REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Zadeva: 007-59/2016/3
Datum: 18. 8. 2016

**Republika Slovenija**
**Ministrstvo za izobraževanje, znanost in šport**
**Direktorat za informacijsko družbo**
**gp.mizs@gov.si**

**Zadeva: mnenje IP k osnutku predloga Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-1C, EVA 2014-3330-0034) – v javni obravnavi**
**Zveza: vaš dopis št. 007-174/2014/105 z dne 18. 7. 2016**

Spoštovani,

Informacijski pooblaščenec (v nadaljevanju IP) je po elektronski pošti prejel vaš dopis, v katerem nam v mnenje pošiljate osnutek novele ZEKom-1 (kot zgoraj), ki je trenutno v postopku javne obravnave na portalu E-demokracija[1].

V skladu s svojimi pristojnostmi po 1. odst. 48. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1) ter 2. člena Zakona o informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP) vam pošiljamo naše mnenje k omenjenemu osnutku.

Upoštevaje, da gre za precej obsežen predlog (76. členov, skupaj 80 strani + 9 strani uvodne obrazložitve), se pri tem omejujemo zlasti na člene, ki zadevajo obdelavo osebnih podatkov. Pri tem pa se vam že uvodoma zahvaljujemo, da ste se pri postopku priprave besedila odločili za uporabo instituta javne obravnave.

Mnenje podajamo po posameznih členih novele, oz. veljavnega zakona.

***K 34. členu novele (nov 132.a člen, spremljanje in nadzor porabe)***

Novo predlagani člen bo operaterje tudi pravno obvezal, da svojim naročnikom »*zagotovi[jo] možnosti za spremljanje in nadzor porabe govornih in podatkovnih storitev*«, še »*zlasti možnost, da končni uporabnik brezplačno določi količinsko oz. finančno mejo porabe, operater pa ga pred oziroma ob njenem dosegu o tem brezplačno obvesti*«. Kot navajate v obrazložitvi, bodo s tem postale obvezne do sedaj prostovoljne aktivnosti operaterjev (tj. »najboljše prakse«) iz AKOS-ovega *Priporočila o preprečevanju izredno visokih zneskov na računih končnih uporabnikov* iz l. 2013[2], še zlasti (VIII. člen), da vzpostavijo ustrezni informacijski sistem za sprotno spremljanje trenutne porabe končnih uporabnikov ter odstopanja te porabe od običajne porabe, da omogočijo nastavljanje zgornje meje porabe, da zagotovijo opozorila (npr. z SMS-om) ali blokado storitev v primeru znatne prekoračitve običajne porabe, da vnaprej blokirajo storitve (npr. klice) z višjo stopnjo tveganja, in še nekatere druge.

1 Glej https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=5111

2 Glej spletno stran AKOS, http://www.akos-rs.si/priporocilo-o-preprecevanju-izredno-visokih-zneskov-na-racunih-koncnih-uporabnikov

Natančno vsebino po novem obveznih aktivnosti nameravate podrobneje opredeliti v splošnem aktu AKOS.

IP ugotavlja, da zlasti domači mobilni operaterji že omogočajo možnost nadzora in omejevanja porabe govornih in podatkovnih storitev, tako doma kot v tujini[3]. Upoštevaje torej, da gre za običajno prakso, IP določitev obveznosti zagotavljanja takšnih storitev podpira, vendar obenem opozarja, da njihovo dosledno izvajanje **zahteva sprotno in zelo podrobno obdelavo podatkov o prometu.** Posledično predlaga dve dopolnitvi.

Prvič, in kot minimalno, IP predlaga, da se obvezno zagotavljanje možnosti spremljanja in nadzora porabe **določi le za tiste storitve, ki se plačujejo po dejanski porabi** (t.i. *metered* oz. *usage-based* storitve), ne pa tudi za storitve s fiksno obveznostjo (t.i. *flat-rate* storitve, zlasti storitve zagotavljanja dostopa do interneta). Pri slednjih takšne obdelave podatkov o prometu ni mogoče upravičiti.

Kot drugo pa predlagamo, da naj se zagotovi (bodisi s spremembo člena bodisi z aktivnostjo regulatorja), da se bo storitev še naprej izvajala kot opcijska storitev z dodano vrednostjo**, ki jo bo še vedno mogoče izklopiti.** Storitev je po mnenju IP sicer lahko vklopljena po privzetem, ker je to lahko koristno zato, da se prepreči nenapovedane skoke v porabi, še zlasti zavoljo zlorab, vendar pa mora še vedno obstajati možnost, da jo naročnik izklopi in s tem operaterju prepove sprotno obdelavo njegovih podatkov o prometu v ta namen.

V kolikor se bo predlagatelj odločil za obvezno zagotavljanje storitve spremljanja in omejevanja porabe, seveda opozarjamo, da je treba to v 151. členu (najbrž 2. odstavku) seveda izrecno predvideti.

***K 35. členu novele (sprememba 134. člena, klici v sili)***

S spremembo 134. člena se uvajajo določene nove oblike komunikacije v sili (*eCall*, *broadcasting* SMS idr.).

Glede novega 5. odst. (*eCall* kot oblika avtomatskega oz. ročnega klica v sili iz vozila v primeru prometne nesreče) opozarjamo, da standard eCall predvideva obvezno prisotnost mobilnega terminala in GPS/Glonass sprejemnika v vsakem novem vozilu[4] (ali njuno namestitev v obstoječa vozila), ter da je treba pripadajoče poskrbeti tudi za številne vidike posegov v zasebnost uporabnikov takšnih vozil, ki lahko zavoljo tega nastanejo. Možnost obdelave podatkov o lokacijah (in telemetriji) vozil namreč predstavlja obsežna tveganja za zasebnost uporabnikov vozil, saj bi ti podatki zanimali številne interesne skupine, zato menimo, da morajo biti v zakonu opredeljene tudi določene varovalke, s katerimi se vnaprej prepove zlorabe tega sistema v druge namene (npr. zavarovalniške, oglaševalske itd.). Že zaradi tega predlagamo premestitev 5. odstavka v ločen in obsežnejši člen (npr. 134.a člen) in po potrebi tudi podrobnejšo ureditev vseh podrobnosti s podzakonskim aktom.

Pri tem seveda upoštevamo, da so tehnične podrobnosti izvedbe *eCall* naprav (angl. IVS, *in-vehicle system* v *eCall* specifikaciji) v veliki meri prepuščene proizvajalcem avtomobilov, in da ZEKom-1 tega dela ne more neposredno regulirati. Tako bo proizvajalcu avtomobila prepuščeno, ali bo uporabil ločeno napravo ali pa jo integriral z obstoječim *in-car* računalniškim sistemom, ali ji bo dodal kakšne

3 Glej npr. pojasnila Si.Mobila, https://www.simobil.si/pomoc-in-informacije/-/pomoc/brez-skrbi-prenos-podatkov-pod-nadzorom , oz. Telekoma Slovenije, http://www.telekom.si/zasebni-uporabniki/mobilno/storitve/monitor in http://www.telekom.si/zasebni-uporabniki/mobilno/storitve/limit-prenosa-podatkov

4 V skladu z Uredbo št. … bo od aprila 2018 vključitev eCall terminala obvezna za vsa nova vozila, glej http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=uriserv:OJ.L_.2015.123.01.0077.01.ENG&toc=OJ:L:2015:123:TOC

dodatne funkcije (npr. po vzoru GM-ovega OnStar), ali bo naprava zahtevala stalno prijavo v GSM omrežje, ali zgolj v primeru prometne nesreče, ali bo naprava podpirala oddaljeno (OTA, *over-the-air*) nameščanje popravkov[5], kako točno bo izveden prenos podatkov (tipično *inband* modem preko GSM *voice* kanala), kateri nabor podatkov bo prenesen (priporočeni MDS nabor[6] ali širši nabor), ter tudi, kako bo o vsem tem obveščen uporabnik vozila.

Vendar pa ZEKom-1 lahko ureja vlogo operaterja pri izvajanju avtomatskih ali ročnih klicev. Predlagamo, da se vloga operaterja izrecno omeji na to vlogo, oz. da se mu prepove, da za Upravo za zaščito in reševanje kot organ, ki obravnava te e-klice, izvaja določene druge storitve.

Tako predlagamo, da se operaterju **posebej prepove obdelovati morebitne prometne podatke eCall naprav za kateri koli drug namen** kot za izvedbo eCall storitev (ter evt. še za preprečevanje zlorab te funkcije, npr. z blokado določenih IMEI številk). Še zlasti operaterji ne smejo uporabljati ali omogočati uporabe teh podatkov za lociranje vozila, oz. za pridobivanje podatkov iz vozila, ali posredovati teh podatkov drugim deležnikom, npr. zavarovalnicam. Teh podatkov tudi ne smejo hraniti v svojih običajnih zbirkah podatkov o prometu oz. podatkov o naročnikih.

Podobno predlagamo, da se operater**jem na splošno prepove proženje kakršnekoli povezave do eCall naprave**, razen t.i. povratnega klica, ki ga lahko sprejemni center za 112 izvede v primeru, da se izvorni, uporabniško sproženi klic poruši. eCall naprave se tako ne sme izrabljati za klicanje voznika, ali za pritajeno prisluškovanje vozniku, ali npr. za onesposobitev voznika. Če naj se te funkcije uporabljajo, naj to poteka čez ločene kanale, ne pa čez vez, ki jo operater zagotavlja med vozilom in Upravo za zaščito in reševanje.

IP v zvezi s predlogom novega 6. odstavka (povratni 112 klic) predlaga, da se obseg te storitve podrobneje opredeli v zakonu oz. v podzakonskem aktu.

***K 142. členu obstoječega zakona (pravica do ugovora in spora)***

Lani poleti je IP podal mnenje k takratnemu predlogu novele ZEKom-1, oz. potem še posebej mnenje k vprašanjem Sekcije operaterjev elektronskih komunikacij (SEOK) pri GZS glede vpliva prihajajočega Zakona o izvensodnem reševanju potrošniških sporov na hrambo podatkov o prometu. Specifično, operaterji so izrazili skrb, da bi uvedba nove, cenovno ugodne in z daljšim rokom omejene možnosti za ugovor zoper račun povzročila potrebo po daljši in obvezni hrambi podatkov o prometu za vse naročnike, da bi jim bili ti podatki potem na voljo v morebitnem kasnejšem (tudi leto dni po nastanku stroška) izvensodnem sporu.

Mnenje IP v zadevi[7] je sicer bilo, da »Obstoj oddaljene (ali kvečjemu manjše) verjetnosti potrebe po starejših prometnih podatkih, zavoljo dokazovanja operaterjeve pozicije v morebitnem kasnejšem sporu, po mnenju IP ne more predstavljati veljavne pravne podlage za dolgotrajno in neselektivno hrambo prometnih podatkov o vseh naročnikih.«

---

5 Eden od proizvajalcev tovrstnih naprav, Sierra Wireless, npr. zagovarja čim bolj fleksibilno rešitev, ki bi omogočala rabo eCall terminal tudi v druge namene. Glej priporočila na strani organizacije GSMA, http://www.gsma.com/connectedliving/wp-content/uploads/2012/04/theecallprogramobverviewanddesignconsiderations.pdf

6 Minimalni nabor podatkov o lokaciji avtomobila, prometni nesreči, idr. je opredeljen v MDS (minimal data set) specifikaciji, ki je del širše eCall specifikacije. Glej http://www.ecall.fi/eCall_msd_en_052009.pdf

7 mnenje št. 007-50/2015/2 z dne 14.7.2015, https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/SOEK_ponovno_mnenje_IP_glede_uskladitve_ZEKom-1_z_dolocbami_ZARPS.pdf

IP k temu dogaja, da je bil Zakon o izvensodnem reševanju potrošniških sporov (Uradni list RS, št. 81/15) vmes tudi sprejet, vendar pa da za reševanje potrošniških sporov z operaterji ni predvidel obvezne možnosti takšnega reševanja sporov. Operaterjem je bilo zato prepuščeno, da se sami odločijo, ali bodo določene izvajalce izvensodnega reševanja sporov šteli kot pristojne za reševanje sporov s svojimi uporabniki. Kolikor je IP znano, se noben od operaterjev za spore iz dobave komunikacijskih storitev ni odločil za priznanje obvezne pristojnosti[8].

Posledično IP opozarja, da ZIsRPS ne more predstavljati pravne podlage za daljšo hrambo podatkov o prometu (kar pa podrobneje pojasnjujemo v komentarju k 151. členu, glej spodaj).

***K 37. členu novele (zaupnost komunikacij, in še zlasti nadzor nad snemanjem telefonskih klicev)***

Glede novega 10. odst., ki zajema prenos določenih nadzornih pristojnosti z AKOS na IP, se v primeru zagotovitve dodatnih kadrovskih virov IP strinja s prenosom inšpekcijskih in prekrškovnih **pristojnosti nad izvajanjem 7. do 9. odstavka tega člena** (snemanje klicev), **ne pa tudi s prevzemom pristojnosti za ta člen v celoti**, oz. kot bi izhajalo iz njegove vsebine, za področje zaupnosti komunikacij (še členi do 161.) v celoti. Soglasja k tako širokemu prenosu pristojnosti namreč IP nikoli ni podal, niti ni Informacijski pooblaščenec sistemsko primeren organ, da bi bil pristojen za inšpekcijski in prekrškovni nadzor nad celotnim členom o zaupnosti komunikacij, ki se primarno nanaša na vsebino komunikacije in ne na osebne podatke in ki je tradicionalno pod nazorom nacionalnih regulatorjev elektronskih komunikacij.

Predlagamo, da se omenjena dikcija popravi in sicer namesto »(10) Informacijski pooblaščenec nadzira izvajanje določb tega člena« v »(10) Izvajanje določb 7. do 9. odstavka tega člena nadzira Informacijski pooblaščenec.«

***K 38. členu novele (zbiranje podatka o vrsti in številki osebnega dokumenta od naročnika v primerih večjih nakupov)***

IP se v skladu s svojim obstoječim mnenjem, podanim na prošnjo SOEK (mnenje št. 007-93/2015 z dne 6. 1. 2016) strinja s predlogom, da se operaterjem pred izvedbo prodaje blaga večje vrednosti na vezavo ali vklopom storitev, ki omogočajo brezgotovinsko plačevanje z mobilnim telefonom, dovoli zbiranje in hrambo **podatka o vrsti in številki uporabnikovega osebnega dokumenta** (torej ne zgolj vpogleda v osebni dokument, kot že zdaj, ne pa seveda tudi fotokopiranja osebnega dokumenta).

Pri tem sicer predlaga, da se v obrazložitvi člena pojem »večje vrednosti« nasloni na definicijo **večje premoženjske vrednosti** po 9. odst. 99. člena Kazenskega zakonika (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15 in 38/16), torej vsaj 500 evrov. Skratka, operater bo smel zabeležiti navedene podatke v primeru, ko bo ekonomska vrednost nakupa z vezavo (začetno plačilo ter vsa mesečna plačila) dosegla vsaj ta znesek. Le v tem primeru bo operater po mnenju IP izpostavljen tolikšnemu dodatnemu tveganju neplačila, da bo zbiranje podatkov z osebnega dokumenta lahko sorazmerno.

Podobno menimo glede izpostavljenosti neplačilu stroškov, ki nastanejo z rabo mobitela kot plačilnega sredstva. Ker ponudniki uporabljajo omejitve pri mesečni porabi, in ker imajo možnost, da naročniku, ki

8 Glej npr. izjave Telekoma, http://www.telekom.si/info-in-obvestila/izvensodno-resevanje-potrosniskih-sporov, ki ne priznava nobenega izvajalca izvensodnega reševanja potrošniških sporov, ali izjavo Si.mobila, ki priznava določenega izvajalca le za spore iz uporabe Monete, https://www.simobil.si/pomoc-in-informacije/obvestila/-/obvestila/2078904

ne poravna zapadlih računov, blokirajo to ali celo vse storitve, IP meni, da pride možnost zbiranja podatkov z osebnega dokumenta v poštev šele v primerih, ko naročnik zahteva določitev ali dvig mesečnega limita za plačevanje na nivo, ki že dopušča, da ustvari za vsaj 500 evrov stroškov do tiste točke, ko mu bo gotovo blokirana storitev. Ker se bo blokada po oceni IP zgodila najkasneje v 4-5 mesecih od izvedbe neplačanega zneska, bi to pomenilo, da bi to tveganje lahko nastopilo le pri naročnikih, ki imajo kot mesečni limit odobren znesek vsaj 100 evrov/mesec. Posledično IP meni, da pri zdajšnjih privzetih limitih (okoli 50 evrov/mesec) operater ne bo izpostavljen večji premoženjski škodi iz tega naslova, saj jo bo prej zajezil. To posledično tudi pomeni, da naročniku že samo zato, ker mu zagotavlja plačevanje z mobilnim telefonom, ne bo smel pobrati podatkov z osebne izkaznice.

Obenem IP predlaga, da se s popravkom člena pojasni, da **pravica zbiranja podatkov z osebnega dokumenta traja le, dokler traja opisana izpostavljenost operaterja do naročnika**. Ko torej naročnik zaključi z vezavo, in ne sklene nove ali jo zamenja z novo v vrednosti vsaj 500 evrov, mora operater že zbrane podatke izbrisati, saj **je prenehal namen, zavoljo katerega jih je hranil**. Podobno mora storiti, če uporabnik zniža limit mesečnih plačil z mobilnim telefonom.

Veliko število uporabnikov (verjetno celo večina) ima namreč pri operaterjih sklenjene anekse (npr. vsi, ki se odločijo za telefon z vezavo), kar bi po novi ureditvi pomenilo, da operaterji vodijo podatke o vrsti in številki uporabnikovega osebnega dokumenta za zelo veliko število posameznikov. Ko je namen obdelave tega podatka izčrpan (ko aneks poteče in so poravnane vse obveznosti iz njega), je treba te podatke izbrisati. Nobenega razloga ni, da bi operaterji hranili podatke o vrsti in številki osebnega dokumenta vseh posameznikov še naprej samo zato, ker so ti enkrat pri njih imeli nek aneks.

***K 151. členu obstoječega zakona (podatki o prometu)***

Obstoječi 151. člen ZEKom-1 zavoljo varstva zaupnosti komunikacij (147. člen) pomembno omejuje dopustne namene oz. čase obdelave podatkov o prometu. **Vendar pa praksa, kot je znana IP, ne sledi tem omejitvam**, oz. so zlasti operaterji mobilne telefonije vzpostavili »dolgoletno prakso« hrambe podatkov o klicih za obdobje zadnjih 3 do 4-mesečnih obračunskih obdobij, in to ne glede na to, ali je naročnik oz. uporabnik obveznosti, vezane na ta obdobja, že poravnal ali ne. Posledično bi bilo po mnenju IP potrebno določneje in deloma tudi ostreje zapisati omejitve pri operaterjevem postopanju s podatki o prometu.

Tako predlagamo, da se 2. odst. zapiše na določnejši način, ter da se vrine nov 3. odst. ki pojasni hrambo podatkov o prometu za potrebe priprave razčlenjenih računov; npr. takole:

> (2) Ne glede na določbo prejšnjega odstavka lahko operater do popolnega plačila storitve~~,~~ ~~vendar najdlje do preteka zastaralnega roka,~~ hrani in obdeluje podatke o prometu, ki jih potrebuje za obračun in za plačila v zvezi z medomrežnim povezovanjem. V kolikor naročnik oz. uporabnik zamudi s plačilom, lahko operater podatke iz prejšnjega odstavka, ki se nanašajo na neporavnane obveznosti, hrani vse do popolnega plačila, vendar najdlje do preteka zastaralnega roka.
>
> (3) Prav tako lahko operater ne glede na določbo prvega in drugega odstavka tega člena hrani podatke o prometu, ki jih potrebuje za pripravo razčlenjenih računov (139. člen), še za obdobje, za katero lahko naročnik oz. uporabnik zahteva pripravo takšnih računov, vendar najdlje za obdobje 3 mesecev od zaključka zadevnega obračunskega obdobja. Ta določba pa ne velja, v kolikor operater ponuja storitev sprotne izdaje razčlenjenega računa (skupaj z računom osnovne stopnje členitve, 121. člen) in naročnik oz. uporabnik to možnost izkoristi,

ali v kolikor naročnik oz. uporabnik izrecno izjavi, da ne želi, da bi se njegovi podatki hranili za ta namen.

Navedene spremembe 2. odst. jasneje pojasnjujejo, da mora operater po tem, ko prejme uporabnikovo plačilo računa za določeno obračunsko obdobje, izbrisati podatke o prometu, ki se nanašajo na to obdobje, saj nima več zakonske podlage, da bi jih (na splošno) še hranil. Le v kolikor naročnik oz. uporabnik zamuja s plačilom, sme operater podatke zadržati zavoljo izvedbe opomina oz. izvršbe, vendar spet, le do poteka zastaralnega roka za vložitev obojega. V kolikor je naročnik predplačnik, ali v kolikor gre za podatke, ki niso potrebni za izvedbo obračuna (*flat rate* paketi, nasploh nerelevantni podatki za potrebe obračuna), pa jih operater na tej podlagi seveda sploh ne sme hraniti.

Ker operaterji podatke pogosto rabijo še za izdajo razčlenjenih računov, je treba pojasniti še hrambo podatkov o prometu v te namene (predlagan nov 3. odst.). Operaterju je tako treba dovoliti, da podatke hrani za toliko časa, za kolikor nazaj naročniku oz. uporabniku omogoča pridobitev razčlenjenega računa. Pri tem mora omogočiti naročniku, da se odreče tej pravici, ter v tem primeru podatke pobrisati takoj, ko zanje več nima podlage po 1. oz. 2. odstavku. V kolikor ponuja sprotno in avtomatizirano izdajo razčlenjenih računov, skupaj z običajnim računom, je treba šteti, da je ta namen izčrpan, in podatke podobno takoj izbrisati.

Upoštevaje da navedeni predlogi predstavljajo pomemben odmik od sedanje prakse, IP predlaga, da se o njih izvede še dodatno usklajevanje z operaterji in AKOS kot pristojnim nadzornim organom. Pri tem predlaga tudi, da se natančneje prouči dopustnost obdelave podatkov o prometu še za druge komercialne namene (obstoječi 3. odst.).

***K 42. in 43. členu (sprememba 4. in 5. odst. 153. člena, nov 153.a člen; nova ureditev neizbrisne registracije o zahtevkih za posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa)***

IP se strinja, da je zavoljo črtanja določb XIII. poglavja, na katere se še vedno sklicuje zdajšnji 4. odst. 153. člena, treba zavarovanje podatkov o zahtevkih za prometne in lokacijske podatke v primerih varovanja življenja in telesa urediti na novo.

Pri tem pa dodatno predlagamo, da se novo predlagani 153.a člen uporabi tudi pri drugih policijskih posegih v zaupnost komunikacij (posredovanje podatkov o prometu, zakonito prisluškovanje idr.).

***K 60. členu (sprememba 3. odst. 203. člena, izjeme od splošne prepovedi omejevati, zadrževati ali upočasnjevati internetni promet)***

IP je **zadržan do** prve novo predlagane nacionalne izjeme, in sicer, da lahko operaterji blokirajo dostop do *»spletnih domen, ki so zaradi posnetkov spolne zlorabe otrok na internetu na Interpolovem seznamu 'IWOL'«*. Menimo, da ne gre za dovolj premišljen predlog, njegov zapis pa bi lahko predstavljal nevarni precedens za nadaljnje blokiranje posameznih omrežnih storitev brez zahteve po izdaji sodne odredbe.

Pri tem mora IP najprej poudariti, da se vsekakor zaveda nujnosti, resnosti in zahtevnosti boja proti storilcem tovrstnih zlorab otrok, ter da se zaveda obstoja nekaterih težav, s katerimi se tako naša kot tuje policije pri tem soočajo.

Nevtralnost interneta je namreč, kljub drugačnemu prvemu vtisu, pomembno povezana z ravnijo varovanja osebnih podatkov. Republika Slovenije je namreč v svojo zakonodajo zapisala zaščito nevtralnosti interneta, ki je obenem tudi močna zaščita za varstvo osebnih podatkov, saj ne dovoljuje zbiranja osebnih podatkov uporabnikov zavoljo razlikovanja med njimi. Kakršno koli dodajanje izjem pomeni rahljanje te zaščite, ki lahko vodi v dodatne izjeme in s tem v nižjo raven varovanja osebnih podatkov. Nujno potrebno je namreč preveriti, ali obstajajo milejši oziroma bolj učinkoviti ukrepi za umik spornih vsebin in vedno najprej poseči po njih.

Ugotavljamo, da je predlog zelo skopo obrazložen, in da ne pojasnjuje številnih vprašanj v zvezi z blokiranjem spletnih strani, ki so se v praksi že odprla v nekaterih preteklih primerih (npr. tekom blokiranja nekaterih tujih športnih stavnic s strani takratnega Urada za nadzor prirejanja iger na srečo). Neustrezno urejene blokade spletnih strani so vodile v inšpekcijski in prekrškovni postopek zaradi zbiranja osebnih podatkov brez pravne podlage in neustreznega zavarovanja osebnih podatkov. Na podlagi preteklih izkušenj izražamo dvom v učinkovitost blokad spletnih stran ter opozarjamo na možnosti nezakonitega zbiranja osebnih podatkov o blokiranih uporabnikih kot nezaželene stranske posledice blokade.

Menimo, da ni pojasnjeno, da bo predlagani ukrep resnično primeren in učinkovit, saj za obid blokade »spletnih domen« obstajajo številne enostavne tehnične rešitve (preklop na drug DNS strežnik, uporaba http proxy-ja, uporaba vpn-ja, uporaba TOR-a idr.), za katere je od uporabnikov, ki si želijo ogledati tako blokirane vsebine, žal treba pričakovati, da jih dobro poznajo. Argumenta, da bo s tem splošni javnosti preprečeno, da se »po nesreči« seznani s takšnimi spletnimi mesti, pa IP tudi ne more šteti kot prepričljivega, saj tovrstnih vsebin na »odprtem« spletu ni mogoče enostavno najti, saj jih spletni iskalniki že aktivno izločajo[9].

Dalje se poraja vprašanje nujnosti predlaganega ukrepa, saj bi bilo za zaščito otrok, katerih slike, posnetki in drugi podatki se nahajajo na teh straneh, mnogo učinkoviteje, in tudi enostavneje, da bi se te domene preprosto odklopilo z interneta. Postopki za to, tudi mednarodno gledano, že obstajajo, predlagatelj pa se v ničemer ne opredeljuje, zakaj se jih ne bo poslužil.

Še dalje močno opozarjamo zoper dopuščanje možnosti, da se operater samostojno odloči, da določenih vsebin ne bo dostavljal svojim naročnikom ali uporabnikom. Takšno dejanje predstavlja *prima facie* kršitev operaterjeve omrežne nevtralnosti, ter hkrati ruši njegovo pozicijo »golega posrednika« podatkov, ki se pretakajo po njegovem omrežju. Samovoljno ukrepanje zoper eno vrsto kršitev, čeravno posebej zavržno, tako ustvarja operaterjevo obveznost ukrepati zoper širjenje drugovrstnih protipravnih vsebin. Do tega dela, ki se križa z Zakonom o elektronskem poslovanju na trgu, pa se predlagatelj žal sploh ne opredeljuje.

Dodatno IP izpostavlja nekatere vidike, ki se nam zdijo pomembni glede predlaganih sprememb ukrepov v primeru izjemnih stanj, pri čemer se glede na svoje pristojnosti seveda ne spušča v razpravo o ustreznosti ukrepov za zagotovitev delovanja kritične državne infrastrukture, temveč želi zgolj prispevati k čim bolj kakovostni zakonski rešitvi.

IP vsekakor pozdravlja nekatere predlagane rešitve, glede opisanih pomislekov pa predlaga ponovni sestanek vseh vpletenih deležnikov, da se premisli o morebitnih učinkovitejših in manj invazivnih alternativah za boj proti širjenju opisanih vsebin.

---

9 Glej npr. https://www.washingtonpost.com/news/the-switch/wp/2015/05/06/how-google-and-other-tech-firms-fight-child-exploitation/

***K 20. členu novele (sprememba 83. člena, ukrepi v primeru izjemnih stanj)***

IP opozarja na manjšo nedoslednost med določbami tako sedanjih kot predlaganih 83. (ukrepi v primeru izrednih stanja) oz. 203. člena (omrežna nevtralnost, ki ga komentiramo zgoraj), ki skupaj urejata primere, ko morajo operaterji omogočiti privilegiranje prometa nosilcev varnostnega in obrambnega sistema, zaščite in reševanja, oz. druge kritične državne infrastrukture.

Obstoječi 2. odst. 83. člena določa (op.p.), da morajo »*operaterji, ki zagotavljajo javno telefonsko omrežje, […] svoje omrežje prilagoditi tako, da omogoča dodelitev prednosti komunikacijam z določenih omrežnih priključnih točk [kritične državne infrastrukture] pred komunikacijami s preostalih omrežnih priključnih točk (v nadaljnjem besedilu: funkcija prednosti)*«, vključno s tem, da »v *izjemnih stanjih lahko operaterji [to izvedejo tako], da omejijo ali prekinejo delovanje preostalega komunikacijskega prometa v takšnem obsegu in toliko časa, kolikor je to nujno potrebno za delovanje omrežnih priključnih točk s prednostjo*«. Predlagana sprememba te obveznosti vsebinsko ne spreminja, ampak jo zgolj širi s telefonskih tudi na druga komunikacijska omrežja (še zlasti internet).

Iz dikcije zadnjega stavka tega odstavka (*»v izjemnih stanjih [...] tudi tako, da [...] prekinejo«*) torej izhaja, da **morajo operaterji tudi v normalnem (ne izjemnem) stanju privilegirati omrežni promet kritične državne infrastrukture**, in sicer tako, da ostali promet po potrebi upočasnijo, da lahko kritični poteka nemoteno z želeno hitrostjo, medtem ko lahko v izjemnih stanjih (vojno ali izredno stanje, stanje nastalo zaradi naravnih ali drugih nesreč ter katastrofalni izpad omrežja) posežejo še dlje (dikcija *»tudi tako«*), se pravi, da ostali promet začasno v celoti prekinejo.

Takšno omejevanje ostalega prometa **v običajnih razmerah** nujno predstavlja dejanje kršitve nevtralnosti operaterjevega omrežja. Vendar pa takšen poseg ni predviden v 3. odst. 203. člena, ki izrecno in taksativno našteva primere, ko so kršitve nevtralnosti omrežja dopustne. Zdajšnji 3. odst. posega v nevtralnost zaradi zagotavljanja delovanja kritične državne infrastrukture sploh ne predvideva, medtem ko novo predlagani jo, vendar zgolj v izjemnih stanjih. Posledično operaterji z doslednim izvajanjem 2. odst. 83. člena trenutno kršijo 203. člen, in ga bodo (v običajnih razmerah) tudi v prihodnje.

IP zatorej predlaga, da predlagatelj zakona ponovno razmisli o obsegu nujnega posega v infrastrukturo in nevtralnost omrežja v običajnih razmerah, ter besedilo predloga zakona ustrezno dopolni.

S pozdravi,

Mojca Prelesnik, univ.dipl.prav.,
Informacijska pooblaščenka