



Številka: U-I-144/19-51

Datum: 6. 7. 2023

DELNA ODLOČBA

Ustavno sodišče je v postopku za oceno ustavnosti, začetem z zahtevo skupine poslancev Državnega zbora, na seji 6. julija 2023

odločilo:

- 1. Člena 149b in 149c ter peti odstavek 156. člena Zakona o kazenskem postopku (Uradni list RS, št. 176/21 – uradno prečiščeno besedilo) se razveljavijo.**
- 2. Šesti odstavek 156. člena Zakona o kazenskem postopku se razveljavi, kolikor se nanaša na peti odstavek 156. člena Zakona o kazenskem postopku.**
- 3. Razveljavitev iz 1. in 2. točke izreka začne učinkovati v roku enega leta od objave te odločbe v Uradnem listu Republike Slovenije.**
- 4. Tretji in sedmi odstavek 148. člena ter 149.č člen Zakona o kazenskem postopku niso v neskladju z Ustavo.**

OBRAZLOŽITEV

A.

1. Skupina poslancev Državnega zbora (v nadaljevanju predlagatelj) poleg druge povedi prvega odstavka 216. člena in 150.a člena Zakona o kazenskem postopku (v nadaljevanju ZKP) izpodbija tudi tretji in sedmi odstavek 148. člena ter 149.b, 149.c, 149.č in 156. člen ZKP.¹

¹ Predlagatelj izpodbija sicer določbe Zakona o kazenskem postopku (Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14, 66/17 in 22/19 – v nadaljevanju ZKP/19), vendar je bil izpodbijani zakon v času odločanja Ustavnega sodišča spremenjen z Zakonom o

2. Tretji odstavek 148. člena ZKP naj bi bil v neskladju z načelom jasnosti in pomenske določljivosti iz 2. člena Ustave in s pravico do enakega varstva pravic iz 22. člena Ustave. Sporna naj bi bila določba, po kateri policija vabi k sebi osebe zaradi zbiranja obvestil in podatkov ter zaslišanja. Pri elektronskem vabilu naj bi bili sporni njegova pristnost in informacijska varnost, pri ustnem in telefonskem vabilu pa odsotnost fizičnega dokazila o vabljenju, in sicer zaradi dokazovanja obstoja, pravilnosti, učinka vabljenja ter istovetnosti vabljenih oseb. Ker naj izpodbijana določba razen glede možnosti prisilne privedbe ne bi razlikovala med različnimi načini vabljenja, naj bi bila v neskladju s pravico do enakega varstva pravic iz 22. člena Ustave.

3. Sedmi odstavek 148. člena ZKP naj bi omogočal različne razlage, ker naj ne bi spreminjal dotedanje ureditve upravičencev za vložitev pritožbe in pritožbenih razlogov, ker naj bi vseboval določbe pedagoške narave in ker naj ne bi konkretiziral ukrepov državnega tožilca na podlagi pritožbe. Zato naj bi bil v neskladju z načelom pravne države (2. člen Ustave).

4. Predlagatelj izpodbija tudi 149.b člen ZKP. Ta naj bi bil v neskladju z načelom jasnosti in pomenske določljivosti, ker naj ne bi določal pomena relevantnega podatka iz prvega odstavka in relevantnega obdobja iz drugega odstavka 149.b člena ZKP. Zato naj bi bila prvi in drugi odstavek 149.b člena ZKP notranje neskladna. Prav tako naj ne bi bil jasen rok prepovedi seznanitve posameznika z izvršitvijo ukrepa po četrtem odstavku 149.b člena ZKP v primeru podaljšanega tega roka. Popolna diskrecija preiskovalnega sodnika pri določitvi tega obdobja naj bi pomenila kršitev načela pravne države (2. člen Ustave), enakosti pred zakonom (14. člen Ustave), enakega varstva pravic (22. člen Ustave) in pravice do sodnega varstva (23. člen Ustave). Izpodbijana določba naj bi pomenila tudi nesorazmeren poseg v komunikacijsko zasebnost, ker naj ne bi določala dopustnega cilja za razlikovanje med različnimi dokaznimi standardi za prikrite preiskovalne ukrepe. Omogočala naj bi namreč, da se ukrep iz prvega odstavka 149.b člena ZKP izvrši tudi zoper osebe iz drugega odstavka 149.a člena ZKP, pri čemer naj bi bil za ukrep iz 149.a člena ZKP določen višji standard (utemeljeni razlogi za sum) kot za izvedbo ukrepa po 149.b členu ZKP (razlogi za sum). Posledično taka ureditev vodi v nesorazmerno izvrševanje ukrepov, kar naj bi bilo v neskladju s 15. členom Ustave.

5. Tudi izpodbijani 149.c člen ZKP naj bi bil v neskladju z načelom jasnosti in pomenske določljivosti. Nejasno naj bi bilo, kateri pogoj iz prvega odstavka 149.c člena ZKP naj bi bil nadomeščen s pogojem "ali že zakoniti uporabnik komunikacijskega sredstva s tem soglaša" in kakšni so razlogi in postopek za podaljšanje ukrepa. Ker naj bi bili za ukrep določeni zgolj razlogi za sum, naj bi bilo posledično arbitrarno odločanje preiskovalnega sodnika v neskladju z 2. členom Ustave, z načelom enakosti pred

spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 200/20 – ZKP-O), ki pa izpodbijanih določb vsebinsko ni spremenil.

zakonom (14. člen Ustave) in enakim varstvom pravic (22. člen Ustave) ter s pravico do sodnega varstva (23. člen Ustave), ureditev pa naj bi bila nesorazmerna.

6. V zvezi s 149.č členom ZKP predlagatelj zatrjuje, da je ureditev postopka preverjanja zakonitosti zahteve za posredovanje podatkov po drugem odstavku 149.č člena ZKP nejasna. V zvezi s tem izpostavlja opredelitev naročniških podatkov in razlogov za sprožitev postopka. Sodna presoja naj bi bila zgolj navidezna, zato naj bi bila ureditev v neskladju z 2., 14., 22. in 23. členom Ustave.

7. Peti odstavek 156. člena ZKP naj ne bi zagotavljal ustreznega sodnega varstva in kontrole, ker naj bi bančne podatke pisno zahteval državni tožilec ali policija. Ureditev naj bi bila tudi v neskladju z 2. in 14. členom Ustave, ker naj bi preiskovalni sodnik po šestem odstavku 156. člena ZKP lahko z odredbo spremenil rok za prepoved razkritja pridobitve teh podatkov.

8. Zahteva je bila na podlagi prvega odstavka 28. člena Zakona o Ustavnem sodišču (Uradni list RS, št. 64/07 – uradno prečiščeno besedilo, 109/12, 23/20 in 92/21 – v nadaljevanju ZUstS) poslana Državnemu zboru, ki nanjo ni odgovoril.

9. Svoje mnenje je poslala Vlada, ki je navedla, da predlagatelj ponavlja argumente iz zakonodajnega postopka, na katere naj bi bilo že odgovorjeno. Spremenjeni tretji odstavek 148. člena ZKP naj bi natančneje urejal vabljenje po policiji v predkazenskem postopku, kot naj bi že potekalo v praksi na podlagi 35. člena Zakona o nalogah in pooblastilih policije (Uradni list RS, št. 15/13, 23/15 – popr., 10/17 in 47/19 – v nadaljevanju ZNPPol), tj. ustno, telefonsko in elektronsko. Prisilna privedba naj bi bila predvidena le ob predhodnem pravnem pouku v pisnem vabilu. Ureditev naj bi bila jasnejša in določnejša. Nova ureditev naj bi olajšala delo policije v primeru prostovoljnega sodelovanja oseb, sledljivost vabljenja naj bi bila zagotovljena z uradnim zaznamkom, čeprav naj ne bi bila bistvena zaradi odsotnosti negativnih posledic za vabljenega.

10. Sedmi odstavek 148. člena ZKP naj bi bil bolj določen in jasen, saj naj bi na novo določal rok, v katerem mora državni tožilec obvestiti pritožnika o sprejetih ukrepih, s tem pa naj bi bil posredno določen tudi rok za ukrepanje tožilca. Določba naj bi tudi odpravljala nejasnost, ali je zoper obvestilo državnega tožilca dovoljeno posebno pravno sredstvo. Državni tožilec naj bi ukrepal zlasti v okviru svojega splošnega pooblastila za usmerjanje policije v (pred)kazenskem postopku, s čimer naj bi bila opravljena tudi razmejitev pritožbe od drugih oblik nadzora nad delom policije (na primer pritožbe zoper delo policistov po IV. poglavju ZNPPol).

11. Namen spremenjenih 149.b, 149.c in 149.č člena ZKP naj bi bila jasna razmejitev med naročniškimi podatki, ki jih lahko pridobita državno tožilstvo in policija sama, in prometnimi podatki, za katere je potreba sodna odredba, ob upoštevanju ustaljene ustavnosodne presoje (zlasti odločbe Ustavnega sodišča št. U-I-65/13 z dne 3. 7. 2014,

Uradni list RS, št. 54/14, in OdlUS XX, 27), prakse Sodišča Evropske unije (v nadaljevanju SEU) in Evropskega sodišča za človekove pravice (v nadaljevanju ESČP), načela sorazmernosti ter zahteve po niansiranem pristopu k posegom v človekove pravice. Ukrep iz dotedanega prvega odstavka 149.b člena ZKP (pridobivanje prometnih podatkov za nazaj) naj bi bil po Zakonu o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 22/19 – v nadaljevanju ZKP-N) podrobneje urejen v novem 149.b členu. Dostop do podatkov naj bi bil vezan na ožji katalog kaznivih dejanj ter oblikovan na podlagi teže in narave kaznivih dejanj. Dodatno naj bi zavezoval tudi ponudnike drugih komunikacijskih storitev po Zakonu o elektronskem poslovanju na trgu (Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15 – v nadaljevanju ZEPT), s čimer naj bi se odpravile nejasnosti iz prakse. Dokazni standard naj bi ostal enak (razlogi za sum). Glede razlogov v zvezi s tem se Vlada sklicuje na zahtevo Državnega sveta v zadevi št. U-I-88/16, poleg tega naj utemeljen sum ne bi bil določen niti za bolj invazivne prikrite preiskovalne ukrepe, taka zahteva pa naj ne bi izhajala niti iz ustaljene ustavnosodne presoje. Previsoko zastavljen prag za dokazni standard naj bi tudi onemogočil učinkovit kazenski pregon (2. in 135. člen Ustave). Obdobje, v katerem ponudnik storitev tretji osebi ne sme razkriti, da je posredoval podatke, naj bi bilo jasno določeno; sodnik naj bi glede na okoliščine konkretnega primera opravil tehtanje med pravico posameznika do seznanitve z obdelavo njegovih osebnih podatkov in interesom tajnosti predkazenskega postopka, določil dolžino roka ter odločitev obrazložil.

12. Ukrep iz 149.c člena ZKP, ki naj bi se izvajal za naprej, naj bi bil bolj osredotočen in manj invaziven, zato naj bi bil zanj ob upoštevanju načela sorazmernosti določen širši katalog kaznivih dejanj. Tudi ta ukrep naj bi zavezoval ponudnike storitev po ZEPT. Dokazni standard naj bi bil enak kot v dotedanjem 149.b členu Zakona o kazenskem postopku (Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14 in 66/17 – v nadaljevanju ZKP/17). Vlada ga utemeljuje z enakimi argumenti kot dokazni standard v 149.b členu ZKP. Pogoj "če zakoniti uporabnik s tem soglaša" iz prvega odstavka 149.c člena ZKP naj bi nadomeščal pogoj "za katerega je predpisana kazen enega ali več let zapora", saj naj bi navezava na kaznivo dejanje morala obstajati v vsakem primeru. S tem naj bi bila odreditev ukrepa možna tudi pri lažjih kaznivih dejanjih, kar naj bi bilo razvidno tudi iz predloga zakona.

13. Člen 149č ZKP, ki naj bi nastal iz tretjega odstavka 149.b člena ZKP/17, naj bi pomenil implementacijo sodbe ESČP v zadevi *Benedik proti Sloveniji* z dne 24. 4. 2018. Drugi odstavek tega člena naj bi urejal situacijo, ko operater oceni, da bi ravnal nezakonito, če bi sledil zahtevi policije ali državnega tožilstva. V tem primeru naj bi se mu nudila dodatna varovalka, ne pa zaveza, da podatke namesto policiji in državnemu tožilstvu posreduje sodišču, ki opravi sodno presojo zakonitosti ukrepa. Z namenom večje jasnosti in določnosti določbe naj bi državni tožilec, ki usmerja policijo, pridobil pooblastila, ki naj bi jih do sedaj imela policija.

14. Predlagatelj naj svojih očitkov glede 156. člena ZKP ne bi konkretiziral. Namen izpodbijane ureditve naj bi bilo razlikovanje med podatki, ki jih lahko državni tožilec in policija pridobita sama po petem odstavku in ki naj ne bi bili podatki o premoženjskem stanju osumljenca, o stanju vlog in depozitov ter o stanju in prometu na računih oziroma v denarnici virtualne valute, in podatki, za katere je po prvem odstavku tega člena potrebna sodna odredba. Razširjen naj bi bil tudi seznam subjektov, ki so zavezani posredovati podatke, poleg tega naj bi tudi pri tem ukrepu državni tožilec, ki usmerja policijo, pridobil pooblastila, ki naj bi jih do sedaj imela policija.

15. Ustavno sodišče je mnenje Vlade poslalo predlagatelju, ki nanj ni odgovoril.

16. Na podlagi 5. člena ZUstS je Ustavno sodišče zaprosilo Banko Slovenije in Agencijo Republike Slovenije za javnopravne evidence in storitve (v nadaljevanju AJ PES) za mnenje, ali so podatki iz petega odstavka 156. člena ZKP objavljeni v registru transakcijskih računov (v nadaljevanju RTR) na podlagi 192. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (Uradni list RS, št. 7/18, 9/18 – popr. in 102/20 – v nadaljevanju ZPlaSSIED) ter javno dostopni v mejah 194. člena ZPlaSSIED. Banko Slovenije pa je zaprosilo še za podatek, ali je kateri izmed navedenih podatkov objavljen v katerem drugem registru in javno dostopen.

17. Banka Slovenije je odgovorila, da se v RTR v skladu s 192. členom ZPlaSSIED vodijo podatki v zvezi s transakcijskimi računi, ki jih vodijo banke in hranilnice s sedežem v Republiki Sloveniji (podatki o imetniku, pooblaščenca, dejanskem lastniku imetnika in transakcijskem računu), ter v zvezi s sefi, ki jih oddajajo banke in hranilnice s sedežem v Republiki Sloveniji. Transakcijski račun naj bi bil podvrsta plačilnega računa, ki ga vodi banka in hranilnica s sedežem v Republiki Sloveniji, med transakcijske račune pa naj ne bi spadali plačilni računi, ki jih vodijo nebančni ponudniki plačilnih storitev (plačilne institucije in družbe za izdajo elektronskega denarja) s sedežem v Republiki Sloveniji, in vsi plačilni računi, ki jih slovenskim državljanom vodijo ponudniki plačilnih storitev s sedežem izven Republike Slovenije. Teh podatkov naj ne bi bilo v RTR. Tudi podatki glede hranilnih vlog, denarnic za hrambo virtualnih valut in denarnih depozitov naj se v RTR ne bi vodili. Banka Slovenije naj bi bila sicer pristojna za vzpostavitev in upravljanje centralnega kreditnega registra na podlagi Zakona o centralnem kreditnem registru (Uradni list RS, št. 77/16 – v nadaljevanju ZCKR), v katerem naj se tudi ne bi vodili podatki glede hranilnih vlog oziroma denarnih depozitov. Tudi sicer pa naj zbirki po ZCKR ne bi bili javni, ampak naj bi pomenili poslovno skrivnost in naj bi vsebovali zaupne podatke, ki naj bi se lahko razkrili samo v zakonsko dopustnih primerih (11., 12. in 20. člen ZCKR). Na podlagi Zakona o preprečevanju pranja denarja in financiranja terorizma (Uradni list RS, št. 48/22 in 145/22 – v nadaljevanju ZPPDFT-2) pa naj bi bil pri Uradu Republike Slovenije za preprečevanje pranja denarja vzpostavljen register ponudnikov storitev virtualnih valut (5. člen ZPPDFT-2), vendar naj se tudi v njem ne bi vodili podatki o denarnicah za hrambo virtualnih valut.

18. AJPES je podobno pojasnila, da se podatki o imetniku transakcijskega računa ter datumu odprtja in zaprtja transakcijskega računa v RTR vodijo že od vzpostavitve RTR (tj. od 1. 7. 2010). Pred tem naj bi se ti podatki vodili na Banki Slovenije, od katere naj bi AJPES prevzela RTR. Po devetem odstavku 192. člena ZPlaSSIED naj bi se podatek o transakcijskem računu izbrisal iz RTR pet let po zaprtju transakcijskega računa. Podatki o pooblaščenцу imetnika transakcijskega računa ter podatki o sefu (njegovem najemniku in trajanju najema) pa naj bi se v RTR vodili od 6. 11. 2021. Navedeni podatki naj bi bili javno dostopni v mejah 194. člena ZPlaSSIED. Podatki o hranilnih vlogah, denarnicah za hrambo virtualne valute ali denarnega depozita ter o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo naj se v RTR ne bi vodili, saj naj 192. člen ZPlaSSIED tega ne bi določal.

19. Odgovora Banke Slovenije in AJPES je Ustavno sodišče poslalo predlagatelju in Državnemu zboru, ki nanju nista odgovorila.

20. Vlada na pojasnila Banke Slovenije ni imela pripomb. Izpostavila pa je, da se lahko AJPES z drugimi državnimi organi, ki so na podlagi posebnega zakona upravičeni za pridobitev podatkov iz registra, dogovori za neposreden elektronski dostop do podatkov iz RTR (peti odstavek 195. člena ZPlaSSIED). Nabor podatkov, do katerih naj bi policija lahko neposredno dostopala v RTR, naj ne bi smel biti širši od nabora podatkov, do katerega naj bi imela policija pravico dostopati na podlagi 156. člena ZKP. Zato naj bi bilo treba ob naslednji spremembi ZKP v njegovem 156. členu jasno določiti možnost neposrednega dostopa do podatkov iz RTR.

21. Mnenje Vlade je Ustavno sodišče poslalo predlagatelju, ki nanj ni odgovoril.

B. – I.

22. Ustavno sodišče je o delu zahteve, ki se nanaša na oceno ustavnosti druge povedi prvega odstavka 216. člena, že odločilo z delno odločbo št. U-I-144/19 z dne 17. 2. 2022 (Uradni list RS, št. 35/22), o delu zahteve, ki se nanaša na oceno ustavnosti 150.a člena ZKP, pa z delno odločbo št. U-I-144/19 z dne 1. 12. 2022 (Uradni list RS, št. 2/23). Ocenilo je, da je zahteva tudi v delu, ki se nanaša na tretji in sedmi odstavek 148. člena ter 149.b, 149.c in 149.č člen ter peti in šesti odstavek 156. člena ZKP, zrela za odločitev. Na podlagi prvega odstavka 6. člena ZUstS in ob smiselni uporabi prvega odstavka 314. člena Zakona o pravnem postopku (Uradni list RS, št. 73/07 – uradno prečiščeno besedilo, 45/08 in 10/17 – ZPP) je odločilo, da bo o tem delu zahteve izdalo delno odločbo.

B. – II.

Izpodbijani 149.b člen ZKP

23. Izpodbijani 149.b člen ZKP določa:

"(1) Če so podani razlogi za sum, da je bilo izvršeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje iz četrtega odstavka prejšnjega člena in je za odkritje, preprečitev ali dokazovanje tega kaznivega dejanja ali odkritje storilca treba pridobiti podatke o prometu v zvezi s komunikacijo osumljenca, oškodovanca ali oseb iz drugega odstavka prejšnjega člena, lahko preiskovalni sodnik na obrazložen predlog državnega tožilca odredi operaterju oziroma ponudniku storitev informacijske družbe, da pristojnemu organu sporoči relevantne podatke v zvezi z omenjeno komunikacijo, ki obstajajo v času izdaje odredbe. Preiskovalni sodnik v odredbi opredeli kategorije podatkov, ki jih zahteva. Odredba se operaterju oziroma ponudniku storitev informacijske družbe vroča v delu, ki se nanaša nanj.

(2) Predlog in odredba morata biti pisna in morata vsebovati podatke, ki omogočajo enolično identifikacijo komunikacijskega sredstva ali uporabnika, utemeljitev razlogov, relevantno časovno obdobje, za katerega se podatki zahtevajo, ostale pomembne okoliščine, ki narekujejo uporabo ukrepa, ter ustrezen rok za izvršitev. Identifikacija komunikacijskega sredstva mora biti dovolj natančna, da zahtevke omejuje na vnaprej omejen in določljiv seznam oseb.

(3) Izjemoma, če pisne odredbe ni mogoče pravočasno pridobiti in če obstaja nevarnost, da bi zaradi odlašanja bilo ogroženo življenje ali zdravje ljudi, lahko preiskovalni sodnik na ustni predlog državnega tožilca odredi izvršitev ukrepa iz prvega odstavka tega člena z ustno odredbo neposredno operaterju oziroma ponudniku storitev informacijske družbe. O ustnem predlogu državnega tožilca preiskovalni sodnik napravi uradni zaznamek. Pisna odredba mora biti izdana najkasneje v 12 urah po izdaji ustne odredbe. Če se med izdelavo pisnega odpravka izkaže, da izrečeni ukrep ni bil upravičen, se postopa po četrtem odstavku 154. člena tega zakona.

(4) Operater oziroma ponudnik storitev informacijske družbe svojemu uporabniku, naročniku ali tretjim osebam ne sme razkriti, da je ali da bo v skladu s tem členom posredoval določene podatke. Tega ne sme razkriti 24 mesecev po preteku meseca, v katerem se je zaključilo izvrševanje odredbe. Preiskovalni sodnik lahko z odredbo določi drugačen rok, rok podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok skrajša ali prepoved seznanitve odpravi.

(5) Na podlagi tega člena ni mogoče zahtevati ali pridobiti podatkov, ki se nanašajo na vsebino komunikacije."

24. V 149.b členu ZKP je urejena pridobitev podatkov o okoliščinah komunikacije od operaterjev in ponudnikov storitev informacijske družbe za nazaj, tj. pridobitev tistih podatkov, ki pri operaterjih in ponudnikih storitev informacijske družbe obstajajo v trenutku sodne odredbe za njihovo pridobitev na podlagi zakonite pravne podlage. Prvi odstavek 149.b člena ZKP ureja pogoje za pridobitev teh podatkov, drugi vsebino

predloga in odredbe, tretji pogoje za izdajo ustne odredbe, četrti prepoved razkritja posredovanja podatkov uporabniku ali tretjim osebam, peti odstavek pa izrecno prepoved pridobitve vsebine komunikacije.

25. Ukrep pridobitve navedenih podatkov od operaterjev je bil prvič urejen z Zakonom o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 43/04 – v nadaljevanju ZKP-F) skupaj s celovito ureditvijo prikritih preiskovalnih ukrepov na podlagi odločb Ustavnega sodišča o prikritih preiskovalnih ukrepih.² ZKP-N je izpodbijano določbo v bistvenem prenovil, tudi v delu, ki ga izpodbija predlagatelj, in sicer s ciljem, da jasno, določno in v skladu s presojo Ustavnega sodišča ter prakso ESČP in SEU uredi ta ukrep, hkrati pa krepí učinkovitost dela policije in državnega tožilstva pri odkrivanju in preiskovanju zahtevnejših oziroma hujših kaznivih dejanj ter pregonu storilcev.³

26. Glede podatkov, ki jih je z ukrepom mogoče pridobiti, je mogoče ugotoviti, da je ZKP/17 vseboval splošno opredelitev podatkov o okoliščinah komunikacije, poleg tega pa je tudi primeroma našteval nekatere take podatke.⁴ ZKP pa podatkov ne našteva več primeroma⁵ in v zvezi z njimi zgolj splošno določa, da se po prvem odstavku 149.b

² Glej odločbe Ustavnega sodišča št. U-I-25/95 z dne 27. 11. 1997 (Uradni list RS, št. 5/98, in OdlUS VI, 158), št. U-I-158/95 z dne 2. 4. 1998 (Uradni list RS, št. 31/98, in OdlUS VII, 56) in št. U-I-272/98 z dne 8. 5. 2003 (Uradni list RS, št. 48/03, in OdlUS XII, 42).

³ Vlada Republike Slovenije, Predlog zakona o spremembah in dopolnitvah Zakona o kazenskem postopku – ZKP-N z dne 4. 2. 2019, EPA: 398 – VIII (v nadaljevanju Predlog ZKP-N), str. 2, 8, 23, 24, 142.

⁴ Prvi odstavek 149.b člena ZKP/17 je našteval podatke o udeležencih, okoliščinah in dejstvih elektronskega komunikacijskega prometa, kot so številka ali druga oblika identifikacije uporabnikov elektronskih komunikacijskih storitev, vrsta, datum, čas in trajanje klica oziroma druge elektronske komunikacijske storitve, količina prenesenih podatkov in kraj, iz katerega je bila elektronska komunikacijska storitev opravljena.

⁵ Iz teorije in sodne prakse sicer izhaja, da naj bi podatki po prvem odstavku 149.b člena ZKP vsebovali podatke o partnerjih, času in trajanju komunikacije; podatke, ki naj bi nakazovali izvor (telefonska številka, IP-naslov ali podobna identifikacija komunikacijske enote, ki jo ponudnik storitev nudi), cilj (destinacija, ki ji je komunikacija namenjena), pot, čas, datum, obseg, trajanje ali vrsto storitve (prenos podatkov, elektronska pošta itd.); tudi t. i. derivativne naročniške podatke, do katerih je mogoče priti zgolj z obdelavo prometnih podatkov. Glej A. Lesjak v: M. Avbelj (ur.), Komentar Ustave Republike Slovenije, Del 1: Človekove pravice in temeljne svoboščine, Nova univerza, Evropska pravna fakulteta, Ljubljana 2019, str. 358; J. A. Tabaković, Prikriti preiskovalni ukrepi po ZKP-N, Pravna praksa, št. 28–29 (2019), str. 12; G. Klemenčič v: L. Šturm (ur.), Komentar Ustave Republike Slovenije – dopolnitev A, Fakulteta za državne in evropske študije, Ljubljana, 2011, str. 531; P. Plesec, Preiskovalna dejanja in ukrepi, v: P. Plesec, P. Gorkič (ur.), Uvodna pojasnila k ZKP-N, Uradni list Republike Slovenije, Ljubljana 2019, str. 32. Glej tudi sodbo SEU v združenih zadevah *Digital Rights Ireland Ltd proti*

člena lahko pridobijo podatki o prometu v zvezi s komunikacijo, da se sporočijo relevantni podatki v zvezi z omenjeno komunikacijo določenih oseb, ki obstajajo v času izdaje odredbe, preiskovalni sodnik pa v odredbi opredeli kategorije podatkov, ki jih zahteva.

27. Pridobiti je mogoče navedene podatke vnaprej omejenega in določljivega kroga oseb prek enolično⁶ določenega komunikacijskega sredstva (drugi odstavek 149.b člena ZKP/19), tj. prometne podatke.⁷

28. Zakon o elektronskih komunikacijah (Uradni list RS, št. 130/22 – v nadaljevanju ZEKom-2) vsebinsko opredeljuje prometne podatke.⁸ Določa, da se zaupnost komunikacij nanaša tudi na podatke o prometu, ki so katerikoli podatki, obdelani za namen prenosa komunikacije⁹ po elektronskem komunikacijskem omrežju ali zaradi njegovega zaračunavanja.¹⁰ Po 3. točki prvega odstavka 2. člena ZEPT pa se ZEPT, ki ureja ponudnike storitev informacijske družbe, ne uporablja za vprašanja, povezana s storitvami informacijske družbe v zvezi z varstvom osebnih podatkov, za katere se tudi uporablja zakon, ki ureja varstvo osebnih podatkov, ali zakon, ki ureja elektronske komunikacije. Posledično je mogoče po prvem odstavku 149.b člena ZKP pridobiti tudi

Minister for Communications, Marine and Natural Resources in drugim ter Kärntner Landesregierung in drugi, C-293/12 in C-594/12, z dne 8. 4. 2014, 26. točka obrazložitve.

⁶ SSKJ določa: "ênolíčen -čna -o prid. (ē-ī) mat. ki ima eno samo vrednost, en sam pomen".

⁷ Predlog ZKP-N, str. 8; P. Gorkič, Hramba in obdelovanje prometnih podatkov za namene kazenskega postopka po razveljavitvi ZEKom-1, Pravna praksa št. 33 (2014), str. 8; sodba Vrhovnega sodišča št. I Ips 31751/2018 z dne 4. 6. 2020.

⁸ Prvi odstavek 214. člena ZEKom-2. Glej tudi G. Klemenčič, v: L. Šturm (ur.), Komentar Ustave Republike Slovenije, Fakulteta za podiplomske državne in evropske študije, Ljubljana 2002, str. 396; A. Lesjak v: M. Avbelj (ur.), nav. delo, str. 358; G. Klemenčič v: L. Šturm (ur.), nav. delo, 2011, str. 522–523. Podobno je bila določena tudi opredelitev prometnih podatkov v času sprejemanja ZKP-F, in sicer v Zakonu o elektronskih komunikacijah (Uradni list RS, št. 13/07 – uradno prečiščeno besedilo, 110/09 in 33/11 – v nadaljevanju ZEKom) in Zakonu o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 81/15 in 40/17 – v nadaljevanju ZEKom-1).

⁹ Komunikacija je vsaka informacija, ki se izmenja ali prenese med končnim številom strank s pomočjo javno dostopne elektronske komunikacijske storitve. Ne vključuje pa informacij, ki so javnosti prenesene kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da informacija povezati s prepoznavnim naročnikom ali uporabnikom, ki jo prejme. Glej 30. točko 3. člena ZEKom-2; K. Šugman Stubbs, P. Gorkič, Dokazovanje v kazenskem postopku, GV Založba, Ljubljana 2011, str. 166; P. Gorkič, Načelo sorazmernosti in odločanje o pridobivanju prometnih podatkov, Pravosodni bilten, št. 3 (2015), str. 10.

¹⁰ Glej 55. točko 3. člena ZEKom-2 in 45. točko 3. člena ZEKom-1. Po ZEKom pa so bili prometni podatki opredeljeni s splošno definicijo in tudi primeroma naštetimi (25. točka 3. člena ZEKom).

podatke o prometu po ZEPT, tj. katerekoli podatke, obdelane za opravljanje storitev informacijske družbe ali zaradi njenega zaračunavanja.¹¹

29. Iz teorije je mogoče razbrati, da ZKP, drugače kot ZEKom-2, ne govori o podatkih o prometu, ki se obdelujejo zaradi prenosa komunikacij ali njihovega zaračunavanja,¹² ampak o relevantnih podatkih, med katere spadajo vsi podatki, s katerimi je mogoče ugotoviti, med katerima komunikacijskima sredstvoma je komunikacija potekala, kakšno sredstvo za komunikacijo je bilo uporabljeno, kdaj in kje je komunikacija potekala, kako pogosto je potekala in ali je bila uspešna. Gre za metapodatke, tj. podatke, ki so ustvarjeni ob pošiljanju, razširjanju ali izmenjevanju vsebine in se lahko uporabijo za določitev vira in cilja komunikacije, njene lokacije, časovnih okoliščin in vrste.¹³ Z navedenim ukrepom ni mogoče pridobiti podatkov, ki se nanašajo na vsebino komunikacije,¹⁴ ali lokacijskih podatkov, ki se ne nanašajo na konkretno komunikacijo.¹⁵ Člen 149b ZKP tudi ne ureja pridobivanja naročniških podatkov (podatkov o lastniku ali uporabniku določenega komunikacijskega sredstva ali storitve informacijske družbe) ali obstoju in vsebini njegovega pogodbenega razmerja z operaterjem oziroma ponudnikom storitev informacijske družbe v zvezi z opravljanjem komunikacijske dejavnosti ali storitev informacijske družbe (novi 149.č člen ZKP).¹⁶

30. Navedeni podatki se lahko nanašajo na osumljenca, oškodovanca in osebe iz drugega odstavka 149.a člena ZKP.¹⁷ Za zadnjo kategorijo oseb je ukrep mogoče odrediti, če je mogoče utemeljeno sklepati, da bi pridobitev podatkov od te osebe privedla do identifikacije osumljenca,¹⁸ čigar osebni podatki niso znani, do prebivališča

¹¹ Storitve informacijske družbe vključujejo zlasti prodajo blaga ali storitev, dostop do podatkov ali oglaševanje na svetovnem spletu ter dostop do komunikacijskega omrežja, prenos podatkov ali shranjevanje prejemnikovih podatkov v komunikacijskem omrežju (11. točka 3. člena ZEPT).

¹² Glej 55. točko 3. člena ZEKom-2 in 45. točko 3. člena ZEKom-1.

¹³ P. Križnar v: M. Šepeč (ur.), Komentar Zakona o kazenskem postopku, GV Založba, Ljubljana 2023, str. 847; K. Šugman Stubbs, P. Gorkič, nav. delo, str. 166.

¹⁴ Peti odstavek 149.b člena ZKP izrecno določa: "Na podlagi tega člena ni mogoče zahtevati ali pridobiti podatkov, ki se nanašajo na vsebino komunikacije." Glej tudi M. Žaucer, Prikriti preiskovalni ukrepi v noveli ZKP-N, Zbornik Konference kazenskega prava in kriminologije (2016), str. 62.

¹⁵ Točka 54 3. člena ZEKom-2. Glej tudi prvi odstavek 214. člena ZEKom-2 in K. Šugman Stubbs, P. Gorkič, nav. delo, str. 166.

¹⁶ Predlog ZKP-N, str. 9, 145; P. Plešec, nav. delo, str. 36–37. Glej 173.–179. točko obrazložitve te odločbe glede ustavnoskladne razlage naročniških podatkov.

¹⁷ ZKP/17 ni določal take izrecne omejitve. P. Gorkič, Novela ZKP-N: prenova Zakona o kazenskem postopku?, Odvetnik, št. 2 (2017), str. 39.

¹⁸ Osumljenec iz prvega odstavka 149.a člena ZKP je opredeljen ožje kot v splošni definiciji osumljenca iz 144. člena ZKP. Zajema namreč samo osumljence določenih težjih kaznivih dejanj ("če obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, izvršuje ali

ali lokacije, kjer je ta osumljenec, oziroma do prebivališča ali lokacije, kjer je oseba, zoper katero je bil odrejen pripor, hišni pripor, tiralica ali odredba za privedbo, pa je pobegnila ali se skriva, in policisti z drugimi ukrepi teh podatkov ne morejo pridobiti oziroma bi bilo to povezano z nesorazmernimi težavami.¹⁹

Pravica do komunikacijske zasebnosti

31. Predlagatelj sicer izrecno izpodbija dokazni standard iz prvega odstavka 149.b člena ZKP in s tem sorazmernost ureditve le v zvezi z osebami iz četrtega odstavka 149.a člena ZKP. Vendar iz predlagateljeve vloge izhaja, da nasprotuje sorazmernosti ureditve ukrepa iz 149.b člena ZKP v splošnem, zato se Ustavno sodišče ni omejilo na presojo izpodbijanega ukrepa le s tega vidika, ampak je presojalo, ali pomeni ureditev ukrepa iz prvega odstavka 149.b člena ZKP nesorazmeren poseg v pravico do komunikacijske zasebnosti iz prvega odstavka 37. člena Ustave.

32. V skladu s prvim odstavkom 37. člena Ustave je zagotovljena tajnost pisem in drugih občil. Del zasebnosti, ki se nanaša na svobodo komuniciranja, Ustava varuje dvakrat: v 35. členu, v katerem postavi splošno pravilo, da ima vsakdo pravico do zasebnosti in da je zasebnost nedotakljiva, in še posebej v prvem odstavku 37. člena, s katerim je zagotovljena tajnost pisem in drugih občil.²⁰ S tem odstavkom Ustava zagotavlja svobodno in nenadzorovano komunikacijo ter zaupnost razmerij, v katera pri sporočanju vstopa posameznik. Poseg v svobodo komuniciranja je dopusten pod pogoji iz drugega odstavka 37. člena Ustave, če: 1) je določen v zakonu, 2) ga z odločbo dovoli sodišče, 3) je določno omejen čas njegovega izvajanja in 4) je nujen za uvedbo ali potek kazenskega postopka ali za varnost države.²¹

33. Pravico do komunikacijske zasebnosti opredelujeta v okviru pravice do spoštovanja zasebnega in družinskega življenja tudi Konvencija o varstvu človekovih pravic in temeljnih svoboščin (Uradni list RS, št. 33/94, MP, št. 7/94 – v nadaljevanju

pripravlja oziroma organizira izvršitev katerega izmed kaznivih dejanj, navedenih v četrtem odstavku 149.a ZKP").

¹⁹ Prvi in drugi odstavek 149.a člena ZKP. Drugi odstavek 149.a člena ZKP implementira Konvencijo o izvajanju schengenskega sporazuma z dne 14. junija 1985 med vladami držav Gospodarske unije Beneluks, Zvezne republike Nemčije in Francoske republike o postopni odpravi kontrol na skupnih mejah (UL L 239, 22. 9. 2000, str. 19–62), kar pa ne velja tudi za prevzem iste kategorije oseb v prvi odstavku 149.b člena ZKP. Predlog zakona o spremembah in dopolnitvah Zakona o kazenskem postopku – ZKP-F z dne 12. 3. 2004, str. 24. Glej tudi Predlog ZKP-N, str. 10–11.

²⁰ Prim. odločbi Ustavnega sodišča št. U-I-25/95 in št. Up-540/11 z dne 13. 2. 2014 (Uradni list RS, št. 20/14, in OdlUS XX, 33), 9. točka obrazložitve.

²¹ Prav tam.

EKČP) v 8. členu²² in Mednarodni pakt o državljanskih in političnih pravicah (Uradni list SFRJ, št. 7/71, in Uradni list RS, št. 35/92, MP, št. 9/92 – v nadaljevanju MPDPP) v 17. členu.²³

34. Pri presoji, katero človekovo delovanje spada v ustavno varovano polje zasebnosti, Ustavno sodišče uporablja t. i. doktrino upravičeno pričakovane zasebnosti,²⁴ ki velja tudi glede komunikacijske zasebnosti. Predmet varstva prvega odstavka 37. člena Ustave je tako tista komunikacija, za katero posameznik upravičeno pričakuje zasebnost in to jasno izkaže navzven.²⁵ Pravica do komunikacijske zasebnosti iz prvega odstavka 37. člena Ustave v prvi vrsti varuje vsebino posredovanega sporočila. Zagotavlja tako varstvo posameznikovega interesa, da se brez njegove privolitve nihče ne seznanja z vsebino sporočila, ki ga posreduje prek kateregakoli sredstva, ki omogoča izmenjavo oziroma posredovanje informacij, kot tudi interes posameznika, da svobodno odloča o tem, komu, v kolikšnem obsegu, na kakšen način in pod kakšnimi pogoji bo določeno sporočilo posredoval.²⁶

35. Poleg vsebine sporočila so varovani tudi okoliščine in dejstva, povezani s komunikacijo, tj. tisti podatki o komunikaciji, ki so njen sestavni del – prometni podatki.²⁷ Kot pojasnjeno, so podatki o prometu kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega

²² EKČP v 8. členu določa: "1. Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. 2. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi."

²³ MPDPP v 17. členu določa: "1. Nikomur se ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v družino, v stanovanje ali dopisovanje ali nezakonito napadati njegovo čast in ugled. 2. Vsakdo ima pravico do zakonskega varstva pred takim vmešavanjem ali pred takimi napadi." Listina Evropske unije o temeljnih pravicah (UL C 202, 7. 6. 2016 – v nadaljevanju Listina) v 7. členu določa pravico vsakogar do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij.

²⁴ Prim. odločbi Ustavnega sodišča št. U-I-25/95, 38. točka obrazložitve, in št. U-I-272/98, 20. točka obrazložitve.

²⁵ Tako odločbi Ustavnega sodišča št. Up-540/11, 14. točka obrazložitve, in št. Up-979/15 z dne 21. 6. 2018 (Uradni list RS, št. 54/18, in OdlUS XXIII, 26), 18. točka obrazložitve.

²⁶ Podobno tudi G. Klemenčič v: L. Šturm (ur.), nav. delo, 2011, str. 522.

²⁷ Glej odločbe Ustavnega sodišča št. Up-106/05 z dne 2. 10. 2008 (Uradni list RS, št. 100/08, in OdlUS XVII, 84), 8. in 10. točka obrazložitve, št. Up-540/11, 14. točka obrazložitve, in št. Up-709/15, Up-710/15 z dne 9. 10. 2019 (Uradni list RS, št. 69/19, in OdlUS XXIV, 33), 43. točka obrazložitve. ESČP presoja prometne podatke v okviru pravice iz 8. člena EKČP (na primer sodbi v zadevah *Ben Faiza proti Franciji* z dne 8. 2. 2018 in *Big Brother Watch in drugi proti Združenemu kraljestvu* z dne 25. 5. 2021). SEU jih presoja v okviru varstva osebnih podatkov in zasebnosti (7. in 8. člen Listine).

obračunavanja.²⁸ Po ustaljeni ustavnosodni presoji je tudi IP-naslov dinamični, prometni podatek,²⁹ prav tako pa je eden od pomembnih vidikov komunikacijske zasebnosti tudi identiteta komunicirajočega posameznika.³⁰ Stališče, da sme policija v predkazenskem postopku pridobiti podatke, ki spadajo v ustavno varovano komunikacijsko zasebnost, brez sodne odločbe, pa pomeni po ustaljeni ustavnosodni presoji kršitev pravice iz 37. člena Ustave.³¹ Tudi po ustaljeni praksi ESČP varstvo 8. člena EKČP uživajo ne samo vsebine sporočil, temveč tudi okoliščine in dejstva, povezani s komunikacijo.³²

Presoja z vidika pravice do komunikacijske zasebnosti

36. Ustavno sodišče je moralo najprej presoditi, ali pomeni pridobitev prometnih podatkov na podlagi izpodbijane določbe poseg v upravičeno pričakovanje komunikacijske zasebnosti (prvi odstavek 37. člena Ustave).³³ V skladu z že ustaljeno ustavnosodno presojo pomeni pridobitev prometnih podatkov, tudi na podlagi izpodbijane določbe, poseg v pritožnikovo pravico iz prvega odstavka 37. člena Ustave.³⁴

37. Po ustaljeni ustavnosodni presoji je mogoče ustavne pravice, tudi pravico do komunikacijske zasebnosti, omejiti le v primerih, ki jih izrecno določa Ustava, in zaradi varstva človekovih pravic drugih (tretji odstavek 15. člena Ustave). Človekovo pravico

²⁸ Odločba Ustavnega sodišča št. Up-540/11, 13. točka obrazložitve. Glej tudi 55. točko 3. člena ZEKom-2.

²⁹ Odločbi Ustavnega sodišča št. Up-540/11, 2. točka obrazložitve, in št. Up-153/17 z dne 9. 9. 2021 (OdlUS XXVI, 48), 12. točka obrazložitve.

³⁰ Odločba Ustavnega sodišča št. Up-540/11.

³¹ Odločba Ustavnega sodišča št. Up-106/05, 8. in 10. točka obrazložitve.

³² Prim. sodbe ESČP v zadevah *Malone proti Združenemu kraljestvu* z dne 2. 8. 1984, 84. točka obrazložitve; *P. G. in J. H. proti Združenemu kraljestvu* z dne 25. 9. 2001, 42. točka obrazložitve; *Ben Faiza proti Franciji*; *Figueiredo Teixeira proti Andori* z dne 8. 11. 2016 in *Benedik proti Sloveniji*. Glej tudi sodbe SEU v zadevi *Privacy International*, C-623/17, z dne 6. 10. 2020; v združenih zadevah *La Quadrature du Net in drugi*, C-511/18, C-512/18 in C-520/18, z dne 6. 10. 2020 ter v zadevi *Kazenski postopek zoper H. K.*, C-746/18, z dne 2. 3. 2021.

³³ Odločbi Ustavnega sodišča št. Up-540/11, 14. točka obrazložitve, in št. Up-979/15, 17. točka obrazložitve.

³⁴ Odločbe Ustavnega sodišča št. Up-106/05, 8. in 10. točka obrazložitve, št. Up-709/15, Up-710/15, 43. točka obrazložitve, in št. Up-540/11. Glej tudi A. Lesjak v: M. Avbelj (ur.), nav. delo, str. 359; G. Klemenčič, v: L. Šturm (ur.), nav. delo, 2002, str. 396. Glej tudi sodbo ESČP v zadevi *Malone proti Združenemu kraljestvu*; načelno pravno mnenje Vrhovnega sodišča z dne 18. in 19. 6. 1996; sodbo in sklep Vrhovnega sodišča št. II Ips 473/2005 in II Ips 474/2005 z dne 10. 10. 2007; sodbo nemškega Zveznega ustavnega sodišča v zadevi št. 1 BvR 2226/94 z dne 14. 7. 1999; sodbo SEU v zadevi *Ministerio fiscal*, C-207/16, z dne 2. 10. 2018, 59.–63. točka obrazložitve.

je mogoče omejiti le, če je zakonodajalec zasledoval ustavno dopusten cilj in če je omejitev skladna z načeli pravne države (2. člen Ustave), in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege države (splošno načelo sorazmernosti). Oceno, ali ne gre morda za prekomeren poseg, opravi Ustavno sodišče na podlagi t. i. strogega testa sorazmernosti, ki obsega presojo primernosti, nujnosti in sorazmernosti v ožjem pomenu.³⁵

38. Poleg teh kriterijev pa Ustava v drugem odstavku 37. člena določa še posebne pogoje za poseg v to pravico.³⁶ Ustava tako dopušča poseg v komunikacijsko zasebnost, če ga določi zakon na podlagi odločbe sodišča za določen čas, če je to nujno za potek ali uvedbo kazenskega postopka (drugi odstavek 37. člena Ustave). V skladu z ustaljeno ustavnosodno presojo je treba pri presoji nujnosti oziroma neogibnosti posega v svobodo komuniciranja iz 37. člena Ustave za uvedbo ali potek kazenskega postopka ali za varnost države upoštevati tudi načelo sorazmernosti,³⁷ ki je tudi sicer priznано kot splošno ustavno načelo, izvedeno iz načela pravne države.³⁸

39. Glede ustavno dopustnega cilja Ustavno sodišče pritrjuje predlagatelju, da iz zakonodajnega gradiva sicer ni mogoče razbrati dopustnega cilja prav za vključitev oseb iz drugega odstavka 149.a člena ZKP v izpodbijano določbo, ki ob razlogih za sum omogoča tudi pridobitev prometnih podatkov o osebah, ki niso osumljenec. Vendar že drugi odstavek 37. člena Ustave kot enega od ustavno dopustnih namenov za poseg v komunikacijsko zasebnost določa nujnost za uvedbo ali potek kazenskega postopka.³⁹ Tudi iz ustaljene ustavnosodne presoje izhaja, da je učinkovitost sodnih postopkov v splošnem ustavno dopusten cilj.⁴⁰ Poleg tega je Ustavno sodišče tudi že navedlo, da je namen prikritih preiskovalnih ukrepov zagotavljanje javnega interesa po kazenskem pregonu najhujših oblik kaznivih dejanj ter s tem varstvo pravic žrtev in drugih posameznikov do osebnega dostojanstva in varnosti (34. člen Ustave). Dokazi, ki so pridobljeni na podlagi izvedbe prikritih preiskovalnih ukrepov, so lahko bistvenega

³⁵ Glej 25. točko obrazložitve odločbe Ustavnega sodišča št. U-I-18/02 z dne 24. 10. 2003 (Uradni list RS, št. 108/03, in OdlUS XII, 86).

³⁶ Odločbi Ustavnega sodišča št. U-I-158/95, 14. točka obrazložitve, in št. Up-979/15, 14. točka obrazložitve.

³⁷ Odločba Ustavnega sodišča št. U-I-25/95, 41. in 44. točka obrazložitve.

³⁸ Prav tam, 47. točka obrazložitve. Ustavno sodišče je intenzivnost posega v komunikacijsko zasebnost upoštevalo tudi v odločbah št. U-I-158/95, 17. točka obrazložitve; št. U-I-272/98, 11. in 12. točka obrazložitve; in št. Up-2094/06 z dne 20. 3. 2008 (Uradni list RS, št. 37/08, in OdlUS XVII, 28), 7. in 11. točka obrazložitve.

³⁹ Odločba Ustavnega sodišča št. U-I-40/12 z dne 11. 4. 2013 (Uradni list RS, št. 39/13, in OdlUS XX, 5), 27., 28. in 37. točka obrazložitve.

⁴⁰ Na primer odločba Ustavnega sodišča št. U-I-173/14, Up-609/14 z dne 9. 3. 2017 (Uradni list RS, št. 15/17), 13. točka obrazložitve.

pomena za ugotavljanje dejanskega stanja v kazenskem postopku,⁴¹ nemožnost uporabe pooblastil za izvrševanje prikritih preiskovalnih ukrepov pa bi lahko izrazito negativno vplivala na možnosti državnih organov za uresničevanje javnega interesa po kazenskem pregonu storilcev kaznivih dejanj in s tem na varstvo pravic žrtev in drugih posameznikov do osebnega dostojanstva in varnosti iz 34. člena Ustave.⁴² Učinkovita izvedba kazenskega postopka je torej ustavno dopusten cilj za pridobitev prometnih podatkov po prvem odstavku 149.b člena ZKP.⁴³

Sorazmernost v ožjem pomenu

40. Ustavno sodišče ocenjuje, ne da bi se spuščalo v presojo, ali je obravnavani poseg zakonodajalca nujen in primeren (ukrep) za zagotovitev zasledovanega cilja, da ta poseg ne prestane preizkusa sorazmernosti v ožjem pomenu.⁴⁴ Poseg je sorazmeren, če je teža tega posega (v tem primeru posega v komunikacijsko zasebnost) sorazmerna vrednosti zasledovanega cilja oziroma pričakovanim koristim, ki bodo zaradi posega nastale.⁴⁵

Dokazni standard

41. Ustavno sodišče se v svoji dosednji presoji še ni opredelilo do dokaznega standarda (v izpodbijani določbi: razlogi za sum storitve kaznivega dejanja), predpisanega za pridobivanje podatkov po izpodbijanem 149.b členu ZKP, je pa dokazni standard že upoštevalo pri presoji sorazmernosti ureditve prisluškovanja komunikacijam in prisluškovanja v prostoru (kot posega v komunikacijsko zasebnost).⁴⁶

⁴¹ Odločba Ustavnega sodišča št. U-I-462/18 z dne 3. 6. 2021 (Uradni list RS, št. 105/21, in OdlUS XXVI, 21), 12. točka obrazložitve.

⁴² Sklep Ustavnega sodišča št. U-I-144/19 z dne 4. 7. 2019 (Uradni list RS, št. 48/19), 9. točka obrazložitve. Glej odločbo Ustavnega sodišča št. Up-320/14, U-I-5/17 z dne 14. 9. 2017 (Uradni list RS, št. 59/17, in OdlUS XXII, 9), 21. in 22. točka obrazložitve. Glej tudi sodbo ESČP v zadevi *K. U. proti Finski* z dne 2. 12. 2008.

⁴³ Glej sodbi SEU v zadevi *Commissioner of An Garda Síochána*, C-140/20, z dne 5. 4. 2022, 48.–50. in 63. točka obrazložitve; in v združenih zadevah *La Quadrature du Net and Others*, 120.–122. točka obrazložitve. Prim. tudi P. Križnar v: M. Šepec (ur.), nav. delo.

⁴⁴ Prim. odločbo Ustavnega sodišča št. U-I-328/05 z dne 18. 10. 2007 (Uradni list RS, št. 101/07, in OdlUS XVI, 78), 14. točka obrazložitve.

⁴⁵ Prim. odločbi Ustavnega sodišča št. U-I-83/20 z dne 27. 8. 2020 (Uradni list RS, št. 128/20, in OdlUS XXV, 18), 55. točka obrazložitve, in št. U-I-25/95, 41., 44. in 47. točka obrazložitve.

⁴⁶ Ker je prisluškovanje v prostoru ukrep, ki najintenzivneje posega v zasebno sfero, je zanj zahtevalo dokazni standard, ki ima lastnosti utemeljenega suma (predhodnost, konkretnost, specifičnost, artikuliranost). Odločba Ustavnega sodišča št. U-I-25/95, 53., 54. in 62. točka obrazložitve. Prim. z odločbo Ustavnega sodišča št. U-I-18/93 z dne 11. 4. 1996 (Uradni list RS, št. 25/96, in OdlUS V, 40), 48. in 49. točka obrazložitve. Glej tudi sodbo SEU v zadevi

42. SEU se v svoji praksi prav tako še ni opredeljevalo do višine dokaznega standarda, ki bi ga za poseg v pravici iz 7. in 8. člena Listine zahteval 15. člen Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (UL L 201, 31. 7. 2002 – v nadaljevanju Direktiva o zasebnosti in elektronskih komunikacijah). V sodbi v zadevi *Tele2 Sverige*, C-203/15, z dne 21. 12. 2016 pa je navedlo, da mora nacionalna zakonodaja temeljiti na objektivnih kriterijih, ki opredeljujejo pogoje in okoliščine, v katerih je mogoče odobriti dostop do prometnih podatkov naročnikov in registriranih uporabnikov. V splošnem je tak dostop v zvezi z bojem proti kaznivim dejanjem mogoče odobriti za posameznike, za katere obstaja sum načrtovanja, izvrševanja ali izvršitve resnega kaznivega dejanja ali drugačne vpletenosti v tako kaznivo dejanje.⁴⁷ V tem delu sodbe se je SEU sklicevalo na analogijo z 260. točko obrazložitve sodbe velikega senata ESČP v zadevi *Roman Zakharov proti Rusiji* z dne 4. 12. 2015,⁴⁸ v kateri je ESČP navedlo, da mora imeti organ, ki odobri dostop do podatkov, možnost preveriti obstoj razumnega suma (angl. *reasonable suspicion*, fr. *soupçon raisonnable*) zoper osebe, zlasti da mora imeti možnost preveriti, ali obstaja dejanska podlaga za sum, da oseba načrtuje, izvršuje ali je izvršila kazniva dejanja ali druga dejanja, ki so lahko podlaga za prikrite preiskovalne ukrepe (na primer dejanja zoper nacionalno varnost).⁴⁹

43. V prvem odstavku 149.b člena ZKP je določen enak dokazni standard, kot je bil v prvem odstavku 149.b člena ZKP/17: razlogi za sum.⁵⁰ Ta dokazni standard po ustaljeni ustavnosodni presoji pomeni najnižjo stopnjo verjetnosti, da je bilo izvršeno

Commissioner of An Garda Síochána, v skladu s katero je mogoče utemeljiti zaradi boja proti kaznivim dejanjem le posege, ki niso resni.

⁴⁷ Podobno sodbi SEU v zadevah *Commissioner of An Garda Síochána*, 105. točka obrazložitve; in *Kazenski postopek zoper H. K.*, 50. točka obrazložitve.

⁴⁸ Sodba SEU v zadevi *Tele2 Sverige*, 119. točka obrazložitve.

⁴⁹ Sodba ESČP v zadevi *Roman Zakharov proti Rusiji*, 260. točka obrazložitve. Iz sodb ESČP v zadevah *Szabo in Vissy proti Madžarski* z dne 12. 1. 2016 in *Kennedy proti Združenemu kraljestvu* z dne 18. 5. 2010 je mogoče zgolj razbrati, da ESČP ne dopušča nediskriminatornega in splošnega nadzora velike količine komunikacij in da zahteva jasno določene objektivne kriterije, zoper katere osebe je mogoče ukrep izvesti (ne pa tudi stopnje verjetnosti za to). V sodbi v zadevi *Big Brother Watch in drugi proti Združenemu kraljestvu* z dne 13. 9. 2018 pa je ESČP celo nasprotno zavrnilo stališče pritožnikov, da bi zgornjo premiso dopolnilo z zahtevo po objektivnem standardu razumnega suma za vsako osebo, zoper katero se izvaja nadzor.

⁵⁰ Člen 149a ZKP za izvršitev ukrepa tajnega opazovanja zapoveduje višji dokazni standard, tj. utemeljene razloge za sum. V primerjavi z ukrepom tajnega opazovanja ZKP za pridobitev prometnih podatkov za osebe iz drugega odstavka 149.a člena določa nižje standarde: razloge za sum, da je bilo izvršeno, se izvršuje ali pripravlja oziroma organizira kaznivo dejanje. S sklicevanjem na krog oseb iz drugega odstavka 149.a člena ZKP je sicer treba poleg dokaznega standarda upoštevati tudi pogoje iz te določbe, ki opredeljujejo krog teh "drugih" oseb, tj. utemeljeno sklepanje, da bi pridobitev prometnih podatkov te osebe privedla do identifikacije osumljenca (iz prvega odstavka 149.a člena ZKP).

kaznivo dejanje. Gre za dokazni standard, ki po ustaljeni ustavnosodni presoji nima lastnosti utemeljenega suma (predhodnost, konkretnost, specifičnost, artikuliranost); gre za minimalno obvestilo, ki pooblašča policijo, da začne izvajati svoja pooblastila v predkazenskem postopku.⁵¹ Razlogi za sum, da je bilo izvršeno kaznivo dejanje, so tako nespecifičen dokazni standard, da lahko obstajajo tudi zoper neznano osebo,⁵² in omogočajo, da se ukrep lahko izvrši zoper zelo širok krog oseb.⁵³ Poleg tega je po prvem odstavku 149.b člena ZKP ta dokazni standard lahko vezan ne le na že izvršeno kaznivo dejanje (dokončano kaznivo dejanje), ampak tudi na kaznivo dejanje, ki se še izvršuje (kazniv poskus⁵⁴), oziroma na kaznivo dejanje, ki se sploh šele pripravlja oziroma organizira (pripravljalna faza, kadar je ta kazniva v skladu s KZ-1). Navedeno povečuje potencialno širino izpodbijanega ukrepa in posega.

44. Pridobitev prometnih podatkov po prvem odstavku 149.b člena ZKP je lahko samostojen ukrep, ki ustvari bogat podatkovni profil določene osebe, kar lahko v določenih primerih pomeni celo hujši poseg v zasebnost kot nadzor vsebine informacij.⁵⁵ Iz skupka prometnih podatkov, četudi torej ne omogočajo vpogleda v vsebino komunikacije, je mogoče izluščiti številne podrobnosti iz življenja posameznika⁵⁶ oziroma informacije o mnogih vidikih zasebnega življenja zadevnih oseb, vključno z občutljivimi informacijami, kot so spolna usmerjenost, politična mnenja, verska, filozofska, družbena ali druga prepričanja in zdravstveno stanje.⁵⁷ Na njihovi podlagi je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih

⁵¹ Odločba Ustavnega sodišča št. U-I-25/95, 53. in 54. točka obrazložitve. O dokaznih standardih glej tudi K. Šugman Stubbs, Pomen dokaznih standardov v kazenskem postopku, Zbornik znanstvenih razprav (2007), str. 245–266.

⁵² Prav tam.

⁵³ P. Gorkič, nav. delo, 2015, str. 9–19.

⁵⁴ Člen 34 Kazenskega zakonika (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21 in 16/23 – v nadaljevanju KZ-1).

⁵⁵ To je Ustavno sodišče ugotovilo že v odločbi št. U-I-65/13 (14. točka obrazložitve), v kateri je zapisalo, da je iz prometnih podatkov (skupaj) mogoče izluščiti podrobnosti iz življenja posameznika, zato morajo ti podatki uživati zaščito z vidika pravice do zasebnosti. Podobno je navedlo za konkretni primer v odločbi št. Up-709/15, Up-710/15 (52. točka obrazložitve). Pri tem se je sklicevalo na sodbo SEU v zadevi *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim ter Kärntner Landesregierung in drugi*. Glej tudi C. Keršmanc, Prispevek k javni predstavitvi mnenj o Predlogu zakona o spremembah in dopolnitvah Zakona o kazenskem postopku z dne 13. 6. 2017, EPA: 1855 - VII, pridobljeno na <https://imss.dz-rs.si/IMiS/ImisAdmin.nsf/ImisnetAgent?OpenAgent&2&DZ-MSS-01/7471a4fa17d3ed4f7a8b4fc4711c48ba040b15d9ebce122bb5e63cdb352f1b5c> (1. 6. 2023), ki navaja, da prometni podatki lahko razgalijo človeka še bolj kot vsebina komunikacije. P. Križnar v: M. Šepc (ur.), nav. delo. Ukrep pa je lahko izveden tudi kot predhodna faza drugim prikritim preiskovalnim ukrepom.

⁵⁶ Odločba Ustavnega sodišča št. U-I-65/13, 14. točka obrazložitve.

⁵⁷ Sodba SEU v zadevi *Commissioner of An Garda Síochána*, 45. točka obrazložitve.

podatki so bili pridobljeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, družbeni odnosi in okolja, ki jih obiskujejo.⁵⁸

45. Izpodbijani ukrep je mogoče odrediti ne le zoper osumljenca, ampak tudi zoper oškodovanca in zoper osebe iz drugega odstavka 149.a člena ZKP (tj. zoper osebo, ki ni osumljenec, če je mogoče utemeljeno sklepati, da bi opazovanje te osebe privedlo do identifikacije osumljenca, čigar osebni podatki niso znani, do prebivališča ali lokacije, kjer je osumljenec, oziroma do prebivališča ali lokacije, kjer je oseba, zoper katero je bil odrejen pripor, hišni pripor, tiralica ali odredba za privedbo, pa je pobegnila ali se skriva, in policisti z drugimi ukrepi teh podatkov ne morejo pridobiti oziroma bi bilo to povezano z nesorazmernimi težavami).

46. ZKP-N je razširil tudi obseg zavezancev za posredovanje prometnih podatkov, saj morajo podatke po prvem odstavku 149.b člena ZKP posredovati ne le operaterji po ZEKom-2,⁵⁹ ampak tudi ponudniki storitev informacijske družbe po ZEPT.⁶⁰

47. Glede na navedeno in glede na dosedanji in potencialni razvoj komunikacijske tehnologije se povečuje tudi obseg obstoječih (in tudi potencialno) relevantnih podatkov, ki jih je mogoče pridobiti na podlagi izpodbijane določbe, pogloblja in širi pa se tudi profil, ki ga je mogoče na podlagi teh podatkov oblikovati o določeni osebi. Ob tem ni mogoče zanemariti še proaktivne narave izpodbijanega ukrepa, saj je njegov namen proaktivno odzivanje na kriminaliteto že v najzgodnejši fazi do kaznivega dejanja, in njegove prikrite narave, zaradi katere oseba ne ve, da se zoper njo izvršuje

⁵⁸ Prav tam. Gl. tudi sodbe SEU v zadevi *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* ter *Kärntner Landesregierung in drugi*, 27. točka obrazložitve; v združenih zadevah *La Quadrature du Net in drugi*, 117. točka obrazložitve; v zadevi *Kazenski postopek zoper H. K.*, 36., 40., 45. točka obrazložitve; in v združenih zadevah *Bundesrepublik Deutschland proti SpaceNet AG in Telekom Deutschland GmbH*, C-793/19 in C-794/19, z dne 20. 9. 2022, 61. točka obrazložitve. Glede primerjave navedenega ukrepa z ukrepom tajnega opazovanja glej P. Gorkič, nav. delo, 2015, str. 10, 11; in P. Plesec, nav. delo, str. 33. V zvezi s tajnim opazovanjem glej sodbi ESČP v zadevah *Uzun proti Nemčiji* z dne 2. 9. 2010 in *Florindo de Almeida Vasconcelos Gramaxo proti Portugalski* z dne 13. 12. 2022 ter sodbo ameriškega Vrhovnega sodišča *Riley proti Kaliforniji*, 573 U. S., z dne 25. 6. 2014.

⁵⁹ Točki 50 in 51 3. člena ZEKom-2.

⁶⁰ Točki 6 in 11 3. člena ZEPT. Glej tudi P. Plesec, nav. delo; odločba Ustavnega sodišča št. Up-153/17; ter P. Križnar v: M. Šepec (ur.), nav. delo, ki navaja tudi izvajalca poštnih storitev po Zakonu o poštnih storitvah (Uradni list RS, št. 51/09, 77/10 in 81/15 – v nadaljevanju ZPSto-2). Glej osmi odstavek 2. člena in 18. člen ZPSto-2.

ukrep.⁶¹ Velika spoznavna, pa tudi dokazna⁶² vrednost pridobitve prometnih podatkov za kazenski postopek tako lahko pomeni intenziven poseg v komunikacijsko zasebnost oseb, zoper katere se ukrep izvaja, pa tudi drugih oseb, ki so se zgolj "ujele" v njihovo komunikacijsko mrežo.

48. Ustavno sodišče tudi poudarja, da ZKP za izpodbijani ukrep v prvem odstavku 149.b člena že sam določa, da ga lahko odredi le preiskovalni sodnik s sodno odredbo (kot to za kakršenkoli poseg v komunikacijsko zasebnost določa že Ustava v drugem odstavku 37. člena). Zahteva po sodni odločbi pa po ustaljeni ustavnosodni presoji ne pomeni zgolj formalne zahteve po sodni odločbi, ampak tudi vsebinsko zahtevo po obrazloženi sodni odločbi.⁶³ Po drugi strani, kot je Ustavno sodišče že navedlo (43. točka obrazložitve te odločbe), pa dokazni standard razlogi za sum po svoji naravi pomeni zgolj minimalno obvestilo o kaznivem dejanju, ki lahko temelji zgolj na občutku policista, izkušnjah ali intuiciji.⁶⁴ V svojem bistvu so namreč razlogi za sum opredeljeni kot dokazni standard, katerega obstoja pogosto ni mogoče, predvsem pa niti ni treba obrazložiti.⁶⁵ Zato sta ustavna in zakonska zahteva po sodni kontroli, ki vsebuje tudi vsebinsko obrazloženost takšne odločbe, pojmovno nezdružljivi z obstojem tega dokaznega standarda.⁶⁶ Pojem pisne in obrazložene sodne odredbe je logično povezan zgolj s tistimi dokaznimi standardi, ki jih je mogoče obrazložiti. To pa so dokazni standardi, ki imajo izrazljivo, konkretizirano in specifično vsebino: utemeljeni razlogi za sum, utemeljen sum in dokazni standard za izrek obsodilne sodbe.⁶⁷

49. Iz vsega navedenega izhaja, da omogoča dokazni standard razlogov za sum, ki je v prvem odstavku 149.b člena ZKP predpisan za odreditev izpodbijanega ukrepa, nesorazmeren poseg v pravico do komunikacijske zasebnosti.

⁶¹ P. Križnar v: M. Šepec (ur.), nav. delo, str. 842, in K. Šugman Stubbs, P. Gorkič, nav. delo, str. 145.

⁶² Gre za izjemo, saj policijska dejanja v predkazenskem postopku praviloma nimajo dokazne vrednosti.

⁶³ Odločba Ustavnega sodišča št. U-I-25/95, 69. točka obrazložitve.

⁶⁴ Glej K. Šugman Stubbs, nav. delo, 2007, str. 279–301.

⁶⁵ Primerjaj s sodbo ameriškega Vrhovnega sodišča *Terry proti Ohio* z dne 10. 6. 1968 z vidika pooblastila *stop and frisk* zaradi občutka ogroženosti policista.

⁶⁶ Glej P. Plešec, nav. delo, str. 33. Glej tudi P. Gorkič, nav. delo, 2015, str. 10, 13; P. Križnar v: M. Šepec (ur.), nav. delo.

⁶⁷ Glej odločbi Ustavnega sodišča št. U-I-25/95 in št. U-I-18/93. O nastanku dokaznega standarda utemeljenih razlogov za sum glej K. Šugman Stubbs, Posegi v osebnostno celovitost posameznika, v: K. Šugman Stubbs (ur.), Izhodišča za modernizacijo kazenskega postopka v Sloveniji, Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2003, in K. Šugman Stubbs, nav. delo, 2007.

Obdobje pridobivanja podatkov

50. Ustava že sama v drugem odstavku 37. člena določa, da je mogoče v varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti poseči zgolj za določen čas. Pomembnost časovnih omejitev pridobitve prometnih podatkov izhaja tako iz ustaljene presoje Ustavnega sodišča⁶⁸ kot tudi iz prakse ESČP.⁶⁹ SEU pa je v sodbi v združenih zadevah *La Quadrature du Net in drugi* večkrat poudarilo, da so hramba prometnih in lokacijskih podatkov za namene nacionalne varnosti, osredotočena oziroma ciljana hramba prometnih in lokacijskih podatkov, nediskriminatorna in splošna hramba IP-naslovov vira internetne povezave z namenom varstva nacionalne varnosti, boja proti hudim kaznivim dejanjem in preprečevanja resnih groženj javni varnosti ter pospešena hramba prometnih in lokacijskih podatkov teh uporabnikov z namenom boja proti hudim kaznivim dejanjem in varstva nacionalne varnosti dopustne le za obdobje, ki je nujno potrebno, ki pa se lahko v določenih primerih podaljša.⁷⁰ Daljše ko je obdobje, za katero se zahteva dostop, večja bo načeloma, po stališču SEU, količina podatkov, ki bi jih ponudniki elektronskih komunikacijskih storitev lahko shranili v zvezi z elektronskimi komunikacijami, ki jih je opravil uporabnik elektronskega komunikacijskega sredstva, v zvezi s kraji, kjer se zadržuje, in z njegovimi premiki, tako da bo mogoče iz pregledanih podatkov razbrati več ugotovitev o zasebnem življenju tega uporabnika.⁷¹ Pristojni nacionalni organi morajo torej zato, da bi izpolnili zahtevo po sorazmernosti, v skladu s katero morajo biti odstopanja od varstva osebnih podatkov in omejitve tega varstva v okviru tega, kar je nujno potrebno (sodba SEU v združenih zadevah *La Quadrature du Net in drugi*, 130. točka obrazložitve), v vsakem posameznem primeru zagotoviti, da so tako vrsta ali vrste zahtevanih podatkov kot obdobje, za katero se zahteva dostop do njih, glede na okoliščine obravnavane zadeve omejeni na to, kar je nujno potrebno za zadevno

⁶⁸ Odločbi Ustavnega sodišča št. U-I-65/13, 25. točka obrazložitve, in št. Up-709/15, Up-710/15, 46. točka obrazložitve. P. Gorkič, nav. delo, 2014, str. 10.

⁶⁹ Glej na primer sodbo ESČP v zadevi *Figueiredo Teixeira proti Andori*, 46. točka obrazložitve.

⁷⁰ Sodba SEU v združenih zadevah *La Quadrature du Net in drugi*, 229. točka obrazložitve. Iz poročila Evropske komisije, ki zajema deset držav članic Evropske unije (Avstrija, Estonija, Nemčija, Francija, Irska, Italija, Poljska, Portugalska, Slovenija in Španija), izhaja, da je povprečen čas hrambe prometnih in lokacijskih podatkov v Republiki Sloveniji 3 mesece, da so v državah članicah določeni daljši roki hrambe za naročniške podatke (kot za prometne, identifikacijske in lokacijske podatke), da je v državah članicah, v katerih obstaja posebna pravna podlaga za hrambo podatkov za namene kazenskega postopka, rok hrambe 12 mesecev, v državah, kjer te pravne podlage ni, pa je ta rok bolj nejasen. Sem sodi tudi Republika Slovenija. Iz poročila tudi izhaja, da naj bi bila najpogostejša največja starost zahtevanega podatka eno leto, običajna starost podatkov pa tri do šest mesecev. European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes: final report, Publication Office of the European Union, Luxembourg 2020, str. 53, 71, 72.

⁷¹ Sodba SEU v zadevi *Kazenski postopek zoper H. K.*, 37. točka obrazložitve.

preiskavo.⁷² Vendar je poseg v temeljni pravici iz 7. in 8. člena Listine, kakršen je dostop javnega organa do vseh podatkov o prometu ali lokaciji, iz katerih so lahko razvidne informacije o komunikacijah uporabnika elektronskega komunikacijskega sredstva ali o lokaciji uporabljene terminalske opreme, po stališču SEU hud, ne glede na dolžino obdobja, za katero se dostop do teh podatkov zahteva, in ne glede na količino ali vrsto podatkov, ki so na voljo za to obdobje, če je mogoče iz vseh teh podatkov natančno sklepati o zasebnem življenju posameznika ali posameznikov, na katere se nanašajo osebni podatki.⁷³

51. ZKP na abstraktni ravni ne omejuje, za kakšno obdobje od trenutka izdaje sodne odredbe za pridobitev podatkov po prvem odstavku 149.b člena ZKP nazaj je mogoče pridobiti te podatke. To sicer ne pomeni, da obdobje pridobivanja podatkov sploh ni zakonsko omejeno. Predlog in odredba morata po drugem odstavku 149.b člena ZKP med drugim vsebovati navedbo relevantnega obdobja, za katero se podatki zahtevajo.⁷⁴ Hkrati pa po prvem odstavku 149.b člena ZKP operater oziroma ponudnik storitev informacijske družbe pristojnemu organu sporočita le relevantne podatke v zvezi z omenjeno komunikacijo, ki obstajajo v času izdaje odredbe.

52. Kateri so ti podatki, pa po razveljavitvi XIII. poglavja Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12 in 110/13 – ZEKom-1/13), ki je urejalo posebno pravno podlago za hrambo prometnih podatkov na podlagi Direktive 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13. 4. 2006 – v nadaljevanju Direktiva o hrambi podatkov) posebej za namene kazenskega postopka, za operaterje in ponudnike storitev informacijske družbe⁷⁵ še vedno opredeljuje ZEKom-2. Ta ureja hrambo podatkov v t. i. "komercialnih bazah", torej na podlagi zakona ali soglasja imetnika podatka.⁷⁶ S tega vidika je torej na abstraktni ravni v področni zakonodaji, ne pa tudi v ZKP, zamejeno obdobje hrambe podatkov in posledično tudi časovni obseg podatkov, ki jih je mogoče pridobiti na podlagi prvega odstavka 149.b člena ZKP. Hkrati tudi v konkretnem primeru iz načela sorazmernosti izhaja zahteva, da lahko državni tožilec na podlagi prvega odstavka 149.b člena ZKP zahteva, preiskovalni sodnik pa odobri zgolj pridobitev prometnih podatkov za relevantno obdobje pred izdajo sodne odredbe, torej za obdobje, ki je vsebinsko upoštevno in nujno potrebno za konkretno (pred)kazensko zadevo.⁷⁷

⁷² Prav tam, 38. točka obrazložitve.

⁷³ Prav tam, 39., 40. in 45. točka obrazložitve.

⁷⁴ Drugi odstavek 149.b člena ZKP.

⁷⁵ Točka 3 prvega odstavka 2. člena ZEPT.

⁷⁶ P. Gorkič, nav. delo, 2014, str. 9; 218. člen ZEKom-2; P. Plesec, nav. delo, str. 34.

⁷⁷ Glej P. Gorkič, nav. delo, 2015, str. 15 in nasl.

53. Ne glede na navedeno pa po stališču Ustavnega sodišča abstraktna omejitev, navedena v področni nekazenski zakonodaji, in omejitev, ki v konkretnem primeru izhaja iz načela sorazmernosti (2. člen Ustave), tj. da je možna le pridobitev podatkov za obdobje, ki je vsebinsko upoštevno in nujno potrebno za konkretno (pred)kazensko zadevo (glej 52. točka obrazložitve te odločbe), ne zadoščata. SEU je v svoji sodbi v zadevi *The Commissioner of the Garda Síochána* navedlo, da sta hramba teh podatkov in dostop do njih, kot je razvidno iz njegove sodne prakse,⁷⁸ ločena posega v temeljni pravici, zagotovljeni v 7. in 11. členu Listine, za katera sta potrebni ločeni utemeljitvi na podlagi prvega odstavka 52. člena Listine. Iz tega po stališču SEU izhaja, da nacionalna zakonodaja, ki zagotavlja polno spoštovanje pogojev, ki izhajajo iz sodne prakse, s katero je bila Direktiva o zasebnosti in elektronskih komunikacijah razložena na področju dostopa do hranjenih podatkov, sama po sebi ne more niti omejiti niti odpraviti resnega posega, ki bi izhajal iz splošne hrambe teh podatkov, ki je določena s to nacionalno zakonodajo, v pravice, zagotovljene s 5. in 6. členom te direktive, in v temeljne pravice, ki jih ta člena konkretizirata.⁷⁹ Navedeno naj bi veljalo tudi obratno; ZKP bi moral na podlagi drugega odstavka 37. člena Ustave sam določati jasno abstraktno časovno omejitev kazenskopravnega posega v komunikacijsko zasebnost s pridobivanjem prometnih podatkov oziroma dostopom do njih, ob upoštevanju načela sorazmernosti in niansiranega pristopa k posegom v človekove pravice in temeljne svoboščine, medtem ko ZEKom-2 že ureja časovne omejitve hrambe prometnih podatkov, do katerih se z izpodbijanim ukrepom dostopa. S tem bi bilo mogoče preprečiti tudi morebitno pridobivanje podatkov, ki po ZEKom-2 sicer ne bi smeli biti več hranjeni, pa vseeno obstajajo.

54. Tako pomeni tudi opustitev določitve časovne omejitve za dostop do prometnih podatkov po stališču Ustavnega sodišča nesorazmeren poseg v komunikacijsko zasebnost.

Katalog kaznivih dejanj

55. Ustavno sodišče je v odločbi št. U-I-25/95 odločilo, da ureditev prisluškovanja v tujem prostoru ni bila sorazmerna tudi zaradi predpisanega kataloga kaznivih dejanj, za katera se je ukrep lahko odredil.⁸⁰ Pri tem je sicer pritrdilo Državnemu zboru, da gre pri kaznivih dejanjih s seznama, ki niso težka, za kazniva dejanja, ki so težko dokazljiva, še posebej, če so storjena v sosterilstvu ali na organiziran način, vendar naj pri njihovem izboru ne bi smelo biti edino vodilo težka dokazljivost. Ob težki dokazljivosti je treba po stališču Ustavnega sodišča namreč v skladu z načelom sorazmernosti upoštevati tudi in predvsem teže družbi nevarnih dejanj.⁸¹ Podobno je Ustavno sodišče

⁷⁸ Glej sodbo SEU v združenih zadevah *La Quadrature du Net in drugi*, 115. in 116. točka obrazložitve in tam navedena sodna praksa.

⁷⁹ Sodba SEU v zadevi *The Commissioner of the Garda Síochána*, 47. točka obrazložitve.

⁸⁰ Prav tam, 55. točka obrazložitve.

⁸¹ Prav tam, 56. točka obrazložitve.

v odločbi št. U-I-272/98 ugotovilo, da je zakonodajalec izvajanje ukrepov iz prvega odstavka 49. člena tedaj veljavnega Zakona o policiji (Uradni list RS, št. 49/98, 66/98 – popr. in 93/01 – v nadaljevanju ZPol/98)⁸² omogočil zoper 516 kaznivih dejanj, ki se preganjajo po uradni dolžnosti, ne da bi jih razvrstil bodisi glede na zagroženo kazen, glede na način izvršitve ter glede na varovane dobrine, in ocenilo, da je taka zakonska rešitev preširoka.⁸³ V odločbi št. U-I-65/13 pa je Ustavno sodišče navedlo, da je z vidika sorazmernosti ukrepa sporno, da zakonodajalec obdelave prometnih podatkov (posebej za namene kazenskega postopka) ni zamejil zgolj na določena (huda kazniva) dejanja, za katera bi ocenil, da zaradi njihove teže hramba podatkov oziroma dostop do njih upravičujeta poseg v zasebnost posameznika. Tudi iz tega razloga je zato ukrep po stališču Ustavnega sodišča nesorazmerno posegal v pravico iz prvega odstavka 38. člena Ustave.⁸⁴

56. Iz ustaljene prakse ESČP in SEU prav tako izhaja, da lahko dostop do hranjenih prometnih podatkov upraviči le boj (preprečevanje, odkrivanje ali pregon kaznivih dejanj) proti hudemu kriminalu oziroma proti najtežjim kaznivim dejanjem (na primer boj proti trgovini z drogo, organizirani kriminaliteti in pranju denarja).⁸⁵ SEU je tako v že omenjeni sodbi v združenih zadevah *La Quadrature du Net in drugi* poudarilo, da lahko hude posege v temeljni pravici, določeni v 7. in 8. členu Listine, upravičita le preprečevanje resnih groženj javni varnosti in boj proti hudemu kriminalu.⁸⁶ Zato je

⁸² Ti ukrepi so bili tajno opazovanje in sledenje z uporabo tehničnih sredstev za dokumentiranje; tajno policijsko delovanje; tajno policijsko sodelovanje; prirejene listine in identifikacijske oznake.

⁸³ Odločba Ustavnega sodišča št. U-I-272/98, 32. točka obrazložitve. Glej tudi odločbo Ustavnega sodišča št. U-I-158/95, 17. točka obrazložitve. Tudi v primerjalnem pravu je dopustnost podobnih ukrepov praviloma omejena na preiskovanje kaznivih dejanj, ki so storjena na organiziran način ali ki so posebej nevarna. Subsidiarna uporaba ukrepov iz prvega odstavka 49. člena ZPol/98 pa po stališču Ustavnega sodišča ni zadostna omejitev glede kaznivih dejanj, za katere uporaba ukrepov sploh ne bi bila dopustna.

⁸⁴ Odločba Ustavnega sodišča št. U-I-65/13, 27. točka obrazložitve. V odločbi št. Up-709/15, Up-710/15 je Ustavno sodišče ugotovilo, da sodišče na podlagi izdanih sodnih odredb ni pridobilo zgolj podatkov o povezavi med določenimi komunikacijskimi napravami in osebno istovetnostjo imetnikov oziroma lastnikov teh komunikacijskih naprav, ampak da iz analitičnih informacij izhajajo pogostost, lokacija in čas komunikacij, zato tak poseg v zasebnost v skladu z ustaljeno sodno prakso SEU in ESČP lahko upraviči le boj proti hudemu kriminalu oziroma proti najtežjim kaznivim dejanjem, kar naj bi bilo v konkretnem primeru tudi izpolnjeno.

⁸⁵ Sodba SEU v zadevi *Tele2 Sverige*, 102. in 103. točka obrazložitve; sodbi ESČP v zadevah *Figueiredo Teixeira proti Andori*, 43. točka obrazložitve, in *Ben Faiza proti Franciji*, 76. točka obrazložitve.

⁸⁶ Iz že omenjenega poročila Evropske komisije izhaja, da hudo kaznivo dejanje (*serious crime*) ni avtonomno opredeljeno v pravu Evropske unije in da lahko obstajajo razlike med opredelitvami tega pojma med različnimi akti Evropske unije (European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes: final

mogoče s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno upravičiti le blažje posege v omenjeni temeljni pravici, tj. posege, od katerih pridobljeni podatki ne omogočajo izpeljave natančnih ugotovitev o zasebnem življenju oseb, za podatke katerih gre.⁸⁷ Dostop javnih organov do vseh podatkov o prometu ali lokaciji, iz katerih so lahko razvidne informacije o komunikacijah uporabnika elektronskega komunikacijskega sredstva ali o lokaciji uporabljene terminalske opreme, omogoča natančne ugotovitve v zvezi z zasebnim življenjem posameznikov, na katere se nanašajo osebni podatki. Ta se po stališču SEU lahko opraviči samo s ciljem boja proti hudemu kriminalu (in preprečevanja hudih nevarnosti za javno varnost), ne da bi lahko drugi dejavniki, povezani s sorazmernostjo zahteve za dostop, kot je trajanje obdobja, za katero se zahteva dostop do takih podatkov, učinkovali tako, da bi bilo mogoče tak dostop upravičiti s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno.⁸⁸ Iz navedene sodne prakse Ustavnega sodišča, ESČP in SEU torej izhaja, da je dostop do prometnih podatkov po prvem odstavku 149.b člena ZKP, ki lahko pomeni hud poseg v pravico do komunikacijske zasebnosti osebe, katere podatki se lahko pridobijo, sorazmeren le za odkrivanje, pregon in dokazovanje hudih kaznivih dejanj.

57. Katalog kaznivih dejanj, za katera se lahko odredi ukrep iz 149.b člena ZKP, je bil z ZKP-N spremenjen. Po prvem odstavku 149.b člena ZKP/17 je bilo mogoče ukrep odrediti za vsako kaznivo dejanje, ki se preganja po uradni dolžnosti. Na podlagi prvega odstavka 149.b člena ZKP pa je prometne podatke mogoče pridobiti za kazniva dejanja iz četrtega odstavka 149.a člena ZKP:

"1) kazniva dejanja, za katera je v zakonu predpisana kazen zapora petih ali več let;

report, nav. delo). Prav tako hudo kaznivo dejanje ni opredeljeno v sami študiji. Hudo kaznivo dejanje naj bi bilo opredeljeno z naravo, težo in kaznijo, na primer kazniva dejanja, za katera je predpisana kazen najmanj pet let zaporne kazni. Po tej študiji je mogoče obravnavane države razdeliti v dve skupini; prva skupina ureditev omogoča pridobitev podatkov ne glede na vrsto kaznivega dejanja, vključno s prekrški, druga pa jo omejuje na določene vrste kaznivih dejanj, bodisi na kazniva dejanja s seznama bodisi glede na predpisano zaporno kazen. V praksi naj bi bil dostop omejen na nujne primere. L. Paoli, A. Adriaenssen, Vi. A. Greenfield, M. Conickx, Exploring Definitions of Serious Crime in EU Policy Documents and Academic Publications: A Content Analysis and Policy Implications, *European Journal on Criminal Policy and Research*, let. 23, št. 3 (2017), str. 269–285. Glede hudega kaznivega dejanja glej sodbo SEU v zadevi *The Commissioner of the Garda Síochána*, 105. točka obrazložitve.

⁸⁷ Sodbe SEU v zadevi *Ministerio Fiscal*, 59.–63. točka obrazložitve; v združenih zadevah *La Quadrature du Net in drugi*, 140. in 146. točka obrazložitve; v zadevi *The Commissioner of the Garda Síochána*, 67. točka obrazložitve; v zadevi *Kazenski postopek zoper H. K.*, 33. točka obrazložitve; ter v združenih zadevah *Bundesrepublik Deutschland proti SpaceNet AG in Telekom Deutschland GmbH*, 73. točka obrazložitve.

⁸⁸ Sodbi SEU v zadevah *Kazenski postopek zoper H. K.*, 35. točka obrazložitve; in *Ministerio Fiscal*, 54. točka obrazložitve.

2) kazniva dejanja iz 2. točke drugega odstavka 150. člena tega zakona in kazniva dejanja protipravnega odvzema prostosti po 133. členu, zalezovanja po 134.a členu, grožnje po 135. členu, zlorabe osebnih podatkov po tretjem, četrtem, petem in šestem odstavku 143. člena, zaposlovanja na črno po drugem in tretjem odstavku 199. člena, goljufije po prvem, tretjem in četrtem odstavku 211. člena, prikrivanja po prvem, drugem in tretjem odstavku 217. člena, goljufije na škodo Evropske unije po 229. členu, napada na informacijski sistem po drugem, tretjem in četrtem odstavku 221. člena, ponareditve ali uničenja poslovnih listin po 235. členu, izdaje in neupravičene pridobitve poslovne tajnosti po prvem, drugem in tretjem odstavku 236. člena, zlorabe informacijskega sistema po 237. členu, zlorabe položaja ali zaupanja pri gospodarski dejavnosti po 240. členu, ponarejanja listin po 251. členu, posebnega primera ponarejanja listin po 252. členu, zlorabe uradnega položaja ali uradnih pravic po 257. členu, izdaje tajnih podatkov po 260. členu, javnega spodbujanja sovraštva, nasilja in nestrpnosti po 297. členu, prepovedanega prehajanja meje ali ozemlja države po 308. členu, onesnaženja pitne vode po prvem, tretjem, četrtem in šestem odstavku 336. člena, onesnaženja živil ali krme po prvem, tretjem, četrtem in šestem odstavku 337. člena ter mučenja živali po drugem, tretjem in četrtem odstavku 341. člena Kazenskega zakonika;

3) kaznivo dejanje pomoči storilcu po storitvi kaznivega dejanja po 282. členu Kazenskega zakonika, in sicer tudi zoper osebe iz četrtega odstavka 282. člena Kazenskega zakonika – za kazniva dejanja, ki so navedena v tem odstavku."

58. Na podlagi primerjalne in jezikovne razlage ZKP in ZKP/17 je mogoče pritrditi zakonodajalcu, da gre v primerjavi z ZKP/17 za ožji katalog kaznivih dejanj in s tem za zaostritev pogojev za odreditev ukrepa ter da je pri oblikovanju kataloga kaznivih dejanj treba upoštevati tudi potrebe policije.⁸⁹

59. Skupina kaznivih dejanj pod točko 1) četrtega odstavka 149.a člena ZKP je opredeljena s težo sankcije; predpisana mora biti kazen pet let ali več zapora. Ta skupina kaznivih dejanj tako upošteva težo kaznivih dejanj kot merilo iz ustaljene ustavnosodne presoje.⁹⁰ Skupina kaznivih dejanj pod točko 2) četrtega odstavka 149.a člena ZKP je opredeljena taksativno in vključuje najprej kazniva dejanja, za katera je mogoče odrediti tudi ukrepe iz 2. točke drugega odstavka 150. člena ZKP⁹¹ in za katera

⁸⁹ Predlog ZKP-N, str. 7, 8, 27, 141, 143.

⁹⁰ Ta skupina naj bi pomenila približno 149 kaznivih dejanj ali njihovih modalitet (od približno 275 členov posebnega dela KZ-1).

⁹¹ Gre za naslednja kazniva dejanja: ugrabitev (134. člen KZ-1), pridobivanje oseb, mlajših od petnajst let, za spolne namene (173.a člen KZ-1), zloraba prostitucije (175. člen KZ-1), prikazovanje, posest, izdelava in posredovanje pornografskega gradiva (176. člen KZ-1), neupravičena proizvodnja in promet s prepovedanimi drogami, nedovoljenimi snovmi v športu

je večinoma spet mogoče izreči kazen vsaj petih let zapora. Vendar pa so v tej točki taksativno naštetja še številna druga kazniva dejanja. Pod točko 3) je kaznivo dejanje določeno taksativno in vezano na 282. člen KZ-1. Tako široka opredelitev kataloga kaznivih dejanj ni sorazmerna v ožjem smislu. Zlasti s taksativno določenimi kaznivimi dejanji pod točko 2) je zakonodajalec preširoko opredelil katalog kaznivih dejanj za ukrep po prvem odstavku 149.b člena ZKP. Pri nekaterih kaznivih dejanjih njihova teža ne upravičuje posega v komunikacijsko zasebnost iz prvega odstavka 37. člena Ustave. Skupina kaznivih dejanj pod točko 2) četrtega odstavka 149.a člena ZKP namreč zajema širok nabor kaznivih dejanj, vključno s kaznivimi dejanji, za katera je za kakšno obliko lahko zagrožena tudi (zgolj) šestmesečna⁹² ali dvoletna zaporna kazen.⁹³ Pri drugih kaznivih dejanjih narava oziroma vsebina posega in podatkov iz 149.b člena ZKP nima nobene razvidne povezave s kaznivim dejanjem.⁹⁴ Nesorazmernost kataloga kaznivih dejanj je še bolj razvidna ob upoštevanju dejstva, da je mogoče ukrep po 149.b členu ZKP izvršiti za širok nabor dejanj: ne le za že izvršena kazniva dejanja, temveč tudi za kazniva dejanja, ki se izvršujejo (torej so vsaj v fazi kaznivega poskusa), ali celo za kazniva dejanja v fazi kaznivih pripravljalnih dejanj ali organizacije, in to zoper tri skupine oseb (osumljenca, oškodovanca in osebe iz četrtega odstavka 149.a člena ZKP) – vse ob istem dokaznem standardu (razlogi za sum).

60. Zakonodajalec bo moral pri oblikovanju novega kataloga kaznivih dejanj upoštevati v prvi vrsti težo kaznivega dejanja v smislu opredelitve hudega kaznivega dejanja iz ustaljene ustavnosodne presoje ter prakse SEU in ESČP.⁹⁵ Poleg tega pa sme v navedeni katalog vključiti tudi določena sicer blažja kazniva dejanja, pri katerih bi bila zaradi narave izvršitve kaznivega dejanja pridobitev prometnih podatkov nujna za izsleditev storilca in izvedbo kazenskega postopka.⁹⁶ Kot navedeno, trenutni katalog

in predhodnimi sestavinami za izdelavo prepovedanih drog (186. člen KZ-1), omogočanje uživanja prepovedanih drog ali nedovoljenih snovi v športu (187. člen KZ-1), izsiljevanje (213. člen KZ-1), zloraba notranje informacije (238. člen KZ-1), nedovoljeno sprejemanje daril (241. člen KZ-1), neupravičeno dajanje daril (242. člen KZ-1), pranje denarja (245. člen KZ-1), tihotapstvo (250. člen KZ-1), oškodovanje javnih sredstev (257.a člen KZ-1), jemanje podkupnine (261. člen KZ-1), dajanje podkupnine (262. člen KZ-1), sprejemanje koristi za nezakonito posredovanje (263. člen KZ-1), dajanje daril za nezakonito posredovanje (264. člen KZ-1), hudodelsko združevanje (294. člen KZ-1), nedovoljena proizvodnja in promet orožja ali razstrelilnih snovi (307. člen KZ-1) in protipravna ravnanja z jedrskimi ali drugimi nevarnimi radioaktivnimi snovmi (334. člen KZ-1).

⁹² Na primer kaznivo dejanje grožnje iz 135. člena KZ-1.

⁹³ Na primer kaznivo dejanje mučenja živali iz drugega odstavka 341. člena KZ-1.

⁹⁴ Na primer kaznivo dejanje onesnaženja pitne vode, kaznivo dejanje onesnaženja živil ali krme in kaznivo dejanje mučenja živali.

⁹⁵ Prim. European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes: final report, nav. delo.

⁹⁶ Prim. prav tam, str. 71–74, 120, 121.

kaznivih dejanj tega kriterija ne izpolnjuje, opredeljen je preširoko, zato tudi ta določa nesorazmeren poseg v pravico iz prvega odstavka 37. člena Ustave.⁹⁷

Odločitev Ustavnega sodišča

61. Zvišanje dokaznega standarda, določitev abstraktnega obdobja, za katero je mogoče pridobiti podatke, ter zoženje kataloga kaznivih dejanj sicer zmanjšujejo učinkovitost (pred)kazenskega postopka, ki je ustavno dopusten cilj za poseg v pravico do komunikacijske zasebnosti iz prvega odstavka 37. člena Ustave, vendar teža posledic ukrepa zgolj ob obstoju nizkega dokaznega standarda razlogov za sum, odsotnosti časovne omejitve izpodbijanega ukrepa v ZKP in ob obstoječem preširokem katalogu kaznivih dejanj pretehta koristi ukrepa. Prvi odstavek 149.b člena ZKP, ki omogoča uporabo ukrepa ob navedenih pogojih, je v neskladju z zahtevo po zagotavljanju sorazmernostnega ravnovesja med težo posledic posega v komunikacijsko zasebnost osebe, zoper katero je ukrep odrejen, in koristmi, ki bi zaradi tega nastale. Zato je ukrep iz prvega odstavka 149.b člena ZKP nesorazmeren v ožjem smislu.⁹⁸

62. Ustavno sodišče je glede na navedeno ugotovilo, da je prvi odstavek 149.b člena ZKP v neskladju z Ustavo, in ga razveljavilo. Ker so drugi do peti odstavek 149.b člena ZKP neposredno povezani s prvim odstavkom 149.b člena ZKP in nimajo samostojnega pomena, je razveljavilo 149.b člen ZKP v celoti (1. točka izreka).

63. V skladu s 43. členom ZUstS začne razveljavitev zakona učinkovati naslednji dan po objavi odločbe o razveljavitvi oziroma po poteku roka, ki ga je določilo Ustavno sodišče. Ker bo treba ureditev ukrepa iz prvega odstavka 149.b člena ZKP v celoti prilagoditi ustavnim zahtevam na način, zapisan v tej odločbi, in ker se z odločbo razveljavlja celotna ureditev tega ukrepa, ki jo bo treba tudi sistemsko uvrstiti v ureditev prikritih preiskovalnih ukrepov v ZKP, pri tem pa bo zakonodajalec moral upoštevati stališča iz te delne odločbe in delne odločbe št. U-I-144/19 z dne 1. 12. 2022, ki se nanašajo na vse izpodbijane ukrepe, ter načelo sorazmernosti in niansiran pristop do posegov v človekove pravice, je Ustavno sodišče učinkovanje razveljavitve odložilo za čas enega leta od objave te odločbe v Uradnem listu Republike Slovenije in s tem zakonodajalcu določilo najdaljši možni rok za uskladitev razveljavljene ureditve z Ustavo (3. točka izreka).

⁹⁷ P. Gorkič, nav. delo, 2014, str. 6–10, sicer meni, da bi bilo možno že 149.b člen ZKP razlagati ustavnoskladno, torej z zoženim naborom kaznivih dejanj. Drugače P. Križnar v: M. Šepec (ur.), nav. delo. Glede sorazmernosti kataloga kaznivih dejanj glej tudi P. Gorkič, nav. delo, 2015, str. 10, ki navaja, da mora biti katalog kaznivih dejanj oblikovan primerno, da je ukrep sorazmeren v ožjem pomenu in da intenzivnost posega odtehta pomen dobrine.

⁹⁸ Prim P. Plesec, nav. delo, str. 33, 34; K. Šugman Stubbs, nav. delo, 2003, str. 203.

B. – III.**Izpodbijani 149.c člen ZKP**

64. Izpodbijani 149.c člen ZKP določa:

"(1) Če so podani razlogi za sum, da je bilo izvršeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in za katerega je predpisana kazen enega ali več let zapora in je za odkritje, preprečitev ali dokazovanje tega kaznivega dejanja ali odkritje storilca treba pridobiti podatke o prometu v zvezi s komunikacijo osumljenca, oškodovanca ali oseb iz drugega odstavka 149.a člena tega zakona ali če zakoniti uporabnik komunikacijskega sredstva s tem soglaša, lahko preiskovalni sodnik na obrazložen predlog državnega tožilca odredi operaterju oziroma ponudniku storitev informacijske družbe, da začne z zavarovanjem potrebnih prometnih podatkov v zvezi s komunikacijo ter sporočanjem le-teh pristojnemu organu. Preiskovalni sodnik mora v odredbi natančno opredeliti kategorije podatkov, ki jih zahteva, in obdobje, za katero se ukrep odreja in ki ne sme biti daljše od treh mesecev. Preiskovalni sodnik lahko z novo odredbo odredi podaljšanje izvajanja ukrepa za tri mesece. Če je zoper komunikacijsko sredstvo odrejen tudi ukrep po 150. členu tega zakona lahko sodnik odreja ukrepe po tem členu za ves čas izvrševanja ukrepov iz 150. člena tega zakona zoper to komunikacijsko sredstvo. Odredba se operaterju oziroma ponudniku storitev informacijske družbe vroča v delu, ki se nanaša nanj.

(2) Predlog in odredba morata biti pisna in morata vsebovati podatke, ki omogočajo enolično identifikacijo komunikacijskega sredstva ali uporabnika, utemeljitev razlogov, relevantno časovno obdobje, za katerega se ukrep odreja, pogostost sporočanja podatkov pristojnemu organu ter ostale pomembne okoliščine, ki narekujejo uporabo ukrepa, vključno z obrazložitvijo sorazmernosti. Identifikacija komunikacijskega sredstva mora biti dovolj natančna, da zahtevke omejuje na vnaprej omejen in določljiv seznam oseb.

(3) Z odredbo ni mogoče zahtevati posredovanja podatkov, ki se nanašajo na lokacijo komunikacijskega sredstva ali uporabnika, razen za kazniva dejanja iz četrtega odstavka 149.a člena tega zakona ali s soglasjem zakonitega uporabnika komunikacijskega sredstva.

(4) Operater oziroma ponudnik storitev informacijske družbe svojemu uporabniku, naročniku ali tretjim osebam ne sme razkriti, da je ali da bo v skladu s tem členom posredoval določene podatke. Tega ne sme razkriti 24 mesecev po preteku meseca, v katerem se je zaključilo izvrševanje odredbe. Preiskovalni sodnik lahko z odredbo določi drugačen rok, rok podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok skrajša ali prepoved seznanitve odpravi. Ne glede na določbe tega odstavka pa v primeru posredovanja podatkov na podlagi soglasja zakonitega uporabnika

operater oziroma ponudnik storitve informacijske družbe v roku osem dni od posredovanja podatkov obvesti zakonitega uporabnika o izvršitvi odredbe.

(5) Na podlagi tega člena ni mogoče zahtevati ali pridobiti podatkov, ki se nanašajo na vsebino komunikacije."

65. V tem členu sta urejena dva vsebinsko različna ukrepa. Prvi odstavek 149.c člena ZKP ureja zavarovanje in pridobivanje oziroma obdobjno sporočanje podatkov operaterja oziroma ponudnika storitev informacijske družbe o prometu v zvezi s komunikacijo osumljenca, oškodovanca ali oseb iz drugega odstavka 149.a člena ZKP v realnem času (torej za naprej; za razliko od 149.b člena ZKP, ki omogoča pridobitev podatkov za nazaj),⁹⁹ in sicer za tri mesece z možnostjo podaljšanja za nadaljnje tri mesece. Če je zoper komunikacijsko sredstvo odrejen tudi ukrep po 150. členu ZKP, lahko sodnik odreja ukrepe po tem členu za ves čas izvrševanja teh ukrepov. V drugem odstavku 149.c člena ZKP je urejena vsebina predloga in odredbe za odreditev izpodbijanega ukrepa, v četrtem prepoved razkritja ukrepa osebi, da so bili njegovi podatki posredovani, v petem pa prepoved pridobivanja vsebine komunikacij. Tako kot pri ukrepu po 149.b členu ZKP gre za pridobivanje prometnih podatkov.¹⁰⁰

66. Tretji odstavek 149.c člena ZKP pa ureja zavarovanje in posredovanje podatkov, ki se nanašajo na lokacijo komunikacijskega sredstva ali uporabnika, v istem obdobju.¹⁰¹ Pridobivanje podatkov o lokaciji je sicer načeloma prepovedano, razen za kazniva dejanja iz četrtega odstavka 149.a člena ZKP ali s soglasjem zakonitega uporabnika komunikacijskega sredstva. Lokacijski podatki v skladu s tem odstavkom se lahko pridobivajo od osumljenca, oškodovanca ali osebe iz drugega odstavka 149.a člena ZKP. Tudi v tem primeru podatke o lokaciji posreduje operater oziroma ponudnik storitev informacijske družbe.¹⁰²

Presoja z vidika načela jasnosti in pomenke določljivosti

67. Predlagatelj izpodbija ureditev 149.c člena ZKP tako z vidika njene jasnosti in pomenke določljivosti (2. člen Ustave) kot tudi z vidika nesorazmernosti posega v človekove pravice in temeljne svoboščine. V zvezi s prvim očitkom tako navaja, da je nejasno, kateri pogoj iz prvega odstavka 149.c člena ZKP naj bi bil nadomeščen s pogojem "ali že zakoniti uporabnik komunikacijskega sredstva s tem soglaša".

68. Iz načela pravne države iz 2. člena Ustave med drugim izhaja tudi zahteva, da so predpisi jasni in določni, tako da je mogoče ugotoviti vsebino in namen pravila. To velja

⁹⁹ Predlog ZKP-N, str. 144.

¹⁰⁰ Prav tam.

¹⁰¹ Oba ukrepa se lahko izvršita tudi s soglasjem zakonitega uporabnika komunikacijskega sredstva (prvi in tretji odstavek 149.c člena ZKP).

¹⁰² V tem delu se ukrep razlikuje od uporabe IMSI lovilca, ki ga uporabi policija sama.

za vse predpise, zlasti pa je to pomembno pri predpisih, ki določajo pravice ali dolžnosti pravnih subjektov. Norme morajo biti opredeljene jasno in določno, tako da jih je mogoče izvajati, da ne omogočajo arbitrarnega ravnanja ter da nedvoumno in dovolj določno opredeljujejo pravni položaj subjektov, na katere se nanašajo.¹⁰³

69. Čim pomembnejša je varovana dobrina, tem bolj poudarjena je zahteva po določnosti zakona.¹⁰⁴ Glede na to, da pomenijo pooblastila represivnih organov, med katera vabljenje na policijsko postajo na podlagi izpodbijane določbe nedvoumno spada, močan poseg v človekove pravice posameznika, morajo temeljiti na posebno natančni ureditvi z jasnimi in podrobnimi pravili. Zakonska ureditev mora biti taka, da izključuje možnost arbitrarnega ravnanja države. Poleg predvidljivosti mora zakonska ureditev zagotavljati zlasti učinkovit pravni nadzor ter ustrezna in učinkovita sredstva zoper zlorabo.¹⁰⁵ Če meja med dovoljenim in nedovoljenim ravnanjem državnih organov ni opredeljena, so lahko vse varovalke zoper arbitrarno uporabo zakona neučinkovite.¹⁰⁶

70. Zahteva po jasnosti in pomenski določljivosti predpisa pa ne pomeni, da morajo biti predpisi taki, da jih ne bi bilo treba razlagati. Uporaba predpisov vedno pomeni njihovo razlago, in tako kot vsi drugi predpisi so tudi zakoni predmet razlage. Z vidika pravne varnosti, ki je eno od načel pravne države iz 2. člena Ustave, pa postane predpis sporen takrat, kadar s pomočjo pravil o razlagi ne moremo priti do njegove jasne vsebine.¹⁰⁷ Predpis torej izpolnjuje zahtevo po jasnosti in pomenski določljivosti, če je mogoče z ustaljenimi metodami razlage ugotoviti vsebino pravila in je na ta način dolžno ravnanje naslovnikov določno in predvidljivo.¹⁰⁸

71. V zvezi z navedbo predlagatelja, da je nejasno, kateri pogoj iz prvega odstavka 149.c člena ZKP naj bi bil nadomeščen s pogojem "ali že zakoniti uporabnik komunikacijskega sredstva s tem soglaša", Ustavno sodišče ugotavlja, da prvi odstavek 149.c člena ZKP določa več kumulativnih prvin: (1) dokazni standard (če so podani razlogi za sum); (2) kaznivo dejanje, na katero se veže dokazni standard (da je bilo izvršeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in za katero je predpisana kazen enega ali več let zapor); (3) potrebo po pridobitvi prometnih podatkov (in je za odkritje,

¹⁰³ Prim. odločbe Ustavnega sodišča št. U-I-131/04 z dne 21. 4. 2005 (Uradni list RS, št. 50/05, in OdlUS XIV, 24), št. U-I-24/07 z dne 4. 10. 2007 (Uradni list RS, št. 101/07, in OdlUS XVI, 74) in št. U-I-155/11 z dne 18. 12. 2013 (Uradni list RS, št. 114/13, in OdlUS XX, 12).

¹⁰⁴ Odločbi Ustavnega sodišča št. U-I-25/95 in št. U-I-18/93.

¹⁰⁵ Prav tam.

¹⁰⁶ Odločba Ustavnega sodišča št. U-I-28/16 z dne 12. 5. 2016 (Uradni list RS, št. 42/16, in OdlUS XXI, 25), 14. točka obrazložitve.

¹⁰⁷ Prim. odločbo Ustavnega sodišča št. U-I-32/02 z dne 10. 7. 2003 (Uradni list RS, št. 73/03, in OdlUS XII, 71).

¹⁰⁸ Prim. sklep Ustavnega sodišča št. U-I-98/02 z dne 28. 10. 2004.

preprečitev ali dokazovanje tega kaznivega dejanja ali odkritje storilca treba pridobiti podatke o prometu); (4) osebe, katerih prometni podatki se pridobijo (v zvezi s komunikacijo osumljenca, oškodovanca ali oseb iz drugega odstavka 149.a člena ZKP); in (5) nadomestni pogoj (ali če zakoniti uporabnik komunikacijskega sredstva s tem soglaša).

72. Ker četrta prvina (osebe, katerih podatki se pridobijo) ni pogoj, se nadomestni pogoj nanjo ne more vezati. Pridobivanje prometnih podatkov, ne da bi bilo to potrebno za odkritje, preprečitev ali dokazovanje kaznivega dejanja ali odkritje storilca, bi bilo v nasprotju z namenom ZKP iz prvega odstavka 1. člena.¹⁰⁹ Razlaga, da soglasje oškodovanca nadomesti procesno potrebo po pridobitvi prometnih podatkov, je jezikovno sicer možna, ne bi pa bila skladna z namenom predpisa. Ob stališčih teorije, da je namen eden od argumentov, ki ima odločujoč vpliv na izbiro med več možnimi rešitvami,¹¹⁰ in da je med več jezikovno možnimi rešitvami treba izbrati tisto, ki najintenzivneje ustreza namenu pravnega pravila,¹¹¹ pa ne pride v poštev.

73. Tudi razlaga, da soglasje nadomesti dokazni standard, ne bi bila združljiva z namenom ZKP iz prvega odstavka 1. člena, kajti če niso podani vsaj razlogi za sum, tj. najnižji obstoječ dokazni standard, ob izostanku drugega pogoja, ki bi kazal na neko možnost obstoja kaznivega dejanja, za izvedbo tega ukrepa ni nobene potrebe. Možnost odreditve ukrepa tudi tedaj, ko ni razlogov za sum izvršitve kaznivega dejanja, bi bila sicer uporabna in smiselna v primeru iskanja pograšanih oseb, vendar pa ima policija za ta namen na voljo posebno pooblastilo za iskanje oseb iz 43. člena ZNPPol.

74. Kot zadnji možni predmet nadomestnega pogoja preostane torej druga prvina, tj. izvršeno, izvrševano ali načrtovano kaznivo dejanje, na katero se veže dokazni standard – tj. kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in za katero je predpisana kazen enega ali več let zapor. Zaradi namena ZKP je spet možna le razlaga, da se s soglasjem uporabnika nadomešča pogoj, da gre za kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in za katero je predpisana kazen enega ali več let zapor. Ker nadomestitev pogoja uradne pregonljivosti ni smiselna (bila bi v nasprotju z namensko razlago), saj je upravičeni predlagatelj tega ukrepa le državni tožilec, ne pa tudi zasebni tožilec ali oškodovanec kot tožilec,¹¹² soglasje uporabnika lahko nadomesti le pogoj, s katerim je določen kaznovalni okvir (za katerega je predpisana kazen enega ali več let zapor). To izhaja tudi iz zakonodajnega gradiva, po katerem naj bi izpodbijani zakonski pogoj pokrival statistično pogoste

¹⁰⁹ Prvi odstavek 1. člena ZKP določa: "Ta zakon določa pravila, ki naj zagotovijo, da se nihče, ki je nedolžen, ne obsodi, storilcu kaznivega dejanja pa izreče kazenska sankcija ob pogojih, ki jih določa kazenski zakon, in na podlagi zakonitega postopka."

¹¹⁰ M. Pavčnik, Teorija prava, 5. izdaja, Ius software, GV Založba, Ljubljana 2019, str. 411.

¹¹¹ Prav tam, str. 380.

¹¹² Prvi odstavek 63. člena ZKP določa, da ima oškodovanec kot tožilec iste pravice kot državni tožilec, razen tistih, ki jih ima državni tožilec kot državni organ.

primere tatvine ali zatajitve mobilnega telefona, v katerih naj bi oškodovanci (tj. zakoniti imetniki mobilnega telefona) dali privolitev za pridobivanje podatkov. Šlo naj bi za alternativo katalogu kaznivih dejanj iz 149.a člena ZKP.¹¹³

75. Glede na to, da je pomen zakonskega besedila določljiv z ustaljenimi metodami razlage (v konkretnem primeru zlasti z jezikovno, namensko in logično), predlagatelj ni izkazal neskladja z načelom jasnosti in pomenke določljivosti predpisov iz 2. člena Ustave.¹¹⁴

76. Predlagatelj izpodbijanemu ukrepu nadalje očita, da ni določen postopek za podaljšanje ukrepa niti ni določeno, ali preiskovalni sodnik odloča po uradni dolžnosti ali na predlog, niti niso določeni razlogi za podaljšanje ukrepa.

77. ZKP v zvezi s podaljšanjem določa, da mora preiskovalni sodnik v odredbi natančno opredeliti kategorije podatkov, ki jih zahteva, in obdobje, za katero se ukrep odreja, to pa ne sme biti daljše od treh mesecev. Z novo odredbo lahko odredi podaljšanje izvajanja ukrepa za tri mesece. Če je zoper komunikacijsko sredstvo odrejen tudi ukrep po 150. členu ZKP, pa lahko sodnik odreja ukrepe po 149.c členu ves čas izvrševanja ukrepov iz 150. člena ZKP zoper to komunikacijsko sredstvo.¹¹⁵

78. Glede odreditve ukrepa ZKP določa, da preiskovalni sodnik odredi ukrep operaterju oziroma ponudniku storitev informacijske družbe na obrazložen predlog državnega tožilca,¹¹⁶ da morata biti predlog in odredba pisna in morata vsebovati podatke, ki omogočajo enolično identifikacijo komunikacijskega sredstva ali uporabnika, utemeljitev razlogov, relevantno obdobje, za katero se ukrep odreja, pogostost sporočanja podatkov pristojnemu organu in druge pomembne okoliščine, ki narekujejo uporabo ukrepa, vključno z obrazložitvijo sorazmernosti. Identifikacija komunikacijskega sredstva mora biti dovolj natančna, da zahtevek omejuje na vnaprej omejen in določljiv seznam oseb.¹¹⁷

79. Postopek odreditve podaljšanja ukrepa resda ni posebej predpisan, je pa mogoče po analogiji zanj uporabiti zakonsko ureditev postopka odreditve ukrepa. Položaja odreditve in podaljšanja ukrepa sta si namreč v bistvenem podobna, kar pomeni, da so pogoji za posamično analogijo izpolnjeni.¹¹⁸ Besedilo prvega odstavka 149.c člena ZKP tako omogoča tudi ustavnoskladno razlago navedene izpodbijane določbe.

¹¹³ Predlog ZKP-N, str. 28, 144. Glej tudi P. Križnar v: M. Šepec (ur.), nav. delo.

¹¹⁴ Ustavno sodišče izpodbijane določbe ni presoјalo z vidika 37. člena Ustave, ker to ni predlog presoје v obravnavanem primeru.

¹¹⁵ Prvi odstavek 149.c člena ZKP.

¹¹⁶ Prav tam.

¹¹⁷ Drugi odstavek 149.c člena ZKP.

¹¹⁸ M. Pavčnik, nav. delo, str. 398–400.

Predlagatelj zato tudi s tega vidika ni izkazal neskladja z načelom jasnosti in pomenske določljivosti predpisov iz 2. člena Ustave.

Presoja ukrepov iz prvega in tretjega odstavka 149.c člena ZKP

80. Predlagatelj izpodbija ureditev iz 149.c člena ZKP tudi z vidika nesorazmernosti posega v človekove pravice in temeljne svoboščine. Iz razlogov, ki jih je Ustavno sodišče navedlo že v zvezi z ukrepom iz prvega odstavka 149.b člena ZKP (63. točka obrazložitve te odločbe), pomeni pridobivanje prometnih podatkov (tudi v realnem času na podlagi prvega odstavka 149.c člena ZKP) poseg v pravico iz prvega odstavka 37. člena Ustave.

81. Z ukrepom po tretjem odstavku 149.c člena ZKP policija pridobi podatke o lokaciji komunikacijskega sredstva ali uporabnika. Lokacijski podatki oziroma podatki o lokaciji so vsakršni podatki, obdelani v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki kažejo na zemljepisni položaj terminalske opreme uporabnika javno dostopne elektronske komunikacijske storitve.¹¹⁹ Telekomunikacijska terminalska oprema, katere lokacijo operater sporoči policiji na podlagi tretjega odstavka 149.c člena ZKP, je proizvod ali njegov ustrezni sestavni del, ki je namenjen za neposredno ali posredno priključitev s katerimkoli sredstvi na vmesnike javnih komunikacijskih omrežij, ki se v celoti ali delno uporabljajo za zagotavljanje javnih komunikacijskih storitev.¹²⁰

82. Ukrep po tretjem odstavku 149.c člena ZKP tako pomeni, da operater ali ponudnik storitev informacijske družbe občasno (pri čemer se pogostost poročanja določi v sodni odredbi)¹²¹ v določenem daljšem obdobju¹²² pridobiva in posreduje pristojnemu organu podatke o tem, kje je, se giblje oziroma premika terminalska oprema in posledično tudi uporabnik javno dostopne elektronske komunikacijske storitve. Ukrep namreč temelji

¹¹⁹ Točka 44 3. člena, 219. in 220. člen ZEKom-2 ter 3. točka prvega odstavka 2. člena ZEPT.

¹²⁰ Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (prenovitev, UL L 321, 17. 12. 2018, str. 36–214) opredeljuje terminalsko opremo tako, kot je opredeljena v 1. točki 1. člena Direktive Komisije 2008/63/ES z dne 20. junija 2008 o konkurenci na trgih za telekomunikacijsko terminalsko opremo (UL L 162, 21. 6. 2008, str. 20–26), kar pomeni (a) vso opremo, ki je neposredno ali posredno priključena na mrežni vmesnik javnega telekomunikacijskega omrežja za pošiljanje, obdelovanje ali sprejemanje informacij; v obeh primerih (neposredna ali posredna) se lahko priključitev izvede z žico, optičnim kablom ali elektromagnetno; priključitev je posredna, če je oprema nameščena med terminalom in javnim mrežnim vmesnikom; in (b) tudi opremo satelitskih zemeljskih postaj. Opredeljujejo jo tudi splošni pogoji poslovanja posameznega operaterja.

¹²¹ Pogostost sporočanja se določi v odredbi (drugi odstavek 149.c člena ZKP).

¹²² Prvi odstavek 149.c člena ZKP.

na predpostavki, da se s sledenjem terminalne opreme sledi tudi njenemu uporabniku, ker naj bi uporabnik mobilno napravo¹²³ (večinoma) imel pri sebi.¹²⁴

83. Ukrep glede na namen (tj. pridobiti lokacijo)¹²⁵ zagotovo cilja na pridobivanje podatkov o lokaciji mobilne naprave, katere bistvena lastnost je mobilnost oziroma možnost spreminjanja lokacije. To izhaja tudi iz zakonodajnega gradiva, v katerem je ukrep poimenovan kot "sledenje v realnem času", glede primera uporabe ukrepa v primeru soglasja pa je poudarjen predvsem primer tatvine mobilnega telefona.¹²⁶

84. Dolgotrajno zavarovanje, hramba in posredovanje podatkov o lokaciji uporabnika lahko (podobno kot pridobitev prometnih podatkov) razkrijejo podatke ne le o lokaciji uporabnika, temveč tudi o tem, kaj na tisti lokaciji počne.¹²⁷ Podatek nam ne pove le točne lokacije mobilne naprave in s tem osebe, pač pa tudi to, kje se je nekdo gibal ali kam je šel, ter nam tako posredno lahko razkrije tudi politične, verske,¹²⁸ prijateljske, ljubezenske, profesionalne in prostčasne aktivnosti te osebe.¹²⁹ Bistvena je zmožnost zbiranja lokacijskih točk in ne sledenje gibanju, saj se iz lokacijskih točk ustvari profil posameznika, ki je tak, da ga povprečen opazovalec življenja opazovanega posameznika z lastnimi čutili in opazovanji ne bi bil zmožen ustvariti. Iz vsebine

¹²³ B. Markelj, I. Bernik, Varnost mobilnih naprav, Univerzitetna založba Univerze v Mariboru, Fakulteta za varnostne vede, Maribor, Ljubljana 2018, str. 3, 4, opredeljujeta mobilne naprave kot vse naprave, ki jih lahko prenašamo in pri katerih je mogoče brezžično dostopati do interneta.

¹²⁴ Ukrep ima sicer vsaj pomanjkljivost, ki pa jo je mogoče zanemariti. Ni namreč nujno, da ima uporabnik mobilno napravo tudi vedno pri sebi. P. Križnar, Varstvo lokacijske zasebnosti s pomočjo mozaične teorije podatkov, Zbornik znanstvenih razprav (2016), str. 106.

¹²⁵ Natančnost določanja lokacije terminalne opreme in s tem uporabnika je odvisna od tehnike in opreme, ki jo operater uporablja. Glej prav tam, str. 105 in nasl. Glede na to, da podatke sporoča operater in jih ne pridobiva policija sama (kot pri IMSI lovilcu), je najverjetnejša metoda pridobivanje podatkov o lokaciji mobilne naprave prek globalnega sistema za mobilno komuniciranje, natančnost ugotavljanja lokacije pa je odvisna od velikosti bazne postaje. Velikost posamezne celice je odvisna od geografskih značilnosti območja in števila uporabnikov, ki jih mora pokriti. I. Kolar, Zakonska ureditev uporabe lovilca IMSI števil, diplomsko delo, Pravna fakulteta Univerze v Ljubljani, Ljubljana 2016.

¹²⁶ Predlog ZKP-N, str. 28. Ustavno sodišče se ne opredeljuje do ustavne skladnosti zakonskega pogoja soglasja, ker to ni predmet presoje v obravnavanem primeru.

¹²⁷ P. Križnar, nav. delo, 2016, str. 114. Podobno ESČP v sodbi v zadevi *Uzun proti Nemčiji*.

¹²⁸ Glej sodbo SEU v združenih zadevah *La Quadrature du Net in drugi*, 117. točka obrazložitve: "Pridobijo se podatki o številčnih vidikih zasebnega življenja uporabnika mobilne naprave, tudi občutljivi podatki, kot so spolna usmerjenost, politično prepričanje, versko, filozofsko, družbeno in drugo prepričanje, zdravstveno stanje." Glej tudi sodno prakso SEU, na katero se to sodišče sklicuje v tej točki obrazložitve.

¹²⁹ Prav tam. Šlo naj ne bi za nič manj občutljive podatke kot pri pridobivanju vsebine komunikacije.

lokacijskih podatkov si je torej mogoče ustvariti sliko o zasebnem življenju opazovanega.¹³⁰

85. Tak skupek lokacijskih podatkov in izoblikovanje celostne podobe pa je predmet varstva zasebnosti,¹³¹ tj. lokacijske zasebnosti. Vsak posameznik mora biti sposoben nadzirati informacije, s katerimi izdaja svojo trenutno ali preteklo lokacijo, oziroma preprečiti, da se s to lokacijo seznanijo nekdo tretji.¹³²

86. Ustavno sodišče se v svoji dosedanji presoji še ni opredelilo, katera določba Ustave varuje lokacijsko zasebnost. Zato je moralo odgovoriti najprej na to vprašanje.

87. Po ustaljeni praksi ESČP so lokacijski podatki predmet varstva splošnega 8. člena EKČP.¹³³ Lokacijski podatki (pridobljeni z GPS napravo) so osebni podatki, če izkazujejo, kje je posameznik, in njegovo gibanje v javnosti.¹³⁴ Obdelavo in uporabo takih podatkov pa je mogoče šteti za poseg v pravico do zasebnega življenja.¹³⁵

88. SEU je v že omenjeni sodbi v združenih zadevah *La Quadrature du Net in drugi* podobno odločilo, da pomeni zbiranje (prometnih in) lokacijskih podatkov poseg v temeljni pravici do zasebnosti in do varstva osebnih podatkov iz 7. in 8. člena Listine, ne glede na občutljivost podatkov in ne glede na to, ali je oseba zaradi tega posega

¹³⁰ P. Križnar, nav. delo, 2016, str. 115.

¹³¹ Prav tam.

¹³² Prav tam, str. 101.

¹³³ Sodbe ESČP v zadevah *Uzun proti Nemčiji*, *Ben Faiza proti Franciji* ter *Florindo de Almeida Vasconcelos Gramaxo proti Portugalski*. Glej tudi M. Naartijärvi, Swedish police implementation of Imsi-Catchers, a European law perspective, *Computer Law & Security Review*, št. 6 (2016), str. 861. V sodbi v zadevi *Ben Faiza proti Franciji* je ESČP odločalo tudi o vprašanju nadzora geolokacije v realnem času. Odločilo je, da pomeni poseg v pravico iz 8. člena EKČP, in ugotovilo, da ukrep ni bil v skladu z zakonom, ker je bila pravna podlaga preveč nejasna.

¹³⁴ Sodba ESČP v zadevi *Uzun proti Nemčiji*, 51. in 52. točka obrazložitve. ESČP je odločilo, da pomeni GPS sledenje poseg v pravico iz 8. člena EKČP, ker pomeni zbiranje podatkov o pritožniku, ne glede na to, da je bil GPS sledilnik nameščen v avto sostorilca. Šlo naj bi za sistematično zbiranje in hrambo podatkov z ugotavljanjem pritožnikovega položaja in gibanja v javni sferi. Načela, ki jih je ESČP razvilo za posege v komunikacijsko zasebnost, naj bi bilo z zadržkom mogoče uporabiti tudi pri GPS nadzoru, ki naj bi pomenil manjši poseg v zasebnost kot nadzor komunikacij. Trajanje ukrepa naj bi bilo sorazmerno, ukrep naj bi bil odrejen zgolj zaradi kaznivega dejanja zadostne teže, z naknadno sodno presojjo, ukrep pa naj bi bil nujen v demokratični družbi (hudo kaznivo dejanje, milejši ukrepi naj ne bi bili učinkoviti, nadzor naj ne bi bil neomejen, ampak naj bi trajal 3 mesece in samo takrat, ko je bil pritožnik v soobdolženčevem avtomobilu). Zato naj ukrep ne bi bil sorazmeren. Glej 51.–53., 66., 69.–71. in 80. točko obrazložitve.

¹³⁵ Prav tam, 51. in 52. točka obrazložitve.

utrpela kakršnekoli neprijetnosti.¹³⁶ Prav tako spada po stališču SEU zbiranje (prometnih in) lokacijskih podatkov ter dostop državnih organov do njih za namene kazenskega postopka ali nacionalne varnosti v okvir Direktive o zasebnosti in elektronskih komunikacijah.¹³⁷

89. Na podlagi navedenega je Ustavno sodišče odločilo, da je varstvo lokacijske zasebnosti zagotovljeno tako s 35. členom kot tudi z 38. členom Ustave.¹³⁸

90. Ustava v prvem odstavku 38. člena zagotavlja človekovo pravico do varstva osebnih podatkov. Ustavno sodišče je večkrat poudarilo, da je ustavodajalec s tem posebej zavaroval enega od vidikov posameznikove zasebnosti, t. i. informacijsko zasebnost.¹³⁹ S tem ko Ustava to pravico ureja posebej, ji daje posebno mesto in pomen v siceršnjem varstvu zasebnosti posameznika.¹⁴⁰

91. Iz odločbe Ustavnega sodišča št. U-I-98/11 z dne 26. 9. 2012 (Uradni list RS, št. 79/12) izhaja, da je temeljna vrednostna podstat te ustavne določbe spoznanje, da ima posameznik pravico zadržati informacije o sebi zase in da je v izhodišču on tisti, ki odloča, koliko informacij o sebi bo razkril in komu. Določena mera skritosti pred pogledi drugih je nujna predpostavka za svoboden razvoj posameznikovih intelektualnih in duhovnih potencialov. V tem smislu varstvo informacijske zasebnosti pospešuje svobodno nastajanje in pretok misli in idej ter utrjuje pluralno demokratično družbo. Zaradi posameznikove vpetosti v družbo pa informacijska zasebnost ne more biti neomejena, absolutna. Posameznik mora tako ob ustavno določenih pogojih dopustiti zbiranje in obdelovanje osebnih podatkov.¹⁴¹

¹³⁶ Sodba SEU v združenih zadevah *La Quadrature du Net in drugi*, 115. točka obrazložitve. Glej tudi mnenje SEU 1/15 (EU-Kanada PNR dogovor) z dne 26. 7. 2017, 124. in 126. točka obrazložitve; in sodbo ESČP v zadevi *Breyer proti Nemčiji* z dne 30. 1. 2020, 81. točka obrazložitve.

¹³⁷ Sodba SEU v združenih zadevah *La Quadrature du Net in drugi*, 68., 104., 117.–120. točka obrazložitve.

¹³⁸ Čeprav se Ustavno sodišče doslej do tega vprašanja še ni izrecno opredelilo, pa je v delni odločbi št. U-I-152/17 (ANPR) z dne 4. 7. 2019 (Uradni list RS, št. 123/20, in OdlUS XXIV, 11) očitke predlagatelja o nesorazmernem posegu ukrepa optične prepoznave tablic (ANPR) v lokacijsko zasebnost presojalo z vidika informacijske zasebnosti iz 38. člena Ustave (34. točka obrazložitve). Vendar je presojo opravilo zgolj z vidika obstoja zakonske podlage za poseg. Ker je ugotovilo, da je ni, niti ni moglo presojati navedb predlagatelja, ali je poseg dopusten pod pogoji iz tretjega odstavka 15. člena in 2. člena Ustave (t. i. strogi test sorazmernosti), prav tako se, kot navedeno, ni izrecno opredelilo do lokacijske zasebnosti.

¹³⁹ Odločba Ustavnega sodišča št. U-I-238/99 z dne 9. 11. 2000 (Uradni list RS, št. 113/2000, in OdlUS IX, 257), 16. točka obrazložitve.

¹⁴⁰ Delna odločba Ustavnega sodišča št. U-I-152/17 (ANPR), 19. točka obrazložitve.

¹⁴¹ Odločba Ustavnega sodišča št. U-I-98/11, 12. točka obrazložitve.

92. Po ustaljeni ustavnosodni presoji pomeni vsako zbiranje in obdelovanje osebnih podatkov poseg v pravico do varstva zasebnosti oziroma v pravico posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi. Temeljna vrednostna podstat te pravice je spoznanje, da ima posameznik pravico zadržati informacije o sebi zase in da je v izhodišču on tisti, ki odloča, koliko informacij o sebi bo razkril in komu.¹⁴²

93. Iz Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS, št. 11/94, MP, št. 3/94 – v nadaljevanju MKVP), Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4. 5. 2016 – v nadaljevanju Direktiva 2016/680),¹⁴³ Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22– v nadaljevanju ZVOP-2)¹⁴⁴ in Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (Uradni list RS, št. 177/20 – v nadaljevanju ZVOPOKD),¹⁴⁵ ki so sprejeli široko, vsevkjučujočo opredelitev, izhaja, da je osebni podatek katerakoli informacija v zvezi z določenim ali določljivim posameznikom; določljiv posameznik pa je tisti, ki ga je mogoče neposredno ali posredno določiti,¹⁴⁶ zlasti z navedbo identifikatorja, kot so ime, identifikacijska številka, podatki o lokaciji in spletni identifikator, ali z navedbo enega ali več dejavnikov, značilnih za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.¹⁴⁷

94. Izpodbijana ureditev predvideva obdelavo osebnih podatkov. Podatek o lokaciji posameznika, njegovem gibanju in poteh (torej lokacijski podatki) se nanaša na informacije v zvezi s terminalsko opremo, najpogosteje mobilno napravo določenega posameznika. Zaradi vezanosti terminalske opreme na njenega uporabnika in zato, ker je namen ukrepa po tretjem odstavku 149.c členu ZKP zbiranje dokazne podlage za vložitev kazenske ovadbe (na stopnji utemeljenega suma) zoper določenega osumljenca, so zbrani podatki osebni podatki. To še toliko bolj velja za podatke, ki jih

¹⁴² Glej npr. odločbi Ustavnega sodišča št. U-I-98/11, 12. točka obrazložitve, in št. U-I-65/13, 16. točka obrazložitve.

¹⁴³ Prvi odstavek 3. člena Direktive 2016/680.

¹⁴⁴ Prvi odstavek 5. člena ZVOP-2 v povezavi s 1. točko 4. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju Splošna uredba o varstvu podatkov) (UL L 119, 4. 5. 2016).

¹⁴⁵ Prvi odstavek 4. člena ZVOPOKD.

¹⁴⁶ Glej tudi mnenje št. 4/2007 Delovne skupine 29 o opredelitvi pojma osebnega podatka, prvi odstavek 5. člena ZVOP-2 v povezavi s 1. točko 4. člena Splošne uredbe o varstvu podatkov.

¹⁴⁷ Prvi odstavek 4. člena ZVOPOKD.

je iz spremljanja lokacijskih podatkov mogoče posredno razbrati; tj. za podatke o posameznikovih navadah in lastnostih.¹⁴⁸ To neposredno izhaja tudi iz Direktive 2016/680 in ZVOPOKD, ki kot identifikatorja za določitev posameznika določata tudi podatek o lokaciji.¹⁴⁹

95. Drugi odstavek 38. člena Ustave določa, da mora zbiranje, obdelovanje in namen uporabe osebnih podatkov določati zakon. Čeprav ta ustavna določba razlikuje med pojmi zbiranje, uporaba in obdelava osebnih podatkov, Ustavno sodišče uporablja pojem obdelava osebnih podatkov kot zbirni pojem za označevanje vseh dejanj, ki se izvajajo v zvezi z osebnimi podatki v skladu s splošno sprejeto terminologijo.¹⁵⁰

96. Po ustaljeni ustavnosodni presoji pomeni vsako obdelovanje osebnih podatkov poseg v ustavno pravico do varstva osebnih podatkov iz 38. člena Ustave.¹⁵¹ Drugi odstavek 38. člena Ustave zahteva, da je obdelovanje osebnih podatkov predmet zakonskega urejanja.¹⁵² Poseg v pravico do varstva osebnih podatkov je dopusten, če je v zakonu med drugim določeno opredeljeno, kateri podatki se smejo zbirati in obdelovati. Zbirati se smejo le podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega namena.¹⁵³

97. Pravici do komunikacijske¹⁵⁴ in informacijske¹⁵⁵ zasebnosti nista neomejeni, nista absolutni. Poseg v navedeni pravici je dopusten v primerih iz tretjega odstavka 15. člena Ustave, če je zakonodajalec zasledoval ustavno dopusten cilj in če je omejitev

¹⁴⁸ Prim. z mnenjem Informacijskega pooblaščenca o varstvu osebnih podatkov pri elektronskem cestninjenju z dne 14. 7. 2008.

¹⁴⁹ Točka 1 3. člena Direktive 2016/680, 1. točka 4. člena ZVOPOKD.

¹⁵⁰ Odločba Ustavnega sodišča št. U-I-98/11, opomba 3, in odločba Ustavnega sodišča št. U-I-411/06 z dne 19. 6. 2008 (Uradni list RS, št. 68/08, in OdlUS XVII, 43), opomba 11. Glej tudi 2. člen MKVP, 4. člen Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4. 5. 2016 – v nadaljevanju Splošna uredba o varstvu podatkov) in 3. člen Direktive 2016/680.

¹⁵¹ Odločba Ustavnega sodišča št. U-I-238/99, 18. točka obrazložitve.

¹⁵² Prav tam, 16. točka obrazložitve, in odločbe Ustavnega sodišča št. U-I-92/01 z dne 28. 2. 2002 (Uradni list RS, št. 22/02, in OdlUS XI, 25), 25. točka obrazložitve, št. U-I-298/04 z dne 27. 10. 2005 (Uradni list RS, št. 100/05, in OdlUS XIV, 77), 7. točka obrazložitve, št. U-I-57/06 z dne 29. 3. 2007 (Uradni list RS, št. 33/07, in OdlUS XVI, 22), 62. točka obrazložitve, in št. U-I-411/06, 62. točka obrazložitve.

¹⁵³ Odločbe Ustavnega sodišča št. U-I-238/99, 18. točka obrazložitve, št. U-I-411/06, 19. točka obrazložitve, in št. U-I-312/11 z dne 13. 2. 2014 (Uradni list RS, št. 15/14, in OdlUS XX, 20), 25. točka obrazložitve.

¹⁵⁴ Drugi odstavek 37. člena Ustave.

¹⁵⁵ Odločba Ustavnega sodišča št. Up-349/14 z dne 16. 5. 2019 (Uradni list RS, št. 44/19, in OdlUS XXIV, 29), 17. točka obrazložitve.

skladna z načeli pravne države (2. člen Ustave), in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege države – splošnim načelom sorazmernosti.¹⁵⁶

98. Kot je Ustavno sodišče navedlo že v 39. točki obrazložitve te odločbe v zvezi s pridobivanjem prometnih podatkov za nazaj (149.b člen ZKP), je učinkovita izvedba kazenskega postopka ustavno dopusten cilj za poseg v komunikacijsko zasebnost.

Sorazmernost v ožjem pomenu

99. Ustavno sodišče ocenjuje, ne da bi se spuščalo v presojo, ali je obravnavani poseg zakonodajalca nujen in primeren (ukrep) za zagotovitev zasledovanega cilja, da ta poseg ne prestane preizkusa sorazmernosti v ožjem pomenu.¹⁵⁷ Poseg je sorazmeren, če je teža tega posega (v tem primeru posega v komunikacijsko zasebnost) sorazmerna vrednosti zasledovanega cilja oziroma pričakovanim koristim, ki bodo zaradi posega nastale.¹⁵⁸

Dokazni standard

100. Za ukrepa po prvem in tretjem odstavku 149.c člena ZKP je predpisan isti dokazni standard kot pri ukrepu iz prvega odstavka 149.b člena ZKP. Kot je Ustavno sodišče že navedlo (glej 44. točko obrazložitve te odločbe), se tudi s pridobivanjem prometnih in lokacijskih podatkov po prvem in tretjem odstavku 149.c člena ZKP lahko izoblikuje izčrpen profil o opazovani osebi. Na podlagi navedenega in na podlagi razlogov, ki jih je Ustavno sodišče navedlo v zvezi z ukrepom iz prvega odstavka 149.b člena ZKP (47.–49. točka obrazložitve te odločbe), Ustavno sodišče ugotavlja, da tudi dokazni standard za ukrepa iz prvega in tretjega odstavka 149.c člena ZKP omogoča nesorazmeren poseg v pravici iz prvega odstavka 37. člena oziroma prvega odstavka 38. člena Ustave.¹⁵⁹

Katalog kaznivih dejanj

101. Glede opredelitve kataloga kaznivih dejanj, v zvezi s katerimi se lahko izvrši ukrep iz prvega in tretjega odstavka 149.c člena ZKP, se Ustavno sodišče prav tako sklicuje na svoja stališča o katalogu kaznivih dejanj v zvezi z ukrepom po prvem odstavku 149.b člena ZKP (glej 55.–56. točko obrazložitve te odločbe). Pri tem še dodatno poudarja, da je SEU v sodbi v združenih zadevah *La Quadrature du Net in drugi* posebej obravnavalo pridobivanje prometnih podatkov v realnem času in pri tem močno poudarilo omejenost kataloga kaznivih dejanj. Dostop do avtomatske analize in do zbiranja prometnih in lokacijskih podatkov v realnem času ter do takega zbiranja

¹⁵⁶ Odločba Ustavnega sodišča št. U-I-18/02, 25. točka obrazložitve.

¹⁵⁷ Prim. odločbo Ustavnega sodišča št. U-I-328/05, 14. točka obrazložitve.

¹⁵⁸ Prim. odločbo Ustavnega sodišča št. U-I-83/20, 55. točka obrazložitve.

¹⁵⁹ Prim. P. Križnar v: M. Šepec (ur.), nav. delo.

tehničnih podatkov glede lokacije uporabe terminalske opreme je dopustilo, med drugim, če 1) je avtomatska analiza omejena na situacije, v katerih se država članica sooča z grožnjo nacionalni varnosti, ki je resna in obstoječa, in 2) je pridobivanje prometnih in lokacijskih podatkov v realnem času omejeno na osebe, v zvezi s katerimi obstajajo veljavni razlogi za sum, da so na neki način vpletene v teroristično dejavnost.¹⁶⁰

102. Prometne podatke v realnem času po prvem odstavku 149.c člena ZKP je mogoče pridobiti za kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in za katero je predpisana kazen enega ali več let zapora. To vključuje praktično vsa kazniva dejanja, ki se preganjajo po uradni dolžnosti, izključena so samo tista, ki se preganjajo na zasebno tožbo.¹⁶¹

103. Pridobitev lokacijskih podatkov po tretjem odstavku 149.c člena ZKP pa je mogoča za kazniva dejanja iz četrtega odstavka 149.a člena ZKP, torej v primeru istih kaznivih dejanj, ki so predvidena za ukrep po prvem odstavku 149.b člena ZKP (glej 57. točko obrazložitve te odločbe).

104. Ustavno sodišče meni, da ni mogoče pritrditi stališču zakonodajalca in Vlade, da gre v primeru ukrepov iz prvega in tretjega odstavka 149.c člena ZKP (v primerjavi s 149.b členom ZKP) za milejši ukrep, ker naj bi bil bolj osredotočen in posledično manj invaziven v primerjavi z neselektivno hrambo, zato naj bi bilo dopustno, da je katalog kaznivih dejanj na podlagi načela sorazmernosti in metode niansiranja ustrezno širši.¹⁶² Drži sicer, da je ukrep bolj osredotočen, saj se v realnem času zavarujejo le prometni oziroma lokacijski podatki osebe, ki je predmet nadzora. Vendar ni mogoče zanemariti, da se vzporedno prometni podatki ostalih oseb še vedno neselektivno hranijo na (komercialni)¹⁶³ pravni podlagi in jih je kot take še vedno mogoče pridobiti na podlagi prvega odstavka 149.b člena ZKP. Le podatki osebe, zoper katero je odrejen ukrep po 149.c členu ZKP, se še dodatno zavarujejo in sporočajo na podlagi prvega in tretjega odstavka 149.c člena ZKP. Poleg tega je Ustavno sodišče že v zvezi z ukrepom po 149.b členu ZKP navedlo, da je iz prometnih podatkov, pridobljenih za nazaj, mogoče izoblikovati celosten profil nadzorovane osebe. To še toliko bolj velja za sledenje prometnim in lokacijskim podatkom v realnem času. V razmerju do osebe, zoper katero je ukrep odrejen, je tako ukrep po 149.c členu ZKP intenzivnejši kot ukrep po 149.b členu ZKP.¹⁶⁴ V vseh teh primerih kakovosten in časovno daljši nadzor ustvari podobo

¹⁶⁰ Sodba SEU v združenih zadevah *La Quadrature du Net in drugi*, 188. točka obrazložitve. Glej tudi P. Križnar v: M. Šepec (ur.), nav. delo.

¹⁶¹ Prim z odločbo Ustavnega sodišča št. U-I-272/98, 32. točka obrazložitve.

¹⁶² Predlog ZKP-N, str. 28, 144.

¹⁶³ Člen 215 ZEKom-2.

¹⁶⁴ P. Križnar, nav. delo, 2016, str. 102, 114, piše o mozaični teoriji (lokacijske) zasebnosti, iz katere izhaja, da različni podatki sami zase nimajo neke dramatične vsebinske vrednosti, ko pa nekdo te podatke združi v celoto, slednja zaradi tega pridobi močan vsebinski pomen.

posameznikovega življenja.¹⁶⁵ Bistveni sta torej kakovost in intenzivnost posega, ki omogoča izoblikovanje profila nadzorovane osebe. Nadzor podatkov v realnem času pa tudi omogoča policiji, da prilagaja izvrševanje svojih pooblastil in na podlagi izsledkov tega nadzora takoj poda pobudo za odreditev novih pooblastil. Take hitre reakcije ukrep po prvem odstavku 149.b člena ZKP ne omogoča. Tudi po stališču ESČP in SEU je treba razlikovati med dostopom do podatkov v realnem času in pridobivanjem podatkov za nazaj. Prvi ukrep naj bi bil bolj invaziven, ker omogoča praktično popoln nadzor nad osebo.¹⁶⁶

105. Glede na navedeno je Ustavno sodišče odločilo, da sta kataloga kaznivih dejanj iz prvega in tretjega odstavka 149.c člena ZKP opredeljena preširoko in omogočata nesorazmeren poseg v pravici iz prvega odstavka 37. člena oziroma prvega odstavka 38. člena Ustave.

Obdobje izvajanja ukrepa

106. Kot je Ustavno sodišče že pojasnilo, je tudi časovni vidik pridobivanja prometnih (in lokacijskih podatkov) zelo pomemben z vidika sorazmernosti posega (prim. 50. točko obrazložitve te odločbe).

107. Drugače kot pri ukrepu iz 149.b člena ZKP je v prvem odstavku 149.c člena ZKP predpisano najdaljše mogoče obdobje za izvrševanje ukrepa. Po prvem odstavku 149.c člena ZKP (ki velja tako za ukrep po prvem kot tudi po tretjem odstavku 149.c člena ZKP¹⁶⁷) mora preiskovalni sodnik v odredbi natančno določiti obdobje, za katero se ukrep odreja in ki ne sme biti daljše od treh mesecev. Z novo odredbo lahko odredi podaljšanje izvajanja ukrepa za tri mesece (skupno lahko torej maksimalno šest mesecev). Če je zoper komunikacijsko sredstvo odrejen tudi ukrep po 150. členu ZKP (skupina ukrepov prisluškovanja), lahko preiskovalni sodnik odreja ukrepe po 149.c členu ZKP za ves čas izvajanja ukrepov iz 150. člena ZKP zoper to komunikacijsko sredstvo. Izvajanje ukrepov iz 150. člena ZKP lahko traja največ en mesec, iz tehtnih razlogov pa se lahko njihovo trajanje podaljša vsakič za en mesec, vendar skupno spet največ za šest mesecev.¹⁶⁸ Razlika med obema opredeljenima časovnima

¹⁶⁵ Prav tam, str. 126. Sklicuje se na odločbo Ustavnega sodišča št. U-I-272/98.

¹⁶⁶ O tem sta se opredelili tudi ESČP, saj so prometni in lokacijski podatki predmet varstva 8. člena EKČP (glej zgoraj zlasti zadevi *Ben Faiza proti Franciji* in *Figueiredo Teixeira proti Andori*), in SEU (sodba v združenih zadevah *La Quadrature du Net in drugi*, 187. točka obrazložitve), ki je navedlo, da je treba razlikovati med realnočasovnim dostopom do podatkov in pridobivanjem podatkov za nazaj. Prvi ukrep naj bi bil bolj invaziven, ker omogoča praktično popoln nadzor nad osebo. SEU se je pri tem sklicevalo tudi na sodbo ESČP v zadevi *Ben Faiza proti Franciji*.

¹⁶⁷ V tretjem odstavku 149.c člena ZKP urejeno pridobivanje lokacijskih podatkov ne pozna posebnih časovnih omejitev glede tega ukrepa, zato tudi za ta ukrep veljajo omejitve iz prvega odstavka 149.c člena ZKP.

¹⁶⁸ Četrti odstavek 152. člena ZKP.

kategorijama torej ni v skupnem trajanju (oboje je lahko največ šest mesecev), temveč v roku, za katerega se ukrepi lahko podaljšujejo (tri mesece po prvem odstavku 149.c člena in en mesec po 150. členu ZKP).¹⁶⁹

108. Glede na pomen trajanja ukrepa za njegovo sorazmernost in glede na težo posega v primeru 149.c člena ZKP ni sporno najdaljše skupno možno trajanje ukrepa. Ustavno sodišče je že v odločbi št. U-I-272/98 navedlo, da je milejše in še vedno učinkovito sredstvo za doseg sicer ustavno dopustnega cilja, ki pa bi v večji meri jamčilo spoštovanje zahteve, da smejo ukrepi trajati najkrajši potrební čas, določitev krajšega dopustnega trajanja ukrepa z možnostjo večkratnega podaljšanja.¹⁷⁰ Zato sta tudi v primeru izpodbijane določbe ustavno sporni začetno obdobje odreditve (tj. tri mesece) in obdobje, za katero se ukrep lahko podaljša (spet tri mesece). Taka ureditev ni sorazmerna z zasledovanim ciljem. Zakonodajalec bo moral urediti krajše obdobje začetne odreditve ukrepa in obdobja enkratnega podaljšanja ukrepa, pri čemer je glede na intenzivnost ukrepa na podlagi prvega in tretjega odstavka 149.c člena ZKP sorazmerno obdobje odreditve ukrepa za en mesec in njegovega (večkratnega) podaljšanja za en mesec.

109. Ustavno sodišče se zaveda, da pomenijo zvišanje dokaznega standarda, zoženje kataloga kaznivih dejanj ter določitev krajšega obdobja za odreditev in večkratno podaljšanje ukrepa zmanjšanje učinkovitosti (pred)kazenskega postopka, sicer legitimnega cilja zakonodajalca. Vendar teža posledic ukrepa ob razlogih za sum, obstoječih časovnih omejitvah in katalogu kaznivih dejanj pretehta koristi ukrepov po prvem in tretjem odstavku 149.c člena ZKP, zato sta ukrepa po prvem in tretjem odstavku 149.c člena ZKP nesorazmerna v ožjem smislu.¹⁷¹

Odločitev Ustavnega sodišča

110. Ukrep iz prvega odstavka 149.c člena ZKP tako pomeni nesorazmeren poseg v pravico do komunikacijske zasebnosti (prvi odstavek 37. člena Ustave), ukrep iz tretjega odstavka 149.c člena ZKP pa nesorazmeren poseg v pravico do informacijske zasebnosti (prvi odstavek 38. člena Ustave), zato je Ustavno sodišče razveljavilo prvi odstavek 149.c člena ZKP in tretji odstavek 149.c člena ZKP, kolikor omogoča pridobivanje lokacijskih podatkov.

111. Ker so preostal del tretjega odstavka in preostali odstavki 149.c člena ZKP (drugi, četrti, peti odstavek 149.c člena ZKP) neposredno povezani s prvim in tretjim odstavkom tega člena v razveljavljenem obsegu in nimajo samostojnega pomena, je Ustavno sodišče razveljavilo 149.c člen ZKP v celoti (1. točka izreka).

¹⁶⁹ Drugi odstavek 152. člena ZKP.

¹⁷⁰ Odločba Ustavnega sodišča št. U-I-272/98, 34. točka obrazložitve odločbe.

¹⁷¹ Tako tudi P. Plesec, nav. delo, str. 33, 34; K. Šugman Stubbs, nav. delo, 2003, str. 203.

112. V skladu s 43. členom ZUstS začne razveljavitev učinkovati naslednji dan po objavi odločbe o razveljavitvi oziroma po poteku roka, ki ga je določilo Ustavno sodišče. Iz razlogov, navedenih v 63. točki obrazložitve te odločbe, je Ustavno sodišče tudi učinkovanje razveljavitve 149.c člena ZKP odložilo za čas enega leta od objave te odločbe v Uradnem listu Republike Slovenije in s tem zakonodajalcu določilo najdaljši možni rok za uskladitev razveljavljene ureditve z Ustavo (3. točka izreka).

B. – IV.

Izpodbijana peti in šesti odstavek 156. člena ZKP

113. Predlagatelj izpodbija peti in šesti odstavek 156. člen ZKP, ki določata:

"(5) Če so podani razlogi za sum, da je bilo izvršeno oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za preprečitev ali odkritje tega kaznivega dejanja ali storilca treba pridobiti podatke o imetniku ali pooblaščenцу določenega ali določljivega plačilnega računa, hranilne vloge, denarnice za hrambo virtualne valute ali denarnega depozita, najemniku ali pooblaščenцу sefa ter o času, v katerem so bili oziroma so v uporabi, ali podatke o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo, ki ne zajemajo podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih oziroma denarnici virtualne valute, lahko državni tožilec ali policija od banke, hranilnice, plačilne institucije, družbe za izdajo elektronskega denarja oziroma podružnice ali zastopnika, ki zanje opravlja plačilne storitve ali distribuira elektronski denar, ali družbe za izdajo, upravljanje oziroma poslovanje z virtualno valuto, pisno zahteva, da tudi brez privolitve osebe, na katero se ti podatki nanašajo, brez odlašanja sporoči te podatke oziroma posreduje dokumentacijo, ki vsebuje te podatke, če ne vsebuje tudi podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih.

(6) Banka, hranilnica, plačilna institucija, družba za izdajo elektronskega denarja oziroma podružnica ali zastopnik, ki zanje opravlja plačilne storitve ali distribuira elektronski denar, ali družba za izdajo, upravljanje oziroma poslovanje z virtualno valuto svoji stranki ali tretji osebi ne sme razkriti, da je ali da bo podatke in dokumentacijo poslala preiskovalnemu sodniku, državnemu tožilcu ali policiji (prejšnji odstavek). Tega ne sme razkriti 24 mesecev po zaključku izvrševanja odredbe preiskovalnega sodnika oziroma posredovanja podatkov državnemu tožilcu ali policiji. Preiskovalni sodnik lahko z odredbo določi drugačen rok, rok podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok skrajša ali prepoved seznanitve odpravi."

114. Izpodbijano določbo je treba razlagati ob upoštevanju celotnega 156. člena ZKP. Prvi odstavek 156. člena ZKP ureja pogoje za odreditev (enkratne) pridobitve zaupnih finančnih podatkov od banke, hranilnice, plačilne institucije, družbe za izdajo elektronskega denarja oziroma podružnice ali zastopnika, ki zanje opravlja plačilne storitve ali distribuira elektronski denar, ali družbe za izdajo, upravljanje virtualne valute oziroma poslovanje z njo. Gre za t. i. *production order*.¹⁷² Nabor zavezancev za izvršitev tega ukrepa se je z novelami ZKP postopoma širil,¹⁷³ nazadnje z ZKP-N. Banke in hranilnice so opredeljene z Zakonom o bančništvu (Uradni list RS, št. 92/21 – v nadaljevanju ZBan-3).¹⁷⁴ Plačilne institucije,¹⁷⁵ družbe za izdajo elektronskega denarja oziroma podružnice ali zastopnik, ki zanje opravlja plačilne storitve ali distribuira elektronski denar,¹⁷⁶ so opredeljeni v ZPlaSSIED, družbe za izdajo, upravljanje virtualne valute oziroma poslovanje z njo¹⁷⁷ pa v ZPPDFT-2.¹⁷⁸

115. Z novelami ZKP se je širila tudi opredelitev oseb, zoper katere je mogoče ukrep odrediti, skladno z razvojem finančnih instrumentov pa se je širil tudi obseg podatkov, ki jih je mogoče pridobiti na podlagi prvega odstavka 156. člena ZKP. Trenutno je tako mogoče pridobiti zaupne podatke in dokumentacijo o stanju vlog in depozitov ter o stanju in prometu na računih ali drugih poslih.¹⁷⁹ Navedene finančne podatke je

¹⁷² Predlog ZKP-N, str. 11.

¹⁷³ Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 72/98 – v nadaljevanju ZKP-A) je kot zavezance določal banke, hranilnice in hranilnokreditne službe, Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 91/11 – v nadaljevanju ZKP-K) še družbo za izdajo elektronskega denarja, ZKP-N pa banke, hranilnice, plačilne institucije, družbe za izdajo elektronskega denarja oziroma podružnice ali zastopnike, ki zanje opravljajo plačilne storitve ali distribuira elektronski denar, in družbe za izdajo, upravljanje virtualne valute oziroma poslovanje z njo.

¹⁷⁴ Člen 4 ZBan-3.

¹⁷⁵ Glej 24. člen ZPlaSSIED.

¹⁷⁶ Glej Predlog ZKP-N, str. 150, 151. Glej tudi K. Merc, Tatvina, v: D. Korošec, K. Filipič (ur.), Veliki znanstveni komentar posebnega dela KZ-1, 2. knjiga, Uradni list Republike Slovenije in Pravna fakulteta Univerze v Ljubljani, Ljubljana 2023, str. 508–511.

¹⁷⁷ Virtualna valuta (denimo bitcoin) ni denar oziroma zakonito plačilno sredstvo. Od Zakona o spremembah in dopolnitvah Kazenskega zakonika (Uradni list RS, št. 186/21 – KZ-1I) se tudi virtualna valuta po KZ-1 šteje za premično stvar, zato odtlej obravnava virtualne valute kot premične stvari ni sporna z vidika načela zakonitosti v kazenskem pravu (ta problematika ostaja odprta le glede knjižnega in elektronskega denarja). O navedenem glej K. Merc, nav. delo, ki meni, da je vrivanje knjižnega in elektronskega denarja ter virtualnih valut v (kazenskopravni) pojem premične stvari izrazito sporno.

¹⁷⁸ Glej B. Valenčič, I. Pridigar, v: M. Šepec (ur.), Zakon o kazenskem postopku s komentarjem, 1. knjiga, GV Založba, Ljubljana 2022, str. 928, 929.

¹⁷⁹ Zakon o kazenskem postopku (Uradni list RS, št. 63/94 – ZKP/94) je določal, da se pridobijo podatki določenih oseb; ZKP-A podatki osebe, zoper katero obstajajo utemeljeni razlogi za sum, in drugih oseb, za katere je moč utemeljeno sklepati, da so udeležene v finančnih transakcijah

mogoče pridobiti, če se nanašajo na osumljenca,¹⁸⁰ obdolženca¹⁸¹ ali druge osebe, za katere je mogoče utemeljeno sklepati, da so udeležene v finančnih transakcijah ali poslih osumljenca ali obdolženca. Ukrep se torej lahko pod navedenimi pogoji odredi tudi zoper osebe, proti katerim se ne vodi (pred)kazenski postopek. V splošnem gre lahko tako za fizične kot tudi za pravne osebe (če narava posameznega podatka tega ne preprečuje).¹⁸² Ukrep odredi preiskovalni sodnik s sodno odredbo na obrazložen predlog državnega tožilca, če bi ti podatki utegnili biti dokaz v kazenskem postopku ali če so potrebni zaradi zasega predmetov ali zavarovanja zahtevka za odvzem premoženjske koristi oziroma premoženja v vrednosti premoženjske koristi.¹⁸³ Iz namena tega ukrepa torej izhaja, da gre za preiskovalni ukrep.¹⁸⁴ Drugi odstavek 156. člena ZKP ureja dolžnost zavezanih subjektov za posredovanje zahtevanih podatkov in dokumentacije preiskovalnemu sodniku in pristojnemu organu, določenemu v odredbi brez odlašanja.

116. Tretji odstavek 156. člena ZKP pa ureja ukrep tekočega¹⁸⁵ spremljanja finančnega poslovanja osumljenca, obdolženca in drugih oseb, za katere je mogoče utemeljeno sklepati, da so udeležene v finančnih transakcijah ali poslih osumljenca ali obdolženca, in sprotno sporočanje zaupnih podatkov o transakcijah ali poslih, ki jih pri njih opravijo ali nameravajo opraviti navedene osebe (t. i. *monitoring order*).¹⁸⁶ Zavezanci za izvršitev ukrepa so isti kot po prvem odstavku 156. člena ZKP, prav tako osebe, katerih podatki se lahko sporočijo. Ukrep prav tako odredi preiskovalni sodnik na obrazložen

ali poslih storilca; Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 111/01 – ZKP-D) podatki osebe, zoper katero obstajajo utemeljeni razlogi za sum, in drugih oseb, za katere je moč utemeljeno sklepati, da so udeležene v finančnih transakcijah ali poslih osumljenca ali obdolženca; Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (Uradni list RS, št. 56/03 – v nadaljevanju ZKP-E) pa podatki osumljenca, obdolženca in drugih oseb, za katere je mogoče utemeljeno sklepati, da so udeležene v finančnih transakcijah ali poslih osumljenca ali obdolženca. Glej tudi Š. Horvat, Komentar Zakona o kazenskem postopku, GV Založba, Ljubljana 2004, str. 352.

¹⁸⁰ Prva alineja 144. člena ZKP.

¹⁸¹ Četrta alineja 144. člena ZKP.

¹⁸² Na podlagi 42. člena Zakona o odgovornosti pravnih oseb za kazniva dejanja (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 65/08 in 57/12 – ZOPOKD) se, če ni v tem zakonu drugače določeno, v kazenskem postopku zoper pravno osebo smiselno uporabljajo določbe zakona, ki ureja kazenski postopek, tudi če postopek teče samo zoper pravno osebo. Glej tudi sklep Višjega sodišča v Ljubljani št. V Kp 14957/2017 z dne 18. 10. 2021.

¹⁸³ Zgodovinsko gledano, je ZKP-A omogočal ukrep, če bi ti podatki utegnili biti pomemben dokaz v kazenskem postopku, ZKP-E pa, če bi ti podatki utegnili biti dokaz v kazenskem postopku ali če so potrebni zaradi zasega predmetov ali zavarovanja zahtevka za odvzem premoženjske koristi oziroma premoženja v vrednosti premoženjske koristi.

¹⁸⁴ B. Valenčič, I. Pridigar, v: M. Šepec (ur.), nav. delo, str. 921.

¹⁸⁵ Rok oziroma pogostost sporočanja je določen v sodni odredbi.

¹⁸⁶ K. Šugman Štubbs, nav. delo, 2003, str. 182.

predlog državnega tožilca pod pogoji iz prvega odstavka 156. člena ZKP. Četrti odstavek 156. člena ZKP določa trajanje tega ukrepa; tj. največ tri mesece, ukrep pa se iz tehtnih razlogov lahko na predlog državnega tožilca podaljša do največ šest mesecev.

117. Peti odstavek 156. člena ZKP ureja še zadnji ukrep iz tega člena, tj. pridobitev določenih podatkov neposredno od zavezancev za izvršitev ukrepa (ki so isti kot zavezanci po prvem in tretjem odstavku 156. člena ZKP) brez sodne odredbe. Šesti odstavek ureja obdobje, v katerem zavezanec za izvršitev ukrepov po 156. členu ZKP ne sme nikomur razkriti, da je prejel sodno odredbo oziroma zahtevo za izvršitev ukrepa po tem členu. Tega ne sme razkriti 24 mesecev po zaključku izvrševanja odredbe preiskovalnega sodnika oziroma posredovanja podatkov državnemu tožilcu ali policiji. Preiskovalni sodnik lahko z odredbo določi drugačen rok, rok podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok skrajša ali prepoved seznanitve odpravi. Iz navedenega izhaja, da gre pri ukrepu iz 156. člena prav tako za prikriti preiskovalni ukrep.¹⁸⁷

118. Brez sodne odredbe je mogoče po petem odstavku 156. člena ZKP pridobiti podatke o imetniku ali pooblaščenцу določenega ali določljivega plačilnega računa, hranilne vloge, denarnice za hrambo virtualne valute ali denarnega depozita, najemniku ali pooblaščenцу sefa ter o času, v katerem so bili oziroma so v uporabi, ali podatke o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo, ki ne zajemajo podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih oziroma v denarnici virtualne valute.

119. Glede podatka o imetniku¹⁸⁸ ali pooblaščenцу¹⁸⁹ plačilnega računa iz odgovora Banke Slovenije izhaja, da je transakcijski račun¹⁹⁰ podvrsta plačilnega računa, ki ga vodi banka in hranilnica s sedežem v Republiki Sloveniji, med transakcijske račune pa ne spadajo 1) plačilni računi, ki jih vodijo nebančni ponudniki plačilnih storitev (plačilne institucije in družbe za izdajo elektronskega denarja) s sedežem v Republiki Sloveniji, in 2) vsi plačilni računi, ki jih za slovenske državljane vodijo ponudniki plačilnih storitev s sedežem izven Republike Slovenije (v nadaljevanju drugi plačilni računi). Plačilni račun, o katerem je mogoče pridobiti podatek, mora biti določen (tj. z mednarodno

¹⁸⁷ B. Valenčič, I. Pridigar, v: M. Šepec (ur.), nav. delo, str. 921; K. Šugman Štubbs, nav. delo, 2003, str. 179.

¹⁸⁸ Prvi odstavek 13. člena ZPlaSSIED.

¹⁸⁹ Člen 74 Obligacijskega zakonika (Uradni list RS, št. 97/07 – uradno prečiščeno besedilo in 20/18 – v nadaljevanju OZ) in naslednji.

¹⁹⁰ Po prvem odstavku 13. člena ZPlaSSIED je transakcijski račun plačilni račun, ki ga odpre banka s sedežem v Republiki Sloveniji ali podružnica banke države članice v Republiki Sloveniji v imenu enega uporabnika ali več uporabnikov za namene izvrševanja plačilnih transakcij in druge namene, povezane z opravljanjem bančnih storitev za uporabnika. Denarna sredstva na transakcijskem računu se štejejo kot vpogledni denarni depozit.

strukturo bančnega računa, *IBAN – International Bank Account Number*, ki je sestavljena iz 19 črkovnih in numeričnih znakov)¹⁹¹ ali pa vsaj določljiv (lahko s kombinacijo več samih zase nepopolnih podatkov). Hranilna vloga je bančni pravni posel po 1043. členu Zakona o obligacijskih razmerjih (Uradni list SFRJ, št. 29/78, 39/85 in 57/89 – v nadaljevanju ZOR), denarni depozit pa bančni pravni posel po 1035. členu ZOR.¹⁹² Denarnica za hrambo virtualne valute je programska oprema, ki vsebuje javni in zasebni ključ ter uspešno deluje v različnih tehnologijah veriženja blokov (angl. *blockchain*) in omogoča uporabnikom, da si izmenjajo valute in beležijo stanje svojih valut. Shranjuje, pošilja in sprejema različne valute.¹⁹³ Glede opredelitve najemnika ali pooblaščenca sefa pa je treba upoštevati 1061. člen ZOR o pogodbi o sefu in naslednje.¹⁹⁴ Tudi hranilna vloga, denarni depozit, denarnica za hrambo virtualne valute in sef morajo biti določeni ali določljivi.

120. ZKP v petem odstavku 156. člena tudi omogoča, da policija ali državni tožilec od zavezanca pridobi podatek o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo. V skladu z ZPPDFT-2 je poslovno razmerje vsak poslovni ali drug pogodbeni odnos (ki ga stranka sklene ali vzpostavi pri zavezancu iz prvega ali drugega odstavka 4. člena ZPPDFT-2 in je povezan z opravljanjem dejavnosti zavezanca ter se zanj ob vzpostavitvi stikov predvideva, da bo trajal, razen ko ta zakon določa drugače).¹⁹⁵ Gre torej za podatek o obstoju pogodbenega razmerja z zavezancem iz petega odstavka 156. člena ZKP.¹⁹⁶

121. Že po jezikovni razlagi podatki po petem odstavku 156. člena ZKP ne vsebujejo tudi podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih. ZKP še dodatno navaja, da zavezanec sporoči te podatke oziroma posreduje dokumentacijo, ki vsebuje te podatke, če ne vsebuje tudi podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih. Tudi iz zakonodajnega gradiva izhaja, da je po petem odstavku 156. člena ZKP mogoče pridobiti statusne podatke o komitentih oziroma pooblaščenih komitentov bank, na primer podatke o imetniku ali pooblaščenču

¹⁹¹ Glej Sklep o vsebini in uporabi slovenske strukture mednarodne številke bančnega računa (Uradni list RS, št. 21/21).

¹⁹² V skladu s 1035. členom ZOR je pogodba o denarnem depozitu sklenjena, kadar se banka zaveže, da sprejme, deponent pa, da položi pri banki določen denarni znesek. S to pogodbo pridobi banka pravico razpolagati z deponiranim denarjem, vrniti pa ga mora pod pogoji, ki so določeni v pogodbi.

¹⁹³ S. Jokić, A. S. Cvetković, S. Adamović, N. Ristić, P. Spalević, Comparative analysis of cryptocurrency wallets vs traditional wallets, *Ekonomika*, št. 3 (2019), str. 67.

¹⁹⁴ Po 1061. členu ZOR se banka s pogodbo o sefu zavezuje, da bo dala uporabniku v rabo sef za določeno dobo, uporabnik pa, da ji bo za to plačal določen znesek. Banka mora ukreniti vse, kar je potrebno za dobro stanje sefa in nadzor nad njim.

¹⁹⁵ Točka 41 3. člena ZPPDFT-2.

¹⁹⁶ Glej 15. člen OZ in naslednje.

določene hranilne vloge, ne pa podatkov in dokumentacije o vlogah, ki govorijo o višini, vrednosti oziroma obsegu premoženja in ki jih je mogoče po prvem odstavku 156. člena ZKP pridobiti le po odredbi sodišča.¹⁹⁷ To poudarja tudi Vlada v svojem mnenju.

122. Podatke je mogoče pridobiti, če je to potrebno za preprečitev ali odkritje kaznivega dejanja po uradni dolžnosti ali storilca. Drugače kot v primeru ukrepov po prvem in tretjem odstavku 156. člena ZKP je torej mogoče podatke po petem odstavku tega člena brez sodne odredbe pridobiti le za preiskovalne namene (in ne tudi za namene izvedbe zasega predmetov oziroma začasnega zavarovanja odvzema protipravne premoženjske koristi).¹⁹⁸

123. Prav tako je, za razliko od prvega in tretjega odstavka 156. člena ZKP, v petem odstavku tega člena neposredno določen dokazni standard (razlogi za sum, da je bilo izvršeno oziroma da se pripravlja kaznivo dejanje).¹⁹⁹

124. Navedene podatke lahko od zavezancev zahtevata državni tožilec ali policija, če so podani razlogi za sum, da je bilo izvršeno oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti. Iz kataloga kaznivih dejanj, v zvezi s katerimi je mogoče pridobiti navedene podatke, so torej izločena zgolj kazniva dejanja, ki se preganjajo na zasebno tožbo.²⁰⁰

125. Časovni obseg pridobivanja bančnih podatkov po prvem (ali katerem drugem) odstavku 156. člena ZKP ni omejen z ZKP, ampak (podobno kot ukrep po prvem odstavku 149.b člena ZKP) zgolj z obvezo naslovnikov odredbe za hranjenje teh podatkov po področni zakonodaji. Minimalno obdobje, za katero morajo finančne institucije hraniti podatke o finančnem poslovanju, določa ZPPDFT-2.²⁰¹ Hkrati ZPlaSSIED določa pravno podlago za hrambo nekaterih podatkov v RTR, pri čemer je

¹⁹⁷ Predlog ZKP-N, str. 151.

¹⁹⁸ O dvojni naravi zasega K. Šugman Stubbs, P. Gorkič, nav. delo, str. 189.

¹⁹⁹ Čeprav iz sodne prakse izhaja, da je iz opredelitve oseb, zoper katere se ukrep lahko odredi (osumljenec, obdolženec in druge osebe), razvidno, da tudi za odreditev ukrepa po prvem in tretjem odstavku 156. člena ZKP prav tako zadoščajo razlogi za sum. B. Valenčič, I. Pridigar, nav. delo. Glej tudi sklep Višjega sodišča v Ljubljani št. V Kp 1356/2016 z dne 27. 8. 2019 in sklepa Višjega sodišča v Celju št. III Kp 32390/2019 z dne 19. 1. 2021 in št. III Kp 49417/2012 z dne 15. 9. 2020.

²⁰⁰ Glej B. Valenčič, I. Pridigar, v: M. Šepec (ur.), nav. delo, str. 923, in K. Šugman Stubbs, P. Gorkič, nav. delo, str. 162.

²⁰¹ Glej 141. člen ZPPDFT-2 in nasl.

relevantno tako dejstvo, od kdaj je zakon sploh določal pravno podlago za hrambo določenega podatka v RTR,²⁰² kot tudi, kdaj se posamezen podatek izbriše.²⁰³

Presoja ukrepov iz petega odstavka 156. člena ZKP

126. Ustavno sodišče je presojalo predlagateljeve navedbe o neskladju izpodbijane določbe ZKP z Ustavo, ker v primeru ukrepa po petem odstavku 156. člena ZKP (za razliko od ukrepa po njegovem prvem in tretjem odstavku) ni zagotovljeno sodno varstvo, saj ni zahtevana sodna odredba.

127. Čeprav so lahko osebe, na katere se nanašajo podatki iz petega odstavka 156. člena ZKP, v splošnem tako fizične kot tudi pravne osebe, lahko pogodbo o hranilni vlogi²⁰⁴ sklene samo fizična oseba,²⁰⁵ zato je tudi po petem odstavku 156. člena ZKP po naravi stvari mogoče pridobiti samo tiste podatke o hranilni vlogi, ki se nanašajo na fizično osebo. Z izjemo podatkov o hranilnih vlogah pa je mogoče v splošnem med osebe po petem odstavku 156. člena ZKP šteti ne le fizične, ampak tudi pravne osebe.

128. Vendar je z vidika pravice do informacijske zasebnosti po Splošni uredbi o varstvu podatkov,²⁰⁶ Direktivi 2016/680,²⁰⁷ zakonodaji²⁰⁸ in sodni praksi²⁰⁹ osebni podatek vezan na fizično osebo. Tudi po ustaljeni ustavnosodni presoji²¹⁰ varstvo informacijske zasebnosti varuje zgolj fizično osebo, ne pa pravne osebe.²¹¹ Pravnim osebam po ustaljeni ustavnosodni presoji torej ne gre pravica iz prvega odstavka 38. člena Ustave.

129. V zvezi s pravnimi osebami po ustaljeni ustavnosodni presoji iz prvega odstavka 74. člena Ustave (svobodna gospodarska pobuda) izhaja tudi varstvo sfere poslovne

²⁰² Iz odgovora AJPES na primer izhaja, da se podatki o imetniku transakcijskega računa ter datumu odprtja in zaprtja tega računa vodijo že od vzpostavitve RTR pri AJPES 1. 7. 2010, pred tem pa naj bi se vodili pri Banki Slovenije, podatki o pooblaščenцу imetnika transakcijskega računa in podatki o sefu pa se vodijo od 6. 11. 2021.

²⁰³ Deveti odstavek 192. člena ZPlaSSIED.

²⁰⁴ Členi 1043–1046 ZOR.

²⁰⁵ Člen 1088 ZOR.

²⁰⁶ Prvi odstavek 1. člena Splošne uredbe o varstvu podatkov.

²⁰⁷ Prvi odstavek 1. člena in prvi odstavek 3. člena Direktive 2016/680.

²⁰⁸ Prvi odstavek 5. člena ZVOP-2 v povezavi s 1. točko 4. člena Splošne uredbe o varstvu podatkov. Glej N. Pirc Musar, S. Bien Karlovšek, J. Bogataj, M. Prelesnik, A. Žaucer, K. Mišič, A. Tomšič, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, GV Založba, Ljubljana 2006, str. 58.

²⁰⁹ Sklep Višjega sodišča v Ljubljani št. V Kp 14957/2017 z dne 18. 10. 2021.

²¹⁰ Odločba Ustavnega sodišča št. U-I-84/03 z dne 17. 2. 2005 (Uradni list RS, št. 24/05, in OdlUS XIV, 5).

²¹¹ Sklep Ustavnega sodišča št. U-I-236/08 z dne 8. 4. 2010.

tajnosti oziroma poslovne skrivnosti.²¹² Zaupnost gospodarskega poslovanja je v temelju zagotovljena s to ustavno določbo. Pravica do svobodne gospodarske pobude poslovnim subjektom zagotavlja, da svobodno odločajo o tem, kdo in v kakšni obliki bo imel dostop do podatkov o njihovem poslovanju oziroma gospodarskem udejstvovanju, vključno s podatki o vrstah in vrednostih sklenjenih pravnih poslov, o osebah, ki so sodelovale pri sklenitvi posla, o nasprotnih pogodbenih strankah, o podizvajalcih, o razvoju in izvrševanju neke transakcije, o sklenjenih aneksih in podobno. Bistvo svobodne gospodarske pobude je v svobodnem poslovanju na trgu kot svobodi izbire gospodarske dejavnosti, izbire načina osvajanja trga in izbire poslovnih partnerjev. Opisano svobodno poslovanje na trgu ni mogoče oziroma bi bilo znatno oteženo brez možnosti poslovnih subjektov, da v razmerju do zunanjega sveta po svoji izbiri prikrivajo informacije iz svoje notranje poslovne sfere. Te informacije imajo namreč za podjetje premoženjsko vrednost in mu pomagajo pri potegovanju za konkurenčno prednost na trgu.²¹³ Svobodna gospodarska pobuda se glede na navedeno v ustavnem redu kaže tudi kot pravica pri poslovanju prikriti, zakriti, omejeno deliti, izključno izkoriščati in zadržati zase. Člen 74 Ustave varuje poslovno skrivnost, ki se nanaša na informacije oziroma podatke poslovne narave, ki: (a) se nanašajo na poslovanje oziroma dejavnost poslovnega subjekta, (b) niso že javno znani, (c) so po vsebini taki, da obstaja verjetnost, da bi njihova prosta dostopnost ali dostopnost poslovnemu konkurentu poslovnemu subjektu povzročila občutno škodo.²¹⁴ Upravičenje do varovanja poslovne skrivnosti, ki je varovano v okviru prvega odstavka 74. člena Ustave, je v javnem interesu lahko predmet pravnega reguliranja, ki lahko sega na raven načina uresničevanja ali na raven omejevanja svobodne gospodarske pobude.²¹⁵

130. Vendar v primeru pridobivanja podatkov po petem odstavku 156. člena ZKP ne gre za pridobivanje podatkov, ki so varovani s poslovno skrivnostjo. Eden izmed (kumulativno določenih) ustavnopravnih pogojev za obstoj poslovne skrivnosti je

²¹² Tako Ustavno sodišče v odločbi št. U-I-201/14, U-I-202/14 z dne 19. 2. 2015 (Uradni list RS, št. 19/15), 22. točka obrazložitve.

²¹³ Prav tam.

²¹⁴ Prav tam, 23. točka obrazložitve. Glej tudi odločbo Ustavnega sodišča št. U-I-52/16 z dne 12. 1. 2017 (Uradni list RS, št. 5/17, in OdlUS XXII, 1), 21. in 22. točka obrazložitve. Zakon o poslovnih skrivnostih (Uradni list RS, št. 22/19 – v nadaljevanju ZPosS), ki je nadomestil opredelitev iz Zakona o gospodarskih družbah (Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 82/13, 55/15, 15/17 in 18/21– ZGD-1). ZPosS sicer ureja področje poslovne skrivnosti, pravila določitve in varstva poslovne skrivnosti pred njeno protipravno pridobitvijo, uporabo in razkritjem. Z njim se v slovenski pravni red prenaša Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (UL L 157, 15. 6. 2016). Glej kritiko določitve 74. člena Ustave kot zgornje premise poslovne skrivnosti v R. Zagradišnik, v: M. Avbelj (ur.), nav. delo, str. 599.

²¹⁵ Odločba Ustavnega sodišča št. U-I-52/16, 21. in 22. točka obrazložitve.

namreč tudi, da je podatek po vsebini tak, da obstaja verjetnost, da bi njegova prosta dostopnost ali dostopnost poslovnemu konkurentu povzročila poslovnemu subjektu občutno škodo. V obravnavanem primeru ne gre za primer proste dostopnosti podatkov ali dostopnosti poslovnemu konkurentu. Po petem odstavku 156. člena ZKP podatke namreč pridobi državni tožilec ali policija za namene (pred)kazenskega postopka.²¹⁶ Policija jih po prvem odstavku 153. člena ZKP pošlje državnemu tožilcu. Vsi izsledki prikritih preiskovalnih ukrepov, ne glede na to, kdo je odredil njihovo pridobivanje, v vsakem primeru končajo pri preiskovalnem sodniku. Ravnanje z izsledki, pridobljenimi z ukrepi, o katerih je samostojno odločil državni tožilec ali celo policija, ureja četrti odstavek 153. člena ZKP.²¹⁷ Če državni tožilec izjavi, da ne bo začel kazenskega pregona zoper osumljenca, ali če v roku dveh let po koncu izvajanja zadnjega od ukrepov, ki jih odreja državni tožilec, ne vloži obtožnega akta niti ne predlaga, odredi ali izvede nobene aktivnosti, ukrepa oziroma preiskovalnega dejanja, usmerjenega v pregon zoper osumljenca, preiskovalnemu sodniku preda tudi celotno gradivo, zbrano s temi ukrepi.²¹⁸ Ko izsledki prikritih preiskovalnih ukrepov pridejo na sodišče, jih sodišče na podlagi prvega odstavka 154. člena ZKP hrani, dokler se hrani kazenski spis oziroma do uničenja po drugem odstavku 154. člena ZKP.²¹⁹ Pregled in prepis posameznih kazenskih spisov pa ureja 128. člen ZKP, ki to dopušča zgolj nekomu, ki ima za to upravičen interes.²²⁰ Zato podatki, ki jih je mogoče pridobiti na podlagi petega odstavka 156. člena ZKP, v tem okviru niso varovani z ustavnopravnim pojmom poslovne skrivnosti.

131. Glede na navedeno je moralo Ustavno sodišče presoditi pridobitev podatkov iz petega odstavka 156. člena ZKP, ki se nanašajo zgolj na fizične osebe, in sicer z vidika varstva osebnih podatkov iz prvega odstavka 38. člena Ustave.

132. Ustavno sodišče se je do sedaj opredelilo zgolj do podatkov iz prvega odstavka 156. člena ZKP. Po njegovem stališču so ti podatki (če se nanašajo na fizično osebo²²¹) osebni podatki, ki jih varuje informacijska zasebnost.²²² Ker pa v obravnavanem

²¹⁶ Poleg tega nekateri podatki, ki jih je po petem odstavku 156. člena ZKP mogoče pridobiti (to so podatki o imetniku ali pooblaščenцу določenega ali določljivega plačilnega računa, najemniku ali pooblaščenцу sefa) in ki se nanašajo na pravno osebo, ne izpolnjujejo pogojev za obstoj poslovne skrivnosti, prav tako pa jih ne izpolnjujejo iz njih izvirajoči podatki, kdaj so bili računi v uporabi, ker so ti podatki objavljeni v RTR ter so javni in brezplačno dostopni na spletni strani AJPES in tudi na nekaterih (plačljivih) spletnih straneh.

²¹⁷ Odločba Ustavnega sodišča št. U-I-246/14 z dne 24. 3. 2017 (Uradni list RS, št. 16/17, in OdlUS XXII, 7), 26. točka obrazložitve.

²¹⁸ Četrti odstavek 153. člena ZKP.

²¹⁹ Prim. z odločbo Ustavnega sodišča št. U-I-246/14, 28. točka obrazložitve.

²²⁰ Prvi odstavek 128. člena ZKP.

²²¹ B. Valenčič, I. Pridigar, v: M. Šepec (ur.), nav. delo, str. 924.

²²² Odločbe Ustavnega sodišča št. Up-709/15, Up-710/15, 34., 36. in 38. točka obrazložitve, št. U-I-298/04 in št. U-I-84/03.

primeru predlagatelj zatrjuje protiuustavnost petega odstavka 156. člena ZKP, je moralo Ustavno sodišče presoditi, ali pomeni tudi pridobitev drugih podatkov o 1) imetniku ali pooblaščenцу določenega ali določljivega plačilnega računa, hranilne vloge, denarnice za hrambo virtualne valute ali denarnega depozita, 2) najemniku ali pooblaščenцу sefa in 3) času, v katerem so bili oziroma so v uporabi, ali 4) obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo, ki pa ne zajemajo podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih oziroma v denarnici virtualne valute, poseg v informacijsko zasebnost.

133. Ti podatki so vsekakor informacija v zvezi z določenim posameznikom, tj. imetnikom ali pooblaščencom določenega ali določljivega plačilnega računa, hranilne vloge, denarnice za hrambo virtualne valute ali denarnega depozita, najemnikom ali pooblaščencom sefa oziroma v zvezi z osumljencem.²²³ Glede na opredelitev osebnega podatka (93. točka obrazložitve te odločbe) in ureditev ZBan-3, ZPlaSSIED²²⁴ in ZPPDFT-2²²⁵ predvideva izpodbijana ureditev obdelavo osebnih podatkov, kadar se podatki nanašajo na fizično osebo, pridobitev navedenih podatkov pa poseg v informacijsko zasebnost.²²⁶

134. Kot je Ustavno sodišče že pojasnilo, pravica do informacijske zasebnosti ni neomejena in absolutna. Poseg vanjo je dopusten v primerih iz tretjega odstavka 15. člena Ustave, če je zakonodajalec zasledoval ustavno dopusten cilj in če je omejitev skladna z načeli pravne države (2. člen Ustave), in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege države, tj. splošnim načelom sorazmernosti.²²⁷

135. V zvezi z ustavno dopustnim ciljem Ustavno sodišče izpostavlja, da pomeni izpodbijana določba zgolj nadgradnjo oziroma dopolnitev že prej obstoječe možnosti pridobitve podatkov brez sodne odredbe po ZKP-K. Iz zakonodajnega gradiva k ZKP-K pa je razvidno, da je bilo kot razlog za uvedbo pridobivanja določenih podatkov brez sodne odredbe navedeno odpravljanje administrativnih in časovnih ovir pri preiskovanju kaznivih dejanj, v katerih je bila pridobljena protipravna premoženjska

²²³ Prim. prvi odstavek 4. člena ZVOPOKD.

²²⁴ Člen 193 ZPlaSSIED

²²⁵ Člen 141 ZPPDFT-2 in nasl.

²²⁶ Ustavno sodišče je v odločbi št. U-I-298/04 odločilo, da RTR v delu, ki se nanaša na imetnike transakcijskih računov, ki so fizične osebe, ki niso zasebniki, vsebuje tudi osebne podatke in da so podatek o številki transakcijskega računa fizične osebe, podatek o tem, pri katerem izvajalcu plačilnega prometa ima odprt transakcijski račun, in podatek o vzpostavljeni evidenci iz sedmega odstavka 8. člena Zakona o plačilnem prometu (Uradni list RS, št. 110/06 – uradno prečiščeno besedilo in nasl. – ZPlaP) osebni podatki.

²²⁷ Odločba Ustavnega sodišča št. U-I-18/02, 25. točka obrazložitve.

korist, in pranje denarja, učinkovitejše preiskovanje finančnih tokov in povezav ter izvorov sumljivega premoženja prek drugih računov.²²⁸

136. Navedeno je v povezavi z učinkovitim (pred)kazenskim postopkom²²⁹ v splošnem zagotovo mogoče šteti za ustavno dopusten cilj, tudi za poseg v pravico do varstva osebnih podatkov iz prvega odstavka 38. člena Ustave.

Sorazmernost v ožjem pomenu

137. Ustavno sodišče ocenjuje, ne da bi se spuščalo v presojo, ali je obravnavani poseg zakonodajalca nujen in primeren (ukrep) za zagotovitev zasledovanega cilja, da ta poseg ne prestane preizkusa sorazmernosti v ožjem pomenu.²³⁰ Poseg je sorazmeren, če je teža tega posega v informacijsko zasebnost sorazmerna vrednosti zasledovanega cilja oziroma pričakovanim koristim, ki bodo zaradi posega nastale.²³¹

138. Ustava za posege v pravico do varstva osebnih podatkov ne zahteva vnaprejšnje sodne odredbe, tako kot jo zahteva po drugem odstavku 36. člena in drugem odstavku 37. člena Ustave za poseg v prostorsko in komunikacijsko zasebnost.²³² V izpodbijanem primeru je upošteven sicer poseg v varstvo osebnih podatkov iz 38. člena Ustave, za katerega Ustava izrecno ne zahteva sodne odredbe. Vendar je po ustaljeni ustavnosodni presoji varstvo osebnih podatkov iz 38. člena Ustave ena od oblik človekove zasebnosti iz 35. člena Ustave. Iz presoje Ustavnega sodišča pa izhaja, da izhaja zahteva po predhodni sodni odločbi za primere najtežjih posegov v pravice iz 35. člena Ustave že iz načela sorazmernosti, na podlagi katerega se presoja dopustnost poseganja v ustavne pravice.²³³ Predhodna sodna odločba ima dvojno vlogo: 1) zagotavlja, da izvršilna oblast pred neodvisno sodno oblastjo *ex ante* upraviči ustavnost in zakonitost posega, s čimer preprečuje ireverzibilne arbitrarne posege izvršilne oblasti v zasebnost posameznikov; in 2) zagotavlja naknadno presojo ustavnih in zakonskih pogojev za poseg v pravico do zasebnosti, kar je še posebej pomembno pri preiskovalnih dejanjih, katerih uspeh je odvisen od učinka presenečenja in ki torej ne prenesejo, da bi se o njihovi utemeljenosti odločalo v predhodnem kontradiktornem postopku. Zahteva po vnaprejšnji sodni odločbi je torej izrazito v funkciji varstva pravic

²²⁸ Vlada Republike Slovenije, Predlog zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (ZKP-K) z dne 2. 6. 2011, EPA 1892 - V, str. 65.

²²⁹ Glej 39. točko obrazložitve te odločbe.

²³⁰ Prim. odločbo Ustavnega sodišča št. U-I-328/05, 14. točka obrazložitve.

²³¹ Prim. odločbo Ustavnega sodišča št. U-I-83/20, 55. točka obrazložitve.

²³² Odločba Ustavnega sodišča št. Up-709/15, Up-710/15, 38. točka obrazložitve.

²³³ Odločba Ustavnega sodišča št. Up-1293/08 z dne 6. 7. 2011 (Uradni list RS, št. 60/11), 23. točka obrazložitve. Tako Ustavno sodišče že v odločbi št. U-I-272/98.

tistega, v čigar zasebnost se posega, in v tem pogledu bistveno pripomore k sorazmernosti posega.²³⁴

139. Ustavno sodišče je zato moralo presoditi, ali je ureditev, po kateri je mogoče pridobiti podatke o imetniku ali pooblaščenцу določenega ali določljivega plačilnega računa, hranilne vloge, denarnice za hrambo virtualne valute ali denarnega depozita, najemniku ali pooblaščenцу sefa ter o času, v katerem so bili oziroma so v uporabi, ali podatke o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo, ki ne zajemajo podatkov o premoženjskem stanju osumljenca oziroma o stanju vlog in depozitov ter o stanju in prometu na računih oziroma v denarnici virtualne valute brez sodne odredbe, v skladu z 38. členom Ustave.

140. Iz zakonodajnega gradiva k ZKP-K izhaja, da naj bi bili podatki o transakcijskih računih in njihovih imetnikih že javno dostopni prek AJPES, prav tako naj pri podatkih, ki jih je mogoče pridobiti brez sodne odredbe, ne bi šlo za zaupne podatke.²³⁵ Iz zakonodajnega gradiva k ZKP-N pa izhaja, da je besedilo ZKP/17 v praksi povzročalo nejasnosti glede razmerja med prvim in petim odstavkom 156. člena ZKP/17.²³⁶ Besedilo prvega odstavka 156. člena ZKP/17 naj bi se namreč deloma prekrivalo s taksativno naštetimi podatki iz petega odstavka 156. člena ZKP/17, ki jih je policija lahko pridobila brez odredbe, zato naj bi obstajala različna praksa sodišč kot tudi finančnih institucij o tem, na zahtevo oziroma odredbo katerega organa morajo posredovati določene podatke za potrebe predkazenskih in kazenskih postopkov.²³⁷ Sprememba petega odstavka 156. člena ZKP naj bi zato zgolj jasneje razmejila podatke, ki jih je mogoče dobiti s sodno odredbo, od tistih, ki jih lahko pridobita državni tožilec in policija neposredno od finančnih institucij. Podatki, pridobljeni brez sodne odredbe, naj ne bi smeli vsebovati podatkov o stanju in prometu na računu oziroma o premoženjskem stanju posameznika (podatki o stanju vlog in depozitov).²³⁸

141. Tako stališče zastopa tudi Vlada; ključno naj bi bilo, da ureditev natančneje ločuje med podatki, ki jih lahko policija in državni tožilec pridobita sama, da sodna odredba že do sedaj ni bila potrebna ter da ne gre za podatke o premoženjskem stanju osumljenca oziroma o stanju vlog, depozitov, računov oziroma denarnic virtualne valute.²³⁹

²³⁴ Odločbe Ustavnega sodišča št. U-I-272/98, 37. točka obrazložitve, št. Up-1293/08, 23. točka obrazložitve, št. U-I-40/12, 27. točka obrazložitve, in št. Up-979/15, 14. točka obrazložitve.

²³⁵ Predlog zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (EVA 2010-2011-0009), Novo gradivo št. 2, 1. 6. 2011, str. 64.

²³⁶ Predlog ZKP-N, str. 11.

²³⁷ Prav tam, str. 32, 151.

²³⁸ Prav tam.

²³⁹ Tako tudi B. Valenčič, I. Pridigar, v: M. Šepec (ur.), nav. delo, str. 932.

142. Po ZBan-3 so zaupni vsi podatki, dejstva in okoliščine o posamezni stranki, s katerimi razpolaga banka.²⁴⁰ Banka mora varovati zaupne podatke, ne glede na način, na katerega je te podatke pridobila,²⁴¹ člani organov banke, delničarji banke, delavci banke oziroma druge osebe, ki so jim v zvezi z njihovim delom v banki oziroma pri opravljanju storitev za banko na kakršenkoli način dostopni zaupni podatki iz prejšnjega člena, pa teh podatkov ne smejo sporočiti tretjim osebam, niti omogočiti, da bi jih uporabile tretje osebe, ali jih sami uporabiti za lastne namene.²⁴² Dolžnost banke glede varovanja zaupnih podatkov ne velja, med drugim, če te podatke zaradi izvedbe predkazenskega ali kazenskega postopka pisno zahteva sodišče, državno tožilstvo ali policija, razen v primerih, ko za posredovanje zaupnih podatkov zakon izrecno določa odredbo preiskovalnega sodnika.²⁴³

143. Na podlagi ZPlaSSIED je vzpostavljen RTR, ki je enotna informatizirana baza podatkov o transakcijskih računih in sefih ter imetnikih transakcijskih računov, pooblaščenih imetnikov transakcijskih računov, dejanskih lastnikih transakcijskih računov in najemnikih sefov, ki jo vzpostavi in upravlja AJPES. Banke, ki vodijo transakcijske račune in oddajajo sefe, Banka Slovenije glede računov bank in hranilnic, ki jih vodi v skladu z zakonom, ter Uprava Republike Slovenije za javna plačila glede podračunov, ki jih vodi v skladu z zakonom, AJPES tekoče zagotavljajo podatke za vzpostavitev in vodenje RTR, razen podatkov o dejanskih lastnikih imetnikov transakcijskih računov, ki se prevzemajo iz registra dejanskih lastnikov.²⁴⁴

144. Iz odgovora Banke Slovenije in AJPES izhaja, da se niti v RTR niti v drugih registrih ne vodijo podatki o imetniku oziroma pooblaščenju hranilnih vlog, denarnic za hrambo virtualne valute, denarnega depozita ter o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo. Na podlagi ZPPDFT-2 pa je pri Uradu Republike Slovenije za preprečevanje pranja denarja vzpostavljen register ponudnikov storitev virtualnih valut, v katerem pa se ne vodijo podatki o denarnicah za hrambo virtualnih valut.

145. V RTR pa se v skladu s 192. členom ZPlaSSIED 1) vodijo podatki v zvezi s transakcijskimi (ne pa tudi drugimi plačilnimi) računi, ki jih vodijo banke in hranilnice s sedežem v Republiki Sloveniji (podatki o imetniku, pooblaščenju, dejanskem lastniku imetnika in transakcijskem računu, datum odprtja in zaprtja), ter 2) podatki o najemniku oziroma pooblaščenju sefov in času njihove uporabe, če gre za sef, ki ga oddajajo banke in hranilnice s sedežem v Republiki Sloveniji.

²⁴⁰ Člen 145 ZBan-3.

²⁴¹ Prvi odstavek 146. člena ZBan-3.

²⁴² Drugi odstavek 146. člena ZBan-3.

²⁴³ Tretja alineja tretjega odstavka 146. člena ZBan-3.

²⁴⁴ Člen 191 in prvi odstavek 192. člena ZPlaSSIED.

146. Tudi podatki, ki se v skladu s 192. členom ZPlaSSIED vodijo v RTR, so javno dostopni le v mejah 194. člena ZPlaSSIED. Podatki o transakcijskih računih fizičnih oseb so namreč osebni podatki, ki se obdelujejo v RTR z namenom, določenim v zakonu.²⁴⁵ V splošnem so sicer podatki v RTR res javni in brezplačno dostopni na spletni strani AJPES, a to ne velja za podatke o pooblaščenih in dejanskih lastnikih imetnikov transakcijskih računov ter najemnikov sefov in osebne podatke fizičnih oseb, razen za podatke o transakcijskih računih podjetnikov in zasebnikov, ki se uporabljajo za opravljanje dejavnosti. Namen javne objave podatkov o transakcijskih računih podjetnikov in zasebnikov, ki se uporabljajo za opravljanje dejavnosti, je namreč zagotavljanje varnosti pravnega prometa v zvezi z opravljanjem dejavnosti.²⁴⁶

147. AJPES varuje osebne podatke v zvezi s sefi, pooblaščenici in dejanskimi lastniki imetnikov transakcijskih računov ter podatke o fizičnih osebah in njihovih transakcijskih računih kot zaupne v skladu z ZVOP-2, razen če so podatki o transakcijskih računih podjetnikov in zasebnikov postali javni v skladu s prvim odstavkom 194. člena ZPlaSSIED.²⁴⁷ Osebne podatke o transakcijskih računih fizičnih oseb pa je na podlagi tretjega do šestega odstavka 194. člena ZPlaSSIED mogoče pridobiti²⁴⁸ za namene izvršbe, preverjanja obstoja transakcijskega računa pri opravljanju plačilnih storitev ter tekočega in učinkovitega opravljanja plačilnih storitev, preverjanja obstoja transakcijskega računa pri obravnavi prošnje za odprtje osnovnega plačilnega računa in v okviru pravice do seznanitve z lastnimi osebnimi podatki. Javno dostopni so torej le podatki iz 145. točke obrazložitve te odločbe, ki se nanašajo na pravne osebe, in podatki o transakcijskih računih podjetnikov in zasebnikov, ki se uporabljajo za opravljanje dejavnosti.

148. Pri obsegu javne dostopnosti teh podatkov je treba upoštevati tudi obdobje, za katero se podatki hranijo in jih je tudi mogoče pridobiti. Kot je navedla AJPES v svojem odgovoru, se podatki o imetniku transakcijskega računa ter datumu odprtja in zaprtja transakcijskega računa v RTR vodijo že od vzpostavitve RTR (tj. od 1. 7. 2010), pred tem pa na Banki Slovenije. Podatki o pooblaščenju imetnika transakcijskega računa in podatki o sefu (njegovem najemniku in trajanju najema) pa se v RTR vodijo zgolj od 6. 11. 2021. Hkrati se navedeni podatki hranijo v arhivu RTR še pet let po zaprtju računa, prenehanju najema sefa, prenehanju pooblastila oziroma po tem, ko fizična oseba ni več dejanski lastnik imetnika transakcijskega računa, razen podatka, da se

²⁴⁵ Drugi odstavek 193. člena ZPlaSSIED.

²⁴⁶ Četrty odstavek 194. člena ZPlaSSIED.

²⁴⁷ Drugi odstavek 194. člena ZPlaSSIED: "Agencija z naslednjim dnem po dnevu izbrisa podjetnika ali zasebnika iz Poslovnega registra Slovenije, ki se šteje za prenehanje opravljanja njegove dejavnosti, samodejno, na podlagi podatkov Poslovnega registra Slovenije, onemogoči javno objavo in dostop do osebnih podatkov podjetnikov ali zasebnikov."

²⁴⁸ Za dostop do podatkov iz arhiva RTR se smiselno uporabljajo prvi do četrty odstavek 194. člena, razen 1. točke tretjega odstavka tega člena, ter 195. in 196. člen ZPlaSSIED (sedmi odstavek 194. člena ZPlaSSIED).

transakcijski račun, katerega imetnik je fizična oseba, uporablja za opravljanje dejavnosti, in podatka, da sredstva na transakcijskem računu ne zadoščajo za izvršitev sklepa o izvršbi ali zavarovanju, ki se hranita eno leto.²⁴⁹ V navedenih časovnih mejah so torej javno dostopni tudi podatki iz 145. točke obrazložitve te odločbe, ki se nanašajo na pravne osebe, in podatki o transakcijskih računih podjetnikov in zasebnikov, ki se uporabljajo za opravljanje dejavnosti.

149. Iz navedenega izhaja, da ni mogoče v splošnem pritrditi navedbam zakonodajalca v gradivu k ZKP-K, na katerega razlogih temelji tudi izpodbijana določba, da podatki iz petega odstavka 156. člena ZKP v splošnem niso zaupni in da so podatki o transakcijskih računih vsi javno dostopni. Javno dostopni (in s tem ne več zaupni) so v navedenih časovnih mejah le naslednji podatki iz petega odstavka 156. člena ZKP: 1) podatki v zvezi s transakcijskimi (ne pa tudi drugimi plačilnimi) računi, ki jih vodijo banke in hranilnice s sedežem v Republiki Sloveniji (podatki o imetniku, pooblaščenцу, dejanskem lastniku imetnika in transakcijskem računu, datum odprtja in zaprtja), ter 2) podatki o najemniku oziroma pooblaščenцу sefov in času njihove uporabe, če gre za sef, ki ga oddajajo banke in hranilnice s sedežem v Republiki Sloveniji, ki se nanašajo na pravne osebe in podatke o transakcijskih računih podjetnikov in zasebnikov, ki se uporabljajo za opravljanje dejavnosti.

150. To pa zagotovo ne velja za navedene podatke, ki se nanašajo na fizične osebe, za podatke o plačilnih računih, ki niso transakcijski računi zavezancev s sedežem v Republiki Sloveniji, ter za podatke o imetniku oziroma pooblaščenцу hranilnih vlog, denarnic za hrambo virtualne valute, denarnega depozita ter o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo. V zvezi z denarnicami za hrambo virtualne valute je treba izpostaviti še njihovo bistveno lastnost, tj. anonimno naravo poslovanja z virtualnimi valutami, saj je vsak podatek o strankah in omrežnih vozliščih skrit s kriptoplačilom.²⁵⁰ Podatek o obstoju pogodbenega oziroma poslovnega razmerja z osumljeno osebo pa sam po sebi niti nujno ne pomeni finančnega podatka, ampak podatek o obstoju kateregakoli pogodbenega razmerja z osumljencem.²⁵¹

151. V obsegu, navedenem v prejšnjem odstavku, pomeni torej pridobivanje podatkov po petem odstavku 156. člena ZKP pridobivanje zaupnih podatkov.

152. Ustavno sodišče poudarja pomen in občutljivost navedenih podatkov. Pomen podatkov o obstoju določene transakcije (*transactional data*) se je povečal. Niso pomembni le podatki o vsebini določene transakcije (to so podatki po prvem in tretjem

²⁴⁹ Drugi odstavek 192. člena ZPlaSSIED.

²⁵⁰ S. Jokić, A. S. Cvetković, S. Adamović, N. Ristić, P. Spalević, nav. delo, str. 74.

²⁵¹ Ustavno sodišče se ne opredeljuje do jasnosti in pomenske določljivosti te določbe, ker to ni predmet presoje v obravnavanem primeru.

odstavku 156. člena ZKP), ampak tudi podatki o obstoju določene transakcije.²⁵² Tako kot je to Ustavno sodišče navedlo že za prometne in lokacijske podatke, združitev do sedaj ločenih podatkov omogoča še bolj poglobljeno vsebinsko oceno o posameznikovem socialnem in ekonomskem položaju. Pomen teh podatkov je še toliko večji, ker omogoča vsebinsko bogato sklepanje o osebnem življenju in dejanskem obnašanju posameznika. Običajno vsebuje na primer čas dogodka, številko računa ali kreditne kartice, podatke o upravičencu računa oziroma kartice. Nekatere finančne navade kažejo na primer relevantne povezave z določenimi verskimi ali političnimi skupnostmi. Plačevanje zdravstvenih računov pa lahko vključuje tudi občutljive podatke, kot je zdravljenje določene bolezni.²⁵³

153. Navedeni zaupni podatki lahko razkrivajo tudi osebne povezave med določenimi posamezniki (na primer med imetnikom in pooblaščenecem določenega računa, sefa, hranilne vloge ali denarnice za virtualno valuto). Še več podatkov je mogoče razbrati iz dejstva, da ima določen osumljenec na primer z banko pogodbo o delu, zavarovalno, menjalno pogodbo ali praktično katerokoli pogodbo po OZ (ali po ZOR, kolikor še velja).

154. Pridobitev zaupnih podatkov po petem odstavku 156. člena ZKP omogoča identifikacijo fizičnih oseb, ki se "skrivajo" za določenim plačilnim računom, hranilno vlogo, sefom ali denarnico za virtualno valuto, bodisi kot imetniki bodisi kot pooblaščenci. Ti plačilni računi, hranilne vloge, sefi ali denarnice za virtualno valuto so relevantni za kazenski postopek, saj je mogoče podatke po petem odstavku 156. člena ZKP pridobiti le, če je to potrebno za preprečitev ali odkritje kaznivega dejanja ali storilca. Iz navedenih zaupnih podatkov se tako ugotovi, kdo stoji za temi kazenskopravno relevantnimi plačilnimi računi, hranilnimi vlogami, sefi ali denarnicami za virtualno valuto. V tem delu se spoznavni postopek v predkazenskem postopku na podlagi petega odstavka 156. člena ZKP razlikuje od spoznavnega postopka finančne uprave ali centra za socialno delo, za delo katerega so relevantni podatki, ki so vezani na določeno osebo, tj. davčnega zavezanca ali vlagatelja za pridobitev pravic iz javnih sredstev. Tudi pridobitev finančnih podatkov po petem odstavku 156. člena ZKP lahko torej pomeni močan poseg v informacijsko zasebnost.

155. Zaupne podatke po petem odstavku 156. člena ZKP lahko pridobita policija in državni tožilec neposredno od zavezancev brez predhodne sodne odredbe in brez jamstev, ki jih ta zagotavlja. Glede na zaupnost podatkov in zgoraj opisani vsebinski pomen teh podatkov, teža posega (tj. pridobivanje zaupnih podatkov iz 150. točke obrazložitve te odločbe brez predhodne sodne odredbe) v varstvo osebnih podatkov oseb, na katere se ti nanašajo (tj. imetniki in pooblaščenci), po oceni Ustavnega sodišča pretehta koristi ukrepa (tj. odpravljanje administrativnih in časovnih ovir pri preiskovanju kaznivih dejanj, s katerimi je bila pridobljena protipravna premoženjska

²⁵² C. Westermeier, Money is data – the platformization of financial transactions, *Information, Communication & Society*, let. 23, št. 14 (2020), str. 2047–2063.

²⁵³ Prav tam.

korist, in pranje denarja, učinkovitejše preiskovanje finančnih tokov in povezav ter izvorov sumljivega premoženja prek drugih računov).

Odločitev Ustavnega sodišča

156. Ukrep iz petega odstavka 156. člena ZKP tako pomeni nesorazmeren poseg v pravico do informacijske zasebnosti (prvi odstavek 38. člena Ustave), zato je Ustavno sodišče razveljavilo peti odstavek 156. člena ZKP (1. točka izreka).

157. Ker je šesti odstavek 156. člena ZKP (kolikor se nanaša na ukrep iz petega odstavka 156. člena ZKP) neposredno povezan tudi s petim odstavkom tega člena in v tem obsegu nima samostojnega pomena, je Ustavno sodišče razveljavilo tudi šesti odstavek 156. člena ZKP, kolikor se nanaša na ukrep iz petega odstavka 156. člena ZKP (2. točka izreka).

158. V skladu s 43. členom ZUstS začne razveljavitev učinkovati naslednji dan po objavi odločbe o razveljavitvi oziroma po poteku roka, ki ga je določilo Ustavno sodišče. Iz razlogov, navedenih v 63. točki obrazložitve te odločbe, je Ustavno sodišče tudi učinkovanje razveljavitve petega in šestega (v navedenem obsegu) odstavka 156. člena ZKP odložilo za čas enega leta od objave te odločbe v Uradnem listu Republike Slovenije in s tem zakonodajalcu določilo najdaljši možni rok za uskladitev razveljavljene ureditve z Ustavo (3. točka izreka).

B. – V.

Presoja izpodbijanega tretjega odstavka 148. člena ZKP

159. Izpodbijani tretji odstavek 148. člena ZKP določa:

"Policija lahko vabi osebe k sebi in od njih zbere obvestila in podatke ali jih zasliši. Vabi jih lahko pisno, neposredno ustno, po telefonu ali po elektronski poti. Osebi mora biti ob vabljenju pojasnjeno, zakaj in v kakšni vlogi je vabljen. Če se oseba vabi zaradi zbiranja obvestil, jo policija lahko prisilno privede, če jo vabi pisno in če pisno vabilo vsebuje pouk, da se jo, če na vabilo ne bo prišla, lahko prisilno privede. Če vabilo ni pisno, se o njem napravi uradni zaznamek.²⁵⁴ Ko ravna po določbah tega člena, policija ne sme oseb zasliševati kot obdolžencev, prič ali izvedencev, razen osumljenca v primeru iz 148.a člena tega zakona."

160. Vabljenje je policijsko pooblastilo,²⁵⁵ podrobneje urejeno v 35. členu ZNPPol. Ta v drugem odstavku izrecno določa, da smejo policisti osebo vabiti pisno, neposredno ustno, po telefonu ali elektronski poti. Osebe, ki policiji niso znane, se lahko vabijo z

²⁵⁴ V poševnem tisku je poudarjen izpodbijani del določbe.

²⁵⁵ Druga alineja prvega odstavka 33. člena ZNPPol.

javnim naznanilom. Vabilo mora vsebovati kraj, čas in razlog vabljenja. Osebo smejo policisti prisilno privedi le v primeru iz druge alineje prvega odstavka 35. člena ZNPPol (tj., da je njena navzočnost nujno potrebna za izvedbo drugega policijskega pooblastila, določenega z ZNPPol ali z drugim zakonom), če se vabilu ni odzvala niti izostanka ni opravičila, v pisnem vabilu pa je bila opozorjena na možnost prisilne privedbe.²⁵⁶ Policisti morajo pred izvedbo nadaljnjih pooblastil, zaradi katerih je bila oseba vabljen, preveriti identiteto osebe, zlasti ko je bilo vabljenje opravljeno po telefonu ali elektronski pošti.²⁵⁷ Za vabila, ki niso pisna, se predvideva uradni zaznamek.²⁵⁸ ZKP-N je tako prenesel v (pred)kazenski postopek ureditev, ki po ZNPPol velja za policijske postopke oziroma policijsko pooblastilo vabljenja na splošno.²⁵⁹

161. Ustavno sodišče je predlagateljeve navedbe o spornosti določbe o vabljenju oseb, zlasti elektronskem, ustnem in telefonskem, na policijo za zbiranje obvestil in podatkov ter zaslišanje presoјalo z vidika načela jasnosti in pomenske določljivosti iz 2. člena Ustave (glej 67.–69. točko obrazložitve te odločbe).

162. Predlagatelj ne nasprotuje temu, da je prisilna privedba možna le pri pisnem vabilu, ki omogoča sledljivost vabljenja. Večina navedb predlagatelja izpostavlja praktične probleme oziroma dokazne probleme v praksi, ki ne pomenijo ustavnopravnih vprašanj. Hkrati je z ustaljenimi metodami razlage (zlasti z jezikovno) mogoče ugotoviti vsebino izpodbijane določbe, zato tretji odstavek 148. člena ZKP ni v neskladju z Ustavo (4. točka izreka).

B. – VI.

Presoja izpodbijanega sedmega odstavka 148. člena ZKP

163. Izpodbijani sedmi odstavek 148. člena ZKP določa:

"Oseba, zoper katero je bilo uporabljeno kakšno dejanje ali ukrep iz drugega ali tretjega odstavka tega člena, ima pravico v roku treh dni pritožiti se pristojnemu državnemu tožilcu. Pristojni državni tožilec najkasneje v roku osmih dni od vložitve pritožbe ustno ali pisno obvesti pritožnika o tem, kar je ukrenil. Zoper obvestilo iz prejšnjega stavka ni dovoljena pritožba ali upravni spor."

²⁵⁶ Drugi do peti odstavek 35. člena ZNPPol. Glej tudi M. Žaberl, M. Nunič, T. Bobnar, R. Ferenc, G. Hudrič, A. Senčar, Zakon o nalogah in pooblastilih policije (ZNPPol) s komentarjem, IUS Software, GV Založba, Ljubljana 2015, str. 118.

²⁵⁷ Prav tam.

²⁵⁸ Predlog ZKP-N, str. 146.

²⁵⁹ Prav tam.

164. Tudi to določbo predlagatelj izpodbija z vidika načela jasnosti in pomenske določljivosti iz 2. člena Ustave.

165. Na podlagi izpodbijane določbe državni tožilec ukrepa zlasti v okviru svojega splošnega pooblastila za usmerjanje policije v predkazenskem postopku.²⁶⁰ V skladu s prvim odstavkom 160.a člena ZKP lahko državni tožilec pri izvrševanju svojih zakonskih pooblastil usmerja delo policije, in sicer z obveznimi navodili, strokovnimi mnenji ter predlogi za zbiranje obvestil in izvedbo drugih ukrepov, za katere je pristojen, z namenom, da se odkrijeta kaznivo dejanje in storilec oziroma da se zberejo podatki, potrebni za njegovo odločitev o kazenskem pregonu. Po drugem odstavku 161. člena ZKP lahko državni tožilec, če iz same ovadbe ne more presoditi, ali so navedbe v njej verjetne, ali če podatki v ovadbi ne dajejo dovolj podlage, da bi lahko odločil, ali naj zahteva preiskavo, ali če je do njega prišel le glas o kaznivem dejanju, zlasti pa, če je storilec neznan, zahteva od policije, če tega ne more storiti sam ali po drugih organih, naj v roku, ki ga določi on, zbere potrebna obvestila in stori druge ukrepe, da se odkrijeta kaznivo dejanje in storilec (148. in 149. člen ZKP). Državni tožilec sme ob vsakem času zahtevati od policije, da ga obvesti, kaj je ukrenila; ta mu je dolžna brez odlašanja odgovoriti.²⁶¹

166. Podrobneje usmerjanje ureja Uredba. Pri tem je relevanten zlasti njen 11. člen, v skladu s katerim usmerjanje predkazenskega postopka s strani državnega tožilca obsega obvezna navodila in predloge za zbiranje obvestil ter izvedbo drugih ukrepov za pridobitev dokazov; obvezna navodila glede ukrepov v primeru odvzema prostosti (osmi odstavek 157. člena ZKP); strokovna mnenja; udeležbo državnega tožilca pri procesnih dejanjih, za katera je pristojen v predkazenskem postopku; ter odločitev državnega tožilca o prikritih preiskovalnih ukrepih in zavarovanju odvzema premoženjske koristi.²⁶² Vzporedno s postopkom po sedmem odstavku 148. člena ZKP je možen tudi tek pritožbenega postopka zoper delo policistov po ZNPPol,²⁶³ saj je pritožba po izpodbijani določbi ZKP namenjena ohranitvi korektnosti kazenskega postopka, pritožba po ZNPPol pa nasprotno nima vpliva na tek konkretnega postopka, v katerem naj bi prišlo do nepravilnosti.²⁶⁴

167. Ker je z ustaljenimi metodami razlage mogoče ugotoviti vsebino izpodbijane določbe (v konkretnem primeru zlasti z jezikovno in sistemsko), določba ni v neskladju z Ustavo (4. točka izreka).

²⁶⁰ Prav tam, str. 140.

²⁶¹ Podrobneje sodelovanje med državnim tožilstvom in policijo ureja Uredba o sodelovanju državnega tožilstva, policije in drugih pristojnih državnih organov in institucij pri odkrivanju in pregonu storilcev kaznivih dejanj ter delovanju specializiranih in skupnih preiskovalnih skupin (Uradni list RS, št. 83/10, 28/21 in 87/22 – v nadaljevanju Uredba).

²⁶² Glej celotno III. poglavje Uredbe z naslovom Usmerjanje.

²⁶³ Člen 139 ZNPPol in naslednji.

²⁶⁴ Predlog ZKP-N, str. 140.

B. – VII.**Presoja izpodbijanega 149.č člena ZKP**

168. Izpodbijani 149.č člen določa:

"(1) Če so podani razlogi za sum, da je bilo izvršeno oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje, preprečitev ali dokazovanje tega kaznivega dejanja ali odkritje storilca treba pridobiti naročniške podatke o lastniku ali uporabniku določenega komunikacijskega sredstva ali storitve informacijske družbe ali obstoju in vsebini njegovega pogodbenega razmerja z operaterjem oziroma ponudnikom storitev informacijske družbe v zvezi z opravljanjem komunikacijske dejavnosti ali storitev informacijske družbe, lahko sodišče, državni tožilec oziroma policija od operaterja oziroma ponudnika storitev informacijske družbe v pisni obliki zahteva, da tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči te podatke. Pisna zahteva mora vsebovati pravni pouk iz drugega odstavka tega člena in navedbo pristojnega sodišča. Državni tožilec oziroma policija morata v pisni zahtevi natančno opredeliti kategorije naročniških podatkov, ki jih zahtevata.

(2) Operater oziroma ponudnik storitev informacijske družbe lahko iz obrazloženih razlogov in na svoje stroške zahtevane podatke skupaj s kopijo zahteve namesto policiji ali državnemu tožilcu pisno posreduje pristojnemu sodišču. Sodišče po prejemu preveri zakonitost kategorij podatkov, ki so navedeni v zahtevi. V primeru, da zahteva vsebuje tudi podatke, ki niso naročniški podatki po prvem odstavku tega člena ali podatke, ki se jih v skladu s četrnim odstavkom tega člena ne sme posredovati, prejete podatke uniči, sicer pa jih posreduje državnemu tožilcu ali policiji. V primeru uničenja preiskovalni sodnik o tem napravi uradni zaznamek, ki ga posreduje operaterju oziroma ponudniku storitev informacijske družbe, vodji pristojnega okrožnega državnega tožilstva ali državnemu tožilcu, ministrstvu, ki je pristojno za nadzor nad delom policije, in policiji.

(3) Operater oziroma ponudnik storitev informacijske družbe svojemu uporabniku, naročniku ali tretjim osebam ne sme razkriti, da je ali da bo v skladu s tem členom posredoval določene podatke. Tega ne sme razkriti 24 mesecev po preteku meseca, v katerem so bili posredovani podatki. V primeru, da operater oziroma ponudnik storitev informacijske družbe v tem roku prejme sodno odredbo, ki se sklicuje na podatke, pridobljene z zahtevo po tem členu, se rok prepovedi razkritja te zahteve podaljša do izteka morebitnega roka iz prejete odredbe. Preiskovalni sodnik oziroma sodišče lahko z odredbo določi drugačen rok, rok podaljša za največ 12 mesecev, vendar ne več kot dvakrat, rok skrajša ali prepoved seznanitve odpravi.

(4) Na podlagi tega člena ni mogoče zahtevati ali pridobiti prometnih podatkov, ki se nanašajo na katero koli določljivo komunikacijo, ali podatkov, za pridobitev katerih je

potrebna obdelava podatkov, ki se lahko pridobijo samo na podlagi 149.b in 149.c člena tega zakona. Na podlagi tega člena prav tako ni mogoče zahtevati ali pridobiti podatkov, ki se nanašajo na vsebino komunikacije."

169. Tudi to določbo predlagatelj izpodbija z vidika načela jasnosti in pomenske določljivosti. Nejasni naj bi bili naslednji pojmi: naročniški podatek, podatek o obstoju in vsebini pogodbenega razmerja ter razlogi za postopek naknadne sodne presoje. Ustavno sodišče je zato tudi to izpodbijano določbo presojalo z vidika načela jasnosti in pomenske določljivosti iz 2. člena Ustave.

Naročniški podatki

170. ZKP naročniških podatkov ne opredeljuje s taksativnim ali vsaj eksemplifikativnim naštevanjem. Določa, da lahko sodišče, državni tožilec oziroma policija od operaterja oziroma ponudnika storitev informacijske družbe v pisni obliki zahteva, da tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči podatke o 1) lastniku ali uporabniku določenega komunikacijskega sredstva ali storitve informacijske družbe ali 2) obstoju in vsebini njegovega pogodbenega razmerja z operaterjem v zvezi z opravljanjem komunikacijske dejavnosti.

171. Za razlago naročniških podatkov je tako treba najprej upoštevati vsebino prvega odstavka 215. člena ZEKom-2, ki opredeljuje podatke o naročnikih, torej naročniške podatke: 1. osebno ime oziroma firmo naročnika in njeno organizacijsko obliko; 2. naslov naročnika; 3. naročniško številko in druge elemente oštevilčenja, ki se uporabljajo za vzpostavitev zveze do naročnika; 4. na željo naročnika akademski, znanstveni ali strokovni naziv, naslov njegove spletne strani in druge vrste njegovih osebnih stikov (npr. IP-naslov) ali njegov e-naslov; 5. davčno številko za fizično osebo ter davčno in matično številko za pravno osebo; 6. na podlagi plačila naročnika še dodatne podatke, če to želi naročnik in se s tem ne poseže v pravice tretjih oseb.²⁶⁵

172. Glede na opredelitev osebnega podatka (prim. 93. točko obrazložitve te odločbe) so naročniški podatki, ki se nanašajo neposredno na fizično osebo, osebni podatki in s tem varovani z 38. členom Ustave.²⁶⁶

173. ZKP v četrtem odstavku 149.č člena določa, da na podlagi tega člena ni mogoče zahtevati ali pridobiti prometnih podatkov, ki se nanašajo na katerokoli določljivo komunikacijo, ali podatkov, za pridobitev katerih je potrebna obdelava podatkov, ki se lahko pridobijo samo na podlagi 149.b in 149.c člena ZKP. Na podlagi tega člena prav tako ni mogoče zahtevati ali pridobiti podatkov, ki se nanašajo na vsebino komunikacije. Iz opredelitve naročniških podatkov iz prvega odstavka 215. člena

²⁶⁵ Tretji odstavek 215. člena ZEKom-2.

²⁶⁶ P. Plesec, nav. delo, str. 37.

ZEKom-2 in posledično prvega odstavka 149.č člena ZKP je treba na tej podlagi že ob uporabi jezikovne razlage izločiti podatke iz četrtega odstavka 149.č člena ZKP.

174. Pri razlagi naročniških podatkov iz prvega odstavka 215. člena ZEKom-2 in posledično prvega odstavka 149.č člena ZKP je treba upoštevati tudi jasno izražen namen zakonodajalca ob sprejemanju ZKP-N, ustaljeno ustavnosodno presojo ter prakso ESČP in SEU. Iz zakonodajnega gradiva namreč izhaja namen zakonodajalca, da izpodbijani 149.č člen ZKP (prav zaradi nejasnosti pretekle prakse ali zaradi zlorab)²⁶⁷ ni namenjen pridobivanju prometnih podatkov oziroma podatkov, za katere njihov imetnik upravičeno pričakuje zasebnost po 37. členu Ustave.²⁶⁸ Izpodbijana ureditev naj bi namreč nastala zaradi implementacije ustaljene ustavnosodne presoje ter prakse ESČP in SEU, zlasti sodbe ESČP v zadevi *Benedik proti Sloveniji*.²⁶⁹

175. Po drugem odstavku 37. člena Ustave je mogoče poseči v komunikacijsko zasebnost med drugim le na podlagi odločbe sodišča. Iz ustaljene ustavnosodne presoje izhaja, da so, poleg vsebine sporočila, varovane tudi okoliščine in dejstva, povezani s komunikacijo, tj. tisti podatki o komunikaciji, ki so njen sestavni del – prometni podatki. Podatki o prometu so kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega obračunavanja, pri čemer je po ustaljeni ustavnosodni presoji IP-naslov, tudi dinamični, prometni podatek.²⁷⁰

176. Iz ustaljene prakse ESČP in SEU izhaja, da sodišči kot merilo za presojo sorazmernosti posega v pravici iz 7. in 8. člena Listine oziroma 8. člena EKČP oziroma za presojo dostopa do prometnih podatkov določata tudi, da dostop do hranjenih podatkov načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, odobri sodišče ali neodvisen upravni organ na obrazložen predlog, odredba tožilstva s sodno kontrolo zadošča, če pa gre za utemeljeno pričakovanje zasebnosti, je potrebna sodna odredba.²⁷¹ ESČP je v omenjeni zadevi *Benedik proti Sloveniji* med drugim presojalo zatrjevano kršitev pravice pritožnika iz 8. člena EKČP zaradi pridobitve podatkov o naročniku, povezanih z njegovim dinamičnim IP-naslovom, in posledično njegove

²⁶⁷ Prav tam, str. 39.

²⁶⁸ Prav tam. Ne gre za poseg v komunikacijsko zasebnost. Š. Horvat, nav. delo, str. 329.

²⁶⁹ Predlog ZKP-N.

²⁷⁰ Odločba Ustavnega sodišča št. Up-153/17, 12. in 15. točka obrazložitve. Glej tudi odločbe Ustavnega sodišča št. Up-106/05, 8. in 10. točka obrazložitve, št. Up-540/11, 14. točka obrazložitve, in št. Up-709/15, Up-710/15, 43. točka obrazložitve, ter 55. točko 3. člena ZEKom-2.

²⁷¹ Odločba Ustavnega sodišča št. Up-709/15, Up-710/15, 46. točka obrazložitve; sodbe SEU v zadevah *Tele2 Sverige*, 111. točka obrazložitve; in *Kazenski postopek zoper H. K.*, 57. točka obrazložitve; ter v združenih zadevah *The Commissioner of the Garda Síochána*, 106., 108. in 109. točka obrazložitve; sodbi ESČP v zadevah *Ben Faiza proti Franciji*, 69.–76. točka obrazložitve, in *Benedik proti Sloveniji*, 130. točka obrazložitve.

identitete brez odredbe sodišča.²⁷² Predvsem na podlagi dejstva, da je njegova spletna dejavnost vključevala visoko stopnjo anonimnosti,²⁷³ je ESČP ocenilo, da je pritožnik upravičeno pričakoval zasebnost in da se ji s svojim ravnanjem ni odpovedal, zato bi bila za pridobitev naročniških podatkov v zvezi z IP-naslovom potrebna sodna odredba. Po stališču ESČP podatki o naročniku v zvezi z določenimi dinamičnimi IP-naslovi, dodeljenimi ob določenih urah, niso bili javno dostopni in jih zato ni mogoče primerjati s podatki v klasičnem telefonskem imeniku ali javno dostopni podatkovni zbirki o registraciji vozil. Ponudnik internetnih storitev naj bi moral namreč za identifikacijo naročnika, ki mu je bil določen dinamični IP-naslov, dodeljen ob določenem času, dostopati do shranjenih podatkov v zvezi z določenimi telekomunikacijskimi dogodki.²⁷⁴ ESČP je še odločilo, da dejstvo, da pritožnik ni skrnil svojega dinamičnega IP-naslava ob domnevi, da je to sploh mogoče storiti, ne more biti odločujoče pri presoji, ali je bilo njegovo pričakovanje zasebnosti upravičeno z objektivnega stališča. Nasprotno; po stališču ESČP naj bi bilo ključno, ali je pritožnik lahko upravičeno pričakoval zasebnost v zvezi s svojo identiteto.²⁷⁵ Na to vprašanje je ESČP odgovorilo pritrdilno;²⁷⁶ anonimnostno pojmovanje zasebnosti naj bi bil pomemben dejavnik, ki ga je treba upoštevati pri presoji, kot tudi dejstvo, da ni bilo zatrjevano, da je pritožnik razkril svojo identiteto v zvezi z obravnavano spletno dejavnostjo, ali da bi ga identificiral določeni ponudnik spletnih storitev prek računa ali kontaktnih podatkov. Pritožnikova spletna dejavnost naj bi vključevala visoko stopnjo anonimnosti, kar naj bi potrjevalo dejstvo, da dodeljenemu dinamičnemu IP-naslovu, čeprav je viden drugim uporabnikom omrežja, ne bi bilo mogoče slediti do določenega računalnika, ne da bi ponudnik internetnih storitev te podatke preveril na zahtevo policije.²⁷⁷ Zato naj bi pritožnik s svojega subjektivnega vidika pričakoval, da bo njegova dejavnost ostala zasebna in da njegova identiteta ne bo razkrita.²⁷⁸

177. Ker izpodbijana ureditev 149.č člena ZKP izrecno ne predvideva sodne odredbe (kot *a contrario* v razmerju do 149.b člena ZKP), je treba za ustavnoskladno razlago

²⁷² Tako tudi kasneje Vrhovno sodišče v sodbi št. I Ips 31751/2018 z dne 4. 6. 2020. ESČP se sicer ni izrecno opredelilo do pridobitve IP-naslava.

²⁷³ Glede anonimnostnega vidika spletne zasebnosti se je ESČP sklicevalo na sodbo velikega senata v zadevi *Delfi AS proti Estoniji* z dne 16. 6. 2015.

²⁷⁴ Sodba ESČP v zadevi *Benedik proti Sloveniji*, 108. točka obrazložitve.

²⁷⁵ Prav tam, 116. točka obrazložitve. Ker je 37. člen Ustave zagotavljal zasebnost korespondence in komunikacij in zahteval, da kakršenkoli poseg v to pravico temelji na odredbi sodišča, po stališču ESČP tudi s stališča zakonodaje, veljavne v tistem času, ni mogoče reči, da pritožnikovo pričakovanje zasebnosti v zvezi s spoštovanjem njegove spletne dejavnosti ni bilo zajamčeno ali upravičeno. Domače pravo, na katerem je ukrep (pridobitev naročniških podatkov brez sodne odredbe) temeljil, pa naj ne bi ustrezalo standardu pravne države. Posledično je ESČP ugotovilo kršitev 8. člena EKČP.

²⁷⁶ Prav tam, 134. točka obrazložitve.

²⁷⁷ Prav tam, 105., 106. in 117. točka obrazložitve.

²⁷⁸ Odločba Ustavnega sodišča št. Up-153/17, 17. točka obrazložitve.

naročniških podatkov iz prvega odstavka 215. člena ZEKom-2 in posledično prvega odstavka 149.č člena ZKP upoštevati 37. člen Ustave oziroma upravičeno pričakovanje komunikacijske zasebnosti ter predstavljeno prakso ESČP in SEU. Na podlagi prvega odstavka 149. člena ZKP ni mogoče pridobiti nobenih podatkov, čeprav so po vsebini to naročniški podatki, ki omogočajo neposredno ali posredno identifikacijo imetnika komunikacijskega sredstva, na primer pridobivanje podatkov, kdo se skriva za kakršnokoli enolično identifikacijsko oznako, ki jo posameznik uporablja za komunikacijo prek komunikacijskega sredstva.²⁷⁹ Na podlagi izpodbijane določbe torej ni mogoče pridobiti podatkov, ki omogočajo identifikacijo naročnika oziroma uporabnika katerekoli komunikacijskega sredstva prek katerekoli enolične označbe, ki ni javno objavljena oziroma glede katere ni podano upravičeno pričakovanje zasebnosti (elektronski naslov, telefonska številka, psevdonom, uporabljen v spletnem komentiranju, itd.).²⁸⁰

178. Kjer je v zvezi s podatkom podano upravičeno pričakovanje komunikacijske zasebnosti, je mogoče podatek pridobiti zgolj na podlagi prvega odstavka 149.b člena ZKP, v katerem pa upravičeno pričakovanje zasebnosti ni podano, je naročniški podatek mogoče pridobiti na podlagi prvega odstavka 149.č člena ZKP.²⁸¹

179. Z ustaljenimi metodami razlage je torej mogoče ugotoviti vsebino naročniških podatkov.

Podatek o obstoju in vsebini pogodbenega razmerja

180. Predlagatelj zatrjuje tudi nejasnost podatka o obstoju in vsebini pogodbenega razmerja

181. Podatki o pogodbenem razmerju pomenijo podatke o pravnem razmerju določene osebe z določenim operaterjem ali podatke, ki so nastali s sklenitvijo pogodbe ali s kasnejšimi aneksi. Pridobiti je torej mogoče podatek, ali ima določena oseba naročniško razmerje z določenim operaterjem, ali podatek o obstoju pogodbenega razmerja. Podatki o vsebini pogodbenega razmerja pa so podatki, ki so določeni v pogodbi ali drugih aktih in so nastajali zaradi teka naročniškega razmerja; opredeljujejo naročnika ali vsebino storitev, ki jih ima na podlagi naročniškega razmerja, ter medsebojne pravice in dolžnosti.²⁸² Pridobiti je mogoče podatke, ki so v pogodbi (o naročniku, podatke iz 215. člena ZEKom-2, kraj in čas sklenitve pogodbe), ter podatke

²⁷⁹ P. Križnar, O ustavni neskladnosti 149.č člena ZKP, Pravna praksa, št. 22 (2020), str. 11–13.

²⁸⁰ Tako tudi prav tam.

²⁸¹ Prim. P. Križnar v: M. Šepec (ur.), nav. delo; P. Križnar, Benedik proti Sloveniji, Pravna praksa, št. 19 (2018), str. 6–8; K. Amon, V. Maček, Bistvene spremembe Zakona o kazenskem postopku, ki jih prinaša novela ZKP-N, Pravnik, št. 5–6 (2019), str. 384.

²⁸² Predlog ZKP-N, str. 144.

v zvezi s pogodbo, ki ne predstavljajo posega, za katerega se zahteva uporaba pooblastil iz 149.b in 149.c člena ZKP.²⁸³

182. Ob upoštevanju 36.–40. točke obrazložitve te odločbe je mogoče navedene podatke pridobiti za znanega naročnika. Ni dopustna torej obratna pot, da bi na podlagi naročniških podatkov neznanega uporabnika operater na podlagi prvega odstavka 149.č člena ZKP sporočil podatek o identiteti nenaročnika, ki se "skriva" za to številko – to je nedvoumno prometni podatek po 149.b členu ZKP.

183. Z ustaljenimi metodami razlage je torej mogoče ugotoviti tudi vsebino izpodbijanega pojma podatek o obstoju in vsebini njegovega pogodbenega razmerja.

Razlogi za postopek naknadne sodne presoje

184. Predlagatelj zatrjuje tudi nejasnost razlogov za postopek naknadne sodne presoje iz 149. č člena ZKP.

185. Na podlagi drugega odstavka 149.č člena ZKP lahko operater oziroma ponudnik storitev informacijske družbe iz obrazloženih razlogov in na svoje stroške zahtevane podatke skupaj s kopijo zahteve namesto policiji ali državnemu tožilcu pisno posreduje pristojnemu sodišču. Sodišče po prejemu preveri zakonitost kategorij podatkov, ki so navedeni v zahtevi. Če zahteva vsebuje tudi podatke, ki niso naročniški podatki po prvem odstavku 149.č člena ZKP, ali podatke, ki se v skladu s četrtem odstavkom 149.č člena ZKP ne smejo posredovati, prejete podatke uniči, sicer pa jih posreduje državnemu tožilcu ali policiji. V primeru uničenja preiskovalni sodnik o tem napravi uradni zaznamek, ki ga posreduje operaterju oziroma ponudniku storitev informacijske družbe, vodji pristojnega okrožnega državnega tožilstva ali državnemu tožilcu, ministrstvu, ki je pristojno za nadzor nad delom policije, in policiji.

186. Drugi odstavek 149.č člena ZKP ureja položaje, v katerih bi operater oziroma ponudnik storitev informacijske družbe ocenil, da bi bil prisiljen ravnati nezakonito, če bi sledil zahtevi policije ali državnega tožilstva po prvem odstavku 149.č člena ZKP. Operaterju je ponujena dodatna možnost (ne pa zaveza), da podatke v takem primeru na svoje stroške posreduje sodišču. Posledica operaterjeve oziroma ponudnikove zahteve po drugem odstavku 149. člena ZKP je sodna presoja zakonitosti ukrepa iz prvega odstavka 149.č člena ZKP.²⁸⁴ Gre za varovalko pred morebitno zlorabo ali nepravilno uporabo 149.č člena ZKP.²⁸⁵

187. Preiskovalni sodnik na podlagi zahteve operaterja ali ponudnika storitev informacijske družbe presodi, kakšni sta narava in kategorija zahtevanih podatkov.

²⁸³ Prav tam, str. 145.

²⁸⁴ Prav tam, str. 144.

²⁸⁵ Prav tam, str. 28.

Oceni torej, ali so bili z dano zahtevo zahtevani podatki, ki jih je zakonito posredovati na podlagi 149.č člena ZKP, ali pa podatki, ki jih ni dopustno posredovati na podlagi tega člena; oziroma razlikovanje med pridobivanjem prometnih podatkov (149.b in 149.c člen ZKP), ki spadajo v okvir 37. člena Ustave, ter naročniških podatkov (149.č člen ZKP), ki ne spadajo v okvir komunikacijske zasebnosti.²⁸⁶ To je treba upoštevati tudi pri razlagi razlogov, iz katerih lahko operater ali ponudnik storitev informacijske družbe vložita zahtevo za presojo zakonitosti zahteve policije ali državnega tožilstva za pridobitev podatkov po prvem odstavku 149.č členu ZKP. Iz navedenega izhaja, da operater vloži zahtevo za sodno presojo,²⁸⁷ ko dvomi, da gre v zahtevi za take kategorije podatkov, ki se lahko zahtevajo po prvem odstavku 149.č člena ZKP brez sodne odredbe, oziroma ko na podlagi zahteve policije ali državnega tožilca presodi, da gre za podatke, ki niso naročniški podatki iz prvega odstavka 149.č člena ZKP. Poleg tega mora po drugem odstavku 149.č člena ZKP svoje dvome o zakonitosti zahteve oziroma razloge za zahtevo po drugem odstavku 149.č člena ZKP tudi obrazložiti.

188. Ker je torej z ustaljenimi metodami razlage mogoče ugotoviti vsebino izpodbijanih pojmov (naročniški podatek, podatek o obstoju in vsebini pogodbenega razmerja ter razlogi za postopek po drugem odstavku 149.č člena ZKP), 149.č člen ZKP ni v neskladju z načelom jasnosti in pomenske določljivosti iz 2. člena Ustave (4. točka izreka).

C.

189. Ustavno sodišče je sprejelo to odločbo na podlagi 43. in 21. člena ZUstS ter tretje alineje tretjega odstavka 46. člena Poslovnika Ustavnega sodišča (Uradni list RS, št. 86/07, 54/10, 56/11, 70/17 in 35/20) v sestavi: predsednik dr. Matej Accetto ter sodnici in sodniki dr. Rok Čeferin, Dr. Dr. Klemen Jaklič (Oxford ZK, Harvard ZDA), dr. Rajko Knez, dr. Neža Kogovšek Šalomon, Marko Šorli in dr. Katja Šugman Stubbs. Odločbo je sprejelo soglasno. Sodnica Šugman Stubbs in sodnik Accetto sta dala pritrilni ločeni mnenji.

dr. Matej Accetto
Predsednik

²⁸⁶ Prav tam. Če torej preiskovalni sodnik presodi, da so zahtevani podatki iz prvega odstavka 149.č člena ZKP, je zahteva zakonita in podatke posreduje državnemu tožilcu ali policiji. Če pa gre za podatke, ki niso podatki iz prvega odstavka 149.č člena ZKP, ali za podatke, ki se v skladu s četrtim odstavkom 149.č člena ZKP ne smejo posredovati, prejete podatke uniči.

²⁸⁷ Gre za naknadno sodno presojo. Glej P. Gorkič, nav. delo, 2017, str. 39, 40.