**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 tudi po elektronski pošti na: info.box@akos-rs.si**

Ljubljana, 09. maj 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**«) je z objavo dne 6. 4. 2023 obvestila javnost, da je na podlagi Zakona o elektronskih komunikacijah (ZEKom-2) pripravila 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 8. maja 2023 posreduje pripombe, predloge ali dopolnitve k predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah.

Temu dopisu prilagamo »Pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije z dne 24. 4. 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.

V tem dokumentu opozarjamo med drugim na naslednje:

i. Definicija kritičnih sredstev je preširoka in pomensko odprta, nejasna ter zajema elemente in funkcije omrežja, ki niso kritični (npr. radijsko dostopovno omrežje, transport in prenosne funkcije 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 sredstev oziroma 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 tako z vidika zahteve po jasnosti in določnosti predpisov kot tudi ustavnega načela sorazmernosti. Že kombinacija splošne klavzule ter seznama oz. njuno dvoumno medsebojno razmerje je dejavnik nepredvidljivosti pri razlagi pravne norme. Raba pogojnikov in nedoločnih pravnih pojmov odpira obsežne možnosti za arbitrarno razlago pri aplikaciji teh norm na konkretne primere. Kot izhaja iz Mnenja gre tako za prenizko stopnjo jasnosti in določnosti predpisa in ni zadoščeno ustavnim zahtevam iz 2. člena Ustave RS, poleg tega pa 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. Nedopustno je tudi sklicevanje v splošnem aktu na objekte kritične infrastrukture, saj je seznam le-teh, kot izhaja iz pojasnil Ministrstva za obrambo, tajen, vezanje pravnih posledic v splošnem aktu na objekte, katerih seznam je tajen (da naslovniki pravne norme iz nje z uporabo uveljavljenih metod pravne razlage ne morejo zanesljivo ugotoviti, kaj so

tiste točke v prostoru, na katere ne sme segati sevalno območje bazne postaje), pa je v nasprotju z osnovnimi zahtevami pravne države, ki izhajajo iz 2. člena Ustave, kot podrobneje pojasnjeno pod točko 2;

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 začrtal 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 in sredstva, 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 podajamo konkretne predloge sprememb besedila predlaganega Splošnega akta.

## 1. Glede kritičnih in nekritičnih sredstev, elementov in funkcij omrežja

Sicer pozdravljamo prizadevanja za večjo varnost komunikacijskih omrežij. Ob pregledu objavljenega predloga Splošnega akta pa na žalost ugotavljamo, da vsebuje (a) v 2. točki prvega odstavka 2. člena pomensko odprto in široko definicijo kritičnih sredstev ter (b) v prilogi (seznamu kritičnih sredstev) še kategorije, ki po vsebini nikakor ne sodijo med »kritična sredstva«, kot na primer celo radijsko dostopovno omrežje (oz. bazne postaje, ki podpirajo tehnologijo 5G ali višje), ki ne eno ne drugo ni v skladu s pravom EU, ki naj bi se implementiralo, ob tem pa načelo lojalne razlage[1], 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« sredstev (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**«)[2]. 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

---

[1] 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 ). Pojem »kritičnosti« uporabljen v ZEKom-2 je tako potrebno razlagati v skladu z Naborom orodij in Usklajeno oceno tveganj.

[2] 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

ZEKom-2, pa je predlagatelj zakona rešitve iz VIII. Poglavja zakona utemeljeval v potrebi po implementaciji Nabora orodij. Nabor orodij priporoča pristop, ki temelji na zagotavljanju kibernetske 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[3]. Posledično se Nabor orodij direktno ne nanaša na nobenega 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 kibernetsko varnost omrežij 5G, ki so bila ugotovljena z Usklajeno oceno tveganj za kibernetsko 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[4]) 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 sredstvi oziroma 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 sredstvi oziroma elementi, kamor se prišteva med drugim RAN (angleško *Radio Access Network*) oziroma bazne postaje, pa tudi transport in prenosne funkcije ter upravljavske 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 kritična *(angl. Critical)* sredstva oziroma elemente, kamor se prišteva jedrne funkcije

---

[3] 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 opreme, kolikor 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.").*

[4] 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

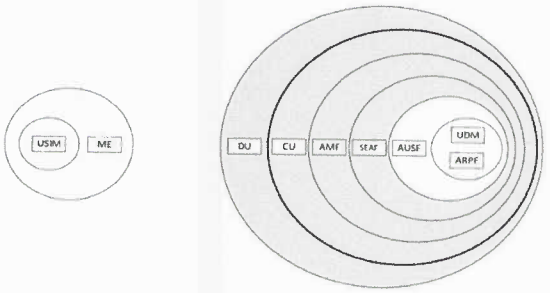
omrežja (angl. *Core network functions*), in preostalimi ne-kritičnimi sredstvi oziroma elementi, kamor se prišteva dostopovno omrežje (angleško Access network) oziroma bazne postaje, transport in prenosne funkcije ter večina upravljavskih sistemov in drugih podpornih sistemov (glejte stran 10 navedene Nacionalne ocene tveganj; od upravljavskih 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 katera sredstva oziroma 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[5] (glejte stran 8/33), po katerih sta enako kot kritična opredeljena zgolj jedrni del omrežja in upravljanje NFV in orkestracija MANO, 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[6], 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

---

[5] Smernice ENISA so dostopne na: https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

[6] 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.

(RAN) v Prilogo, kot tudi vključitev drugih nekritičnih komponent, na primer tudi vključitev točke »upravljavski sistemi in drugi podporni sistemi« in »transport in prenosne funkcije«.

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 kritičnosti baznih postaj. Z varnostnega vidika bi kakršenkoli napad na posamezno bazno postajo zahteval bodisi predhodni (oddaljeni) napad na jedrni del omrežja, bodisi fizično prisotnost, vsakem primeru bi bil kakršenkoli učinek kakršnegakoli incidenta zelo omejen (še posebej za kakršnekoli rizike vezane na tretje države).[7] Tako z vidika tveganosti radijskemu dostopovnemu omrežju RAN ni možno pripisati kritičnosti.

ii. Enako velja za »upravljavske sisteme in druge podporne sisteme«, ki jih Priloga predloga Splošnega akta ravno tako neutemeljeno karakterizira kot kritične dele omrežja. Upravljavski sistemi in drugi podporni sistemi bi lahko bili relevantni samo v obsegu, kolikor gre morebiti za upravljanje jedrnega dela omrežja in sisteme zaznavanja varnostnih dogodkov, anomalij, grožnj in njihovo upravljanje. Sicer pa je potrebno 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. Nameščanje in administracija virtualiziranih omrežij in podomrežij (NFV) bi prišla v poštev le za jedrni del omrežja (core), za preostalo omrežje pa ni relevantne uporabe.

iii. Tudi »transport in prenosne funkcije« priloga predloga Splošnega akta neutemeljeno karakterizira kot kritične dele omrežja. Funkcije transporta in prenosa so v skladu s tehničnimi ocenami Evropske komisije glede tveganosti ocenjene kot še manj tvegane kot RAN. Transport in prenosne funkcije se nanašajo samo na posredovanje podatkovnega prometa in v ničemer ne nadzorujejo ali vplivajo na promet v večjem obsegu.

[7] Napad na jedrni cel 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). Zajezitev incidentov vezanih na bazne postaje bi bila relativno enostavna.

Glede transporta in prenosnih funkcij je potrebno opozoriti, da ga ravno tako Usklajena ocena tveganj za kibernetsko varnost omrežij 5G kot tudi Nabor orodij ne opredeljujeta kot kritičnega dela omrežja. Funkcije transporta in prenosne funkcije bi bilo potrebno z vidika ocenjevanja profila tveganosti opredeliti celo kot še manj tvegane od RANa.

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 nekritična sredstva, 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 prestati testa sorazmernosti.

Preširoka in pomensko odprta definicija, kakor je predlagana v Splošnem aktu v povezavi s prilogo, ki izrecno opredeljuje kot kritična sredstva, sredstva, ki niso kritična 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 (gotovo vsaj v primeru izdaje odločbe po 117. členu ZEKom-2) pripeljala do posledic v nasprotju s pravom EU in mednarodnim pravom, kar bo 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[8]).

[8] Nemški sistem (seznam kritičnih funkcij z dne 13.8.2021 pripravljen na podlagi relevantnih nemških zakonov TKG in BSIG s strani zvezne agencije za komunikacijska omrežja - BNetzA) se sklicuje, da sta (absolutno) kritični zgolj kategoriji (a) (jedrne omrežje 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

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

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

*»2. Kritična sredstva so sredstva, ki vključujejo elemente, funkcije ter storitve omrežja ter podporni informacijski sistemi v fizični, programski ali kakršni koli virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, ki operaterju takšne storitve zagotavlja, katerih potencialna odpoved ali zloraba bi lahko imela zelo velik negativni vpliv na razpoložljivost, avtentičnost, celovitost ali zaupnost v njih shranjenih, prenesenih ali obdelanih podatkov ali podatkov, ki so prek njih dostopni ter s tem ogrozila varnost in nemoteno delovanje storitev kritičnih subjektov ali na varnost in nemoteno delovanje zasebnih omrežij kritičnih subjektov ali bi kako drugače pomembno ogrozila vitalne gospodarske ali družbene aktivnosti države oziroma njeno nacionalno varnost.«*

Predlog Splošnega akta vsebuje seznam sredstev, ki vključuje med drugim naslednje kategorije:

- Upravljanje z naročniki in šifrirni mehanizmi;
- Vmesniki za medomrežno povezovanje;
- Upravljane omrežne storitve;
- Upravljanje virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), vključno z virtualizacijsko infrastrukturo;
- Radijsko dostopovno omrežje (Bazne postaje, ki podpirajo tehnologijo 5G ali višje, katerih sevalno območje sega na območje objektov kritične infrastrukture);

---

avstrijskega zakona je dostopno na https://www.parlament.gv.at/PAKT/VHG/XXVII/I/I_01043/index.shtml# 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

- Upravljavski sistemi in drugi podporni sistemi;
- Transport in prenosne funkcije;
- Zakonito prestrezanje.

Informacija, kaj naj bi bili objekti kritične infrastrukture, ni javna. Ministrstvo za obrambo sicer pojasnjuje (družba Huawei je prejela v vednost odgovor Ministrstva za obrambo vezano na zahtevo po Zakonu o dostopu do informacij javnega značaja - ZDIJZ), da obstaja Sklep Vlade RS o določitvi kritične infrastrukture Republike Slovenije št. 80200-1/2019/6 z dne 7.2.2019, vendar pa je dokument označen s stopnjo tajnosti, kar predstavlja izjemo od vpogleda javnosti vanj skladno z ZDIJZ. Zato se splošna javnost, ravno tako pa na primer družba Huawei kot dobavitelj opreme, ki se uporablja v omrežjih, ne more seznaniti s tem, kaj naj bi bili objekti kritične infrastrukture, kar je, v kolikor bi bil Splošni akt sprejet v predlagani vsebini, v nasprotju z 2. členom Ustave, kot je podrobneje pojasnjeno v nadaljevanju.

Iz Mnenja izhajajo med drugim naslednji zaključki:

1. Mnenje opozarja, da mora v primeru izdaje odločbe po prvem odstavku 117. člena ZEKom-2, operater sam sprejeti odločitev v katerih elementih operater te opreme oz. storitev ne sme uporabljati, z razlago definicije kritičnih elementov v SAVOPS, morebitna napačna razlaga definicije kritičnih elementov, zaradi katere bi operater uporabil opremo dobavitelja tudi v kritičnem elementu, za katerega bi po *bona fide* razlagi definicije kritičnih elementov štel, da ni kritičen, bo lahko vodila do (vsaj) dveh izrazito negativnih posledic za operaterja, in sicer poleg plačila globe (25. točka prvega odstavka 299. člena ZEKom-2) tudi razveljavitev odločbe o dodelitvi radijskih frekvenc, saj kot pojasnjuje Mnenje, razpisni pogoji nedavnih razpisov za dodelitev radijskih frekvenc namreč predvidevajo, 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. Kot opozarja Mnenje, sta obe možni negativni posledici zelo težki, razveljavitev odločbe o dodelitvi frekvenc še mnogo hujša in invazivnejša in lahko pomeni uničujoč udarec za gospodarsko aktivnost operaterja, kakršnakoli naknadna zamenjava opreme pa je povezana z znatnimi stroški. Mnenje opozarja, da so težke posledice relevantne z vidika teže posega v svobodno gospodarsko pobudo, po drugi strani pa tudi glede zahteve po jasnosti in določnosti predpisov. Mnenje opozarja na tveganje, da bi se operaterji lahko zaradi (nejasnosti) predloga Splošnega akta razumno in ekonomično raje odločili, da sploh ne uporabljajo opreme, za katero je

bila izdana odločba vlade po prvem odstavku 117. člena ZEKom-2 - torej ne le, da se tej opremi izognejo v kritičnih elementih, temveč v celotnem omrežju, saj definicija kritičnih elementov v bistvenem sodefinira obseg posega (prepovedi uporabe opreme iz petega odstavka 116. člena ZEKom-2), obenem pa je problematična tako z vidika zahteve po jasnosti in določnosti predpisov kot tudi z vidika načela sorazmernosti, sodišča pa je *de facto* ne bodo imela priložnosti interpretirati.

2. 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.[9] 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 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 izhaja iz Mnenja, je obravnavana definicija v kontekstu drugih, določb ZEKom-2 sporna tako z vidika zahteve po jasnosti in določnosti predpisov kot tudi z vidika zahteve po sorazmernosti.

---

[9] 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. 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". 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.Z vidika dobavitelja opreme, ki bi bil določen za dobavitelja z visokim tveganjem, gre takorekoč za izključitev iz sodelovanja na trgu in tako brez dvoma za poseg.

3. Kot izhaja iz Mnenja, je definicija kritičnih sredstev oziroma elementov sestavljena iz splošne, abstraktno zastavljene definicije v 2. členu SADVZO in seznama. Razmerje med tema dvema normama ni povsem jasno, saj bi splošna definicija teoretično morala služiti presoji konkretnega vprašanja, ali je neko sredstvo/element kritično ali ne. Seznam iz priloge bi lahko po eni strani šteli za taksativen (zaprt) seznam, kar bi pomenilo, da ni mogoče opredeliti dodatnih sredstev kot kritičnih sredstev; v tem primeru bi bilo vprašljivo, kakšen je sploh pravni učinek splošne definicije iz 2. člena. Po drugi strani bi bilo glede na obstoj splošne klavzule morda bolj logično zaključiti, da gre za enumerativen (odprt) seznam. A te možnosti predlog SADVZO na noben način ne nakazuje z uporabo morebitnega odkazila na enumerativno naštevanje (kot z izrazi "na primer", "drugo", "primeroma našteti"...). Tako je že pristop SADVZO k definiranju kritičnih elementov konfuzen in predstavlja dejavnik nejasnosti in nedoločnosti predpisa.

4. Problem pomanjkljive jasnosti in določnosti norm pa se, kot izhaja iz Mnenja, pojavlja ne le v kombinaciji obeh prvin definicije (splošne definicije na eni strani in seznama na drugi strani), temveč tudi v vsaki prvini posebej. V zvezi s splošno definicijo iz 2. točke prvega odstavka 2. člena predloga SADVZO Mnenje ugotavlja, da je pomensko zelo ohlapna, na kar kaže uporaba nedoločnih pravnih pojmov ("zelo velik negativni vpliv", "*vitalne* gospodarske ali družbene aktivnosti države") in uporaba glagola v pogojniku v kombinaciji s prislovom "lahko", ki po Slovarju slovenskega knjižnega jezika "izraža možnost uresničitve dejanja ali stanja": "ki bi lahko imela…". Uporaba pogojnega naklona logično pomeni, da norma zajame veliko večje število situacij, tudi takšnih, kjer je veliko manjša verjetnost, da pride do nezaželene posledice. Zaradi naštetih lastnosti definicije gre za normo, ki krši ustavno zahtevo po določnosti in jasnosti predpisov. V zvezi s seznamom iz priloge, posebej in kot primer pa v zvezi s kategorijo "radijsko dostopovno omrežje", ki kot kritično sredstvo opredeljuje "bazne postaje, ki podpirajo tehnologijo 5G ali višje, katerih sevalno območje sega *na območje objektov kritične infrastrukture*", pa Mnenje ugotavlja, da pregled pravnih predpisov pokaže, da pojem objekta kritične infrastrukture ni definiran. Zakon o kritični infrastrukturi sicer definira *sektorje* kritične infrastrukture,[10] a iz te definicije ni moč v konkretnem primeru presoditi, ali je nek objekt del kritične infrastrukture ali ne. Enako velja za omembo objektov kritične infrastrukture v prvem odstavku 128. člena Zakona o katastru nepremičnin.[11] Zakon o obrambi določa po eni strani pravila v zvezi z upoštevanjem obrambnih potreb pri infrastrukturnih objektih (28. člen) in po drugi strani definira obrambne objekte (29. člen), kar so nedvomno pravne norme z ožjim poljem uporabe.[12] Iz tega sledi, da je definicija baznih postaj, ki se štejejo za kritična sredstva, takšna, da naslovnikom pravne norme iz nje z uporabo uveljavljenih metod pravne razlage ni moč zanesljivo ugotoviti, kaj sploh so tiste točke v prostoru, na katere

[10] 13. točka 3. člena Zakona o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M)

[11] Uradni list RS, št. 54/21.

[12] Zakon o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo, 95/15 in 139/20).

ne sme segati sevalno območje bazne postaje, da ne šteje za kritično sredstvo. To povsem onemogoča naslovnikom pravne norme, da bi lahko svoja ravnanja prilagodili predpisom in se izognili negativnim posledicam potencialne kršitve pravne norme. Sicer bi bilo možno razumeti odločitev državne oblasti, da v interesu javne varnosti in obrambe države ter izven konteksta urejanja kibernetske varnosti po ZEKom-2 natančen seznam objektov kritične infrastrukture skrije pred očmi javnosti. Vendar pa sprejetje takšne odločitve v drugem kontekstu zakonodajnega urejanja in vodenja državnih politik nato pomeni, da morajo spoznavno nedostopnost takšnih informacij, kot je seznam objektov kritične infrastrukture, naslovnikom pravnih norm, upoštevati normodajalci na drugih področjih. Da bi bilo za naslovnike pravnih norm sploh možno, da svoje ravnanje začrtajo v skladu s predpisi, se morajo normodajalci, kot je v tem primeru Agencija, odkazovanju na nejavne informacije povsem izogniti.

5. Kot izhaja iz Mnenja, pa poleg problema neskladnosti z zahtevo po jasnosti in določnosti predpisov je predlagana ureditev neskladna tudi 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.

6. Kot izhaja iz Mnenja, je po dostopnih informacijah v postopku zbiranja informacij in analize stanja za potrebe ocene tveganja kibernetske 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 kibernetskih 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 upravljavskimi sistemi (Management systems and supporting services) ter transportom in prenosnimi funkcijami (Transport and transmission functions). Obe kategoriji sta v poročilu skupine za sodelovanje NIS označeni 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 kibernetske 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 (upravljavski 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 zaključi, da je definicija kritičnih elementov, predvidena v predlogu SADVZO in sestavljena iz splošne klavzule ter seznama kritičnih elementov v prilogi k splošnemu aktu, ustavnopravno izjemno sporna z vidika prvič, zahteve po jasnosti in določnosti predpisov in drugič, ustavnega načela sorazmernosti. Že kombinacija splošne klavzule ter seznama oz. njuno dvoumno medsebojno razmerje je dejavnik nepredvidljivosti pri razlagi pravne norme. Raba pogojnikov in nedoločnih pravnih pojmov odpira obsežne možnosti za arbitrarno razlago pri aplikaciji teh norm na konkretne primere. Po Mnenju gre tako za prenizko stopnjo jasnosti in določnosti predpisa, da bi zadostil ustavnim zahtevam iz 2. člena Ustave RS. Poleg tega pa primerjava predlaganih dikcij 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[13];

ii. Nemčija: nemški BSI (organ za kibernetsko varnost) in BNetzA (regulator telekomunikacij), ne

[13] 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

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 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[14].

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

Pri tem opozarjamo še na terminološko razhajanje saj peti odstavek 116. člena ZEKom-2 daje AKOS pooblastilo za sprejem splošnega akta, ki naj bi opredelil »kritične elemente« omrežja in pripadajočih informacijskih sistemov, predlog Splošnega akta pa govori o »kritičnih sredstvih.«

## 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, med drugim kršil:

[14] 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

- 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).

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 omejevanje sploh ni jasno zamejeno in se razteza tudi na elemente in sredstva, 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.[15] V

[15] 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).

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.[16] 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 blaga v primerjavi z domačim blagom/storitvami.[17][18][19]

Predlagani splošni akt spada na področje uporabe prava WTO, saj vpliva na uporabo omrežne opreme.[20] 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.[21] Izjema nacionalne varnosti v skladu s členom XXI(b) Splošnega sporazuma o carinah in trgovini (GATT) lahko

---

[16] A je podobna obveznost določena tudi v členu I(3)(a) Splošnega sporazuma o trgovini s storitvami ("**GATS**").

[17] Ti vključujejo Splošni sporazum o carinah in trgovini ("**GATT**"), GATS in Sporazum WTO o tehničnih ovirah v trgovini ("**Sporazum TBT**").

[18] Člen I:1 GATT, člen II:1 GATS in člen 2.1 Sporazuma TBT.

[19] Člen III:4 GATT in člen XVII:1 GATS.

[20] 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.

[21] Člen XXI GATT.

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.[22] Po oceni odbora se taka situacija (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[23] 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

[22] *Rusija - Ukrepi v zvezi s prometom v tranzitu*, DS512, 26. aprila 2019, točka 7.71.

[23] *Rusija - Ukrepi v zvezi s prometom v tranzitu*, DS512, 26. aprila 2019, točka 7.76.

splošnega akta prepoved nanašala tudi na nekritična sredstva, na primer dostopovni del omrežja (RAN), upravljavske in/ali druge podporne sisteme ter transportne in/ali prenosne funkcije.

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 kibernetske varnosti, nikakor v nobenem primeru ne more prestati 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 dostopovnega 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[24].

[24] Kot izhaja iz sodbe v združenih zadevah od C-184/13 do C-l 87/13, 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.

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

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

> *»(1) Operaterji v dobavni verigi kritičnih sredstev in storitev podpore tretje ravni v celotnem življenjskem ciklu zagotavljajo in upoštevajo najmanj naslednje usmeritve:*
>
> ...
>
> *7. izogibanje enemu samemu dobavitelju, da se prepreči odvisnost ter zagotovi odpornost v primeru kritičnih ranljivosti sredstev, katastrofalne okvare omrežja oziroma grožnje za varnost omrežij in storitev kritičnih subjektov s strani tretjih fizičnih ali pravnih oseb javnega ali zasebnega prava. «*

Peti odstavek 6. člena predloga Splošnega akta določa:

> *(5) Operater preprečuje svojo odvisnost od posameznega dobavitelja oziroma ponudnika storitev tretje ravni (t.i. »vendor lock–in«) tudi z izogibanjem dolgoročnim pogodbam (pet let ali več) s posameznim dobaviteljem oziroma ponudnikom storitev tretje ravni oziroma ima možnost njune menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnih subjektov na najmanjšo možno raven.*

7. člen Splošnega akta gre tako daleč, da določa celo vsebino pogodbenega razmerja med operaterjem in dobaviteljem kritičnih sredstev oz. ponudniki storitev, in sicer določa, kaj mora operater vključiti v pogodbena 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)."[25] 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 Group)[26] *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures.*[27] 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."[28] 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 kibernetske varnosti in s sodelovanjem vseh držav članic in pristojnih institucij ter teles EU.[29] 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.[30] Mnenje opozarja, da je na podlagi obstoječih virov mogoče

---

[25] Služba Vlade RS za zakonodajo, Nomotehnične smernice, 3., spremenjena in dopolnjena izd., 2018, tč. 102, str. 69.

[26] 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 kibernetske 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.

[27] 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.

[28] *Cybersecurity of 5G Networks - EU Toolbox of risk mitigating measures*, str. 4.

[29] Po določbi tretjega odstavka 14. člena direktive NIS 2 Skupino sestavljajo "predstavniki držav članic, Komisije in Agencije Evropske unije za kibernetsko varnost (ENISA)."

[30] 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...*)."

priti do prepričljive in ustrezno ozke razlage dikcije "drugih usmeritev".

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 nedovršnem glagolskem vidu.[31] Verjetno je Agencijo pri izbiri te besede vodila želja, pravne učinke predlagane norme prikazati kot manj invazivne, kot v resnici 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 naslovnik 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.[32] 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.[33] Kot opozarja Mnenje, je prepoved sklepanja pogodb težak in invaziven ukrep, ki operaterjem

---

[31] Dovršna različica "izogniti", denimo, je za odtenek pomensko jasnejša.

[32] 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.

[33] Prim. Rose-Ackerman, The Regulatory State, v: Rosenfeld in Sajo (ur.), Oxford Handbook of Comparative

bistveno omejujejo svobodno izbiro poslovnih partnerjev. Slednje upravičenje spada po stališču komentatorice Ustave Republike Slovenije v samo jedro polja ustavnega varstva svobodne gospodarske pobude.[34] Mnenje dodaja, da je svobodna izbira poslovnih partnerjev s ciljem zasledovanja poslovnega uspeha, ustvarjanja dobička in konkurenčnosti na prostem trgu tudi izraz avtonomije pogodbene volje.[35] Podobno trdi za določitev trajanja veljavnosti pogodbe, ki jo lahko štejemo za bistveno sestavino tovrstnih pogodbenih razmerij, ter za zahtevo po vključitvi določenih pogodbenih klavzul, za katere se morda operater po logiki poslovne presoje ne bi sam odločil.[36] Brez dvoma lahko *de facto* prepoved sklepanja pogodb s svobodno izbranimi pogodbenimi strankami ter za obdobja, ki presegajo v petem odstavku 6. člena SADVZO določeno najdaljše obdobje 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 z načelom sorazmernosti.

3. Mnenje pod točko 6. 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

Constitutional Law, OUP 2013, str. 676.

[34] 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.

[35] Prim. odločbo US RS U-I-202/93, tč. 4.

[36] 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..."

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 kritičnih subjektov 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).[37] 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.[38] 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

[37] Tako Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 635.

[38] Ibid.

Državnega zbora, pač pa tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon.[39] 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.[40] 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.[41] 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 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.[42] 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

[39] Odločba Ustavnega sodišča RS št. U-I-40/96 z dne 3. 4. 1997, tč. 13.

[40] Tako Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 636.

[41] Primerjajte: odločba Ustavnega sodišča RS U-I-246/14 z dne 24. 3. 2017, tč. 19.

[42] Primerjajte: Pirnat, v: Avbelj (ur.): Komentar Ustave Republike Slovenije (I. knjiga), 2019, str. 637.

prepuščeno splošnemu aktu AKOS, da ta samostojno ureja pravice in obveznosti.[43] 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.[44] 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 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,

---

[43] Glejte odločbo Ustavnega sodišča RS U-I-73/94 z dne 25. 5. 1995, tč. 19.

[44] 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.

ki bo zagotovil učinkovito varstvo javne koristi ter hkrati kar najmanj posegel v ustavno pravico.[45] 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[46] iz Nabora orodij, kar naj bi se naslavljalo z ukrepom SM05[47], 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

[45] 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.

[46] Rizik imenovan v angleščini »R4-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis«

[47] 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.

Prvi odstavek 4. člena predloga Splošnega akta določa:

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

Tretji odstavek istega člena določa:

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

*1. dobaviteljevo poslovno prakso oziroma poslovno prakso ponudnika storitev podpore tretje ravni,*

*2. zmožnost dobavitelja oziroma ponudnika storitev tretje ravni, da zagotavlja neprekinjenost dobave dogovorjenih kritičnih sredstev oziroma storitev podpore tretje ravni, tudi glede na nacionalne in evropske usmeritve in potencialne omejitve,*

*3. dobaviteljevega ugleda oziroma ugleda ponudnika storitev tretje ravni glede zagotavljanja kibernetske varnosti ter transparentnosti.«*

Prvi odstavek 3. člena pa določa:

*»(1) Operaterji v dobavni verigi kritičnih sredstev in storitev podpore tretje ravni v celotnem življenjskem ciklu zagotavljajo in upoštevajo najmanj naslednje usmeritve:*

*1. za vsakega dobavitelja kritičnega sredstva ali ponudnika storitev tretje ravni izvajajo oceno tveganja z vidika lastništva, dobave, združljivostjo z opremo drugih proizvajalcev, kakovosti in varnosti proizvodov in z vidika potencialnih negativnih vplivov na delovanje storitev operaterja in kritičnih subjektov;*

*...*

*6. za vsakega potencialnega dobavitelja kritičnega sredstva iz seznama v prilogi se ocenjuje in upošteva tudi tveganja glede njegove dostopnosti do potrebnih surovin, polprevodnikov, pravic 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« glede na nacionalne in evropske usmeritve in potencialne omejitve (kar implicira geografsko oddaljenost proizvodnje oz. meri na državo izvora) (2. točka tretjega odstavka 4. člena predloga Splošnega akta), nedefiniran in neopredeljen pojem »ugleda« (3. točka tretjega odstavka 4. člena predloga Splošnega akta), nedefinirana in neopredeljena tveganja glede na primer »lastništva« in »dobave« (1. točke prvega odstavka 3. člena predloga Splošnega akta), nedefinirana in neopredeljena tveganja glede dostopnosti (do surovin, polprevodnikov, pravic uporabe ključnih tehnologij) (6. 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).

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 potencialno neizvršljivost oziroma neuporabljivost 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.

## 7. Predlog

Predlagamo spremembo definicije iz 2. točke prvega odstavka 2. člena Splošnega akta, tako da se glasi:

> »2. Kritična sredstva, elementi in funkcije omrežja in pripadajočih informacijskih sistemov so tista kritična sredstva, elementi in funkcije omrežja in pripadajočih informacijskih sistemov, ki jih je v Usklajeni oceni tveganj za kibernetsko varnost omrežij 5G, 9. oktober 2019 (»EU Coordinated risk assessment of the cybersecurity of 5G networks«) opredelila Skupina za sodelovanje glede varnosti omrežij in informacij, in sicer (a) jedrne omrežje funkcije (CORE) ter (b) upravljanje virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), kot so opredeljene v navedenem dokumentu.«

in da se v celoti briše priloga, ali pa (podrejeno), da se (poleg spremembe splošne definicije) v prilogi brišejo vsaj naslednje vrstice, ki po vsebini ne predstavljajo kritičnih sredstev:

| | |
|---|---|
| Radijsko dostopovno omrežje | - Bazne postaje, ki podpirajo tehnologijo 5G ali višje, katerih sevalno območje sega na območje objektov kritične infrastrukture. |
| Upravljavski sistemi in drugi podporni sistemi | - Nadzor delovanja in upravljanja omrežja, vključno z dostopovnim delom (RAN/O-RAN),<br>- Nameščanje in administracija virtualiziranih omrežij in podomrežij, |
| Transport in prenosne funkcije | - Transportne funkcije, ki omogočajo prenos in usmerjanje občutljivega govora in podatkov (usmerjanje, SMSC, IMS). |

Predlagamo črtanje določb splošnega akta, ki presegajo zakonsko pooblastilo za sprejem splošnega akta iz 116. člena ZEKom-2, med drugim 7. 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. in 6. točke prvega odstavka 3. člena predloga Splošnega akta.

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 24. 4. 2023, Inštituta za primerjalno pravo pri Pravni fakulteti Univerze v Ljubljani, Poljanski nasip 2, Ljubljana;

- Nacionalna ocena tveganj Republike Slovenije (National 5G Cybersecurity Risk Assessment of the Republic of Slovenia);

- Odgovor Ministrstva za obrambo vezano na poizvedbe po ZDIJZ (odločba 090-24/2023-2 z dne 25.4.2023), iz katerega izhaja, da je seznam kritične infrastrukture označen s stopnjo tajnosti.

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.