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, 31. marec 2023

Številka: **0073-3/2023**

Zadeva: **Pripombe in predlogi k predlogu novega »Splošnega akta o varnosti omrežij, storitev in podatkov«, 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 17. 2. 2023 obvestila javnost, da je na podlagi sedmega odstavka 115. člena Zakona o elektronskih komunikacijah (ZEKom-2) pripravila predlog Splošnega akta o varnosti omrežij, storitev in podatkov (v nadaljevanju tudi »**Splošni akt**« ali »**SAVOPS**«). Agencija je povabila zainteresirano javnost, da do vključno 31. marca 2023 posreduje pripombe, predloge ali dopolnitve k predlogu novega Splošnega akta o varnosti omrežij, storitev in podatkov.

Temu dopisu prilagamo »Pravno mnenje o skladnosti definicije kritičnih elementov v predlogu Splošnega akta o varnosti omrežij, storitev in podatkov, ki ga je pripravila Agencija za komunikacijska omrežja in storitve, v povezavi z upoštevnimi določbami Zakona o elektronskih komunikacijah (ZEKom-2), z Ustavo Republike Slovenije (URS)« iz marca 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.

1. Uvodno

Seznanjeni smo s stališčem AKOS, da naj bi nameraval AKOS objaviti še predlog tretjega splošnega akta s področja varnosti omrežij, in sicer splošni akt, ki ga predvideva 116. člen ZEKom-2, vendar pa na žalost posvetovanje v zvezi z objavljenim predlogom Splošnega akta po 115. členu ne poteka sočasno s posvetovanjem o predlogu akta po 116. členu, temveč naj bi se posvetovanje v zvezi z zadnjim aktom s področja varnosti omrežij začelo šele po izteku javnega posvetovanja za predmetni Splošni akt. Tako ne moremo poznati morebitnega součinkovanja različnih aktov s področja varnosti omrežij. Smiselno se zdi, da bi posvetovanje v zvezi z vsemi akti s področja varnosti omrežij potekalo sočasno, da bi zainteresirana javnost imela čim boljše razumevanje predlagane podzakonske ureditve v fazi javnega posvetovanja. Glede na navedeno predlagamo, da se objavi tudi preostali akt s področja varnosti omrežij in izvede skupno posvetovanje.

Sicer pozdravljamo prizadevanja za večjo varnost komunikacijskih omrežij. Ob pregledu objavljenega predloga Splošnega akta pa na žalost ugotavljamo, da vsebuje pomensko odprto in široko definicijo kritičnih sredstev, ki ni v skladu s pravom EU, ki naj bi se implementiralo, ob tem pa načelo lojalne razlage[1], ki temelji na načelu lojalnosti iz

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

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 115. 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. 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

---

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

[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."*). Tako bi bilo tudi sklic na Usklajeno oceno tveganj potrebno postaviti v kontekst priporočil Evropske komisije, kot izhajajo iz Nabora orodij.

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 relevantni Splošni akt v 3. točki prvega odstavka 9. člena. Usklajena ocena tveganj pri tem (glejte stran 16 in 17 le-te) jasno razmejuje med kritičnimi sredstvi oziroma elementi (angleško *critical*), kamor se prišteva jedrne funkcije omrežja (angleško *core network functions*), in preostalimi ne-kritičnimi sredstvi oziroma elementi, kamor se prišteva RAN (angleško *Radio Access Network*) oziroma bazne postaje. 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 omrežja (angl. *core network functions*), in preostalimi ne-kritičnimi sredstvi oziroma elementi, kamor se prišteva dostopovno omrežje (angleško Access network) oziroma bazne postaje (glejte stran 10 navedene Nacionalne ocene tveganj). 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«. Poskus širjenja pomena navedene besede 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, tako odstopa od prava EU in navedene 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[4]). Obenem se v nadaljevanju pripomb osredotočamo tudi na pomensko odprto in nejasno določbo 6. točke prvega odstavka 4. člena Splošnega akta in na prvi odstavek 9. člena, saj bi bilo potrebno sklic na Usklajeno oceno tveganj postaviti v kontekst relevantnih priporočil. V zaključku mnenja podajamo tudi konkreten predlog sprememb Splošnega akta.

2. Glede definicije kritičnih sredstev in ugotovitev pridobljenega Mnenja

Iz priloženega Mnenja med drugim izhajajo naslednje ugotovitve:

1. Kljub temu, da je zakonodajalec pooblastilo za to, da opredeli "kritične elemente omrežja in pripadajočih informacijskih sistemov" iz petega odstavka 116. člena, Agenciji podelil v šestem odstavku 116. člena, pa vsebuje pripravljeni predlog SAVOPS v 5. točki prvega odstavka 2. člena definicijo "kritičnih sredstev" in sicer so to:

   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 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 bi lahko ogrozilo tudi nacionalno varnost* (poudarek dodan).

[4] 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.

2. 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.

3. Obravnavana definicija kritičnih sredstev in elementov je pomensko zelo ohlapna, na kar kaže uporaba večjega števila nedoločnih pravnih pojmov ("zelo velik negativni vpliv", "*vitalne* gospodarske ali družbene aktivnosti države") in uporaba več glagolov v pogojniku ("ki bi lahko imela…", "ki bi kako drugače ogrozila", "bi lahko ogrozilo…"). 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, pri kateri se, kot opozarja Mnenje, postavlja utemeljeno vprašanje, ali ne krši ustavne zahteve po določnosti in jasnosti predpisov. Po standardu varstva načela jasnosti in določnosti predpisov, kot se je uveljavil v ustavnosodni presoji Ustavnega sodišča, to načelo ne terja, da bi morali biti predpisi »taki, da jih ne bi bilo treba razlagati«. Uporaba predpisov vedno pomeni njihovo razlago. Z vidika pravne varnosti je predpis sporen takrat, "kadar s pomočjo pravil o razlagi pravnih norm ni mogoče jasno ugotoviti njegove vsebine."[5]

4. Mnenje opozarja, da bo poseg v svobodno gospodarsko pobudo v konkretni situaciji le delno izvršen preko oblastnega akta. Res je, da bo za to, da bo do posega prišlo, Vlada morala izdati odločbo po prvem odstavku 117. člena ZEKom-2. Vendar pa bo s tem določena le oprema oziroma storitve, ne pa tudi, v katerih elementih operater te opreme oz. storitev ne sme uporabljati. Odločitev, v katerih elementih operater opremo/storitev sme in kje jih ne sme uporabljati, bo operater sprejel sam, z razlago definicije kritičnih elementov v SAVOPS. ZEKom-2 ne predvideva možnosti, da bi operater pravilnost svoje razlage preveril pri državnem organu. 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

[5] Odločba USRS U-I-246/14-20 z dne 24. 3. 2017, tč. 20.

elementov štel, da ni kritičen, bo lahko vodila do (vsaj) dveh izrazito negativnih posledic za operaterja.

5. Prva negativna posledica je, kot izhaja iz Mnenja, kaznovalno-pravna sankcija, predvidena že po določbah ZEKom-2, in sicer lahko prekrškovni organ operaterja, ki ne upošteva dodatnih varnostnih zahtev in omejitev iz 116. člena, kaznuje s plačilom globe (25. točka prvega odstavka 299. člena ZEKom-2). Mnenje opozarja še na drugo možno negativno posledico za razlago definicije kritičnih elementov s strani operaterja, ki ne ustreza razumevanju pojma kritičnih elementov s strani Agencije, ki celo ni predvidena v zakonu, ampak jo je možno razbrati iz razpisnih pogojev nedavno objavljenega javnega razpisa za dodelitev radijskih frekvenc za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom. [6] V razpisni dokumentaciji je namreč predvideno, 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.[7] Oboje negativne posledice so zelo težke, pri čemer je razveljavitev odločbe o dodelitvi frekvenc hujša in invazivnejša. Pomeni lahko namreč uničujoč udarec za gospodarsko aktivnost operaterja. Alternativna pot odprave domnevnih kršitev, ki je denimo predvidena v citirani razpisni dokumentaciji in s katero bi se lahko operater izognil razveljavitvi odločbe o dodelitvi frekvence, pa bi terjala zamenjavo opreme, kar pa prinaša znatne stroške, ki bi gotovo presegli znesek globe, predvidene v prekrškovnih določbah ZEKom-2. V zvezi s tem Mnenje opozarja, da se bo lahko v takšni situaciji operater povsem razumno in ekonomično raje odločil, da *sploh* ne uporablja opreme, za katero bi bila izdana odločba vlade po prvem odstavku 117. člena ZEKom-2 - torej ne le, da se tej opremi izogne v kritičnih elementih, temveč v celotnem omrežju.

---

[6] Sklep o uvedbi javnega razpisa z javno dražbo za dodelitev radijskih frekvenc za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom je Agencija objavila v UL RS 191/2020; prečiščeno besedilo razpisne dokumentacije, ki jo navajamo v našem besedilu, je dostopno na https://www.akos-rs.si/fileadmin/user_upload/Razpisna_dokumentacija_za_vecfrekvencno_drazbo_05022021_koncna.pdf.

[7] Točka A.5.6 razpisne dokumentacije, str. 32.

6. Kot izhaja iz Mnenja, tovrsten, povsem možen razvoj dogodkov pokaže, da je državna oblast[8] s kombinacijo prepovedi uporabe opreme oziroma storitev po petem odstavku 116. člena ZEKom-2 in nedoločne definicije kritičnih elementov povsem zaobšla zahtevo po sorazmernosti v povezavi z zahtevo po jasnosti in določnosti predpisov kot element načela pravne države po 2. členu URS. S pomensko odprto definicijo, ki pa je ne bodo imela priložnosti interpretirati sodišča, bo Agencija dosegla, da bo *de facto* učinek odločbe iz prvega odstavka 117. člena ZEKom-2 segel preko dometa, ki ga je predvidel zakonodajalec v prepovedi iz petega odstavka 116. člena ZEKom-2. Državna oblast operaterjem s tem, ko jih postavi pred pomensko izredno široko definicijo, povsem zoži prostor za svobodno sprejemanje poslovnih odločitev. Postali bodo pravzaprav izvrševalci izjemno intenzivnega posega v svobodno gospodarsko pobudo dobaviteljev.

7. Ta poseg je tako intenziven, da bi, če bi bil transparentno predviden v zakonodaji, obenem pa bi bila pooblastila za izvrševanje dana oblastnim organom, ne prestal presoje skladnosti z ustavo - načelom sorazmernosti in načelom jasnosti in določnosti predpisov. Stališče Mnenja je, da je to prav tako nedopustno oz. neskladno z zahtevami URS, če so norme oblikovane tako, da lahko logično pričakujemo, da bodo do istih posledic pripeljale tako rekoč edine možne odločitve zasebnih subjektov - akterjev na trgu.

8. Iz Mnenja izhaja, da je možno bolj jasno in določno formulirati predpis (ne glede na pomislek, da tehnološki razvoj, terja hitro spremembo oz. prilagoditev razumevanja tega, kaj je kritični element). Vendar pa v tem konkretnem primeru ni mogoče govoriti o pomanjkanju informacij, ki bi narekovalo pomensko odprto formuliranje definicije oz. v kontekstu ustavnopravne analize služilo kot argument proti zahtevi po jasni in določni formulaciji. Po dostopnih informacijah je 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.[9] V okviru priprave usklajene ocene tveganja je bila opravljena tudi analiza vprašanja, katere ključne

[8] Mnenje pojasnjuje, da gre za kombinacijo zakonodajnega urejanja v ZEKom-2, za katerim stoji zakonodajna veja oblasti, in podzakonskega urejanja s strani Agencije v SAVOSP.

[9] Skupina za sodelovanje NIS (NIS Cooperation Group), ki jo je predvidela Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL EU L 194/1, 2016

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*).[10] 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 (denimo, spet, bazne postaje niso bile uvrščene med elemente s kritično stopnjo občutljivosti).

9. Veliko bolj natančna kategorizacija v postopku analize tveganja nasprotno kaže na to, da je zelo verjetno, da je tudi zavezujoče pravne norme mogoče oblikovati tako, da bodo iz njih naslovniki (pa tudi posredno prizadeti subjekti) lažje predvideli pravne posledice in zanesljiveje ocenili svoj pravni položaj. Obenem bi seveda jezikovna jasnost in določnost omogočila pravno urejanje, ki ne bi zaobšlo ustavne zahteve po sorazmernosti, saj se je, kot kažeta evropsko in nacionalno poročilo, preširokemu oblikovanju kategorije kritičnih elementov povsem mogoče izogniti.

10. Ob tem pa gre poudariti, da je obravnavana definicija kritičnih elementov predmet urejanja v splošnem aktu Agencije, torej na podzakonski ravni. V pravni stroki je splošno sprejeto, da je za urejanje na podzakonski ravni značilna možnost hitrejšega odzivanja na spremenjene razmere v družbi zaradi manj zapletenih postopkov sprejemanja predpisov. Za ustavnoskladno razmerje med urejanjem na zakonski ravni na eni strani in na podzakonski ravni na drugi strani bi bilo, kot izhaja iz Mnenja, najbolj smiselno, da bi zakon ob podelitvi pooblastila za podzakonsko urejanje (v 116. oziroma 117. členu ZEKom-2) opredelil tudi izhodišče za podzakonsko urejanje, tako da bi bilo mogoče enostavno ugotoviti namen, iz katerega je bilo dano

---

- 11. člen), je oktobra 2019 objavila poročilo o usklajeni oceni tveganj kibernetske varnosti omrežij 5G (v nadaljevanju: Poročilo NIS, v izvirniku: *EU coordinated risk assessment of the cybersecurity of 5G networks*, dostopno preko https://digital-strategy.ec.europa.eu/sl/node/1448).

[10] Poročilo NIS, tč. 2.21, str. 16.

pooblastilo. Na ravni podzakonskega urejanja pa bi Agencija ob zavedanju, da je mogoče splošni akt relativno hitro spremeniti, morala kritične elemente definirati bistveno bolj določno, z upoštevanjem ugotovitev iz analize tveganj.[11]

11. Po stališču Mnenja predstavlja prepoved uporabe opreme in storitev po petem odstavku 116. člena ZEKom-2 poseg v ustavno zagotovljeno pravico do svobodne gospodarske pobude. Obseg in težo tega posega pa sodoloča obravnavana definicija kritičnih elementov iz SAVOPS, zato je treba učinek obeh norm na prizadete pravne subjekte ustavnopravno analizirati v medsebojni povezavi.

12. Za to, da bi poseg v pravico po 74. členu URS šteli za dopusten, bi moral biti skladen z načelom sorazmernosti; obenem pa se pri predpisih, ki posegajo v človekove pravice, postavlja dodatna, relativno stroga zahteva po jasnosti in določnosti predpisov.

13. Ker je procesna konstelacija, v kateri se bo uporabljala kombinacija prepovedi iz petega odstavka 116. člena ZEKom-2 in definicije kritičnih elementov po SAVOPS takšna, da bodo prave posledice prizadete subjekte zadele možnosti ustrezne razlage predpisov s strani sodne veje oblasti, lahko zaključimo, da pomensko zelo ohlapna definicija kritičnih elementov krši ustavno zahtevo po jasnosti in določnosti predpisov. Ker tako ohlapna definicija po naravi stvari vodi v prekomerne in neuravnotežene negativne posledice za dobavitelje, ne more prestati presoje skladnosti z ustavnim načelom sorazmernosti.

14. Iz mnenja tako izhaja zaključni predlog, da bi glede obravnavanih pravnih norm preuredili razmerje med zakonodajnim urejanjem in podzakonskim urejanjem, zlasti tudi tako, da bi v okviru podzakonskega urejanja zagotovili mnogo **bolj jasno in določno formuliranje pravnih norm, s tem pa bistveno višjo predvidljivost za vse prizadete subjekte**.

---

[11] Mnenje opozarja, da bi v grobem lahko ta pristop primerjali z ureditvijo v ZR Nemčiji, kjer je Zvezna agencija za omrežja izdala Seznam kritičnih funkcij (*Liste der kritischen Funktionen*, dostopna preko www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Sicherheitsanforderungen-node.html) na podlagi določbe zveznega Zakona o telekomunikacijah, ki vsebuje pooblastilo za podzakonsko urejanje, obenem pa napotuje na določbo Zakona o zveznem uradu za varnost v informacijski tehnologiji ("BSI-Gesetz"), ki opredeljuje "kritične komponente" (trinajsti odstavek 2. člena). Seznam kritičnih funkcij sam navaja, da je ocena in kategorizacija posledica raziskav, med drugim tudi tistih, zajetih v Poročilu NIS (Liste der kritischen Funktionen, odsek 3, str. 3).

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 (glejte na primer člene 7, 8 in 11) ter načelo sorazmernosti (glejte tudi člen 52 (1) Pogodbe o delovanju Evropske unije). Splošni akt bi, če bi bil sprejet v takšni vsebini, v povezavi z izdajo kakršnekoli odločbe po 117. členu ZEKom-2, 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).

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, če omejevanje sploh ne bi bilo jasno zamejeno in bi se raztezalo tudi na elemente in sredstva, ki ne štejejo za kritične po Usklajeni oceni tveganj 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. Končno, vsakršen poskus izključitve ali omejevanja možnosti dobaviteljev opreme glede na sedež pri prodaji 5G v EU bo v vsakem primeru z gospodarskega vidika kontraproduktiven, vse še toliko bolj, če bi se prepoved nanašala tudi na nekritična sredstva, na primer dostopovni del omrežja (RAN).

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.

4. Glede dobavnih verig in 4. člena Splošnega akta in sklica na Usklajeno oceno tveganj v 9. členu

Skladno s 6. točko prvega odstavka 4. člena Splošnega akta:

> *»(1) Operater pri načrtovanju, izvajanju, spremljanju in izboljševanju informacijske varnostne politike ter pripadajočih ukrepov zajame zlasti: ... 6. zagotavljanje zanesljivosti dobavnih verig, vključno z vidiki povezanimi z varnostjo oziroma dodatnimi varnostnimi zahtevami na podlagi splošnega akta, ki ureja dodatne varnostne zahteve in omejitve,«*

Ni jasno, na kaj naj bi se nanašalo besedilo: »oziroma dodatnimi varnostnimi zahtevami na podlagi splošnega akta, ki ureja dodatne varnostne zahteve in omejitve«. Menimo, da bi bile kakršnekoli dodatne obveznosti, ki bi bile naložene operaterjem (ki jih ne predvideva že ZEKom-2) 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 bo pojasnjeno v nadaljevanju. Navedena določba je tudi nejasna in pomensko odprta, med drugim ni jasno, na kateri splošni akt se člen sploh sklicuje, kar je v nasprotju z 2. členom Ustave, kot bo tudi pojasnjeno v nadaljevanju. Navedena določba bi predstavljala 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. Neskladje s 74. členom Ustave je ravno tako podrobneje obrazloženo v nadaljevanju.

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).[12] Temeljna vsebina drugega odstavka 120. člena Ustave je zahteva po vsebinski

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

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.[13] 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.[14] 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.[15] 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.

Že iz predlaganega besedila "*z varnostjo oziroma dodatnimi varnostnimi zahtevami na podlagi splošnega akta, ki ureja dodatne varnostne zahteve in omejitve*" sploh ni mogoče z gotovostjo ugotoviti, na kateri "*splošni akt, ki ureja dodatne varnostne zahteve in omejitve*" se besedilo sploh sklicuje in kakšne naj bi bile dodatne varnostne zahteve in omejitve, ki naj bi jih v zvezi z dobavnimi verigami morali upoštevati operaterji. Predlagano besedilo je torej 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

[13] Ibid.

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

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

namen norme.[16] 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.[17] 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.[18] 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.

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.[19] 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,

---

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

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

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

[19] 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.

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, ki bo zagotovil učinkovito varstvo javne koristi ter hkrati kar najmanj posegel v ustavno pravico.[20] 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.

Obenem 9. člen Splošnega akta vsebuje sklic na določene dele Usklajene ocene tveganj (ranljivosti, potencialne grožnje in zlonamerne akterje), ne da bi bila Usklajena ocena tveganj umeščena v kontekst, ki ga podajajo priporočila Evropske komisije (Nabor orodij EU). Tako menimo, da bi bilo potrebno navedeni sklic na Usklajeno oceno tveganj postaviti v relevanten kontekst, da se ne bi posredno nedovoljeno (v nasprotju z opisanim pravom EU in temeljnimi ustavnimi načeli) poseglo v trg dobave opreme in storitev. Nabor orodij zahteva, da morajo biti ukrepi primerni in sorazmerni dejansko ugotovljenim tveganjem in da se ne sme ogroziti odprtost trga za opremo in storitve, ki ustrezajo varnostnim standardom.

---

[20] 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.

5. Predlog in zaključno

Predlagamo spremembo definicije iz 5. točke prvega odstavka 2. člena Splošnega akta, tako da se glasi:

»5. 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.«

Predlagamo spremembo 6. točke prvega odstavka 4. člena Splošnega akta, tako da se črta besedilo »oziroma dodatnimi varnostnimi zahtevami na podlagi splošnega akta, ki ureja dodatne varnostne zahteve in omejitve« in da se nova šesta točka glasi:

»6. zagotavljanje zanesljivosti dobavnih verig, vključno z vidiki povezanimi z varnostjo,«

Predlagamo tudi spremembo prvega odstavka 9. člena Splošnega akta, kot izhaja spodaj:

»(1) Ne glede določbe prvega odstavka 4. člena tega splošnega akta, operater, ki upravlja z elementi in funkcijami omrežja 5G, ob upoštevanju primernosti in sorazmernosti glede na dejansko ugotovljena tveganja, upošteva naslednje:

...

3. pri pripravi ukrepov upošteva, kolikor to terjajo varnostni razlogi na podlagi objektivne ocene ugotovljenih tveganj, tudi ranljivosti in potencialne grožnje, kot so navedeni v dokumentu NIS Cooperation Group Usklajena ocena tveganja za kibernetsko varnost omrežij 5G (angl. »EU Coordinated risk assessment of the cybersecurity of 5G networks , report 9«, oktober 2019)«

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 definicije kritičnih elementov v predlogu Splošnega akta o varnosti omrežij, storitev in podatkov, ki ga je pripravila Agencija za komunikacijska omrežja in storitve, v povezavi z upoštevnimi določbami Zakona o elektronskih komunikacijah (ZEKom-2), z Ustavo Republike Slovenije (URS), 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).