiem, kas attiecas uz valstu regulatoru pilnvarām un telesakaru operatoru lomu.

4.13. EESK ir atzinusi ([15]), ka pastāv elektromagnētiskās hipersensitivitātes problēma, un uzsver savas bažas, uzskatot par iepriecinošu norādīt, ka tiek turpināti padziļināti pētījumi, lai izprastu šo problēmu un tās cēloņus, un mudināja EK turpināt un atjaunināt darbu šajā jomā.

4.14. 5G telesakaru un lietojumprogrammu pakalpojumu sniedzēju uzticamība, pēc EESK domām, ir būtiska, ņemot vērā to, ka informācijas pārvaldība internetā ir tādu apkopotu datu pakalpojumu pamatā, kurus lietotāji vāc un apstrādā, izmantojot tehnoloģiskos, juridiskos un nodokļu mehānismus, un savstarpēji saistot objektus, ierīces un algoritmus.

4.15. EESK ir ierosinājusi ([16]) pāriet no datu īpašumtiesību jēdzieniem uz fizisko un juridisko personu datu tiesību definīciju. Patērētājiem vajadzētu būt iespējai kontrolēt pievienoto ierīču iegūtos datus, lai nodrošinātu patērētāju privātumu ar piekļuvi, savietojamību un datu pārsūtīšanu, vienlaikus nodrošinot pienācīgu datu aizsardzību un konfidencialitāti, godīgu konkurenci un plašāku pakalpojumu izvēli patērētājiem.

4.16. Vispārējā datu aizsardzības regula (GDPR) būtu jāpapildina ar skaidriem piemērošanas norādījumiem, lai panāktu vienotu piemērošanu un augstu datu un patērētāju aizsardzības līmeni, ņemot vērā ierīču un objektu savietojamību, un ir jāpārskata noteikumi par civiltiesisko atbildību un produktu apdrošināšanu, lai tos pielāgotu situācijai, kad lēmumus arvien biežāk pieņems programmatūra pilnīgas drošības ietvaros.

4.17. EESK uzskata, ka ir ļoti svarīgi, lai dalībvalstis ievērotu stratēģiskos un tehniskos ieteikumus, kas iekļauti ES rīkkopā, izvairoties no īpašu valsts pieeju izstrādes, piemēram, papildu testēšanas un sertificēšanas, kas varētu izraisīt tirgus sadrumstalotību, kavēšanos tehnoloģiju ieviešanā un neatbilstības starp tirgiem, radot risku mazināt uzticību testēšanas un sertifikācijas sistēmām.

4.18. EESK uzskata, ka ir svarīgi izmantot pasaules mēroga standartus, nodrošinot lielāku Eiropas atbalstu, kā arī dalītu un atzītu paraugpraksi, lai ļautu efektīvi pārvaldīt apdraudējumus, radīt apjomradītus ietaupījumus, novērst sadrumstalotību un nodrošināt Eiropas sistēmu sadarbspēju. Sarunas par tehniskajiem standartiem nodrošinās vajadzīgo skaidrojumu, kas ļaus uzņēmumiem atkal konkurēt un iesaistīties tajās pamatdarbībās, kuras visos tirgos ļauj ieviest progresīvas tehnoloģijas, piemēram, 5G un mākslīgo intelektu.

4.19. EESK jo īpaši uzskata, ka ir būtiski novērtēt piegādātāju riska profilu un piemērot attiecīgus ierobežojumus iespējamajiem paaugstināta riska piegādātājiem – tostarp izņēmumus, kas vajadzīgi, lai efektīvi mazinātu riskus –, to attiecinot uz nozīmīgākajiem aktīviem, kas koordinētajā riska novērtējumā ES līmenī atzīti par būtiskiem un jūtīgiem.

4.20. EESK uzskata, ka ir svarīgi palielināt operatoru un piegādātāju ieguldījumus jaunos tehniskās drošības elementos – šādiem ieguldījumiem jāspēj iet roku rokā ar tirgus spēju atzīt un atlīdzināt visas tās iniciatīvas, kuru mērķis ir palielināt sistēmu drošību un noturību. Lielāka koncentrēšanās uz ieguldījumiem drošības jomā varētu radīt jaunas priekšrocības tirgū.

([15]) OV C 242, 2.7.2015., 31. lpp.
([16]) OV C 353, 18.10.2019., 79. lpp.

4.21. EESK stingri atbalsta kopīgus pasākumus rūpniecības attīstības atbalstam un 5G ieviešanai: izvērtēt iespējamos tirgus robus vai nepilnības 5G vērtību ķēdē, kuri varētu būt par iemeslu vai nu selektīvai intervencei nākamā ilgtermiņa budžeta ietvaros, vai iespējamam projektam visas Eiropas interesēs 5G kiberdrošības jomā (drošība un drošums).

4.22. EESK uzsver, ka, lai arī digitālā infrastruktūra ir izrādījusi noturību un stabilitāti Covid-19 krīzes laikā, ir vajadzīgi turpmāki ieguldījumi 5G infrastruktūrā, lai pārvarētu joprojām pastāvošo digitālo plaisu, kas var ierobežot iedzīvotāju piekļuvi e-veselībai, e-mācībām un tāldarbam.

4.23. Runājot par tehnoloģisko diplomātiju, EESK uzskata, ka ir svarīgi, lai ES nodrošinātu līdzsvarotākus un savstarpīgākus nosacījumus tirdzniecībai un ieguldījumiem, jo īpaši attiecībā uz uzņēmumu piekļuvi tirgum, subsīdijām, publisko iepirkumu, tehnoloģiju nodošanu, rūpniecisko īpašumu, kā arī sociālajiem un vides standartiem, jo īpaši ja ir "sistēmiski konkurenti, kas veicina alternatīvus pārvaldības modeļus", un vienlaikus tirgū sekmētu pilnīgu konkurenci un tehnisko inovāciju.

4.24. EESK stingri atbalsta vajadzību uzturēt daudzveidīgu un ilgtspējīgu 5G piegādes ķēdi, lai novērstu ilgtermiņa atkarības, paredzot vairāku piegādātāju klātbūtni aizstājamības un sadarbspējas ietvaros, un lai turpinātu stiprināt Eiropas 5G un tai sekojošās tehnoloģijas spējas un tehnoloģiskās suverenitātes programmas un iniciatīvas saskaņā ar finanšu shēmu 2021.–2027. gadam.

4.25. Saistībā ar Eiropas atveseļošanas plānu, kas pieņemts 2020. gada 27. maijā, 2020. gada Digitālās ekonomikas un sabiedrības indekss (DESI) būs informācijas avots katrai valstij paredzētā analīzē, kas pamato Eiropas pusgadā iekļautos ieteikumus digitalizācijai. Tas palīdzēs dalībvalstīm mērķtiecīgi noteikt un piešķirt prioritāti vajadzīgajām reformām un ieguldījumiem, tādējādi veicinot piekļuvi 560 miljardu euro vērtajam Atveseļošanas un noturības mehānismam. Šis rīks nodrošinās dalībvalstīm līdzekļus, lai padarītu to ekonomiku noturīgāku un nodrošinātu, ka ieguldījumi un reformas sekmē zaļo pārkārtošanos un digitālo pārveidi. Tā kā pandēmijai bija būtiska ietekme uz katru no piecām DESI dimensijām, 2020. gada secinājumi par 5G būtu jāskata saistībā ar daudzajiem EK un dalībvalstu veiktajiem pasākumiem krīzes pārvarēšanai un atveseļošanas veicināšanai.

Briselē, 2020. gada 16. septembrī

Eiropas Ekonomikas un sociālo lietu komitejas
priekšsēdētājs
Luca JAHIER