

Huawei Technologies Ljubljana d.o.o.  
Ameriška ulica 8, 1000 Ljubljana

Agencija za komunikacijska omrežja in storitve Republike Slovenije

Stegne 7

p. p. 418

1001 Ljubljana

poslano po elektronski pošti na: [info.box@akos-rs.si](mailto:info.box@akos-rs.si)

Ljubljana, 18. september 2023

Številka: 0073-3/2023

Zadeva: **Pripombe in predlogi k predlogu novega »Splošnega akta o dodatnih varnostnih zahtevah in omejitvah«, vključno z analizo ustavne spornosti predloga splošnega akta**

Spoštovani,

Agencija za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju tudi »AKOS« ali »Agencija«) je z objavo dne 7. 8. 2023 obvestila javnost, da je na podlagi Zakona o elektronskih komunikacijah (ZEKom-2) pripravila nov predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (v nadaljevanju tudi »Splošni akt« ali »SADVZO«), ki naj bi temeljil na podlagi šestega odstavka 116. člena ZEKom-2 in naj bi določal usmeritve, ki jih morajo upoštevati in izvajati operaterji mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja kritičnim subjektom. Agencija je povabila zainteresirano javnost, da do vključno 18. septembra 2023 posreduje pripombe, predloge ali dopolnitve k predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah.

Temu dopisu prilagam »Pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije z dne 13. 9. 2023« (v nadaljevanju tudi »Mnenje«). Mnenje je pripravil ugledni pravni strokovnjak prof. dr. Samo Bardutzky, univ. dipl. pravnik, raziskovalec na strokovnem področju ustavno pravo, sicer tudi predstojnik Katedre za ustavno pravo Pravne fakultete Univerze v Ljubljani.

Sprejem takšnega akta bi povzročil izjemno negotovost (tudi če ne pride do izdaje odločbe po 117. členu ZEKom-2 in tudi če ne pride do formalne izključitve kateregakoli dobavitelja s trga), saj bi že sama možnost, da se lahko kadarkoli izda odločba po 117. členu v povezavi s preširoko definicijo kritičnih elementov omrežja, predstavljala veliko tveganje, da se lahko praktično kadarkoli prepove oprema tudi v nekritičnih delih javnih komunikacijskih omrežij. To predstavlja velike omejitve za razvoj omrežja in vpliva na izbor dobaviteljev (tudi v fazi, ko ne obstaja kakršnekoli prepoved kateregakoli dobavitelja) in bistveno vpliva na načrtovane investicije operaterjev, operaterjem pa bi bilo onemogočeno, da bi sami poiskali najboljše in najbolj varne tehnološke rešitve za svoje omrežje in njihove uporabnike. Po nekaterih ocenah bi lahko predlagana ureditev v prihodnjih letih privedla do kumulativno več milijard evrov višjih naložbenih stroškov, brez kakršnegakoli pomembnega pozitivnega učinka na varnost omrežij (učinek bi lahko bil celo nasproten), zakasnila hitrost vzpostavitve omrežij 5G in na dolgi rok negativno vplivala na gospodarstvo in gospodarsko rast. Če je pomislek, ki ga skuša naslavlјati Agencija, varnost namenskih (nejavnih) omrežij za potrebe varnosti, policije, obrambe in zaščite, reševanja in pomoči, bi se navedeno vprašanje dalo v splošnem aktu rešiti drugače, kot da se nasploh posega v radijsko dostopovno omrežje javnih komunikacijskih omrežij, kar bo imelo v končni fazi hude posledice za slovensko gospodarstvo in potrošnike.

V tem dokumentu opozarjamo med drugim na naslednje:

- i. Definicija kritičnih elementov omrežja je preširoka, zajema elemente in funkcije omrežja, ki niso kritični (npr. radijsko dostopovno omrežje ter upravljavske sisteme in druge podporne sisteme) in je nasprotju z dosedanjimi stališči Republike Slovenije (med drugim nacionalno oceno tveganj, katere pripravo je koordiniral ravno AKOS), pa tudi v nasprotju s smernicami EU, mednarodnimi standardi in pravom EU, tudi vsebinsko oziroma strokovno-tehnično pa je takšna razporeditev povsem neutemeljena – kot pojasnjeno na

primer pod točko 1 teh pripomb;

- ii. Pod točko 2. teh pripomb še dodatno opozarjamo na spornost definicije kritičnih elementov in funkcij omrežja in se sklicujemo tudi na pridobljeno Mnenje. Iz Mnenja izhaja, da je definicija kritičnih elementov, predvidena v predlogu splošnega akta, v nasprotju z Ustavo Republike Slovenije. Kot izhaja iz Mnenja, primerjava predlaganih dikcij v splošnem aktu z Usklajeno oceno tveganj (in drugimi viri na nivoju EU) kaže na obstoj manj invazivnih alternativ, zaradi česar predlagana ureditev ne bi prestala testa nujnosti, negativen rezultat testa nujnosti kot prvina presoje z vidika načela sorazmernosti pa posledično pomeni, da obravnavana ureditev ni skladna s tem temeljnim ustavnim načelom;
- iii. Omejevanje glede na državo izvora (glejte kriterije iz prvega odstavka 117. člena ZEKom-2 v povezavi s splošnim aktom, ki gre celo preko okvirov, ki jih je načrtoval ZEKom-2) bi bilo v nasprotju z načeli nediskriminacije in sorazmernosti, ki izhajajo iz Ustave Republike Slovenije, zapisana pa so tudi v Pogodbah EU in Listini Evropske unije o temeljnih pravicah. Navedeno je toliko bolj problematično, ker omejevanje ni jasno zamejeno in se razteza na elemente, ki ne štejejo za kritične po pravu EU, med drugim vključno z Usklajeno oceno tveganj in Naborom orodij, pa tudi Nacionalni oceni tveganj Republike Slovenije. Poleg tega bi bili učinki tovrstnih ukrepov v nasprotju z mednarodnimi obveznostmi Republike Slovenije. Predlagani splošni akt bi, če bi bil sprejet v taki vsebini, kršil pravo EU in pravo WTO, kar je vse podrobneje pojasnjeno pod točko 3;
- iv. Glede obveznosti naloženih dobaviteljem, vključno s preprečevanjem odvisnosti od posameznega dobavitelja, je potrebno poudariti, da tudi iz Mnenja izhaja, da predlog splošnega akta prekoračuje zakonsko pooblastilo iz ZEKom-2 ter da določanje vsebine pravnih poslov, ki jih bodo operaterji sklepali z dobavitelji, kot je predvideno v obravnavanih določbah splošnega akta, presega pooblastilo za določitev »drugih zlasti tehničnih usmeritev«. Določitev obveznosti »izogibanja«, ki omeji in nadomesti svobodo oblikovanja pogodbenih razmerij, pomeni, kot izhaja iz Mnenja, *de facto* prepoved, ki ne more biti prepuščena podzakonskemu urejanju, zlasti tudi ne zaradi določbe 87. člena Ustave RS. Mnenje se opira tudi na Nabor orodij, iz katerega izhaja, da je moč tveganje prevelike odvisnosti od dobaviteljev zmanjšati tudi z manj invazivnimi ukrepi, v primerjavi z obravnavanimi določbami splošnega akta, zato predlagana ureditev ne bi prestala testa nujnosti in je posledično predlagana ureditev zahtev po diverzifikaciji v neskladju z načelom sorazmernosti, kot vse podrobneje pojasnjeno pod točko 4;

- v. Pod točko 5 opozarjamo na spornost netehničnih kriterijev;
- vi. Akos in Republika Slovenija tudi nista izpolnila postopkovnih obveznosti po pravu WTO in kot izhajajo iz SMT Direktive, kršitev obveznosti pa pomeni postopkovno napako tehničnega predpisa (t.j. predlaganega Splošnega akta), kar bi imelo za posledico potencialno neizvršljivost oziroma neuporabljivost le-tega, opustitev pa predstavlja kršitev, ki ima lahko za posledico postopek pred Sodiščem EU proti Sloveniji kot tudi spor v okviru mehanizmov WTO, kot podrobneje pojasnjeno pod točko 6.;
- vii. Pod točko 7 se opredeljujemo do Sklepa vlade RS z dne 22.6.2023, ki ni bil objavljen v Uradnem listu Republike Slovenije in posledično že iz tega razloga glede na stališče Ustavnega sodišča ni nikoli začel veljati, ne učinkuje in se ga ne sme uporabljati, istočasno pa je bil sprejet ob kršitvi postopkovnih pravil, je nezakonit, neustaven, krši pravo EU (in je neizvršljiv in neuporabljiv po pravu EU) in pravu WTO, kot vse podrobneje pojasnjeno v nadaljevanju, in ne bi smel v nobenem primeru vplivati na odločitev Agencije (tudi ob upoštevanju avtonomije Agencije in tega, da je določitev kritičnih elementov omrežja po ZEKom-2 prepuščena agenciji kot strokovnemu, samostojnemu in neodvisnemu regulatorju, ki bi moral sprejeti strokovno odločitev);
- viii. Pod točko 8 se opredeljujemo do postopkovnih kršitev, ki obremenjujejo predmetno javno posvetovanje, med drugim kršitev statuta Agencije, ker ni bil omogočen vpogled po drugem odstavku 19. člena Statuta, kršitev statuta in ZEKom-2, ker ni bil v zakonskem in statutarnem roku objavljen odgovor na že podane pripombe in predloge vezano na prvi krog javnega posvetovanja, opozarjamo na kršitev 32. člena Uredbe o upravnem poslovanju, ker so se posvetovanja med Agencijo in URSIV vršila na ne-transparenten način, brez ustreznega dokumentiranja, ki ga zahtevajo Uredba in temeljna načela upravnega poslovanja. Ob tem opozarjamo, da smo v pojasnilih, ki jih je posredovala Agencija, zaznali protislovje, in sicer se v utemeljitev odločitve za uvrstitev radijskega dostopovnega omrežja med kritične elemente omrežja Agencija sklicuje na vire, ki ravno obratno radijskega dostopovnega omrežja ne uvrščajo med kritične elemente omrežja. Iz pojasnil ravno obratno izhaja, da ne obstajajo kakršnikoli vsebinski oziroma strokovni razlogi za takšno odločitev (ali pa jih vsaj Agencija ni razkrila). Pod navedeno točko predlagamo, da se odpravijo postopkovne kršitve, ki obremenjujejo proces javnega posvetovanja in opozarjamo, da bo sicer prišlo do hudih kršitev pravic, škode na javni dobrini in izjemne premoženjske škode, ki se meri v milijardah evrov, kot potrjujejo izvedene študije;
- ix. Pod točko 9 podajamo konkretne predloge sprememb besedila predlaganega Splošnega akta.

### **1. Glede kritičnih in nekritičnih elementov in funkcij omrežja**

Sicer pozdravljamo prizadevanja za večjo varnost komunikacijskih omrežij. Ob pregledu objavljenega predloga Splošnega akta pa na žalost ugotavljamo, da vsebuje Priloga splošnega akta (Seznam, kritičnih elementov omrežja

in pripadajočih informacijskih sistemov), na katero se sklicuje definicija kritičnih elementov omrežja iz 2. točke prvega odstavka 2. člena kategorije, ki po vsebini nikakor ne sodijo med »kritične elemente«, kot na primer celo radijsko dostopovno omrežje (oz. bazne postaje, ki podpirajo tehnologijo 5G ali višje), kar ni v skladu s pravom EU, ki naj bi se implementiralo, ob tem pa načelo lojalne razlage<sup>1</sup>, ki temelji na načelu lojalnosti iz člena 4(3) Pogodbe o Evropski uniji (»PEU«), zahteva, da bi bilo potrebno nacionalno pravo, med drugim tudi pojem »kritičnih elementov« in funkcij omrežja, razlagati v skladu s pravom EU, ki naj bi se implementiralo, ob tem pa, kot izhaja iz Mnenja, je predlog Splošnega akta tudi neskladen z Ustavo Republike Slovenije.

Na ravni EU več različnih dokumentov ureja varnost telekomunikacijskih omrežij. Evropska komisija je januarja 2020 izdala priporočila o Naboru orodij EU za varnost 5G (v nadaljevanju tudi »Nabor orodij«)<sup>2</sup>. Navedeni Nabor orodij sicer ni pravno zavezujoč, predstavlja smernice prava EU oz. tako imenovano mehko pravo. Podlaga za sprejem relevantnega Splošnega akta naj bi bil 116. člen Zakona o elektronskih komunikacijah (ZEKom-2), ki je del poglavja VIII (Varnost omrežij in storitev ter delovanje v stanjih ogroženosti), v zakonodajnem postopku sprejemanja ZEKom-2, pa je predlagatelj zakona rešitve iz VIII. Poglavlja zakona utemeljeval v potrebi po implementaciji Nabora orodij. Nabor orodij priporoča pristop, ki temelji na zagotavljanju kibernetске varnosti na podlagi tako imenovanega pristopa presoje tveganj »izključno iz varnostnih razlogov« in ki temelji na »objektivni oceni ugotovljenih tveganj« ob polnem spoštovanju odprtosti enotnega trga EU<sup>3</sup>. Posledično se Nabor orodij direktno ne nanaša na nobenega

<sup>1</sup> Doktrino lojalne razlage pojasnjuje tudi sodna praksa slovenskih sodišč, in sicer, da je potrebno določbe nacionalne pravne ureditve razlagati v skladu z namenom določb prava EU (primerjajte na primer sodbo Vrhovnega sodišča Republike Slovenije v zadevi VIII Ips 12/2020, dostopna na:

[https://sodnapraksa.si/?q=lojalne%20razlage&database\[SOVS\]=SOVS&\\_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111442180](https://sodnapraksa.si/?q=lojalne%20razlage&database[SOVS]=SOVS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111442180) ). Pojem »kritičnosti« uporabljen v ZEKom-2 je tako potrebno razlagati v skladu z Naborom orodij in Usklajeno oceno tveganj.

<sup>2</sup> Varna uvedba tehnologije 5G v EU – izvajanje nabora orodij EU (Secure 5G deployment in the EU – Implementing the EU toolbox), [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=64481](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481)

<sup>3</sup> Nabor orodij zahteva primeren in sorazmeren odgovor na objektivno ugotovljena tveganja (*»respond appropriately and proportionately to the presently identified and future risks«*) in pristop osredotočen na dejanska tveganja (*»following a risk-based approach«*); ob tem pa Komisija opozarja, da je potrebno ohraniti trg odprt proizvodom in storitvam, ki spoštujejo varnostne zahteve (*»The Commission will fully support the implementation of the EU's cybersecurity approach to 5G networks while ensuring that EU markets remain open to products and services that respect the evolving requirements for cybersecurity and trust.«*). Iz Nabora orodij jasno izhaja, da mora ostati trg odprt za vso opremo, kolikor

konkretnega dobavitelja ali državo in zagovarja primerne objektivne in sorazmerne varnostne ukrepe, ki veljajo za vse, in si prizadeva za harmonizacijo varnostnih standardov po vsej EU in certificiranje za celotno EU. Cilj Nabora orodij pa je naslavljanje tveganj za kibernetško varnost omrežij 5G, ki so bila ugotovljena z Usklajeno oceno tveganj za kibernetško varnost omrežij 5G (angl. »EU Coordinated risk assessment of the cybersecurity of 5G networks«, oktober 2019, v nadaljevanju tudi »Usklajena ocena tveganj«). Na navedeno Usklajeno oceno tveganj se sklicuje tudi predlog splošnega akta AKOS po 115. členu ZEKom-2 (predlog Splošnega akta o varnosti omrežij, storitev in podatkov<sup>4</sup>) v 3. točki prvega odstavka 9. člena. Nabor orodij (glejte stran 39 in 40 le-tega) in Usklajena ocena tveganj (glejte stran 16 in 17 le-te) pri tem jasno razmejujeta med kritičnimi elementi (angleško *critical*), kamor se prišteva zgolj jedrne funkcije omrežja (angleško *core network functions*), upravljanje virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), in vsemi preostalimi nekritičnimi elementi, kamor se prišteva med drugim RAN (angleško *Radio Access Network*) oziroma bazne postaje, pa tudi transport in prenosne funkcije ter upravljaljske sisteme in druge podporne sisteme. Tudi Republika Slovenija je prispevala svojo Nacionalno oceno tveganj (priložena; National 5G Cybersecurity Risk Assessment of the Republic of Slovenia, v nadaljevanju »Nacionalna ocena tveganj«, ki je bila upoštevana v Usklajeni oceni tveganj, s praktično enako razmejitvijo na kritične (angl. *Critical*) elemente, kamor se prišteva jedrne funkcije omrežja (angl. *Core network functions*), in preostalimi nekritičnimi elementi, kamor se prišteva dostopovno omrežje (angleško *Access network*) oziroma bazne postaje, transport in prenosne funkcije ter večina upravljaljskih sistemov in drugih podpornih sistemov (glejte stran 10 navedene Nacionalne ocene tveganj; od upravljaljskih sistemov in drugih podpornih sistemov Nacionalna ocena tveganj kot kritična šteje zgolj sistema ocenjevanja in zaračunavanja). Z uporabo doktrine lojalne interpretacije se da torej jasno določiti, na katere elemente in funkcije se sklicuje zakon (ZEKom-2) s pridevnikom »kritični«. Takšna opredelitev, kot jo predvideva predlog Splošnega akta, bi bila tudi v nasprotju s smernicami ENISA<sup>5</sup> (glejte stran 8/33), po katerih sta enako kot kritična opredeljena zgolj jedrni del omrežja in upravljanje NFV in orkestracija MANO,

---

ustreza varnostnim standardom, torej uporabe opreme ni možno prepovedati na podlagi "strateških" kriterijev, dokler (ob upoštevanju objektivne ocene tveganj) ustreza varnostnim standardom in je varna ("This approach is in full respect of the openness of the EU internal market as long as the risk - based EU security requirements are respected.").

<sup>4</sup> Predlog je bil objavljen na: <https://www.akos-rs.si/javna-posvetovanja-in-razpisi/novica/agencija-objavlja-predlog-splosnega-akta-o-varnosti-omrezij-storitev-in-podatkov>

<sup>5</sup> Smernice ENISA so dostopne na: <https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eccc>

radijsko dostopovno omrežje (Radio Access Network – RAN) in bazne postaje pa ne. Takšna opredelitev, kot jo predvideva predlog Splošnega akta bi bila tudi v nasprotju z ETSI/3GPP standardom<sup>6</sup>, po katerem imajo različne kategorije omrežja dodeljene različne profile tveganja, samo jedrni del omrežja (CORE in upravljanje NFV ter orkestracija MANO) so definirani kot kritični. Bazne postaje, ki so v diagramu ETSI/3GPP standarda prikazane z oznako »DU/CU« so manj občutljivi deli omrežne arhitekture. Navedeni sklic na standard 3GPP, vključno z diagramom prikazanim pod opombo 6 tega dokumenta in navedeno pojasnilo vsebuje celo Nacionalna ocena tveganj Republike Slovenije, katere pripravo je koordiniral ravno AKOS (glejte stran 9).

Tako je sporna in v nasprotju s pravom EU, smernicami in standardi vključitev radijskega dostopovnega omrežja (RAN) v Prilogo (Seznam, kritičnih elementov omrežja in pripadajočih informacijskih sistemov), kot tudi vključitev drugih nekritičnih komponent, na primer tudi vključitev točke »upravljavski sistemi in drugi podporni sistemi«.

Tudi vsebinsko oz. strokovno-tehnično pa bila takšna razvrstitev povsem neutemeljena:

- i. RAN ne nadzoruje bistveno dostopa do omrežja in prometa in velja za manj občutljiv element omrežne arhitekture, kot ponazarja standard 3GPP. Trenutni in prihodnji razvoj 5G RAN verjetno ne bo spremenil operativnega modela RAN. Profil tveganja, opredeljen v Naboru orodij za RAN, ki ni kritičen, še vedno velja. Trenutno je po vsem svetu več kot tri milijone baznih postaj 5G po 3GPP standardu v komercialni uporabi in pri baznih postajah niso bile ugotovljene nobene ranljivosti, ki bi lahko vplivale na oceno

<sup>6</sup> Gre za standard TR 121 915 – V.15.0.0, ki vsebuje naslednji diagram:



Navedeni diagram je skupaj s pojasnili vključen tudi v slovensko nacionalno oceno tveganj (National 5G Cybersecurity Risk Assessment of the Republic of Slovenia), katere pripravo je koordiniral ravno AKOS – glejte stran 9 od 24.

kritičnosti baznih postaj. Z varnostnega vidika posamezne bazne postaje na daljavo tehnično ni mogoče napasti, potencialno bi bilo to možno le ob fizični prisotnosti na lokaciji posamezne bazne postaje RAN. Kakršenkoli napad na daljavo na bazne postaje RAN pa zaradi izoliranosti povezav baznih postaj od javnega interneta ne bi bil mogoč. To bi bilo teoretično možno le na jedrno omrežje, ki se stika z javnim internetom. V vsakem primeru bi bil kakršenkoli vpliv katerega koli incidenta zelo omejen (še posebej v zvezi s kakršnimikoli tveganji, povezanimi s tretjimi državami).<sup>7</sup> Tako z vidika tveganosti radijskemu dostopovnemu omrežju RAN ni možno pripisati kritičnosti.

- ii. Enako velja za »upravljaljske sisteme in druge podpome sisteme«, ki jih Priloga predloga Splošnega akta ravno tako neutemeljeno karakterizira kot kritične dele omrežja. Potrebno je ugotoviti, da takšni sistemi bistveno manj vplivajo na uporabnika in jih ni upravičeno opredeliti kot kritične, saj dejansko ne morejo imeti pomembnega vpliva na dostop do komunikacijskega omrežja ali na promet v omrežju.

Poskus širjenja pomena »kritičnosti« v podzakonskem aktu Akos pa je v nasprotju z doktrino lojalne razlage, kot tudi v nasprotju z zakonskim pooblastilom za sprejem splošnega akta in posledično v nasprotju s 120. členom Ustave Republike Slovenije. Obenem takšna razširjena razlaga »kritičnosti«, ki bi zajemala tudi nekritične elemente in funkcije omrežja v povezavi z možnostjo izdaje odločbe po 117. členu ZEKom-2 in prepovedjo (iz petega odstavka 116. člena ZEKom-2) uporabe opreme in storitev iz 117. člena ZEKom-2 v kritičnih elementih in funkcijah tega omrežja in pripadajočih informacijskih sistemih, ne more prestatiti testa sorazmernosti.

Priloga splošnega akta, ki izrecno opredeljuje kot kritične elemente, elemente, ki niso kritični po pojmovanju prava EU in Nacionalne ocene tveganj Republike Slovenije, tako odstopa od prava EU, Usklajene ocene tveganj, pa tudi od Nacionalne ocene tveganj Republike Slovenije. Da je takšna definicija v neskladju z Ustavo Republike Slovenije izhaja tudi iz priloženega Mnenja, in bi (v primeru izdaje odločbe po 117. členu ZEKom-2, dejansko pa tudi če takšna odločba ne bo nikoli izdana) pripeljala do posledic v nasprotju s pravom EU in mednarodnim pravom, kar bo

---

<sup>7</sup> Napad na jedrni del omrežja na primer zlahka prizadene več kot 15% uporabnikov omrežja, medtem ko bi na primer napad na bazno postajo lahko vplival na zelo malo uporabnikov (manj kot 0,1% uporabnikov omrežja). Zaježitev incidentov vezanih na bazne postaje bi bila relativno enostavna.



podrobneje pojasnjeno v nadaljevanju. V kolikor bi bila definicija sprejeta v takšni vsebini, bi pomenila tudi odstop od dobrih praks drugih evropskih držav (npr. Nemčije, Avstrije, Finske in Madžarske<sup>8</sup>).

## 2. Glede definicije kritičnih elementov in ugotovitev pridobljenega Mnenja

2. točka prvega odstavka 2. člena predloga Splošnega akta vsebuje naslednjo opredelitev:

*»2. Kritični elementi omrežja so tisti omrežni elementi, funkcije, storitve in podporni informacijski sistemi v fizični, programski ali virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, kot so navedeni v prilogi tega splošnega akta.«*

Predlog Splošnega akta vsebuje prilogo (Seznam, kritičnih elementov omrežja in pripadajočih informacijskih sistemov), ki vključuje med drugim naslednje kategorije:

- Upravljanje z naročniki in šifrirni mehanizmi;
- Medomrežno povezovanje;
- Upravljanje omrežne storitve;
- Upravljanje in orkestracija virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), vključno z virtualizacijsko infrastrukturo;
- Radijsko dostopovno omrežje (Bazne postaje, ki podpirajo tehnologijo 5G ali višje);

---

<sup>8</sup> Nemški sistem (seznam kritičnih funkcij z dne 13.8.2021 pripravljen na podlagi relevantnih nemških zakonov TKG in BNetzG s strani zvezne agencije za komunikacijska omrežja - BNetzA) se sklicuje, da sta (absolutno) kritični zgolj kategoriji (a) (jedrne omrežne funkcije) in (b) (upravljanje virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO)), pri čemer se seznam, ki ga je pripravil BNetzA sklicuje na Usklajeno oceno tveganj (EU Coordinated risk assessment ... ) in Nabor orodij (EU 5G Toolbox). Sicer je presoja kritičnosti prepuščena operaterjem. Avstrija in Madžarska sploh ne definirata kakršnihkoli kritičnih komponent omrežja, ravno tako ne postavljata nobenih omejitev s tem v zvezi. Besedilo avstrijskega zakona je dostopno na [https://www.parlament.gv.at/PAKT/VHG/XXVII/1/1\\_01043/index.shtm!#](https://www.parlament.gv.at/PAKT/VHG/XXVII/1/1_01043/index.shtm!#) Finska je uveljavila definicijo skladno z Naborom orodij (EU 5G Toolbox), in sicer je Nabor orodij implementirala v decembru 2020 s sprejemom novele njihovega Zakona o elektronskih komunikacijskih storitvah (t.i. Laki sähköisen viestinnän palveluista). Besedilo finskega zakona je dostopno na strani finlex <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>

- Upravljaljski sistemi in drugi podporni sistemi;
- Zakonito prestrezanje.

Iz Mnenja izhajajo med drugim naslednji zaključki:

1. Mnenje opozarja, da predstavljajo določba 117. člena ZEKom-2 in tam določena pooblastila vladi za izdajo odločbe v kombinaciji z definicijo kritičnih elementov po predlogu splošnega akta podlago za poseg v pravico do splošne gospodarske pobude (74. člen Ustave RS), in sicer poseg v svobodno gospodarsko pobudo tako operaterja kot dobavitelja. Zakonska podlaga za prepoved uporabe opreme se v individualnem primeru konkretizira na specifičen način, saj bo le delno izvršen preko oblastnega akta. V sklepu Vlade bi bila določena le oprema oziroma storitve, ne pa tudi, v katerih elementih operater te opreme oz. storitev ne sme uporabljati. Mnenje opozarja, da si lahko predstavljamo, da se bo operater lahko poslovno racionalno, v internih procesih odločanja in brez dodatnih posegov javne oblasti odločil, da se v celoti izogne opremi, ki jo ponuja dobavitelj – naslovnik odločbe Vlade in pravne posle v celoti sklepal z dobavitelji, za katere ni bila izdana odločba po 117. členu ZEKom-2. Mnenje opozarja, da iz tega lahko logično izpeljemo zahtevo, da mora biti Agencija pri oblikovanju splošnega akta in določitvi kritičnih elementov dodatno pozorna na ustavno zapoved, da ravna sorazmerno. Določitev specifične opreme ali storitev kot kritične lahko od primera do primera vodi do različno intenzivnega vplivanja na odločitve operaterjev pri izbiri dobavitelja. Mnenje opozarja, da je to še posebej upoštevno, ker nad operaterjem, ki sprejema poslovne odločitve glede dobave opreme in storitev, visi poleg kaznovalnopravne sankcije za morebitno operaterjevo neupoštevanje dodatnih varnostnih zahtev in omejitev iz 116. člena (tj. globa po 25. točki prvega odstavka 299. člena ZEKom-2), še dodatna, »skrita« potencialna sankcija (ki ni predvidena v zakonu, temveč jo je možno razbrati iz razpisnih pogojev nedavno objavljenega javnega razpisa za dodelitev radijskih frekvenc za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom<sup>9</sup>), in sicer da lahko Agencija odločbo o dodelitvi radijskih frekvenc razveljavi, če "pristojen organ v postopku inšpekcijskega nadzora nad izvajanjem zakonskih in podzakonskih obveznosti s področja varnosti omrežij ugotovi kršitve", imetnik frekvence pa jih ne odpravi.<sup>10</sup>

---

<sup>9</sup> Sklep o uvedbi javnega razpisa z javno dražbo za dodelitev radijskih frekvenc za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom je Agencija objavila v Uradnem listu RS, št. 191/2020; prečiščeno besedilo razpisne dokumentacije, na katero se sklicuje Mnenje, je dostopno na [https://www.akos-rs.si/fileadmin/user\\_upload/Razpisna\\_dokumentacija\\_za\\_vecfrekvencno\\_drazbo\\_05022021\\_konena.pdf](https://www.akos-rs.si/fileadmin/user_upload/Razpisna_dokumentacija_za_vecfrekvencno_drazbo_05022021_konena.pdf).

<sup>10</sup> Točka A.5.6 razpisne dokumentacije, str. 32.

2. Kot opozarja Mnenje, je razveljavitev odločbe o dodelitvi frekvenc lahko še mnogo hujša in invazivnejša negativna posledica od izreka globe in lahko pomeni uničujoč udarec za gospodarsko aktivnost operaterja, kakršnakoli naknadna zamenjava opreme pa je povezana z znatnimi stroški. Mnenje opozarja, da na presojo sorazmernosti posega tako vpliva *de facto* nezmožnost sodne veje oblasti, da bi intervenirala in zavarovala pravice dobavitelja oziroma, videno iz zornega kota dobavitelja, ki mu je bila izrečena odločba Vlade po 117. členu ZEKom-2, da bi dosegel sodno varstvo, saj so lahko, še preden pride do odločitev sodišč, sprejete poslovne odločitve operaterjev, na katere je v bistvenem vplivalo ravnanje oblastnih organov, in ki močno vplivajo na možnost dobaviteljev, nastopati na trgu in s tem uresničevati svojo pravico do svobodne gospodarske pobude. Tako je lahko *de facto* učinek oblastnega ravnanja in postavljanja pravnih pravil na ustavne pravice mnogo večji od tistega, ki ga je *prima facie* moč razbrati iz besedila pravnih pravil in hitreje preide na polje nesorazmernega, s tem pa tudi nedopustnega poseganja. Kakor pojasnjuje Mnenje, po določbi petega odstavka 116. člena ZEKom-2 operater mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja določenemu krogu uporabnikov, "v kritičnih elementih in funkcijah tega omrežja in pripadajočih informacijskih sistemih ne sme uporabljati opreme in storitev podpore tretje ravni, katere uporaba bi lahko ogrozila nacionalno varnost." 117. člen ZEKom-2 daje vladi pristojnost, da z odločbo določi takšno opremo in storitve tretje ravni. Prepoved uporabe opreme in storitev iz petega odstavka 116. člena ZEKom-2, ki jo določi Vlada po prvem odstavku 117. člena ZEKom-2, je z vidika dobaviteljev opreme in storitev nedvomno poseg v pravico do svobodne gospodarske pobude iz prvega odstavka 74. člena Ustave Republike Slovenije (URS), saj tem subjektom onemogoča, da bi sodelovali na trgu in zasledovali premoženjsko korist z izvajanjem svoje gospodarske dejavnosti.<sup>11</sup> Po stališču US gre za poseg v svobodno gospodarsko pobudo "praviloma takrat, ko zakonodajalec subjektom neko ravnanje prepoveduje" ali "zapoveduje točno določeno ravnanje, ki subjektu ne omogoča prav nikakršnega polja za prosto podjetniško odločanje".<sup>12</sup> Z vidika dobavitelja opreme, ki bi bil določen za dobavitelja z visokim tveganjem, gre tako rekoč za izključitev iz sodelovanja na trgu in tako brez dvoma za poseg. Obseg tega posega pa je odvisen tudi od definicije *kritičnih elementov in funkcij*, v katerih operater opreme in storitev ne sme uporabljati. Obseg posega je v ključnem delu odvisen od razlage te definicije zato, ker so kriteriji za določitev opreme in storitev, ki bi lahko ogrozili nacionalno varnost, v prvem odstavku 117. člena ZEKom-2 formulirani tako, da se nanašajo na lastnosti bodisi dobavitelja bodisi države dobavitelja. V številnih primerih bo tako pojmovno tako rekoč nemogoče, da bi vlada z določbo iz prvega odstavka 117. člena ZEKom-2 določila le določen tip opreme oziroma storitev. V primeru, da Vlada za določenega dobavitelja ugotovi, da on ali njegova država dosega vsaj štiri od naštetih meril, bo - ob tako oblikovani določbi 117. člena - logični zaključek, da mora odločba vlade

<sup>11</sup> Prim. opredelitev polja varovanja pravice iz 74. člena URS v Zagradišnik, Komentar 74. člena, v: Avbelj (ur.) Komentar URS (Človekove pravice, 2019), rob. št. 10.

<sup>12</sup> Odločba US RS v zadevah U-I-446/20-11, U-I-448/20-8, U-I-455/20-8 in U-I-467/20-8 z dne 15. 4. 2021, tč. 16.

zajeti vso njegovo opremo/storitve. Iz tega izhaja zaključek, da bo obseg prepovedi uporabe, s tem pa posega v pravico do svobodne gospodarske pobude, odvisen od tega, kako bo interpretiran zakonski termin "kritični elementi in funkcije (tega omrežja)" iz petega odstavka 116. člena ZEKom-2. Kot opozarja Mnenje Splošni akt v 2. točki 1. člena kot vsebino splošnega akta navaja, da splošni akt določa »kritične elemente omrežja in pripadajoče informacijske sisteme z njihovimi funkcionalnostmi iz šestega odstavka 116. člena Zakona o elektronskih komunikacijah [...], kot so navedeni v prilogi, ki je sestavni del tega splošnega akta [...]« in so posledično ključni elementi in funkcionalnosti, določeni v prilogi k splošnemu akta, zlasti je sporna vključitev radijskega dostopnega omrežja, kjer so kot edina funkcionalnost navedene »bazne postaje, ki podpirajo tehnologijo 5G ali višje«, ter upravljaljske sisteme. Iz Mnenja izhaja, da je določba v nasprotju z ustavo z vidika zagotavljanja sorazmernosti pri posegih v svobodno gospodarsko pobudo.

3. Kot izhaja iz Mnenja, je predlagana ureditev neskladna glede na načelo sorazmernosti. Da bi poseg v svobodno gospodarsko pobudo bil dopusten, bi moral gotovo prestati vsaj test primernosti in test nujnosti. Z vidika testa nujnosti odpira uvrstitev baznih postaj v seznam kritičnih elementov vprašanje, ali se brez tega ne da doseči zasledovanih ciljev.
4. Kot izhaja iz Mnenja, je po dostopnih informacijah v postopku zbiranja informacij in analize stanja za potrebe ocene tveganja kibernetске varnosti omrežij 5G nastalo poročilo, s katerim so se strinjale države članice EU. V okviru priprave usklajene ocene tveganja opravljena tudi analiza vprašanja, katere ključne elemente (key elements) je mogoče šteti za kritične (critical), katere pa je po drugi strani moč razvrstiti v druge kategorije občutljivosti (visoka - high in zmerna - moderate). V tej klasifikaciji je denimo jasno, da med državami članicami bazne postaje niso uvrščene med elemente, ki bi jih označili kot "kritične", temveč v nižjo kategorijo "visokega tveganja". Po razpoložljivih informacijah je tudi Slovenija v svojem nacionalnem poročilu o oceni tveganja kibernetских tveganj v omrežjih 5G za posamezne kategorije elementov omrežij določila relativno stopnjo občutljivosti, pri čemer je določene kategorije označila kot kritične, določene pa kot visoko tvegane. Bazne postaje tudi v slovenskem poročilu niso bile uvrščene med elemente s kritično stopnjo občutljivosti). Podobne zaključke nudi primerjava med vsebino seznama iz priloge k SADVZO na eni strani ter opredelitvijo kritičnih elementov v poročilu skupine za sodelovanje NIS EU coordinated risk assessment of the cybersecurity of 5G networks na drugi strani v zvezi z upravljaljskimi sistemi (Management systems and supporting services). Tudi ta kategorija je v poročilu skupine za sodelovanje NIS označena s še nekoliko nižjo stopnjo občutljivosti - zmerno do visoko tvegani (moderate/high level of sensitivity). Predlog SADVZO pa jih prav tako uvršča med kritične elemente. Na področjih pravnega urejanja, za katera je značilna pomembna vloga strokovnih dognanj, kakršno je gotovo tudi področje kibernetске varnosti, je za izvedbo testa nujnosti ključno upoštevati strokovna dognanja, s pomočjo katerih je moč ugotoviti, kateri izmed možnih alternativnih ukrepov predstavlja najmanj invaziven

poseg v človekovo pravico, pa je z njim obenem še mogoče doseči cilj, ki ga zasledujemo. To velja tako za pripravljavca predpisa kot za sodno vejo oblasti v morebitni kasnejši fazi ustavnosodne kontrole predpisa. V procesu identifikacije tveganj, ki je temeljilo na stroki in katerega rezultat sta zgoraj omenjeni evropsko poročilo in nacionalno slovensko poročilo, bazne postaje ne glede na njihovo lokacijo kot tudi še nekateri drugi elementi (upravljalovski sistemi, transport in prenosne funkcije) niso bile prepoznane kot kritični element omrežja. Mnenje opozarja, da bi bilo možno zasledovani cilj doseči tudi brez uvrstitve baznih postaj in drugih omenjenih elementov v seznam, breme, da pojasni racionalne in strokovne razloge za drugačno odločitev, ki po eni strani odstopa od javno predstavljenih in javnosti dostopnih strokovnih ugotovitev, po drugi strani pa težje prizadene naslovnike pravnih norm, bi bilo na pripravljalcu predpisa. Mnenje zaključuje, da je definicija kritičnih elementov, predvidena v predlogu Splošnega akta, ustavnopravno izjemno sporna z vidika ustavnega načela sorazmernosti. Primerjava predlaganih diktij v splošnem aktu z informacijami iz dokumenta EU coordinated risk assessment of the cybersecurity of 5G networks kaže na obstoj manj invazivnih alternativ, zaradi česar predlagana ureditev ne bi prestala testa nujnosti, negativen rezultat testa nujnosti kot prvina presoje z vidika načela sorazmernosti pa posledično pomeni, da obravnavana ureditev ni skladna s tem temeljnim ustavnim načelom.

Iz Mnenja tako povsem jasno izhaja, da predlog Splošnega akta ni v skladu z Ustavo Republike Slovenije. Iz Mnenja izhaja tudi predlog, da glede na odsotnost primerljivih drugih predhodnih mehanizmov zagotavljanja spoštovanja hierarhije pravnih aktov v slovenskem pravnem sistemu in ustavnem redu v primeru normodajne dejavnosti agencij smatra za smiselno, da opravi predhodno presojo SADVZO skladnosti z Ustavo RS in zakoni, če bo prišlo do sprejema v predlaganem besedilu, Služba Vlade RS za zakonodajo po določbah 10. člena Zakona o uradnem listu.

Takšne rešitve bi odstopile od dobrih praks drugih držav članic EU:

- i. Avstrija: sploh ne pozna definicije kritičnih komponent omrežja<sup>13</sup>;
- ii. Nemčija: nemški BSI (organ za kibernetično varnost) in BNetzA (regulator telekomunikacij), ne opredeljujeta sama po lastni presoji kritičnih komponent, temveč morajo operaterji določiti, katero komponento je treba obravnavati kot "kritično komponento" na podlagi seznama, ki ga zagotovita BSI in BNetzA;
- iii. Finska: definicija kritičnih komponent (elementov) je v pristojnosti Traficom (finski organ za telekomunikacije), in sicer so kritične komponente (elementi) definirane kot „ključne funkcije in

<sup>13</sup> Glejte avstrijski zvezi zakon o telekomunikacijah TKG 2021 dostopen na: [https://www.ris.bka.gv.at/Dokumente/ErV/ERV\\_2021\\_1\\_190/ERV\\_2021\\_1\\_190.pdf](https://www.ris.bka.gv.at/Dokumente/ErV/ERV_2021_1_190/ERV_2021_1_190.pdf)

ukrepi omrežja, ki se na pomemben način uporabljajo za nadzor in upravljanje dostopa do omrežja in omrežnega prometa“. Pripravljen je tudi posebni seznam, ki ne vključuje radijskega dostopovnega omrežja 5G (RAN), transportnih in prenosnih funkcij, vmesnikov za medomrežno povezovanje ter zakonitega prestrezanja<sup>14</sup>.

- iv. Madžarska: ne uveljavlja definicije kritičnih elementov in tudi ne postavlja nobenih omejitev s tem v zvezi.

### 3. Glede kršitve prava EU in mednarodnega prava

Zadeve nacionalne varnosti Slovenije so v pristojnosti Republike Slovenije in ukrepi za varovanje varnosti komunikacijskih omrežij so očitno dobrodošli, vendar morajo kakršnekoli omejitve dosledno in ustrezno upoštevati nacionalne pravne standarde in pravice ter temeljne svoboščine varovane z Ustavo Republike Slovenije in Listino Evropske unije o temeljnih pravicah ter načelo sorazmernosti. Splošni akt bi, če bi bil sprejet v takšni vsebini, v povezavi z izdajo kakršnekoli odločbe po 117. členu ZEKom-2 (pa tudi če takšna odločba ni izdana), med drugim kršil:

- načelo enakosti (14. člen Ustave in člen 20 Listine Evropske unije o temeljnih pravicah (»Listina EU«));
- pravico do zasebne lastnine (33. člen Ustave, 1. člen Dodatnega protokola k Evropski konvenciji o varstvu človekovih pravic (»EKČP«), člen 17 Listine EU);
- pravico svobodne gospodarske pobude (74. člen Ustave, člen 16 Listine EU) in varstvo konkurence in splošne svobode ravnanja (35. člen Ustave);
- prepoved diskriminacije (14. in 22. člen Ustave, 14. člen EKČP, člen 21 Listine EU).

---

<sup>14</sup> Ureditev kritičnih delov omrežja izhaja iz dokumenta: TRAFICOM/161584/03.04.05.00/2020, dostopen na: [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Regulation\\_on\\_critical\\_parts\\_of\\_a\\_communications\\_network.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Regulation_on_critical_parts_of_a_communications_network.pdf)

Omejevanje glede na državo izvora (glejte kriterije iz prvega odstavka 117. člena ZEKom-2) bi bilo v nasprotju z načeli nediskriminacije in sorazmernosti, ki izhajajo iz Ustave Republike Slovenije, zapisana pa so tudi v Pogodbah EU in Listini Evropske unije o temeljnih pravicah. Navedeno je toliko bolj problematično, ker se omejevanje razteza tudi na elemente, ki ne štejejo za kritične po pravu EU (med drugim Usklajeni oceni tveganj in Naboru orodij in smernicami ENISA), mednarodnih standardih in Nacionalni oceni tveganj Republike Slovenije. Poleg tega bi bili učinki tovrstnih ukrepov v nasprotju z mednarodnimi obveznostmi Republike Slovenije. Natančneje, prepoved, ki *de facto* temelji na državi izvora dobavitelja opreme, bi kršila tudi načeli največjih ugodnosti in nacionalne obravnave, ki sta ključni v skladu s pravom WTO in veljavnimi bilateralnimi investicijskimi sporazumi.

Kršitev prava WTO pomeni tudi kršitev dolžnosti Slovenije glede lojalnega sodelovanja v skladu s členom 4(3) Pogodbe o Evropski uniji (PEU), torej da učinkovito izvaja in varuje pravo Unije v skladu s členoma 197(1) in 291(1) Pogodbe o delovanju Evropske unije (PDEU), saj se pravo WTO šteje za sestavni del pravnega reda Unije.<sup>15</sup> V skladu s členom XVI(4) Sporazuma o ustanovitvi Svetovne trgovinske organizacije mora vsaka članica WTO zagotoviti usklajenost svojih zakonov, predpisov in upravnih postopkov s svojimi obveznostmi, torej mora v okviru notranjega pravnega reda zagotoviti, da so njene obveznosti iz prava WTO izpolnjene na njenem ozemlju.<sup>16</sup> Sporazumi WTO prepovedujejo članicam WTO, vključno s Slovenijo in Kitajsko, diskriminacijo uvoženega izdelka, storitev ali ponudnika storitev. Načelo največjih ugodnosti državam članicam WTO preprečuje, da bi diskriminirali svoje trgovinske partnerje. Načelo nacionalne obravnave članicam WTO prepoveduje diskriminacijo uvoženega

---

<sup>15</sup> Tako Sodba Sodišča Evropske unije iz oktobra 2020, *Komisija proti Madžarski*, C-66/18, EU:C:2020:792, odstavki 69–71, v katerih je navedeno, da je *mednarodni sporazum, ki ga je sklenila Unija, sestavni del pravnega reda Unije od začetka njegove veljavnosti. [...] Sporazum o ustanovitvi WTO - katerega del je GATS - je nato 22. decembra 1994 s Sklepom 94/800 podpisala in odobrila Unija. Sporazum je začel veljati... GATS je torej del prava Unije. Poleg tega je Sodišče Evropske unije menilo, da neizpolnjevanje teh [mednarodnih] sporazumov s strani držav članic spada v pravo EU in je neizpolnitev obveznosti lahko predmet tožbe v skladu s členom 258 PDEU.* (odstavek 65).

<sup>16</sup> A je podobna obveznost določena tudi v členu I(3)(a) Splošnega sporazuma o trgovini s storitvami ("GATS").

blaga v primerjavi z domačim blagom/storitvami.<sup>171819</sup>

Predlagani splošni akt spada na področje uporabe prava WTO, saj vpliva na uporabo omrežne opreme.<sup>20</sup> Prepoved opreme, ki bi temeljila na povezavi dobavitelja z državo izvora ali na lokaciji dobavitelja v določeni državi (glejte predlagani splošni akt, ki še širi domet ZEKom-2 tudi na nekritične elemente in funkcije omrežja, med drugim radijsko dostopovno omrežje, v povezavi s kriteriji iz prvega odstavka 117. člena ZEKom-2 vezanimi na tretjo državo) vodi v diskriminacijo med proizvodi s poreklom iz določene države in izdelki s poreklom iz Slovenije/EU, pri tem pa krši načelo največjih ugodnosti in obveznosti nacionalne obravnave.

Teh kršitev ni mogoče opravičiti na podlagi izjeme bistvenih varnostnih interesov iz prava WTO. Izjema v pravu WTO je še bolj ozka od že tako strogih pogojev izjeme javne varnosti v skladu z zakonodajo EU o notranjem trgu.<sup>21</sup> Izjema nacionalne varnosti v skladu s členom XXI(b) Splošnega sporazuma o carinah in trgovini (GATT) lahko upraviči samo ukrep (i) v zvezi z materiali za fizijo in fuzijo ali z materiali, iz katerih so pridobljeni; (ii) v zvezi s trgovino z orožjem, strelivom in vojnimi pripomočki in s takšno trgovino z drugim blagom in materialom z neposrednim ali posrednim namenom oskrbovanja vojaške ustanove; ali (iii) sprejetih v času vojne ali drugega izrednega stanja v mednarodnih odnosih. Določbe predlaganega splošnega akta očitno ne padejo pod nobeno od teh treh vrst ukrepov in zato kršijo zakonodajo WTO. V zvezi z razlago izraza »izredne razmere v mednarodnih odnosih« v členu XXI(b)(iii) GATT je odbor WTO v Rusiji odločil, da je pristojen za presojo izjeme nacionalne varnosti in da ima pravico objektivno določiti pomen izrednih razmer v mednarodnih odnosih.<sup>22</sup> Po oceni odbora se taka situacija

---

<sup>17</sup> Ti vključujejo Splošni sporazum o carinah in trgovini ("GATT"), GATS in Sporazum WTO o tehničnih ovirah v trgovini ("Sporazum TBT").

<sup>18</sup> Člen I:1 GATT, člen II:1 GATS in člen 2.1 Sporazuma TBT.

<sup>19</sup> Člen III:4 GATT in člen XVII:1 GATS.

<sup>20</sup> GATT se nanaša vse zakone, predpise in zahteve, ki vplivajo na domačo prodajo, ponudbo za prodajo, nakup, prevoz, distribucijo ali uporabo proizvodov. V primeru trgovine s storitvami GATS zajema vse ukrepe, ki jih sprejmejo članice WTO, ki vplivajo na trgovino s storitvami. V zvezi s tehničnimi predpisi člen 2.1 Sporazuma TBT zahteva, da se s tehničnimi predpisi proizvodi, uvoženi z ozemlja države članice, ne obravnavajo manj ugodno kot proizvodi nacionalnega porekla in podobni proizvodi s poreklom iz katere koli druge države.

<sup>21</sup> Člen XXI GATT.

<sup>22</sup> *Rusija - Ukrepi v zvezi s prometom v tranzitu*, DS512, 26. aprila 2019, točka 7.71.



(to je izredne razmere v mednarodnih odnosih) na splošno nanaša na oboroženi spopad ali latenten oboroženi spopad ali povečano napetost ali krizo ali splošno nestabilnost, ki zajame in obkroža državo. Zato bi izjema prišla v poštev samo v primeru vojne ali vojni podobnih razmer. Jasno je, da se Republika Slovenija ne sooča z nobeno vojno ali vojni podobnimi razmerami<sup>23</sup> z nobeno državo. Enaka presoja se smiselno uporablja za člen XIV bis Splošnega sporazuma o trgovini s storitvami (GATS), saj se izjema nacionalne varnosti lahko upraviči le z ukrepom: (i) ki se nanaša na opravljanje storitev z neposrednim ali posrednim namenom oskrbovanja vojaške ustanove; (ii) v zvezi z materiali za fizijo in fuzijo ali z materiali, iz katerih so pridobljeni; (iii) sprejetim v času vojne ali drugega izrednega stanja v mednarodnih odnosih; ali (iv) ki se sprejme v skladu z obveznostmi države članice po Ustanovni listini Združenih narodov za vzdrževanje mednarodnega miru in varnosti. Jasno je, da splošni akt v povezavi z ZEKom-2 ne opravičuje nobene od izjem nacionalne varnosti.

Diskriminatorno obravnavanje iz predlaganega splošnega akta v povezavi z določbami ZEKom-2, torej diskriminiranje med proizvodi iz tretjih držav in proizvodi iz Slovenije/EU je v nasprotju z načelom nacionalne obravnave in načelom največjih ugodnosti in je predlagani splošni akt tako v nasprotju s pravom WTO in pravom EU tudi iz tega razloga.

Obenem bi vsakršen poskus izključitve ali omejevanja možnosti dobaviteljev opreme glede na sedež pri prodaji 5G v EU bil v vsakem primeru z gospodarskega vidika kontraproduktiven, vse še toliko bolj, ker bi se glede na predlog splošnega akta prepoved nanašala tudi na nekritične elemente, na primer dostopovni del omrežja (RAN) ter upravljaljske in/ali druge podporne sisteme.

Poleg tega obstajajo manj omejevalni in celo učinkovitejši načini za ublažitev varnostnih tveganj omrežja, kot so vzpostavitev strožjih splošnih varnostnih standardov in certificiranja, zaveze dobaviteljev, lokalizacija zmogljivosti, zahteve glede lokalnega shranjevanja občutljivih podatkov, zahteve po skladnosti z veljavnimi varnostnimi standardi opreme itd. Splošni akt, ki bi v povezavi z 117. členom ZEKom-2 pripeljal do tega, da bi se lahko prepovedalo tudi dostopovno omrežje in celo pasivna oprema, ki nikakor ne more biti kritična v smislu kibernetске varnosti, nikakor

---

<sup>23</sup> Rusija - Ukrepi v zvezi s prometom v tranzitu, DS512, 26. aprila 2019, točka 7.76.

v nobenem primeru ne more prestatl testa sorazmernosti.

Splošni akt bi bil tudi v nasprotju s predpisi s področja varstva konkurence. Skladno z Zakonom o preprečevanju omejevanja konkurence (ZPOmK-2) so prepovedana tudi oblastna omejevanja konkurence (glejte VII. del). Vlada, državni organi, organi lokalnih skupnosti in nosilci javnih pooblastil ne smejo omejevati prostega nastopanja podjetij na trgu, pri čemer se za omejevanje prostega nastopanja podjetij na trgu štejejo splošni in posamični akti in dejanja, s katerimi se v nasprotju z ustavo in zakonom omejujejo svobodna menjava blaga in storitev, svoboden vstop na trg, svobodno nastopanje na trgu ali s katerimi se kako drugače preprečuje konkurenca (107. člen ZPOmK-2). Splošni akt (s katerim bi se omejila konkurenca glede dostopnega omrežja in drugih elementov, ki jih splošni akt v nasprotju s smernicami EU opredeljuje kot kritične) bi tako (še posebej v primeru izdaje odločbe po 117. členu ZEKom-2) izkrivljal konkurenco in bi imel za posledico zvišanje cen, znižanje kvalitete in zmanjšanja izbire in inovacij. Omejevanje konkurence s strani države članice bi bilo tudi v nasprotju s pravom EU<sup>24</sup>.

#### **4. Glede obveznosti naloženih dobaviteljem, vključno s preprečevanjem odvisnosti od posameznega dobavitelja**

9. točka prvega odstavka 3. člena predloga Splošnega akta določa:

*»(1) Operaterji v dobavni verigi komponent kritičnih elementov omrežja in storitev podpore tretje ravni za te komponente v celotnem življenjskem ciklu upoštevajo najmanj naslednje usmeritve: ...*

*9. izogibanje enemu samemu dobavitelju, da se prepreči odvisnost ter zagotovi odpornost v primeru kritičnih ranljivosti komponent, katastrofalne okvare omrežja oziroma grožnje za varnost omrežij in storitev kritičnih subjektov s strani tretjih fizičnih ali pravnih oseb javnega ali zasebnega prava. «*

---

<sup>24</sup> Kot izhaja iz sodbe v združenih zadevah od C-184/13 do C-187/13, C-194/13, C-195/13 in C-208/13 se člena 101 PDEU in 102 PDEU sicer res nanašata le na ravnanje podjetij in ne na zakonodajo ali druge predpise, ki jih sprejmejo države članice, vendar ta člena v povezavi s členom 4(3) PEU, ki določa dolžnost sodelovanja med Evropsko unijo in državami članicami, državam članicam nalagata, da ne sprejmejo ali ne ohranjajo v veljavi ukrepov, tudi zakonskih ali podzakonskih, ki bi lahko izničili polni učinek pravil konkurence, ki veljajo za podjetja.

Peti odstavek 6. člena predloga Splošnega akta določa:

*(5) Operater preprečuje svojo odvisnost od posameznega dobavitelja oziroma ponudnika storitev tretje ravni (t.i. angl. »vendor lock-ins«) tudi z izogibanjem dolgoročnim pogodbam s posameznim dobaviteljem oziroma ponudnikom storitev podpore tretje ravni oziroma ima možnost njune menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnim subjektom na najmanjšo možno raven.*

7. člen Splošnega akta gre tako daleč, da določa celo vsebino pogodbenega razmerja med operaterjem in dobaviteljem komponent kritičnih elementov omrežja, in ponudniki storitev podpore tretje ravni, in sicer določa, kaj mora operater vključiti v pogodbeno določila.

Kot izhaja iz Mnenja, tovrstne določbe kršijo zakonsko pooblastilo za sprejem splošnega akta in bi bile v nasprotju z Ustavo Republike Slovenije. Iz Mnenja tako izhajajo naslednji zaključki:

1. Mnenje opozarja na zakonsko pooblastilo za podzakonsko urejanje iz 116. člena ZEKom-2, kjer je zakonodajalec Agencijo pooblastil, da določi "druge usmeritve", pri čemer gre v prvi vrsti in predvsem za tehnične usmeritve. Z dodatkom besede "zlasti" je zakonodajalec razširil pomensko oz. interpretativno polje tega pooblastila. Izraz "zlasti" sodi namreč z vidika nomotehnične stroke med tako imenovane "difuzne izraze," pri katerih "sta potrebni posebna previdnost in preudarnost zaradi ohlapnosti njihovega pomena in določenosti, tako da jih je pri izvrševanju predpisa nujno razlagati (bolj kot druge izraze)."<sup>25</sup> Mnenje opozarja, da je potrebno dikcije, ki uporabljajo difuzne izraze, natančno razlagati. Povsem v nasprotju z logiko ustavnega načela legalitete bi bilo, če bi besedici zlasti v našem kontekstu pripisali moč, da zakonsko pooblastilo razširi na "kakršne koli druge usmeritve". Zaradi ustavno zajamčene vezanosti uprave na ustavo in zakon (120. člen URS) je treba dikcijo "druge zlasti tehnične usmeritve" razlagati ozko in si predvsem zastaviti vprašanje, kakšne druge, "netehnične" usmeritve bi še utegnile biti takšne, da bi se s podzakonskim urejanjem le-teh doseglo učinkovito izvrševanje zakonske norme. Mnenje s tem v zvezi opozarja tudi na dokument Skupine za sodelovanje na področju varnosti omrežij in informacij (ang. NIS Cooperation

<sup>25</sup> Služba Vlade RS za zakonodajo, Nomotehnične smernice, 3., spremenjena in dopolnjena izd., 2018, tč. 102, str. 69.

Group)<sup>26</sup> *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*.<sup>27</sup> Dokument je bil zamišljen kot "podlaga za identifikacijo ukrepov za zmanjševanje tveganj, ki se jih lahko uporabi na ravni države članice in na ravni Unije."<sup>28</sup> V kontekstu razlage zakonskega pooblastila po 116. členu ZEKom-2 lahko služi (vsaj) kot interpretativni okvir, saj je nastal v okviru izgradnje skupnega evropskega sistema zagotavljanja kibernetične varnosti in s sodelovanjem vseh držav članic in pristojnih institucij ter teles EU.<sup>29</sup> Ta dokument tako v okviru instrumentov za zmanjševanje tveganj, ki so predvideni na ravni Unije (str. 6) kot tudi pri prikazu pravil v državah članicah, s katerimi so le-te implementirale pravila za telekomunikacije v EU (str. 9), omenja dva tipa ukrepov. Poleg tehničnih, ki so v jedru zakonskega pooblastila po šestem odstavku 116. člena ZEKom-2, tudi *organizacijske* ukrepe. Po oceni Mnenja se lahko organizacijski ukrepi razlagajo kot vzpostavitev ustreznih sistemov oziroma mehanizmov, s katerimi operater svojo notranjo strukturo ter organizacijo delovnih procesov in človeških virov uredi tako, da mu omogoči učinkovito izvajanje ukrepov za zmanjševanje tveganj.<sup>30</sup> Mnenje opozarja, da je na podlagi obstoječih virov mogoče priti do prepričljive in ustrezno ozke razlage dikcije "drugih usmeritev". Stališče Mnenja je, da mora organ, ki sprejme podzakonski predpis in s tem postavi obvezujoče pravne norme, kadar je postavljen pred izbiro med po eni strani ozke, z zakonskim pooblastilom skladne variante na eni strani, in široke, zakonsko pooblastilo presegajoče variante na drugi strani, uporabiti prvo, da ne bi prišlo do kršitve zapovedi vezanosti uprave na zakon (120. člen Ustave RS).

2. Iz Mnenja izhaja, da je vsebino pravne norme težko okarakterizirati kako drugače kot prepoved. Glagol "izogibati" je pomensko ohlapen, še posebej, ker je v nedovršenem glagolskem vidu.<sup>31</sup> Verjetno je Agencijo pri izbiri te besede vodila želja, pravne učinke predlagane norme prikazati kot manj invazivne, kot v resnici

---

<sup>26</sup> Skupina za sodelovanje na področju varnosti omrežij in informacij (NIS Cooperation Group) je predvidena v 14. členu Direktive (EU) 2022/2555 Parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetične varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148, UL EU L 333/80 (krajše: direktiva NIS 2). Gl. tudi <https://digital-strategy.ec.europa.eu/sl/policies/nis-cooperation-group>.

<sup>27</sup> NIS Cooperation Group, *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*, CG Publication 01/2020, dokument je objavljen na [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=64468](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468).

<sup>28</sup> *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*, str. 4.

<sup>29</sup> Po določi tretjega odstavka 14. člena direktive NIS 2 Skupino sestavljajo "predstavniki držav članic, Komisije in Agencije Evropske unije za kibernetično varnost (ENISA)."

<sup>30</sup> Za ilustracijo teh procesov, pri katerih je moč terjati organizacijske prilagoditve operaterja lahko vzamemo navedbo iz *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*, str. 10., po kateri varnostni ukrepi zajemajo "...ukrepanje ob incidentih, menedžment v zvezi s kontinuiteto poslovanja, nadzor, preglede in testiranje... (...*handling of security incidents, business continuity management, monitoring, auditing and testing...*)."

<sup>31</sup> Dovršna različica "izogniti", denimo, je za odtенок pomensko jasnejša.

so. Z vidika naslovnika pravne norme pa tudi na videz mehkejši izraz nima bistveno drugačnih posledic. Če želi preprečiti nastanek pravne sankcije oz. negativne posledice (bodisi izreka globe v prekrškovnem postopku bodisi odvzema frekvence, kot pojasnjeno) lahko utemeljeno pričakujemo, da bo naslovník obveznost *izogibanja* sklepanju pogodb bral in razlagal kot *prepoved* sklenitve pogodbe. Glede na zaključke Mnenja glede razlage zakonskega pooblastila iz petega odstavka 116. člena, prepoved sklepanja pogodb ne more biti zajeta z drugim delom pooblastila, saj presega pooblastilo za določitev "drugih zlasti tehničnih usmeritev". To dodatno utemeljujeta še dva argumenta. Prvi izhaja iz jezikovne analize, in sicer izraz "usmeritev" nakazuje, da gre za mehkejše oblike navodil, ki nimajo nujno kakovosti pravne norme.<sup>32</sup> Vsebinsko zajemajo zlasti navodila, oblikovana na podlagi strokovnih dognanj, medtem ko omejevanje svobode poslovnega ravnanja, četudi bi bilo hipotetično ustavnopravno dopustno, terja višjo stopnjo demokratične legitimnosti, zaradi česar se ga sme urejati predvsem v zakonu. To dopolnjuje ugotovitev Mnenja, da je vloga javnih agencij v našem ustavnem sistemu zlasti v tehnični regulaciji, utemeljeni na strokovnem znanju, ne pa na legitimnosti za sprejemanje širših, invazivnejših in po naravi bolj političnih odločitev.<sup>33</sup> Kot opozarja Mnenje, je prepoved sklepanja pogodb težak in invaziven ukrep, ki operaterjem bistveno omejujejo svobodno izbiro poslovnih partnerjev. Slednje upravičenje spada po stališču komentatorice Ustave Republike Slovenije v samo jedro polja ustavnega varstva svobodne gospodarske pobude.<sup>34</sup> Mnenje dodaja, da je svobodna izbira poslovnih partnerjev s ciljem zasledovanja poslovnega

<sup>32</sup> Pregled predpisov v pravnoinformacijskem sistemu RS (PISRS) kaže, da je uporaba izraza "usmeritev" oz. "usmeritve" v zakonodajnem urejanju prejkone redka. Gre večino za zakonodajo, ki ne velja več. Pregled nekaterih zakonov kaže, da se v zakonodaji ta izraz uporablja npr. za informacije, ki jih političnim odločevalcem posredujejo strokovna telesa (po že ne več veljavnem Zakonu o raziskovalni in razvojni dejavnosti (Uradni list RS, št. 22/06 – uradno prečiščeno besedilo, 61/06 – ZDru-1, 112/07, 9/11, 57/12 – ZPOP-1A, 21/18 – ZNOrg, 9/19 in 186/21 – ZZrID) je Svet za znanost in tehnologijo Republike Slovenije kot strokovno posvetovalno telo Vlade le-tej predlagal "usmeritve" za pripravo raziskovalne strategije Slovenije; kadar gredo usmeritve v drugo smer, torej od političnih odločevalcev (vlada, ministrstva, Državni zbor) k bolj strokovnim ali poslovnim subjektom (npr. agencijam, pravnim osebam javnega prava), morajo biti te "splošne in ne smejo posegati v vodenje postopkov oziroma odločanje o posamičnih zadevah," kot je to predvideval 5. člen že ne več veljavnega Zakona o preprečevanju omejevanja konkurence (Uradni list RS, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13 – odl. US, 63/13 – ZS-K, 33/14, 76/15, 23/17 in 130/22 – ZPOmK-2) - prim. tudi "usmeritve" ministrstva Družbi za upravljanje terjatev bank po 4. členu že ne več veljavnega Zakona o ukrepih Republike Slovenije za krepitev stabilnosti bank (Uradni list RS, št. 105/12, 63/13 – ZS-K, 23/14 – ZDIJZ-C, 104/15, 26/17 – ORZUKSB33, 27/17 – popr. in 174/20 – ZIPRS2122). Ti primeri kažejo na to, da je izraz "usmeritve" v slovenskem zakonodajnem izrazju namenjen informacijam ali navodilom, ki ne dosegajo kakovosti pravne norme.

<sup>33</sup> Prim. Rose-Ackerman, *The Regulatory State*, v: Rosenfeld in Sajo (ur.), *Oxford Handbook of Comparative Constitutional Law*, OUP 2013, str. 676.

<sup>34</sup> Prim. opredelitev polja varovanja pravice iz 74. člena URS v Zagradišnik, *Komentar 74. člena*, v: Avbelj (ur.) *Komentar URS (Človekove pravice, 2019)*, rob. št. 10.

uspeha, ustvarjanja dobička in konkurenčnosti na prostem trgu tudi izraz avtonomije pogodbene volje.<sup>35</sup> Podobno trdi za določitev trajanja veljavnosti pogodbe, ki jo lahko štejejo za bistveno sestavino tovrstnih pogodbenih razmerij. Ob tem Mnenje dodaja še, da predlog Splošnega akta uporablja zelo ohlapen pravni pojem "dolgoročnih pogodb", ki se jim morajo izogibati operaterji.<sup>36</sup> Vprašanje, kako dolgo mora biti obdobje veljavnosti pogodbe, da ga oblastni organi ne bodo šteli za sestavino »dolgoročne pogodbe«, postane z uporabo tako ohlapnega pravnega pojma vprašanje za operaterja, ki ga le-ta ne more vnaprej preveriti in si tako zagotoviti potrebne pravne varnosti. Povsem mogoče je, da se bo operater enostavno izognil določenemu dobavitelju, ker bo sklenitev v zadostni meri »kratkorodne« pogodbe dejavnik tveganja v poslovnih odločitvah, zaradi katere bo dal prednost konkurenčnim dobaviteljem. S tem se bo, kot opozarja Mnenje, poseg v svobodno gospodarsko pobudo na »skrit« način razširi od transparentnih oblastno določenih pravil z vplivanjem na poslovne odločitve operaterjev, v končni posledici pa so možnosti dobavitelja, da bi uresničil pravico do svobodne gospodarske pobude, dodatno zožene. Mnenje opozarja, da enako velja za zahtevo po vključitvi določenih pogodbениh klavzul, za katere se morda operater po logiki poslovne presoje sam ne bi odločil, zlasti vključitev klavzule, s katero si bo lahko operater zagotovil možnost »menjave« dobavitelja oz. ponudnika,<sup>37</sup> kar bi bilo v pogodbo najverjetneje vključeno kot močnejša pravica operaterja, da enostransko odpove pogodbo pred potekom prvotno določene veljavnosti.

3. Brez dvoma lahko *de facto* prepoved sklepanja pogodb s svobodno izbranimi pogodbenimi strankami ter sklepanja dolgoročnih pogodb ustavnopravno klasificiramo kot poseg oz. omejitev ustavne pravice do svobodne gospodarske pobude iz 74. člena Ustave RS. Posledica te ustavnopravne klasifikacije je, da je treba obravnavani določbi SADVZO presojati z vidika dveh zahtev temeljnega ustavnopravnega načela pravne države (2. člen Ustave RS) v povezavi z načelom legalitete po 120. členu Ustave RS. Prvič, posege v človekove pravice in temeljne svoboščine je treba načeloma urediti v zakonu. Drugič, da bi bili skladni z ustavo, morajo biti v skladu z načelom sorazmernosti. Stališče Mnenja je, da zakonskega pooblastila iz šestega odstavka 116. člena ne moremo razlagati tako, da bi Agenciji omogočal določanje omejitev poslovne svobode operaterjev. Tako obravnavane določbe kršijo ustavnopravno načelo legalitete. Če bi javna oblast v Sloveniji želela določiti tovrstne omejitve pogodbene avtonomije v okviru pravice iz 74. člena Ustave RS, bi morala to storiti z zakonom. Mnenje pod točko 4.2 opozarja tudi na neskladnost zahtev po diverzifikaciji

---

<sup>35</sup> Prim. odločbo US RS U-I-202/93, tč. 4.

<sup>36</sup> Ob tem je treba opozoriti, da je bila v prejšnjem predlogu SADVZO, ki ga je Agencija objavila na svoji spletni strani (in dala v javno razpravo) dne 7. 4. 2023, dikcija "dolgoročne pogodbe" dopolnjena s pojasnilno navedbo v oklepaju "pet let ali več", medtem ko obravnavani predlog SADVZO te pojasnilne navedbe ne vključuje.

<sup>37</sup> Po dikciji petega odstavka 6. člena predloga SADVZO "...oziroma ima možnost njune menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnih subjektov na najmanjšo možno raven..."

z načelom sorazmernosti.

4. Mnenje pod točko 4.3. še povzema, da gre za preseganje zakonskega pooblastila iz šestega odstavka 116. člena Zakona o elektronskih komunikacijah (ZEKom-2), določanje vsebine pravnih poslov, ki jih bodo operaterji sklepali z dobavitelji, kot je predvideno v obravnavanih določbah SADVZO, presega pooblastilo za določitev »drugih zlasti tehničnih usmeritev«, kot se glasi upoštevna dikcija zakonskega pooblastila. Določitev obveznosti »izogibanja« določenim odločitvam, ki omeji in nadomesti svobodo oblikovanja pogodbenih razmerij, je *de facto* prepoved, ki ne more biti prepuščena podzakonskemu urejanju, zlasti tudi ne zaradi določbe 87. člena Ustave RS. Navedbe iz dokumenta *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*, glede na katere je moč tveganje prevelike odvisnosti od dobaviteljev zmanjšati tudi z manj invazivnimi ukrepi, v primerjavi z obravnavanimi določbami SADVZO, pa pomeni, da predlagana ureditev ne bi prestala test nujnosti. Posledično iz Mnenja izhaja, da je predlagana ureditev zahtev po diverzifikaciji v neskladju z načelom sorazmernosti.

Kakršnekoli dodatne obveznosti, ki bi bile naložene operaterjem (ki jih ne predvideva že ZEKom-2) bi bile v nasprotju z zakonskim pooblastilom za izdajo splošnega akta po 115. in 116. členu ZEKom-2 in posledično v nasprotju s 120. členom Ustave, kot je bilo pojasnjeno in bo pojasnjeno tudi še v nadaljevanju. Navedena določba je tudi nejasna in pomensko odprta, med drugim ni jasno, kaj je mišljeno z možnostjo *»menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnim subjektom na najmanjšo možno raven.«*

Navedene določbe bi predstavljale tudi poseg v svobodno gospodarsko pobudo varovano s 74. členom Ustave, saj kakršnekoli dodatne omejitve vezano na nabavo opreme na eni strani, na drugi strani nujno pomenijo poseg v svobodo gospodarske pobude dobaviteljev, ki takšno opremo ponujajo. Posledično bi morale kakršnekoli dodatne obveznosti vezane na dobavo biti že zakonsko predvidene in prestati tudi ustavni splošni test sorazmernosti.

Drugi odstavek 120. člena Ustave določa, da upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov. Drugi odstavek 120. člena Ustave ureja načelo zakonitosti delovanja uprave ali načelo legalitete. Poleg načela zakonitosti ureja ta določba tudi zahtevo po samostojnosti delovanja uprave. Obe načeli v medsebojni povezanosti zagotavljata razmerje med zakonodajno in izvršilno vejo oblasti, ki je skladno z načelom delitve oblasti

(drugi odstavek 3. člena Ustave RS).<sup>38</sup> Temeljna vsebina drugega odstavka 120. člena Ustave je zahteva po vsebinski vezanosti uprave na ustavo in zakon pri njenem delovanju. Vsebinska vezanost zagotavlja tako razmerje med zakonodajno in izvršilno vejo oblasti, v katerem je izvršilna veja oblasti vezana na temeljne odločitve zakonodajne veje oblasti, kar v vsebinskem smislu pomeni vezanost uprave na zakon. S tem je zagotovljeno ravnotežje med tema dvema vejama oblasti, v katerih ima ena neposredne vzvode izvrševanja oblasti, druga pa sprejema temeljne odločitve, kako se ti vzvodi uporabljajo.<sup>39</sup> V 87. členu Ustave RS je določeno, da lahko pravice in obveznosti državljanov ter drugih oseb Državni zbor določa le z zakonom. Ta določba ne pomeni le opredelitve zakonodajne pristojnosti Državnega zbora, pač pa tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon.<sup>40</sup> Načelo zakonitosti delovanja uprave (drugi odstavek 120. člena Ustave) tako zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali.<sup>41</sup> Načelo zakonitosti je nadalje povezano z drugim odstavkom 15. člena Ustave RS, ki določa, da je mogoče predpisovati način uresničevanja človekovih pravic in svoboščin z zakonom, kadar tako določa ustava ali če je to nujno zaradi narave pravice oziroma svoboščine. Tretji odstavek 15. člena Ustave RS pa na drugi strani ureja možnost omejevanja človekove pravice in svoboščine, pri čemer je to dopustno, če je to potrebno zaradi varstva pravic drugih in če tako določa Ustava RS. Ključno je, da ne glede na to, ali gre za omejevanje ali za predpisovanje načina uresničevanja človekove pravice ali svoboščine, je eno ali drugo mogoče le z zakonom.

Predlagano besedilo je nejasno, kar pomeni njegovo neskladnost z načelom jasnosti in določnosti predpisov, ki je eno od (pod)načel pravne države iz 2. člena Ustave. To načelo namreč zahteva, da je iz besedila predpisa mogoče nedvoumno ugotoviti vsebino in namen norme.<sup>42</sup> Ne glede na to, ali vsebino navedene določbe štejemo kot omejitev ali kot predpisovanje načina uresničevanja svobodne gospodarske pobude, v obeh primerih velja, da je to dopustno

---

<sup>38</sup> Tako Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 635.

<sup>39</sup> Ibid.

<sup>40</sup> Odločba Ustavnega sodišča RS št. U-I-40/96 z dne 3. 4. 1997, tč. 13.

<sup>41</sup> Tako Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 636.

<sup>42</sup> Primerjajte: odločba Ustavnega sodišča RS U-I-246/14 z dne 24. 3. 2017, tč. 19.



normirati le z zakonom, ne pa s pravnimi akti, ki so hierarhično nižji od zakona, kamor uvrščamo tudi splošne akte AKOS. V obsegu, kolikor skuša Splošni akt AKOS kot podzakonski predpis urejati zakonsko materijo, to ni ustavno dopustno, saj so po Ustavi RS zakonu pridržana tako vprašanja, ki pomenijo urejanje zakonskih pravic, kot vprašanja, ki pomenijo bistveno sestavino pravic in obveznosti posameznika ali pravne osebe in mora biti vsebovana že v zakonu.<sup>43</sup> V konkretnem primeru tudi ZEKom-2 ne določa vsebinskega okvira podzakonskega predpisa dovolj jasno in določno v smeri kakršnihkoli konkretnih dodatnih obveznosti vezanih na dobavne verige, in tako ne more biti prepuščeno splošnemu aktu AKOS, da ta samostojno ureja pravice in obveznosti.<sup>44</sup> Glede na odprtost in splošnost pooblastila vsebovanega v 115. in 116. členu ZEKom-2 za izdajo splošnih aktov preprosto ni mogoče šteti, da bi splošni akt kot podzakonski predpis sploh lahko podrobneje urejal zakonsko materijo in pri tem sledil namenu in ciljem zakona. Navedeno pa smiselno potrjuje tudi pridobljeno Mnenje.

Kakršnokoli omejevanje dobave ali dobavnih verig, pa ne vpliva le na operaterje, temveč po sami naravi stvari omejuje tudi dobavitelje in posega v svobodo gospodarske pobude (74. člen Ustave). Pri tem torej ne gre le za neskladnost z ustavnim načelom legalitete (drugi odstavek 120. člena Ustave), temveč tudi neskladnost s 74. členom Ustave RS. Na podlagi prvega stavka drugega odstavka 74. člena Ustave RS ima zakonodajalec po ustaljeni ustavnosodni presoji pooblastilo, da uredi način uresničevanja pravice iz prvega odstavka 74. člena Ustave RS tudi, ko gre za opravljanje gospodarske dejavnosti.<sup>45</sup> Uresničevanje pravice iz prvega odstavka 74. člena Ustave RS bi moralo biti v konkretnem primeru urejeno v zakonu, ne pa v splošnem aktu AKOS kot podzakonskemu predpisu, zato je Splošni akt v nasprotju tudi s 74. členom Ustave. Drugi stavek drugega odstavka 74. člena Ustave RS prepoveduje izvajanje gospodarske dejavnosti v nasprotju z javno koristjo. Ta določba predstavlja ustavno pooblastilo zakonodajalcu (in le zakonodajalcu), da sme pravico do svobodne gospodarske pobude omejiti, kadar to zahteva javna korist. Iz obstoječe sodne prakse izhaja, da zakonodajalčeva svoboda pri omejevanju pravice do

<sup>43</sup> Primerjajte: Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 637.

<sup>44</sup> Glejte odločbo Ustavnega sodišča RS U-I-73/94 z dne 25. 5. 1995, tč. 19.

<sup>45</sup> Gre npr. za urejanje obratovalnega časa trgovin (U-II-2/03), pogojevanje pridobitve licence za prevoze stvari v cestnem prometu s parkirnim oz. vzdrževalnim mestom za vozilo (U-I-266/01), prepoved postavitve avtomatov s hrano in pijačo v vrtcih, šolah ali vzgojno-izobraževalnih zavodih (U-I-189/10) in še nekaj drugih primerov. Tako: Zagradišnik, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 590.

svobodne gospodarske pobude ni absolutna in neomejena. Zakonodajalca veže splošno načelo sorazmernosti, ki mu dovoljuje, da ustavno pravico omeji le toliko, kolikor je zaradi varovanja javne koristi, zaradi katere je ustavno dopustno poseči v pravico, v pravico treba poseči. Zato mora zakonodajalec pri uzakonitvi omejitve izbrati tak ukrep, ki bo zagotovil učinkovito varstvo javne koristi ter hkrati kar najmanj posegel v ustavno pravico.<sup>46</sup> Glede na to, da zakon ne daje ustrezne podlage za nalaganje kakršnihkoli dodatnih obveznosti vezanih na dobavne verige, takšnih obveznosti ni možno originarno naložiti s splošnim aktom AKOS, v nobenem primeru pa tudi ni in ne more biti podana sorazmernost za takšen ukrep.

Zdi se, da ukrep, ki ga skuša uveljaviti Splošni akt povezan z rizikom R4<sup>47</sup> iz Nabora orodij, kar naj bi se naslavljal z ukrepom SM05<sup>48</sup>, navedeni ukrep, ki dejansko samim operaterjem prepušča, da pripravijo ustrezno strategijo, je manj invaziven in zato ukrepi predvideni v predlogu splošnega akta ne morejo prestati testa sorazmernosti. Ukrep, ki ga predvideva Splošni akt je tako nesorazmeren in nepotreben in gre preko tega, kar bi bilo potrebno za implementacijo evropskih smernic, t.i. Nabora orodij EU.

## 5. Glede netehničnih kriterijev

Prvi odstavek 4. člena predloga Splošnega akta določa:

*»(1) Operater pri ugotavljanju tveganosti dobavitelja komponent in ponudnika storitev tretje ravni za kritične elemente omrežja upošteva tako tehnične kot netehnične vidike tveganosti, ki jih vrednoti.«*

---

<sup>46</sup> O tem: Zagradišnik, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 590 in odločba Ustavnega sodišča RS U-I-163/05 z dne 27. 10. 2005, tč. 20 in odločba Ustavnega sodišča RS U-I-212/03 z dne 24. 11. 2005, tč. 13.

<sup>47</sup> Rizik imenovan v angleščini »R4-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis«

<sup>48</sup> Ukrep naslovljen v angleščini »SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies«, vsebina katerega se v angleščini glasi: "Ensure that each MNO has an appropriate multi-vendor strategy of taking into account the technical interoperability requirements of the different parts of a 5G network:

- It avoids or limits any major dependency on a single supplier (or suppliers with a similar risk profile);
- It avoids dependency on suppliers considered to be high risk within the meaning of SM03.

Tretji odstavek istega člena določa:

*»(3) Pri vrednotenju netehničnih vidikov tveganosti iz prvega odstavka operater ocenjuje in upošteva glede na javno dostopne podatke vsaj:*

- 1. zmožnost dobavitelja oziroma ponudnika storitev podpore tretje ravni, da varuje podatke o prometu in komunikacijske podatke in onemogoča nepooblaščen dostop do njih,*
- 2. zmožnost dobavitelja oziroma ponudnika storitev podpore tretje ravni, da zagotavlja neprekinjenost dobave dodatnih komponent kritičnih elementov omrežja ali vzdrževanje obstoječih oziroma izvajanje storitev podpore tretje ravni,*
- 3. transparentnost pri zagotavljanju kibernetike varnosti. «*

Prvi odstavek 3. člena pa določa:

*»(1) Operaterji v dobavni verigi komponent kritičnih elementov omrežja in storitev podpore tretje ravni za te komponente v celotnem življenjskem ciklu upoštevajo najmanj naslednje usmeritve:*

*1. za vsakega dobavitelja izvajajo oceno tveganja z vidika dobave in potencialnih možnih vplivov s strani tretjih, združljivosti z opremo drugih proizvajalcev, kakovosti in varnosti proizvodov in z vidika potencialnih negativnih vplivov na delovanje storitev operaterja in kritičnih subjektov ;*

*...*

*4. da je varnost ter njihova neprekinjena dobava zagotovljena in je potrjeno, da podpira visoke varnostne lastnosti v skladu z mednarodno priznanimi (3GPP) in evropskimi standardi (ETSI),*

*...*

*6. za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana z dobavo opreme, nadomestnih delov ali storitev podpore tretje ravni,;*

*...*

*8. za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana s pravicami uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme in s tem posledično omejitve ali prekinitve pri dobavi opreme, nadomestnih delov ali za storitve podpore tretje ravni,*

*...«*

Predlog splošnega akta torej izrecno predvideva vrednotenje netehničnih vidikov tveganosti (prvi odstavek 4. člena), obenem pa navaja vrsto netehničnih meril, ki so dejansko diskriminatorna glede na državo izvora, na primer glede »neprekinjenosti dobav« (kar implicira geografsko oddaljenost proizvodnje oz. meri na državo izvora) (2. točka tretjega odstavka 4. člena predloga Splošnega akta), nedefinirana in neopredeljena tveganja glede na primer »dobave« oz. neprekinjenosti dobav (1., 4., 6. in 8. točka prvega odstavka 3. člena predloga Splošnega akta, kar spet implicira geografsko oddaljenost proizvodnje oz. meri na državo izvora), nedefinirana in neopredeljena tveganja glede dostopnosti (do nadomestnih delov, pravic uporabe ključnih tehnologij) (6. in 8. točka prvega odstavka 3. člena predloga Splošnega akta).

Pri tem se sklicujemo na vso dosedanjo argumentacijo:

- (i) navedene določbe so nejasne in pomensko odprte, kar nujno privede do možnosti arbitrarnih razlag in zlorabe, predstavlja pa posledično tudi nasprotje z načelom jasnosti in določnosti predpisov, ki je eno od (pod)načel pravne države iz 2. člena Ustave;
- (ii) kakršnekoli dodatne obveznosti, ki bi bile naložene operaterjem (ki jih ne predvideva že ZEKom-2), bi bile v nasprotju z zakonskim pooblastilom za izdajo splošnega akta po 115. in 116. členu ZEKom-2 in posledično v nasprotju s 120. členom Ustave, kot je bilo že pojasnjeno. Skladno z 87. členom lahko pravice in obveznosti državljanov ter drugih oseb Državni zbor določa le z zakonom. To pomeni, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Načelo zakonitosti delovanja uprave (drugi odstavek 120. člena Ustave v povezavi s 15. členom Ustave) tako zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali;
- (iii) kakršnokoli omejevanje dobave ali dobavnih verig, pa ne vpliva le na operaterje, temveč po sami naravi stvari omejuje tudi dobavitelje in posega v svobodo gospodarske pobude (74. člen Ustave). Pri tem torej ne gre le za neskladnost z ustavnim načelom legalitete (drugi odstavek 120. člena Ustave), temveč tudi neskladnost s 74. členom Ustave RS. Uresničevanje pravice iz prvega odstavka 74. člena Ustave RS bi moralo biti v konkretnem primeru urejeno v zakonu, ne pa v splošnem aktu AKOS kot podzakonskemu predpisu, zato je Splošni akt v nasprotju tudi s 74. členom Ustave. Glede na to, da zakon ne daje ustrezne

podlage za nalaganje kakršnihkoli dodatnih obveznosti vezanih na dobavne verige, takšnih obveznosti ni možno originarno naložiti s splošnim aktom AKOS, v nobenem primeru pa tudi ni in ne more biti podana sorazmernost za takšen ukrep.

Za primerjavo, nemška ureditev se osredotoča na certifikacijo komponent v skladu z Uredbo (EU) 2019/881.

## 6. Opustitev notifikacije po Mehanizmu TRIS

Splošni akt, ki opredeljuje kritične elemente omrežja, bi moral biti notificiran po TRIS postopku, pa ni bil - vse v kontekstu sodne prakse, na primer sodbe Komisija proti Belgiji (C-145/97), da morajo države članice posredovati po TRIS mehanizmu tudi besedilo drugih predpisov, kolikor je poznavanje takega besedila potrebno za oceno posledic osnutka tehničnega predpisa (ZEKom-2 je bil sicer predmet notifikacije, vendar pa bi moral biti notificiran tudi relevantni splošni akt). Slovenija, kot članica WTO, bi morala izvesti tudi notifikacijo po členu 2.9.2 Sporazuma o tehničnih ovirah v trgovini (TBT) – skladno s prakso Sodišča EU je navedeni sporazum del prava EU, kršitev sporazuma TBT pa predstavlja tudi kršitev prava EU. Slovenija bi skladno s členom 2.9.2 morala obvestiti druge članice WTO v dovolj zgodnji fazi. Pri mehanizmu, kakor izhaja iz 116. in 117. člena ZEKom-2, gre za tehnični predpis v smislu prava WTO, ravno tako pri predmetnem Splošnem aktu, ki opredeljuje bistven element tega mehanizma (to je kritične elemente omrežja, na katere naj bi se nanašala prepoved).

SMT Direktiva torej državam članicam EU nalaga obveznost, da Evropsko komisijo vnaprej obvestijo o vseh osnutkih tehničnih predpisov ali pravil o storitvah informacijske družbe. V skladu s prakso sodišča EU je posledica kršitve te obveznosti neuporabljenost in neizvršljivost relevantnega predpisa<sup>49</sup>. Sodišče EU je prav tako pojasnilo, da to, da je država članica kršila obveznost predhodne priglasitve ukrepov, ki omejujejo svobodo zagotavljanja storitev informacijske družbe (enako pa po naravi stvari velja tudi za druge kršitve postopka TRIS), povzroči, da zadevna

<sup>49</sup> Glejte na primer sodbe v zadevah: C-194/94, C-443/98 in C-390/18

ureditev za zasebne subjekte ne učinkuje<sup>50</sup>, obveznost pa z vidika njene vsebine dovolj jasna, natančna in brezpogojna, da se ji prizna neposredni učinek in se nanjo lahko sklicujejo zasebni subjekti pred nacionalnimi sodišči (točka 90)<sup>51</sup>.

Akos in Republika Slovenija torej nista izpolnila obveznosti iz SMT Direktive, kršitev obveznosti pa pomeni postopkovno napako tehničnega predpisa (t.j. predlaganega Splošnega akta), kar bi imelo za posledico neizvršljivost oziroma neuporabljenost le-tega, Akos pa predlagamo, da izpolni postopkovne predpostavke pred sprejemom Splošnega akta. V nasprotnem primeru ima lahko kršitev za posledico tudi postopek pred Sodiščem EU proti Sloveniji, kot tudi spor v okviru mehanizmov WTO, ravno tako pa bi morala navedeno neuporabljenost in neizvršljivost Splošnega akta (če bo sprejet brez ustrezne priglasitve po mehanizmu TRIS in WTO) upoštevati vsa nacionalna sodišča (vključno z upravnim sodiščem).

## 7. Dodatno glede sklepa Vlade RS z dne 22.6.2023

Vlada Republike Slovenije naj bi dne 22.6.2023 po nekaterih poročanjih sprejela sklep o spremembi sklepa Vlade Republike Slovenije o sprejemu ukrepov za zmanjšanje tveganj v omrežjih 5G z dne 29. 9. 2020, in sicer na predlog Urada Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju tudi »URSIV«). Navedeni sklep naj bi bil sprejet na podlagi Zakona o kritični infrastrukturi (ZKI) in naj bi na novo določal kritične elemente omrežja in pripadajoče informacijske sisteme, v katerih naj operaterji mobilnih komunikacijskih omrežij naj ne bi smeli uporabljati opreme in storitev dobaviteljev z visokim tveganjem, ki jih opredeli Vlada Republike Slovenije.

V Uradnem listu Republike Slovenije kakršenkoli takšen sklep Vlade RS ni objavljen, s sprejemom pa je bil kršen

---

<sup>50</sup> Glejte točko 88 odločitve C-390/18: »88 Ugotoviti je torej treba, ali to, da je država članica kršila obveznost predhodne priglasitve ukrepov, ki omejujejo svobodo zagotavljanja storitev informacijske družbe iz druge države članice, določeno v členu 3(4)(b), druga alineja, Direktive 2000/31, povzroči, da zadevna ureditev za zasebne subjekte ne učinkuje, kakor velja za posledice, ki izhajajo iz tega, da je država članica kršila obveznost predhodnega sporočanja tehničnih predpisov, ki je določena v členu 5(1) Direktive 2015/1535 (glej v tem smislu sodbo z dne 30. aprila 1996, CIA Security International, C-194/94, EU:C:1996:172, točka 54).«

<sup>51</sup> Glejte točko 90 iste odločitve: »Obveznost iz te določbe je torej z vidika njene vsebine dovolj jasna, natančna in brezpogojna, da se ji prizna neposredni učinek in se nanjo lahko sklicujejo zasebni subjekti pred nacionalnimi sodišči (glej po analogiji sodbo z dne 30. aprila 1996, CIA Security International, C-194/94, EU:C:1996:172, točka 44).«

poslovnik vlade, pravo EU in pravo WTO<sup>52</sup>. Takšen Sklep (tudi če je bil morebiti sprejet) ne bi smel v ničemer vplivati na odločanje Agencije. Skladno s povsem jasno prakso Ustavnega sodišča Republike Slovenije, navedeni Sklep ni zavezujoč, ker ni bil objavljen v Uradnem listu Republike Slovenije, ni začel veljati ter se ni smel in se ne sme uporabljati<sup>53</sup>. Navedeni sklep (če je bil sprejet) neutemeljeno med kritične elemente omrežja prišteva tudi elemente, ki po naravi stvari ne morejo biti kritični, na primer radijsko dostopovno omrežje (bazne postaje, ki podpirajo tehnologijo 5G ali višje). Navedeni sklep (če je bil sprejet) je nezakonit in neustaven, za sprejem navedenega sklepa, pa ne obstaja ustrezna zakonska podlaga, saj Zakon o kritični infrastrukturi (ZKI) Vladi ne daje pristojnosti, da nalaga operaterjem omejitve glede možnosti nabave opreme na trgu (gre za poskus omejevanja svobodne gospodarske pobude iz 74. člena Ustave, pri čemer je takšno urejanje pridržano zakonu ob upoštevanju ustavnopravnih omejitev, ne more pa biti podzakonska materija), ZKI pa ravno tako Vladi ne daje pristojnosti določanja dobaviteljev z visokim tveganjem. V vsakem primeru bi bilo pred sprejemom kakršnihkoli predpisov s tega področja potrebno zagotoviti sodelovanje javnosti, URSIV kot predlagatelj predpisa bi moral povabiti strokovno in drugo javnost k sodelovanju pri pripravi predpisa s splošnim vabilom, kateremu je priložen osnutek predpisa, na spletnih straneh, rok za odziv javnosti, pa bi moral biti od 30 do 60 dni od objave (glejte 9. člen Poslovnika Vlade Republike Slovenije), pa takšna objava in sodelovanje javnosti pred sprejemom Sklepa nista bila izvedena in je bil Sklep sprejet povsem nepričakovano, brez predhodne napovedi in ne da bi bilo izvedeno posvetovanje z deležniki.

---

<sup>52</sup> Sklep ni objavljen skladno s 154. členom Ustave RS in tudi ni bil sprejet ob upoštevanju postopkovnih pravil, ki veljajo za sprejem splošnih aktov. Ob tem niso bili izpolnjeni formalni pogoji za sprejem splošnega akta, saj ni bil predhodno javno objavljen osnutek predpisa in ni bilo izvedeno javno posvetovanje skladno z 9. členom Poslovnika Vlade Republike Slovenije, zato menimo, da tudi niso izpolnjeni pogoji za objavo le-tega oziroma bi se škodljive posledice z objavo navedenega sklepa zgolj še povečale. Ugotavljamo, da tudi ni bila upoštevana Resolucija o normativni dejavnosti (ReNDej), ravno tako pred sprejemom sklepa ni bila izvedena priključitev skladno z mehanizmom TRIS (Direktiva (EU) 2015/1535), ki bi morala biti izvedena, kot tudi ni bila izvedena notifikacija po členu 2.9.2 Sporazuma o tehničnih ovirah v trgovini (TBT), ki bi jo morala izvesti Slovenija, kot članica WTO. Republika Slovenija tvega nastanek izjemne gospodarske škode in se izpostavlja potencialni odgovornosti za škodo, navedene posledice pa morebiti sploh niso bile zaznane, ker ni bila narejena presoja posledic s strani URSIV predlaganega Sklepa.

<sup>53</sup> Ustavno sodišče RS v takih primerih dosledno zavzema stališče, da je ne glede na izpolnjevanje formalnih pogojev treba šteti za predpis akt, v katerem so vsebovane splošne in abstraktne pravne norme, s katerimi se urejajo pravice in obveznosti pravnih subjektov ali če bi te norme navzven povzročale pravne učinke. Pri presoji teh sklepov Ustavno sodišče v svoji praksi zaključuje, da ker akt ni bil objavljen v Uradnem listu, ni začel veljati, se ni smel in se ne sme uporabljati. Ustavno sodišče se iz tega razloga v ustavnosodni praksi sploh ne spušča v presojo njegove ustavnosti in zakonitosti. Glejte odločbo USRS št. U-I-291/02 z dne 12. 12. 2002, tč. 7).

Ravno tako ni bila izvedena opredelitev in korektna predstavitev posledic (skladno z 8. členom Poslovnika), posledice omejevanja operaterjev glede nabave opreme pa bi bile izjemno hude, tako za operaterje, kot v končni fazi za potrošnike in nasploh slovensko gospodarstvo. Ravno tako ni bila upoštevana Resolucija o normativni dejavnosti (ReNDej), ravno tako pred sprejemom sklepa ni bila izvedena priglasitev skladno z mehanizmom TRIS (Direktiva (EU) 2015/1535). Navedeno področje (prepovedi uporabe tvegane opreme v kritičnih elementih in funkcijah omrežja) je zakonsko podrobno normirano v petem odstavku 116. člena ZEKom-2 in 117. členu ZEKom-2, ne URSIV, ne Vlada pa nimata pristojnosti, da bi v nasprotju z zakonom (in brez ustrezne podlage) na drugačen način vzpostavila nekakšen vzporedni mehanizem določanja dobaviteljev z visokim tveganjem. Glede na to, da navedeni Sklep ni začel veljati ter se ni smel in se ne sme uporabljati, Akos v nobenem primeru ni kakorkoli vezan na sklep.

Agencija bi morala opraviti svojo strokovno nalogo in kot neodvisni organ (na podlagi strokovnih kriterijev, npr. standard ETSI/3GPP, in dokumentov na ravni EU, npr. Usklajena ocena tveganj EU za kibernetiko varnost omrežij 5G, Zbirka orodij EU za kibernetiko varnost omrežij 5G, smernic ENISA itd.) v splošnem aktu določiti kritične elemente omrežja in pripadajočih informacijskih sistemov na način, da se opredelitve omejijo na dejansko kritične elemente, in da se ne vključuje elementov, ki niso kritični (npr. radijsko dostopno omrežje). Agencija bi morala biti samostojna po 230. členu ZEKom-2 in Direktivi (EU) 2018/1972 z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah, ki zahteva politično neodvisnost in objektivnost delovanja Agencije kot nacionalnega regulativnega organa.

#### **8. Dodatno glede postopkovnih kršitev povezanih z javnim posvetovanjem, našega dopisa in odgovora Agencije ter škode, ki bi nastala s sprejemom takšnega splošnega akta**

Agencija je sprva z objavo dne 6. 4. 2023 obvestila javnost, da je na podlagi ZEKom-2 pripravila (prvotni) predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah in je povabila zainteresirano javnost, da do vključno 8. maja 2023 posreduje pripombe, predloge ali dopolnitve k navedenemu predlogu. Huawei je dne 8.5.2023 poslal svoje pripombe in predloge, vključno z analizo ustavne spornosti predloga splošnega akta, AKOS pa je dne 17. 5. 2023 objavil pripombe prejete v postopku javnega posvetovanja, med drugim tudi pripombe družbe Huawei, s pripisom,



da bo Agencija odgovor na prejete pripombe objavila naknadno.

Skladno z 269. členom ZEKom-2 mora agencija pred sprejemom (splošnega) akta predlog objaviti in zbirati mnenja v objavljenem roku, ki ne sme biti krajši od 30 dni, po poteku navedenega roka in pred sprejetjem akta pa mora agencija objaviti pridobljena mnenja in pripombe ter **v objavi navesti način, kako so bila upoštevana, ali razloge, zaradi katerih niso bila upoštevana.** Agencija bi torej v objavi pripomb (z dne 17. 5. 2023) morala objaviti tudi odziv, torej, kako so bile pripombe in predlogi oziroma mnenje Huawei upoštevani, ali razloge, zaradi katerih niso bili upoštevani. Glede na to, da odziv na komentarje Huawei ni bil objavljen, gre za postopkovno kršitev, ki obremenjuje postopek javnega posvetovanja. Ključno bi bilo, da bi se deležniki pred vnovičnim javnim posvetovanjem (in vnovično podajo pripomb in predlogov) seznanili z odzivom Akos na že podane pripombe in z razlogi, zakaj njihovi dosedanji predlogi morebiti niso bili upoštevani. Agencija ne bo mogla stanja sanirati na način, da se kar hkrati opredeli do pripomb vezanih na prvotno verzijo in pripomb vezanih na drugo verzijo. Menimo, da bi se agencija do že podanih pripomb iz prvega kroga javnega posvetovanja morala (v roku iz statuta in ZEKom-2) opredeliti pred ponovitvijo javnega posvetovanja, vsekakor pa pred iztekom roka za novo javno posvetovanje.

19. člen Statuta Agencije<sup>54</sup> določa, da kadar tako določa zakon, agencija zagotovi vpliv javnosti pri sprejemanju splošnih aktov tako, da pred sprejetjem objavi osnutek na svoji spletni strani in povabi zainteresirano javnost, da predloži pisne pripombe, predloge ter mnenja k objavljenemu gradivu v roku, ki ne sme biti krajši od 30 dni, Agencija pa nato v roku, ki ne sme biti daljši od 7 dni od preteka roka za predložitev pripomb, na spletni strani objavi vse prispele pripombe, predloge in mnenja ter v roku, ki ne sme biti daljši od 15 dni od preteka roka za predložitev pripomb, na svoji spletni strani (pred sprejetjem dokumenta) objavi, kako so bile pripombe, predlogi in mnenja upoštevani ter razloge, zaradi katerih niso bili upoštevani, pri čemer se lahko iz utemeljenih razlogov rok podaljša, vendar največ za 15 dni.

Drugi odstavek 19. člena statuta Agencije pri tem določa, da mora Agencija v roku (v katerem povabi zainteresirano

---

<sup>54</sup> Na spletni strani Agencije je objavljena povezava do statuta Agencije za komunikacijska omrežja in storitve Republike Slovenije (Uradni list RS, št. 43/18). Na strani: <https://www.akos-rs.si/zakoni-in-priporocila> je povezava na: [http://www.pisrs.si/Pis\\_web/pregledPredpisa?id=STAT243](http://www.pisrs.si/Pis_web/pregledPredpisa?id=STAT243)

javnost, da predloži pisne pripombe, predloge ter mnenja k objavljenemu gradivu v roku, ki ne sme biti krajši od 30 dni) zainteresirani javnosti zagotoviti vpogled v dokumentacijo, na podlagi katere je bil pripravljen dokument (iz prvega odstavka), razen v delih, ki so zaupne narave, in ji na njeno zahtevo in proti plačilu stroškov omogoči prepis ali kopiranje dokumentacije ali njenih delov, za katere je dovoljen vpogled.

Agenciji smo poslali dopis, v katerem smo:

- prosili za pojasnilo, zakaj Agencija na svoji spletni strani ni objavila, kako so bile pripombe, predlogi in mnenja Huawei upoštevana oziroma razlogov, zaradi katerih niso bili upoštevana in Agencijo pozvali, da čim prej objavi odziv na pripombe in predloge Huawei, skladno z določbo 269. člena ZEKom-2 in 19. člena statuta;
- prosili za vpogled v dokumentacijo, na podlagi katere je bil pripravljen splošni akt (tako prvotna verzija kot nova verzija objavljena 7.8.2023) oziroma da družbi Huawei posreduje sken te dokumentacije (oziroma omogoči prepis ali kopiranje dokumentacije ali njenih delov skladno z 19. členom statuta).

Prejeli smo odgovor Agencije (številka: 0073-3/2023/56 z dne 16. 8. 2023), iz katerega izhaja, da sta se URSIV in agencija na delavnici 8. 5. 2023 nagibala v smeri, da bi seznam kritičnih sredstev spremenila na način, kot je bilo večinsko izraženo v prejetih pripombah, da pa je po izvedeni delavnici 8. 5. 2023 na nacionalnem kot tudi na evropskem nivoju prišlo do pomembnih sprememb, ki imajo neposreden vpliv na odločitve agencije in URSIV pri pripravi splošnega akta. Agencija se pri tem sklicuje na ugotovitve poročila Skupine za sodelovanje glede varnosti omrežij in informacij (NIS Cooperation Group) o napredku držav članic pri izvajanju Sklopa orodij EU za varnost 5G glede implementacije strateških ukrepov, pri čemer se v opombi 1 sklicuje na vir datiran 29. januar 2020. Sklop orodij EU za varnost 5G, na katerega se sklicuje agencija (iz januarja 2020), ravno radijsko dostopovno omrežje opredeljuje kot ne-kritični del omrežja. Agencija se torej v obrazložitve svoje odločitve sklicuje na vir, ki vsebuje diametralno nasprotno stališče, kot ga zavzema Agencija.

Agencija nadalje pojasnjuje, da naj bi pri presoji kritičnosti posameznih elementov omrežja Agencija izhajala tudi iz usklajenih ocen tveganj za omrežja 5G na ravni EU (Ocena tveganj), pri čemer se pod opombo 2 sklicuje na vir iz 9. oktobra 2019. Tudi navedeni vir pa radijsko dostopovno omrežje opredeljuje kot ne-kritični del omrežja. Agencija

se torej ponovno svojo odločitev utemeljuje z virom, ki vsebuje diametralno nasprotno stališče, kot ga zavzema Agencija.

Dodatno Agencija pojasnjuje, da naj bi v juniju 2023 prišlo tudi do novih ugotovitev v zvezi s stanjem kibernetске varnosti 5G omrežij na ravni EU, ki naj bi bile zajete v Drugem poročilu držav članic o napredku implementacije ukrepov iz 5G Toolbox-a. Agencija v opombi 3 kot vir navaja objavo iz 15. junija 2023. Iz navedenega poročila na straneh 7-8 sicer izhaja, da se omejitve v določenih državah članicah nanašajo tudi na določene ne-kritične dele omrežje (npr. radijsko dostopovno omrežje), vendar pa navedeno poročilo v opombi 15 jasno pojasnjuje, da so kritični elementi omrežja zgolj jedrni del omrežja (core network) in upravljanje virtualiziranih omrežnih funkcij in omrežna orkestracija (MANO) (network function virtualisation management and orchestration (MANO)), ne pa radijsko dostopovno omrežje (Radio Access Network (RAN)). Torej navedeni vir ne predstavlja kakršnekoli drugačne razmejitev med kritičnimi in nekritičnimi deli omrežja. V Sloveniji je zakon (ZEKom-2) omejil domet ukrepov iz 116. člena na kritične elemente omrežja, naloga AKOS pa je, da le-te opredeli, nima pa AKOS pristojnosti, da bi ob sklicevanju na Drugo poročilo držav članic o napredku implementacije ukrepov iz 5G Toolbox-a, torej, da ukrepi v določenih državah članicah zajemajo tudi radijsko dostopovno omrežje, ki ni kritičen del omrežja, ukrep iz 116. člena (ki je zamejen na kritične dele omrežja) prek preširoke definicije raztegnil tudi ne-kritične in s tem dejansko presegel zakonsko pooblastilo in odločitev zakonodajalca, da je v Sloveniji ukrep po 116. členu ZEKom-2 zamejen na kritične dele omrežja.

Agencija se sklicuje še na neveljavni in nezakoniti sklep Vlade Republike Slovenije št. 381000-2/2023/2 z dne 22. 6. 2023, ki med kritične elemente omrežja 5G uvršča tudi RAN, ki sploh ni objavljen v Uradnem listu in se tako glede na prakso Ustavnega sodišča ne uporablja in ne sme uporabljati (enako kot da ne bi obstajal). Vlada Republike Slovenije tudi ni nad zakonom (ki je ukrep po 116. členu ZEKom-2 zamejil na kritične elemente omrežja), sklep Vlade pa se nanaša na povsem drug zakon (Zakon o kritični infrastrukturi) in ne sme posegati v avtonomijo AKOS, še posej ne glede področja urejanja, ki se nanaša na drug zakon (Zakon o elektronskih komunikacijah). Sklep Vlade tako ne more biti podlaga za uvrstitev nekritičnih elementov omrežja med kritične.

Predvsem gre lahko za politično odločitev, ravno v izogib temu, da bi bila odločitev glede kritičnih elementov

politična, pa je bila v zakonu odločitev prepuščena Agenciji kot neodvisnemu regulatorju. Agencija bi pri tem morala upoštevati spoznanja stroke, ne pa morebitnih odločitev Vlade kot političnega organa. Če bi bila politična odločitev vladajoče koalicije, da se ukrepe iz 116. člena ZEKom-2 razširi tudi na nekritične dele omrežja kot je radijsko dostopovno omrežje, bi bila pravilna pot zakonodajna sprememba 116. člena ZEKom-2, ki bi jo spremljal tudi ustrezní zakonodajni postopek (ki glede na Resolucijo o normativni dejavnosti (ReNDej) in Poslovnik državnega zbora (PoDZ-1) med drugim vključuje izvedbo ustreznih primerjalno-pravnih analiz (ureditve v drugih pravnih sistemih in prilagojenosti predlagane ureditve pravu Evropske unije; prikaz ureditve v drugih pravnih sistemih), presojo posledic (med drugim na gospodarstvo, razvojno načrtovanje in druga področja), pravno preverbo rešitve preko Zakonodajno-pravne službe Državnega zbora, vključno s preverbo skladnosti z Ustavo Republike Slovenije itd.), javno posvetovanje kot je predvideno za sprejem zakona, obravnavanje na ustreznih delovnih telesih itd., glasovanje v Državnem zboru in morebiti v Državnem svetu, ter morebitni referendum, ne more pa Agencija obiti navedenega postopka na način, da kar sama razširi domet 116. člena ZEKom-2 tako da nekritične elemente omrežja opredeli kot kritične.

Agencija pri tem v svojem odgovoru ne poda prav nobenega vsebinskega razloga, zakaj bi na primer glede na spoznanja stroke bila ustrezna sprememba opredelitve radijskega dostopovnega omrežja. Tako kot kaže takšni vsebinski razlogi ne obstajajo.

Agencija v odgovoru še pojasnjuje, da naj bi Agencija v sodelovanju z URSIV pripravila novo verzijo predloga splošnega akta, ki ga je objavila 7. 8. 2023 in se sklicuje na pojasnila za vnovično objavo akta. Glede pojasnil, ki so spremljala objavo z dne 7.8.2023 ravno tako ugotavljamo, da se objava pavšalno sklicuje, da naj bi se na nacionalnem in na evropskem nivoju zgodilo več pomembnih dogodkov, ki naj bi vplivali na vsebino in zahteve predmetnega splošnega akta, vendar pa ni opredeljeno, kateri naj bi bili ti dogodki. Agencija je v objavi še pojasnila, da naj bi kritičnost elementov omrežja agencija presojala skupaj z URSIV, predvsem iz vidika, da se ti elementi uporabljajo v omrežjih, prek katerih se zagotavljajo storitve za kritične subjekte, to so izvajalci bistvenih storitev, upravljavci kritične infrastrukture, izvajalci nalog zaščite in reševanja, vojska in podobno. Navedeno pojasnilo je nerazumljivo, saj splošni akt ni zamejen na namenska (nejavna) omrežja, temveč se nanaša na javna omrežja v splošni uporabi (potencialno na vsa javna mobilna komunikacijska omrežja v Republiki Sloveniji). Če je pomislek, ki ga skuša

naslavljeni Agencija, varnost namenskih (nejavnih) omrežij za potrebe varnosti, policije, obrambe in zaščite, reševanja in pomoči, bi se navedeno vprašanje dalo v splošnem aktu rešiti drugače, kot da se nasploh posega v radijsko dostopovno omrežje javnih komunikacijskih omrežij, kar bo imelo v končni fazi hude posledice za slovensko gospodarstvo in potrošnike.

V zvezi z zahtevo Huawei za vpogled v dokumentacijo, na podlagi katere sta bili pripravljena prvotna in aktualna verzija splošnega akta, je Agencija še sporočila, da je pri pripravi akta uporabila lastno strokovno znanje, navedene dokumente, pa tudi Poročila ENISE. Pri tem se četrti vir, ki ga Agencija navaja, nanaša na priporočila Enise iz 2019, torej ravno tako ne more iti za neka nova spoznanja, do katerih bi prišli po maju 2023. Ravno tako priporočila Enise ne odstopajo od usklajene ocene tveganj, predvsem pa nikakor ne opredeljujejo radijskega dostopovnega omrežja kot kritični del omrežja. Agencija se torej sklicuje na vir, ki ne daje opore za odločitev Agencije, da RAN vključi med kritične dele omrežja.

Agencija sicer ne omenja političnega govora oz. političnih izjav komisarja Bretona, pa vseeno v zvezi z navedenim opozarjamo, da morebitne politične izjave komisarja, ne morejo biti relevantne. Ne gre za kakršenkoli pravni ali drugačen »vir«, ki bi bil upošteven pri odločanju AKOS. V zvezi z navedenim sicer opozarjamo, da je komisar Breton pred nekaj dnevi (dne 6. september 2023) za CNN<sup>55</sup> Portugalska pojasnil, da imajo različni deli opreme različen profil tveganja, da Nabor orodij ne omenja nobenega konkretnega dobavitelja, omenja pa tveganja, ki naj bi se jim države skušale izogniti in da ni na njem da bi se izrekel, ali se Nabor orodij nanaša na katerokoli konkretno družbo, dodaja pa še konkretno glede Huawei, da glede določenih delov opreme, le-ta nesporno nima prav nobenih težav. Komisar Breton pri tem pojasnjuje, da je na državah članicah, da izpolnijo obveznosti glede Nabora orodij (ob tem, kot pojasnjeno, ravno Nabor orodij jasno določa, da radijsko dostopovno omrežje in upravljavski sistemi in drugi podporni sistemi niso kritični).

Agencija se sicer sklicuje na sodelovanje z URSIV pri pravi splošnega akta, pa vendar samo stališče URSIV (pa niti

---

<sup>55</sup> Glejte članek dostopen na: <https://cnnportugal.iol.pt/5g/huawei/5g-bruxelas-apoia-decisao-de-portugal-e-admite-algum-problema-com-huawei/20230906/64f8ab03d34e65afa2f50e23>

ne vemo, kakšno je, ker ni dokumentirano oz. razkrito zainteresirani javnosti) brez ustrezne utemeljitve, ne more biti podlaga za vključitev radijskega dostopovnega omrežja med kritične elemente omrežja brez kakršnihkoli dejanskih (npr. varnostnih) razlogov oziroma spoznanj.

Agencija je pri tem pojasnila, da sodelovanje z URSIV poteka predvsem v obliki »delovnih sestankov«, na katerih »ne nastajajo zapisniki«, pač pa se razpravlja o vseh relevantnih virih za odločanje v relevantni zadevi in skladno z njimi oblikuje besedilo predloga splošnega akta. Agencija pojasnjuje, da naj bi v okviru tega sodelovanja Agencija tudi upoštevala »strokovne predloge in priporočila«, ki jih je od omenjenega organa prejela. Navedeni odgovor je zaskrbljujoč in kaže na netransparentno sprejemanje odločitev ob kršitvi temeljnih načel upravnega poslovanja glede dokumentiranja sprejemanje odločitev.

Dne 11.9.2023 je družba Huawei skušala prek pooblaščenca v času uradnih ur Agencije (neuspešno) vpogledati v dokumentacijo skladno z drugim odstavkom 19. člena Statuta agencije. Družbi Huawei je bil omogočen zgolj vpogled v »popis zadeve«, pri čemer so bili nekateri podatki v tem popisu zakriti. Iz popisa izhaja, da je v zadevi večje število zaznamkov in drugih listin, vendar njihova vsebina ni razvidna, iz popisa izhajajo zgolj nazivi listin, ki naj bi bile v »spisu«, vendar se iz njih ne da sklepati na vsebino. Družbi Huawei v nasprotju s statutom Agencije ni bil omogočen vpogled v samo dokumentacijo, kar predstavlja bistveno kršitev postopkovnih jamstev javnega posvetovanja glede na statut Agencije.

Agencija je zavezanec na podlagi Uredbe o upravnem poslovanju (Uradni list RS, št. 9/18, 14/20, 167/20, 172/21, 68/22, 89/22, 135/22 in 77/23). Le-ta v 2. členu splošno določa obveznost dokumentiranja in evidentiranja, v 32. členu pa je način dokumentiranja natančneje specificiran. Prvi odstavek navedenega člena določa: *»Delo organov se dokumentira z ustreznim zapisom: dokumentom, zaznamkom ali pisarniško odredbo tako, da je mogoče delo pozneje pregledovati, preverjati njegovo pravilnost, pravočasnost in kakovost izvajanja, dokazovati dejstva in ohraniti zapise za znanost in kulturo ali za pravno varnost pravnih in fizičnih oseb.«*

Agencija bi torej morala posvetovanja oziroma sodelovanje z URSIV ustrezno dokumentirati skladno z 32. členom navedene Uredbe. Toliko bolj, ker že zakon (šesti odstavek 116. člena ZEKom-2) določa, da pri pripravi splošnega akta (iz navedenega odstavka) agencija sodeluje z organom, pristojnim za informacijsko varnost. Takšno posvetovanje oziroma sodelovanje bi moralo biti ustrezno dokumentirano z ustreznim zapisom: (a) dokumentom, (b) zaznamkom ali (c) pisarniško odredbo tako, da je mogoče delo pozneje pregledovati, preverjati njegovo pravilnost,

pravočasnost in kakovost izvajanja, dokazovati dejstva in ohraniti zapise, med drugim za pravno varnost pravnih in fizičnih oseb. Glede na izjemen odstop od prava EU, spoznanj stroke in dosedanjih stališč Republike Slovenije, ter ob upoštevanju izjemne škode, ki grozi s sprejemom takšnega splošnega akta, je transparentnost (ki jo med drugim predvideva tudi Statut agencije) toliko bolj pomembna. Zainteresirana javnost bi se morala imeti možnost seznaniti s tem, kdo, iz kakšnih razlogov (na podlagi katerih spoznanj ter zakaj) je predlagal uvrstitev radijskega dostopovnega omrežja med kritične elemente omrežja.

V kolikor vsebinski (npr. varnostni) argumenti za uvrstitev radijskega dostopovnega omrežja med kritične dele omrežja ne obstajajo in gre za prosto (ne strokovno, temveč politično) odločitev, pa je tudi ključna transparentnost, za čigavo odločitev konkretno gre oz. na čigav predlog je bilo navedeno izvedeno.

V kolikor bi Agencija razkrile vire, torej na kaj opira odločitev za uvrstitev radijskega dostopovnega omrežja, bi bilo na navedeno v pripombah mogoče argumentirano odgovoriti. Zaradi pomanjkanja transparentnosti in kršitev osnovnih načel upravnega poslovanja in statuta Agencije glede vpogleda v dokumentacijo, pa to ni možno.

Glede na navedeno menimo, da bi zaradi navedenih kršitev zakona in statuta Agencije, Agencija morala najprej navedene kršitve odpraviti, vključno z zadostno transparentnostjo posvetovanja med Agencijo in URSIV, torej, da se skladno z Uredbo o upravnem poslovanju to posvetovanje ustrezno dokumentira in skladno s Statutom razkrije zainteresirani javnosti, nato pa bi bilo potrebno javno posvetovanje ponoviti ob upoštevanju relevantnih določb ZEKom-2 in Statuta Agencije.

V kolikor Agencija (in konkretne uradne osebe oziroma javni uslužbenci, ki so udeleženi v procesu javnega posvetovanja, priprave in sprejemanja navedenega Splošnega akta) kljub v dosednji korespondenci in v konkretnih pripombah vsebovanih konkretnih opozoril glede kršitve predpisov, teh kršitev ne bo odpravila (oziroma ne bodo odpravili), izrecno opozarjamo, da menimo, da bo zaradi tega nastala huda kršitev pravic, škoda na javnih dobrinah in premoženjska škoda izjemnih razsežnosti.

S sprejemom takšnega splošnega akta AKOS in Republika Slovenija tvegata tudi nastanek izjemne gospodarske škode, Republika Slovenija pa je izpostavljena potencialni odgovornosti za škodo, ob tem pa sploh ni bila narejena presoja posledic s strani Agencije predlaganega splošnega akta.

Omejitve možnosti nekaterih dobaviteljev, da bi delovali na trgu, bi prikrajšale Slovenijo za prednosti konkurence. Sprejetje ukrepov, ki bi omejili ali preprečili dobaviteljem opreme s sedežem na Kitajskem, da bi delovali na trgu opreme 5G, bi škodovalo slovenskemu pa tudi evropskemu gospodarstvu, kot prikazano v

študiji Oxford Economics<sup>56</sup>. V skladu z ugotovitvami študije Oxford Economics glede posledic za gospodarstvo, bi takšni omejevalni ukrepi verjetno pripeljali do več milijard evrov višjih naložbenih stroškov, zakasnili hitrost vzpostavitve omrežij 5G in na dolgi rok povzročili počasnejšo tehnološko rast in inovacije, nižje dohodke za gospodinjstva in nižjo gospodarsko rast. Sklicujemo se tudi na študijo (Ekonomski učinki omejevanja konkurence pri ponudbi 5G tehnologije na slovensko gospodarstvo, ki jo je pripravil Center poslovne odličnosti Ekonomske fakultete Univerze v Ljubljani – CPOEF, 2020), iz katere izhaja, da bi bile posledice v primeru izključitve Huawei s slovenskega trga 5G opreme: (i) zamuda pri uvajanju 5G tehnologije, ki bi znižala slovenski BDP med 217,6 in 468,1 milijona EUR, kumulativne izgube BDP v 10 letih pa bi znašale med 1,7 milijarde EUR in 3,7 milijarde EUR.

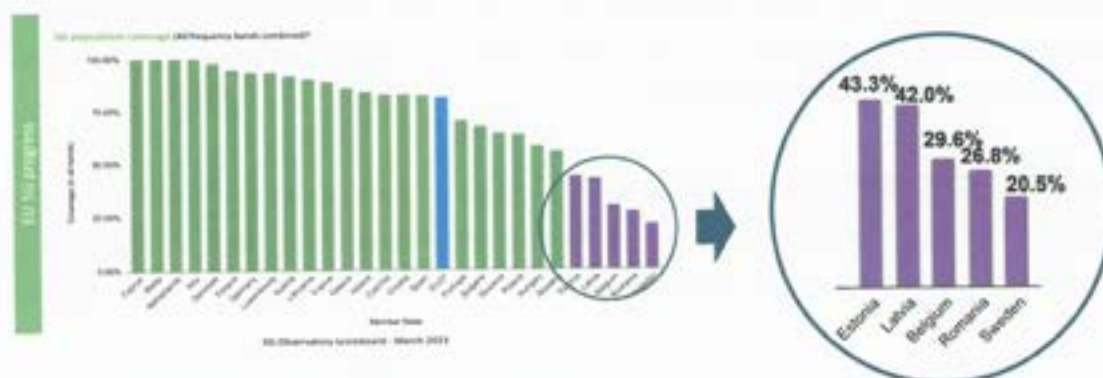
Poročilo »5G Observatory« s podporo Evropske komisije, pri tem jasno kaže, da je ravno pet držav, ki so prepovedale Huawei (Švedska, Romunija, Belgija, Estonija in Latvija) na dnu lestvice EU27 glede uvajanja tehnologije 5G in pokritosti prebivalstva<sup>57</sup>.

Podoben učinek kot izključitev s trga pa ima lahko že sam sprejem spornega Splošnega akta (tudi če odločba po 117. členu ZEKom-2 sploh ni nikoli sprejeta), saj lahko sama nevarnost prepovedi nabave opreme tudi glede nekritičnih elementov omrežja (RAN) – in to celo brez kakršnihkoli konkretnih varnostnih pomislekov - v praktično vseh javnih komunikacijskih omrežjih, vpliva na obnašanje operaterjev glede nabave opreme določenih dobaviteljev in s tem povzroči opisano škodo in opisane negativne posledice.

<sup>56</sup> <https://www.oxfordeconomics.com/resource/the-economic-impact-of-huawei-in-europe/> ter

<https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/>

<sup>57</sup> Glejte spodnji graf dostopen na: <https://5gobservatory.eu/>, iz poročila za april 2023 (s podporo Evropske komisije), da so Švedska, Romunija, Belgija, Estonija in Latvija na samem repu (znotraj EU) glede pokritosti prebivalstva s 5G:



Source: 5G Observatory Report 18 – April 2023, supported by the European Commission  
<https://5gobservatory.eu/report-18-april-2023/>



## 9. Predlog sprememb

Predlagamo, da se v prilogi Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (Seznam, kritičnih elementov omrežja in pripadajočih informacijskih sistemov), črtata vrstici, ki po vsebini ne predstavlja kritičnega elementa omrežja:

Radijsko dostopovno omrežje	- Bazne postaje, ki podpirajo tehnologijo 5G ali višje
-----------------------------	--

pa tudi:

Upravljavski sistemi in drugi podporni sistemi	- Nadzor delovanja in upravljanja mobilnega komunikacijskega omrežja, vključno z dostopnim delom (RAN/O-RAN), - Sistemi zaznavanja varnostnih dogodkov, anomalij, groženj in njihovo upravljanje (varnostne funkcije vključno s SIEM/SOAR).
--	--

Predlagamo črtanje določb splošnega akta, ki presegajo zakonsko pooblastilo za sprejem splošnega akta iz 116. člena ZEKom-2, med drugim 9. točka prvega odstavka 3. člena predloga Splošnega akta, 6. člen Splošnega akta (ki nalaga obveznosti v nasprotju z zakonskim pooblastilom), 7. člen predloga Splošnega akta (ki nalaga obveznosti v nasprotju z zakonskim pooblastilom).

Enako predlagamo črtanje določb, ki se nanašajo na netehnične kriterije, črtanje besedila »kot netehnične« v prvem odstavku 4. člena predloga Splošnega akta, črtanje tretjega odstavka 4. člena predloga Splošnega akta in črtanje 1., 6. in 8. točke prvega odstavka 3. člena predloga Splošnega akta in črtanje v 4. točki istega odstavka besedila »ter njihova neprekinjena dobava«.

Glede na vse navedeno Vas vljudno prosimo, da pripombe in predloge preučite v okviru svojih pristojnosti in jih v največji meri upoštevate.

S spoštovanjem,

Huawei Technologies Ljubljana d.o.o.



**Priloge:**

- Pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije z dne 13. 9. 2023, Inštituta za primerjalno pravo pri Pravni fakulteti v Ljubljani, Poljanski nasip 2, Ljubljana;
- Nacionalna ocena tveganj Republike Slovenije (National 5G Cybersecurity Risk Assessment of the Republic of Slovenia);
- Dopis Agencije številka: 0073-3/2023/56 z dne 16. 8. 2023;
- Popis zadeve, klasifikacijska številka: 0073-3/2023;
- Ekonomski učinki omejevanja konkurence pri ponudbi 5G tehnologije na slovensko gospodarstvo, ki jo je pripravil Center poslovne odličnosti Ekonomske fakultete Univerze v Ljubljani – CPOEF, 2020.

---

Huawei Technologies Ljubljana, družba za informacijsko in komunikacijsko tehnologijo, d.o.o., je družba s sedežem v Ljubljani in poslovnim naslovom: Ameriška ulica 8, 1000 Ljubljana, matična številka: 6950752000, osnovni kapital: 250.000,00 EUR, vpisana pri Okrožnem sodišču v Ljubljani, elektronski naslov: [huaweislovenia@huawei.com](mailto:huaweislovenia@huawei.com).