REPUBLIKA SLOVENIJA
DRŽAVNI SVET

Komisija za državno ureditev

Številka: 060-05-5/2018

Osnutek

Ljubljana, 4. 6. 2018

ZAPISNIK

5. seje Komisije Državnega sveta za državno ureditev, ki je bila v sredo, 7. marca 2018 v sejni sobi 209, Ljubljana. Seja se je začela ob 14. 00 uri in se je končala ob 15. 30.

Prisotni:
- predsednik: Rajko Fajt
- člani: Milan Ozimič, Marjan Maučec, Franc Kangler, Bojan Kekec, Bojan Kontič, Branimir Štrukelj, mag. Marko Zidanšek in Bojana Potočan.

Sejo je vodil predsednik Rajko Fajt.

Na seji so bili prisotni tudi:

Pri 1. in 2. točki dnevnega reda predstavniki Ministrstva za javno upravo:
- mag. Ksenija Klampfer, državna sekretarka
- mag. Bojan Križ, generalni direktor Direktorata za informacijsko družbo in
- Barbar Pernuš Grošelj, vodja Sektorja za zakonodajo informacijske družbe
- Tina Bizjak Ahačič, podsekretarka v Sektorju za zakonodajo informacijske družbe.

Predlog dnevnega reda:

1. Predlog zakona o informacijski varnosti (ZInfV), druga obravnava, EPA 2594-VII
2. Predlog zakona o dostopnosti spletišč in mobilnih aplikacij (ZDSMA), druga obravnava, EPA 2552-VII
3. Potrditev zapisnikov 4. seje komisije in 1. izredne seje komisije
4. Pobude in vprašanja

Predlog dnevnega reda je bil soglasno sprejet.

Ad1) Predlog zakona o informacijski varnosti (ZInfV), druga obravnava, EPA 2594-VII
Člani komisije so prejeli mnenje Združenja občin Slovenije in mnenje Zakonodajno-pravne službe Državnega zbora (ZPS).

Predstavnik MJU je predstavil predlog zakona. Z njim se želi povečati raven informacijske varnosti v Republiki Sloveniji in v EU. Uresničevanje predloga zakona bo zagotovilo visoko raven varovanja omrežij in informacijskih sistemov, ki so bistvenega pomena za nemoteno delovanje države in s katerimi se zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Predlog zakona vzpostavlja minimalne varnostne zahteve, prav tako pa tudi zahteve za priglasitev incidentov in pristojnosti, naloge in organizacijo odgovornega nacionalnega organa, ki bo oblikovan kot organ v sestavi ministrstva pristojnega za informacijsko družbo. Predlog zakona predvideva tudi enotne kontaktne točke, nacionalne skupine za obravnavo incidentov in pa skupino za obravnavo incidentov v organih državne uprave. Po predlogu zakonu bodo zavezanci izvajalci bistvenih storitev z naslednjih področij: energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura bančnega trga. V naši različici predloga zakona sta na seznam bistvenih storitev vključena še preskrba s hrano in varstvo okolja, kar se sklada z Zakonom o kritični infrastrukturi. Organizacije, zavodi oziroma podjetja, ki bodo prepoznani kot izvajalci bistvenih storitev bo določila uredba, ki jo bo sprejela Vlada na podlagi priporočil, ki jih bo pripravila EU. Po predlogu zakona bodo zavezanci tudi ponudniki digitalnih storitev, to so spletne tržnice, spletni iskalniki in računalništvo v oblaku. Gre za zavezance, ki jih je določila evropska direktiva, po našem predlogu zakona pa bodo zavezanci tudi organi državne uprave. Zavezanci bodo morali v skladu z zakonom poleg ključnih varnostnih zahtev voditi tudi posebno varnostno dokumentacijo in sprejemati določene varnostne ukrepe. Predviden je način priglasitve incidentov in določeni so organi, ki jim bo treba poročati o zaznanih incidentih. Predlog ureja tudi nadzor nad izvajanjem zakona, ki ga bodo opravljali inšpektorji za informacijsko varnost. Naloge informacijske varnosti bo do 1. januarja 2020 opravljal Urad za varovanje tajnih podatkov, od takrat naprej pa nacionalni organ v sestavi ministrstva pristojnega za informacijsko družbo. Vseh finančnih posledic predloga zakona še ni bilo mogoče predvideti, saj so na ravni zakona našteti zgolj sektorji, ki se jih zakon dotika, medtem, ko bodo zavezanci s posameznih sektorjev določeni šele na podlagi vladne uredbe. Merila bodo šla v smer, da pride npr. v poštev banka, ki bo imela določeno število komitentov ali osnovnega kapitala v povezavi z BDP in tako naprej. EU želi, da imajo vse države področje urejeno enotno. Predlog zakona želi dvigniti splošen nivo zavedanja o pomenu zagotavljanja informacijske varnosti, področju v zadnjih letih ni bilo namenjeno dovolj pozornosti. Vladna uredba mora biti pripravljena v roku 6 mesecev po sprejetju zakona, Ministrstvo za javno upravo (MJU) bo uredbo dalo v javno obravnavo in različni deležniki, tudi lokalne skupnosti, bodo imeli možnost sodelovati pri njenem nastajanju in nastajanju meril za določitev kriterijev za zavezance.
V razpravi so državni svetniki izpostavili pomen informacijske varnosti in krepitve zavesti o tem področju. Gre za nujne ukrepe, s kateri že zamujamo, glede na to, da ni več nobenega poslovnega procesa, ki ne bi bil podprt z informacijsko tehnologijo. Člani komisije so se strinjali, da bodo zahteve in naloge za zavezance pospešile zavedanje podjetij in zaposlenih, da potrebujejo nova znanja s področja informacijske varnosti. Na komisiji je bila dana primerjava, da imamo glede požarne varnosti in zaščite pri delu stalna usposabljanja, medtem, ko jih na področju informacijske varnosti nimamo. Zato bo treba poleg ustrezne zakonodaje vzpostaviti tudi stalno osveščanje o pomenu informacijske varnosti. Komisija je menila, da je predlog zakona nujen odziv na razmere v svetu in pri nas, saj smo brez ustrezne zaščite ranljivi in izpostavljeni kibernetskim napadom. Predlog zakona je, kot so dejali člani komisije, nekakšen »stres test« za sisteme v državi, da se bodo bolj zavedali nevarnosti in se bodo znali ustrezno odzivati na incidente. Predlagatelj je na komisiji izpostavil 27. člen predloga zakona, ki govori o pristojnem nacionalnem organu, ki bo moral v skladu s 7. točko koordinirati usposabljanja, vaje in izobraževanja o informacijski varnosti in skrbeti za dvig zavedanja javnosti o pomenu in načinih informacijske varnosti.

Na komisiji so bila predlagateljem zastavljena tudi vprašanja glede odgovornosti za zagotavljanje informacijske varnosti in kaj je z odškodninsko odgovornostjo podjetij in zavodov, če pride do kibernetskih vdorov in morebitnih odtujitev osebnih podatkov

uporabnikov storitev (zdravstvene storitve, komunalne storitve in drugo), ali predlog zakona predvideva kakšne sankcije za neizvajanje varnostnih standardov. Ali predlog zakona sam po sebi prinaša kakšno direktno zaščito za potrošnika v primeru zlorabe podatkov, do katerih bi prišlo zaradi kibernetskih napadov in ali ima podjetje ali institucija do posameznika kakšno odškodninsko odgovornost, ker je slabo zaščitila njihove podatke? Predlagatelj je v zvezi z navedenimi vprašanji članom komisije pojasnil, da je za informacijsko varnost najprej odgovoren vsak organ zase. Kot je za vsako organizacijo pomembno vodenje financ ali kadrovskih vprašanj, bo morala postati pomembna tudi odgovornost za izvajanje postopkov za informacijsko varnost in zavedanje vsakega organa, da bo moral poskrbeti za informacijsko varnost svojih sistemov. V večini primerov se namreč izkaže, da do posameznih incidentov prihaja zaradi človeške napake zaposlenih (neurejen sistem gesel, nedefinirano posodabljanje sistemov…). Država mora urediti zakonodajni del, ki predstavlja sistematičen okvir delovanja in koordinacijo celotnega sistema na enem mestu. Prav tako mora država skrbeti za višanje osveščenosti o pomenu informacijske varnosti, saj se sistemi povezujejo med seboj in informacijska tehnologija je vpeta v vedno več delovnih procesov. Predlagatelj je v skladu z 11. členom predloga zakona še poudaril, da bo moral vsak zavezanec narediti ocenjevalni postopek in preko njega preveriti stanje svojega informacijskega sistema in na osnovi tega stanja pripraviti varnostno dokumentacijo, ki bo morala vsebovati mehanizme preprečitve kibernetskih vdorov in imeti za primere incidenta izdelane postopke ravnanj. Po mnenju predlagatelja je izjemno pomembno, da se zaznajo tudi vse grožnje in nameni za incidente in se o tem poroča organom in centralni enoti in tako se tudi drugi sektorji zavedajo groženj in se nanje ustrezno pripravijo in okrepijo varnost. Ta predlog zakona je v prvi vrsti namenjen preventivi in ne toliko kurativi. Predlog zakona stremi k temu, da se na tem področju uveljavi resno in sistematično delo, saj se z digitalizacijo družbe možnost za kibernetske napade povečuje in moramo pripraviti ustrezno obrambo. V zvezi z direktno odgovornostjo, tudi finančno oziroma odškodninsko posameznih podjetij oziroma ustanov, pa je bilo s strani predlagateljev izpostavljeno 11. poglavje predloga zakona - kazenske določbe, ki pravi, da mora vsak zavezanec narediti celoten postopek ocene in predvidenih ukrepov, v tem delu so tudi specificirane globe, če zadeve niso izvedene ali niso ustrezno izvedene. Sankcije so predvidene, vendar pa je predlog zakona bolj usmerjen v ozaveščanje zavezancev in javnosti o pomenu informacijske varnosti. Predlagatelj je pojasnil, da predlog zakona ne ureja pravic potrošnikov, saj ta izhaja iz zakonodaje o varstvu potrošnikov, seveda pa nihče ne izključuje splošnih pravil o odškodninski odgovornosti. Predlog zakona vzpostavlja sistem informacijske varnosti preko določanja zavezancev, ki so odgovorni zanjo.

Na komisiji je bilo postavljeno tudi vprašanje ali so predpisi s področja informacijske varnosti usklajeni s predpisi in dolžnostmi, ki izhajajo iz sprememb zakonodaje na področju varstva podatkov, ki bodo veljali na mednarodni ravni, kjer je tudi predpisanih precej ukrepov in nalog. Predlagatelj je članom komisije zagotovil, da so predpisi med seboj usklajeni. V 3. členu predloga zakona je tako definirana obdelava podatkov in da vsaka obdelava osebnih podatkov poteka v skladu s trenutno veljavnim Zakonom o varovanju osebnih podatkov. Enako kot evropska direktiva, ki se jo prenaša s tem predlogom zakona, se tudi predlog zakona sklicuje na splošno uredbo in evropske predpise o varstvu osebnih podatkov in na direktivo, ki je trenutno prenesena z Zakonom o varstvu osebnih podatkov, pa tudi na splošno uredbo o varstvu osebnih podatkov EU, ki je neposredno uporabljiva. Člane komisije je zanimalo ali bodo med zavezance za digitalne storitve vključena tudi podjetja, ki se ukvarjajo s kripto valutami, pri katerih je zaradi kibernetskih napadov že prišlo do določenih škod. Komisija je razmišljala tudi o stroških, ki jih bo imelo gospodarstvo s prilagoditvijo predlogu zakona, saj jih bo izvajanje ukrepov dodatno obremenjevalo in kakšna bodo za podjetje administrativna bremena za izpolnjevanje zahtev iz predloga zakona. Člani komisiji so še izpostavili, da je v proračunu za 2018 za večanje informacijske varnosti namenjeno 530.000 evrov in jih je zanimalo za kaj točno se bodo ta finančna sredstva porabila. Predlagatelj je glede zavezancev z digitalnega področja članom komisije pojasnil, da gre v tem primeru predvsem za podjetja, ki delujejo na globalnem trgu in ponujajo oblačne storitve,

spletne tržnice ali pa spletne iskalnike, vendar je teh ponudnikov v Sloveniji zelo malo. Prav tako spisek zavezancev še ni znan, ker se šele pripravlja uredba, ki bo določila merila za izbor zavezancev. Glede podjetij, ki se ukvarjajo s kripto valutami je bilo s strani predlagatelja opozorjeno, da v primeru, če bi takšno podjetje sodilo med zavezance, bo moralo zagotavljati enake varnostne standarde kot drugi. Predlagatelj se je sicer strinjal, da zagotavljanje informacijske varnosti nekaj stane, vendar se je treba zavedati, da so kibernetski napadi še mnogo dražji in da je treba vlagati finančna sredstva v dvig informacijske varnosti. Višja raven informacijske varnosti je lahko tudi konkurenčna prednost EU pred drugimi območji sveta. Predlagatelj je pojasnil, da so predvidena finančna sredstva v višini nekaj več kot 500.000 evrov namenjena vzpostavitvi enotnega nacionalnega organa za skrb nad informacijsko varnostjo, del sredstev pa bo namenjen nakupu programske opreme za višanje nivoja varnosti na področju informacijsko-komunikacijskih sistemov v državnih organih. Z novo zakonodajo se želi čim manj administrativno obremenjevati podjetja in druge zavezance, zato se je pri vseh obveznostih predvideva, da v kolikor imajo zavezanci varnostno dokumentacijo že pripravljeno na podlagi druge zakonodaje - o kritični infrastrukturi, varstvu osebnih podatkov itd., potem jo skladno s tem zakonom samo dopolnijo. Velike družbe, podjetja in organizacije, ki bodo v večini tudi zavezanci, imajo v glavnem te stvari že dobro urejene in bo šlo samo za manjše dograditve sistema.

Komisijo je zanimalo ali je bila pred samo pripravo predloga zakona pripravljena kakšna analiza stanja glede informacijske varnosti znotraj državnih organov (npr. na upravnih enotah, ki izdajajo biometrične potne listine, varnost elektronskih podpisov…) in v zasebnem sektorju. Predlagatelj je ravno v zvezi s tem vprašanjem članom komisije posebej izpostavil, da evropska direktiva organov državne samouprave ne vključuje med zavezance, pri nas pa smo zaradi zavedanja, kako šibki smo na tem področju varnosti, vključili med zavezance tudi organe državne uprave. Gre za nacionalno določbo, ker se želimo sistematično lotiti dela v tem sektorju. Glede analiz stanja informacijske varnosti predlog zakona vsebuje t.i. test MSP (test malih in srednjih podjetij), preko katerih se je ocenjevalo ustreznost nivoja informacijske varnosti (ocenjevalo se je 300 gospodarskih subjektov, od tega je bilo 75 ocenjenih kot neustreznih), kar daje nek vpogled v situacijo. Posledično je v MSP testih ocenjen tudi strošek za izboljšanje informacijske varnosti in se ga ocenjuje na približno 2 milijona evrov, kar ni velik strošek, glede na morebitno škodo v primeru kibernetskih incidentov. Informatika organov državne uprave se centralizira, določeni organi so že bili ali pa bodo centralizirani, kar bo pripomoglo k višji stopnji varnosti. Na MJU se gradijo 3 oblaki infrastrukture - državni oblak, hibridni oblak in oblak za razvoj in raziskave in v sklopu državnega računalniškega oblaka so določena ministrstva že centralno vsebovana (podatki, aplikacije…) in v tem delu je nivo informacijske varnosti zadovoljiv.

Na komisiji je bilo glede informacijske varnosti in preverjanja le-te predstavljen tudi primer eAsistent, ki se uporablja v izobraževanju in preko katerega se vodi mnogo osebnih podatkov učencev, pri tem pa je podjetje, ki je lastnik eAsistenta zasebno podjetje. Postavlja se vprašanje, kdo je odgovoren, če pride do razkritja ali uničenja podatkov, če portal eAsistent ne bi bil dovolj dobro zavarovan pred kibernetskimi napadi. Predlagatelj je izpostavil, da gre v tem primeru v prvi vrsti za problem varovanja osebnih podatkov in je vprašanje, če bo ta sistem po uredbi sodil med zavezance za informacijsko varnost. Vsekakor pa predlog zakona tudi takšne sisteme skuša osveščati in opozarjati na potrebo po večji skrbi in odgovornosti vsakega subjekta za informacijsko varnost, saj so posledice lahko izredno boleče in na številnih področjih.

Komisija je v zvezi s poslanimi pripombami na predlog zakona s strani Združenja občin Slovenije opozorila na finančne posledice za lokalne skupnosti in na neurejeno usklajevanje povprečnin ter na nove obremenitve lokalnih skupnosti, čeprav je bila obljubljena celo njihova razbremenitev. V končni točki lahko del obremenitev pade tudi na porabnike javnih storitev, če bodo določena javna podjetja sodila med zavezance in bodo morala večja finančna sredstva vložiti v izboljšanje informacijske varnosti. Tudi ostala podjetja, ki bodo postala

zavezanci lahko del stroškov prevalijo na uporabnike storitev, komisija se je strinjala, da to ni prav. Predlagatelj ni zanikal določenih finančnih posledic, vendar še ni narejen spisek zavezancev in zato vseh finančnih posledic v predlogu zakona ni bilo mogoče ovrednotiti. En kibernetski napad organizacijo stane več, kot pa je celoten strošek za zagotavljanje informacijske varnosti. V začetku bodo finančne posledice večje, ker bo treba pripraviti oceno tveganja in popisati celoten informacijski sistem, vzpostaviti sistem ukrepanja, določiti odgovorno osebo v sami organizaciji, ki bo odgovorna za poročanje, vse skupaj pa bo moralo postati del samega vodenja organizacije, da bo zagotovila minimalne varnostne standarde, vendar je odpravljanje posledic dražje, kot pa pravočasno ukrepanje.

Po končani razpravi je komisija sprejela naslednja sklepa:

1. Komisija za državno ureditev je **podprla** Predlog zakona o informacijski varnosti (ZInfV), druga obravnava, EPA 2594-VII. Sklep je bil sprejet soglasno.
2. Komisija je za poročevalca na seji matičnega odbora določila državnega svetnika Rajka Fajta. Sklep je bil sprejet soglasno.

Ad2) Predlog zakona o dostopnosti spletišč in mobilnih aplikacij (ZDSMA), druga obravnava, EPA 2552-VII

Člani komisije so prejeli mnenje Zakonodajno-pravne službe Državnega zbora in mnenje Združenja občin Slovenije in s pripombami Nacionalnega sveta invalidskih organizacij Slovenije.

S predlagano direktivo se v naš pravni red prenaša Direktiva o dostopnosti spletišč in mobilnih aplikacij. Uporabnikom se tako želi omogoči lažji dostop do informacij in storitev javnega sektorja in lažje uveljavljanje njihovih pravic, kar je še zlasti pomembno za uporabnike z različnimi oblikami oviranosti (gibalno ovirani, slepe in slabovidne osebe, gluhe in naglušne osebe, osebe s težavami v kognitivnem funkcioniranju in starejši uporabniki), s čimer se bo povečala digitalna vključenost teh kategorij prebivalstva. Po podatkih Statističnega urada Republike Slovenije je ocenjeno, da v Sloveniji med 12–13 % prebivalstva sodi v eno od kategorij invalidnosti. Zavezanci po tem zakonu so državni in lokalni organi in osebe javnega prava v skladu z Zakonom o javnem naročanju. Ocenjuje se, da je teh zavezancev okoli 1360. Predlog zakona določa tudi izjeme, npr. RTV, in sicer gre za izjemo, ki jo je določila že Evropska komisija v direktivi, istočasno pa je v predlogu zakona tudi izjema, ki se tiče vrtcev, osnovnih in srednjih šol. Direktiva namreč dopušča možnost, da se te ustanove izvzame kot zavezance, razen za vsebine, ki se nanašajo na spletne upravne funkcije (osnovne informacije o zavodu, urniki, šolski koledarji in vpisni pogoji). Predlagatelj je omenil, da je bilo že v času razprave izpostavljeno stališče, da bodo kljub izjemi, ki je zapisana v predlogu zakona, nastale finančne posledice za šole. Predlagatelj je opozoril, da finančnih posledic ne bo, če bo šola omogočala objavo teh podatkov na e-portalu. V tem primeru bodo vsi podatki že avtomatsko prilagojeni vsem standardom in zahtevam, ki jih postavlja predlog zakona in šole s tem ne bodo imele dodatnih stroškov. To je bil tudi dogovor z Ministrstvom za izobraževanje, znanost in šport in ta izjema je bila upoštevana v predlogu zakona.

Obveznosti zavezancev po predlogu zakonu so, da skladno s standardom, ki ga predpisuje predlog zakona, zagotavljajo, da bodo spletišča in mobilne aplikacije zaznavne, delujoče, razumljive, robustne in dostopne. To v praksi pomeni, da si bo uporabnik lahko prilagodil vsebino na način, da bo zanj uporaben, določil si bo npr. velikost pisave, kontraste, uporabo Braillove tipkovnice in podobno. Vsak zavezanec bo moral izdelati oceno nesorazmernega bremena, kar pomeni, da bo lahko manjša organizacija upoštevala finančne vire, notranjo organizacijo in dejavnost, ki jo opravlja v primerjavi s koristmi za uporabnike in če bo ta primerjava nesorazmerna in bo šlo za prevelik strošek, organizaciji ne bo treba izpolnjevati kriterijev iz predloga zakona. Predlog zakona predvideva tudi določen inšpekcijski nadzor, ki

bo preprečeval, da bi se nesorazmerno breme izkoriščalo in da bodo ocene pravilno pripravljene. Ministrstvo za javno upravo (v nadaljevanju: MJU) bo poskrbelo za usposabljanje zavezancev, javnih uslužbencev in drugih pripravljavcev drugih javnih spletišč in mobilnih aplikacij, spodbujala pa se bo tudi večja ozaveščenost uporabnikov, da bodo uporabljali vsebine, in spodbujali tiste, ki ne bodo obvezni za vstop v sistem, da pa bi svoje spletne povezave vseeno prilagodili v skladu s standardi, ki jih prinaša predlog zakona. Predlagatelj se je odzval še na višino predvidenih glob, ki naj bi bile previsoke, vendar je njihova višina izenačena z globami s področja informacijske družbe. Predlog zakona predvideva, da bi za nova spletišča začel veljati 2019, za obstoječa spletišča 2020 in 2021 za mobilne aplikacije.

Komisija je predlog zakona podprla, saj večja dostopnost spletnih vsebin povečuje digitalno vključenost ranljivih skupin, zlasti invalidov in starejših, kar je v današnjem svetu bistveno za dostop do informacij, storitev javnega sektorja in za uveljavljanje pravic vsakega posameznika. Komisija je pri predlagateljih preverjala, zakaj določene pripombe invalidskih organizacij niso bile upoštevane. V obrazložitvi k predlogu zakona je navedeno, da določenih predlogov Nacionalnega sveta invalidskih organizacij Slovenije ni bilo mogoče upoštevati. Izpostavljene so bile obveznosti, ki bi bile naložene nevladnim organizacijam, da bi se tudi te prilagodile standardom iz predloga zakona in da bi bilo to zanje preveliko oziroma nesorazmerno finančno breme. Komisijo je zanimalo, ali je bila v zvezi z obremenitvami narejena kakšna analiza in na podlagi česa se je ocenjevalo to nesorazmerno breme. Predlagatelj je članom komisije pojasnil, da je MJU od samega začetka pri pripravi predloga zakona sodeloval z različnimi invalidskimi organizacijami, bilo je veliko srečanj, izvedeno pa je bilo tudi neke vrste javno naročilo, v katerem je MJU pozvala zainteresirane deležnike, da se vključijo v samo pripravo osnutka zakona, spodbujalo se je predvsem deležnike, ki področje dobro poznajo. Na poziv se je prijavila mariborska Fakulteta za računalništvo in informatiko, ki sodeluje z NVO in so pripravili vhodne podatke, ki so jih pripravljavci zakona proučili in analizo teh podatkov vključili v predlog zakona, kot na primer tudi oceno stroškov prilagoditve spletišč za tovrstne namene in ostale zahteve invalidskih organizacij. Predlagatelj je posebej izpostavil, da ne drži očitek, da bi se pri prenosu direktive prenesel minimum zahtev. Na komisiji je predlagatelj navedel podatek, da po direktivi vključitev znakovnega jezika ni bila zahteva, vendar je v predlog zakona vključen. Prav tako je v predlog zakona vključen inšpekcijski nadzor, česar direktiva prav tako ne predvideva, vendar je bilo stališče MJU, da je treba poskrbeti, da ne bi prihajalo do izkoriščanja zavezancev glede t. i. nesorazmernega bremena. Inšpekcijski nadzor bo preverjal, ali določena vsebina na spletišču zaradi pretiranega finančnega bremena res ne more biti prilagojena novemu zakonu. Predlagatelj je opozoril, da je odraz dobrega in stalnega sodelovanja mnogih deležnikov pri pripravi predloga zakona tudi to, da je prvi osnutek med izjeme uvrščal vrtce, osnovne in srednje šole in tudi fakultete, ki pa so bile po predstavljenih argumentih s seznama izjem umaknjene. Predlagatelj je v tem primeru sledil argumentom, da je posameznik na fakulteti samostojna oseba in če ne more samostojno dostopati do podatkov na spletišču, pomeni, da mu je onemogočena enakost dostopa do informacij in zato so fakultete postale zavezanci. Po tehtanju vsebinskih razlogov pa je bila sprejeta smotrna odločitev, da se ostale izobraževalne ustanove izključi iz teh obvez, ker obstaja bojazen, da bi pretirano nalaganje obveznosti lahko privedlo do situacije, da bi začele ustanove umikati vsebine s spletišč in mobilnih aplikacij, kar pa bi bilo v škodo vseh uporabnikov. Predlagatelj je izpostavil, da se je pri urejanju tega področja tesno sodelovalo z Ministrstvom za izobraževanje, znanost in šport in se je tako prišlo do kompromisnega predloga, da so vsebine o spletnih upravnih funkcijah teh ustanov objavljene na e-portalu, kar pa pomeni, da so vsi podatki že avtomatsko prilagojeni vsem standardom in zahtevam, ki jih postavlja predlog zakona.

Komisija je menila, da je treba v prihodnje prilagojenost spletišč in mobilnih aplikacij še spodbujati in v primerih, ko prihaja do nesorazmernih stroškov in je to problem za posamezne organizacije, bi morala država zaradi pomena, ki ga ima digitalna dostopnost,

iskati tudi parcialne rešitve, kot so državni razpisi, na katerih bi organizacije lahko pridobile finančne vire za prilagoditev spletišč in mobilnih aplikacij. Predlagatelj je pri tem na seji komisije poudaril, da šole, ki delajo po prilagojenih programih, ne sodijo med izjeme za prilagoditev spletišč in mobilnih aplikacij. Predlagatelj je članom komisije predstavil tudi pilotni projekt Ministrstva za izobraževanje, znanost in šport. V projektu se spletišča osnovnih šol obravnava centralno, predvideva se vzpostavitev platforme, ki bi dobivala informacije od različnih osnovnih šol, ki bi jih prek uporabniškega vmesnika prilagodila, s tem pa bi se znižali stroški tovrstnih prilagoditev. Ker pa gre za pilotni projekt, se tega ni želelo prejudicirati že s tem zakonom in tako osnovne šole avtomatsko vzpostaviti kot zavezance po predlogu zakona. Komisija je predlagatelje opozorila na pripombe Nacionalnega sveta invalidskih organizacij Slovenije in jih zaprosila, da jih skrbno proučijo in po možnosti upoštevajo. Komisija je še opozorila, da spletne učilnice niso namenjene samo telesno oviranim osebam, ampak jih uporabljajo npr. v šolah tudi dijaki, ki so dalj časa odsotni od pouka in da je treba razmišljati tudi o dostopu do spletišč tem kategorijam uporabnikov. Predlagatelj je pri tem poudaril, da v 1. členu predloga zakona piše, da velja za vse uporabnike, zlasti za uporabnike z različnimi oblikami oviranosti.

Po končani razpravi je komisija sprejela naslednja sklepa:

1. Komisija za državno ureditev je **podprla** Predlog zakona o dostopnosti spletišč in mobilnih aplikacij (ZDSMA), druga obravnava, EPA 2552-VII. Sklep je bil sprejet soglasno.
2. Komisija je za poročevalca na seji matičnega odbora določila državnega svetnika Rajka Fajta. Sklep je bil sprejet soglasno.

Ad3) Potrditev zapisnikov 4. seje komisije in 1. izredne seje komisije
Zapisnika sta bila soglasno podprta.

Ad4) Pobude in vprašanja
Pobud in vprašanj ni bilo.

mag. Mateja Poljanšek l.r.
sekretarka

Rajko Fajt l.r.
predsednik