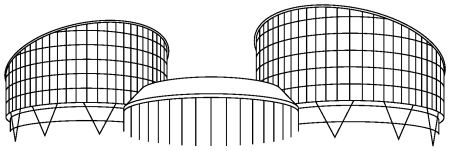

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

ČETRTI ODDELEK

ZADEVA BENEDIK proti SLOVENIJI

(pritožba št. 62357/14)

SODBA

STRASBOURG

24. april 2018

Ta sodba bo postala dokončna v okoliščinah, navedenih v drugem odstavku 44. člena konvencije. Mogoči so uredniški popravki.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

V zadevi Benedik proti Sloveniji

Evropsko sodišče za človekove pravice (četrti oddelek) kot senat v sestavi:

Ganna Yudkivska, *predsednica*,
Vincent A. De Gaetano,
Faris Vehabović,
Carlo Ranzoni,
Georges Ravarani,
Marko Bošnjak,
Péter Paczolay, *sodniki*,
in Andrea Tamietti, *namestnik sodnega tajnika oddelka*,

po razpravi, zaprti za javnost, ki je bila 20. marca 2018,
izreka to sodbo, sprejeto navedenega dne:

POSTOPEK

1. Zadeva se je začela s pritožbo (št. 62357/14) proti Republiki Sloveniji, ki jo je na podlagi 34. člena Konvencije o varstvu človekovih pravic in temeljnih svoboščin (v nadaljnjem besedilu: konvencija) pri Sodišču vložil Igor Benedik.

2. Pritožnika je pred Sodiščem zastopal M. Jelenič Novak, odvetnik iz Ljubljane. Slovensko vlado (v nadaljnjem besedilu: vlada) je zastopala J. Morela, državna odvetnica.

3. Pritožnik je zlasti trdil, da so bile kršene njegove pravice po 8. členu konvencije, ker je policija nezakonito pridobila informacije od ponudnika internetnih storitev, ki so omogočile, da ga je bil identificiran.

4. Vlada je bila o pritožbi obveščena 8. aprila 2015.

DEJSTVA

I. OKOLIŠČINE ZADEVE

5. Pritožnik je bil rojen leta 1977 in živi v Kranju.

A. Preiskava

6. Leta 2006 je švicarska kantonalna policija kantona Valais opravljala sistematični pregled mreže internetnih uporabnikov z imenom "Razorback." Švicarska policija je ugotovila, da so nekateri uporabniki posedovali in si izmenjevali otroško pornografijo v obliki fotografij ali video posnetkov. Datoteke z nezakonito vsebino so se izmenjevale po sistemu mreže

imenovanem "p2p" (peer-to-peer), kar pomeni, da je vsak računalnik povezan v sistem deloval sočasno kot prejemnik in kot razdeljevalec vsebin. Iz tega sledi, da je vsak od uporabnikov imel možnost dostopa do in prenosa k sebi vseh datotek, ki so jih dali na voljo oziroma v delitev drugi uporabniki mreže. Švicarska policija je med naslovi dinamičnega internetnega protokola ("IP"), naletela tudi na določen dinamični IP-naslov, ki je bil kasneje povezan s pritožnikom.

7. Na podlagi podatkov, prejetih s strani švicarske policije, je slovenska policija dne 7. avgusta 2006, ne da bi pridobila odredbo sodišča, od ponudnika oziroma operaterja internetnih storitev, podjetja S zahtevala, naj razkrije podatke o naročniku, ki je 20. februarja 2006 ob 12:28 uri uporabljal zgoraj navedeni IP-naslov. Policija je svojo zahtevo utemeljila s tretjim odstavkom 149. b člena Zakona o kazenskem postopku (v nadaljevanju ZKP, glej 36. odstavek spodaj), ki od operaterjev elektronskih komunikacijskih storitev zahteva, da policiji razkrijejo informacije o identiteti lastnikov ali uporabnikov določenih elektronskih komunikacijskih sredstev, ki niso na voljo v ustreznem imeniku. Zato je ponudnik internetnih storitev 10. avgusta 2006 policiji sporočil ime in naslov pritožnikovega očeta, ki je bil naročnik internetne storitve na zadevnem IP-naslovu.

8. Dne 12. decembra 2006 je policija podala pobudo Okrožnemu državnemu tožilstvu v Kranju, naj preiskovalni sodnik Okrožnega sodišča v Kranju izda odredbo, ki bi operaterju in ponudniku internetnih storitev naložila razkritje osebnih podatkov naročnika ter podatkov o prometu, povezanih z zadevnim IP-naslovom. Dne 14. decembra 2006 je bila takšna odredba sodišča pridobljena na podlagi prvega odstavka 149. b člena ZKP in ponudnik internetnih storitev je policiji sporočil zahtevane podatke.

9. Dne 12. januarja 2007 je preiskovalni sodnik Okrožnega sodišča v Kranju izdal odredbo za hišno preiskavo v družinskem domovanju pritožnika. V odredbi je bil kot osumljenec označen pritožnikov oče. Med hišno preiskavo sta policija in preiskovalni sodnik zasegla štiri računalnike in pozneje naredila kopije njihovih trdih diskov.

10. Na podlagi razgovorov z družinskimi člani pritožnika, o katerih ni na voljo zapisov, je policija kot osumljenca začela obravnavati pritožnika.

11. Ob pregledu zadevnih trdih diskov je policija ugotovila, da je eden od njih vseboval otroško pornografijo. Policija je ugotovila, da je pritožnik na enega od računalnikov namestil program za izmenjavo datotek eMule, s katerim je nato od drugih uporabnikov programa na svoj računalnik lahko prenašal različne datoteke in tudi samodejno ponujal in razširjal svoje lastne datoteke drugim uporabnikom. Med datotekami, ki jih je na svoj računalnik prenesel pritožnik, jih je manjši odstotek vseboval otroško pornografijo.

12. Dne 26. novembra 2007 je okrožni državni tožilec v Kranju zahteval uvedbo kazenske preiskave proti pritožniku.

13. V svoji obrambi pred preiskovalnim sodnikom je pritožnik navedel, *inter alia,* da ni poznal vsebine zadevnih datotek. Trdil je tudi, da je ponudnik

internetnih storitev nezakonito, brez sodnega naloga, policiji predal njegove podatke, vključno z njegovim naslovom.

14. Dne 5. marca 2008 je preiskovalni sodnik Okrožnega sodišča v Kranju zoper pritožnika uvedel sodno preiskavo zaradi utemeljenega suma storitve kaznivega dejanja prikazovanja, izdelave, posesti in razširjanja pornografskega gradiva na podlagi tretjega odstavka 187. člena Kazenskega zakonika. Sodnik je med drugim ugotovil, da je bil imetnik prepoznanega IP-naslova pritožnikov oče in da se je pritožnik prijavljal v zadevni program z imenom "Benet".

15. Dne 17. marca 2008 je pritožnikov zagovornik vložil pritožbo proti sklepu o uvedbi sodne preiskave. Trdil je, *inter alia*, da so bili dokazi v zvezi z identiteto uporabnika zadevnega IP-naslova pridobljeni nezakonito. Te informacije so bile v zvezi s podatki o prometu in zato ne bi smele biti pridobljene brez sodnega naloga.

16. Dne 21. marca 2008 je izvenobravnavni senat pritožbo zavrnil z ugotovitvijo, da čeprav je zagovornik navajal, da je bila identiteta uporabnika IP-naslova pridobljen nezakonito, pa ni zahteval izločitve določenih dokumentov iz spisa.

B. Sojenje

17. Dne 29. maja 2008 je Okrožno državno tožilstvo v Kranju vložilo obtožnico proti pritožniku zaradi zgoraj navedenega kaznivega dejanja.

18. Na obravnavi 8. oktobra 2008 je pritožnikov zagovornik vložil pisno vlogo z zahtevo za izločitev nezakonito pridobljenih dokazov, vključno z informacijami o uporabniku zadevnega IP-naslova, pridobljenimi brez odredbe sodišča.

19. Dne 5. decembra 2008 je sodišče zavrnilo pritožnikovo zahtevo, ker je menilo, da so bili podatki o uporabniku zadevnega IP-naslova pridobljeni v skladu s tretjim odstavkom 149. b. člena ZKP.

20. Dne 5. decembra 2008 je Okrožno sodišče v Kranju spoznalo pritožnika za krivega storitve kaznivega dejanja, za katerega je bil obtožen. Na podlagi mnenja izvedenca računalniške stroke je sodišče odločilo, da je moral biti pritožnik seznanjen z vsebino 630 pornografskih fotografij in 199 videoposnetkov mladoletnih, ki jih je na svoj računalnik prenesel prek omrežja p2p in omogočil njihovo delitev z drugimi uporabniki. Pritožnik je bil obsojen na pogojno zaporno kazen osem mesecev s preizkusno dobo dveh let.

C. Postopek pred Višjim sodiščem v Ljubljani

21. Proti sodbi sodišča prve stopnje sta se pritožila tako državni tožilec kot tudi pritožnik. Pritožnik je izpodbijal dejstva, kot jih je ugotovilo okrožno sodišče. Trdil je tudi, da bi morali biti podatki o naročniku, ki jih je slovenska

policija pridobila brez odredbe sodišča in torej nezakonito, kot dokazi izločeni. Posledično bi morali biti izločeni vsi dokazi, ki so bili pridobljeni na podlagi teh nezakonito pridobljenih podatkov.

22. Dne 4. novembra 2009 je Višje sodišče v Ljubljani deloma ugodilo pritožbi okrožnega državnega tožilca, in sicer tako, da je pogojno kazen spremenilo v šestmesečno zaporno kazen. Pritožnikova pritožba je bila zavrnjena kot neutemeljena. Višje sodišče je presodilo, da je prvostopenjsko sodišče pravilno ugotovilo dejstva o zadevi, pa tudi, da so bili podatki o uporabniku IP-naslova pridobljeni zakonito, saj za tak namen ni bila potrebna odredba sodišča.

D. Postopek pred vrhovnim sodiščem

23. Pritožnik je vložil zahtevo za varstvo zakonitosti pred vrhovnim sodiščem, v kateri je ponovno poudaril, da dinamičnega IP-naslova ni mogoče primerjati s telefonsko številko, ki ni vpisana v telefonski imenik, saj je ob vsaki prijavi uporabnika računalniku dodeljen nov IP-naslov. Zato je treba te podatke šteti za podatke o prometu, ki so okoliščine in dejstva, povezana z elektronsko komunikacijo, in ki spadajo v področje varstva zasebnosti komunikacije. Pritožnik je trdil, da švicarska policija ne bi smela pridobiti zadevnega podatka o dinamičnem IP-naslovu brez odredbe sodišča, prav tako brez nje slovenska policija ne bi smela dobiti podatka o identiteti naročnika, povezanega z IP-naslovom.

24. Dne 20. januarja 2011 je Vrhovno sodišče RS zavrnilo pritožnikov predlog za revizijo z obrazložitvijo, da je glede na splošno dostopnost spletnih strani in dejstvo, da je švicarska policija lahko preverjala izmenjavo v omrežju p2p le z opazovanjem uporabnikov, ki so si izmenjevali določene vsebine, tj. brez kakršnega koli posebnega poseganja v internetni promet, zadevna komunikacija ne more veljati za zasebno in zato zaščiteno po 37. členu Ustave RS. Poleg tega je bilo stališče vrhovnega sodišča tudi, da slovenska policija ni pridobila podatkov o prometu v zvezi s pritožnikovim elektronskim komuniciranjem, temveč samo podatke o uporabniku določenega računalnika, prek katerega se je dostopalo na internet.

E. Postopek pred ustavnim sodiščem

25. Pritožnik je vložil ustavno pritožbo pred ustavim sodiščem, ponavljajoč pritožbe, ki jih je prej predložil na nižjih sodiščih.

26. Ustavno sodišče je za mnenje v tej zadevi zaprosilo informacijsko pooblaščenko. Informacijska pooblaščenka je bila mnenja, da je bil razlog za pridobitev identitete posameznega uporabnika elektronske komunikacije prav to, da je komuniciral prek bolj ali manj javno dostopnih spletnih strani. Informacijska pooblaščenka je menila, da ni mogoče ločiti podatkov o prometu od podatkov o naročniku, saj podatki o prometu sami po sebi nič ne

pomenijo, če se ne ugotovi, kdo je oseba za temi podatki, ta zadnja informacija pa velja za izredno pomemben del komunikacijske zasebnosti. Informacijska pooblaščenka je poudarila, da so določbe takrat veljavnega Zakona o elektronskih komunikacijah zahtevale odredbo sodišča za pridobitev vseh podatkov v zvezi z elektronskimi komunikacijami ne glede na to, ali so se nanašali na podatke o prometu ali na identifikacijske podatke. Določba tretjega odstavka 149. b člena ZKP, ki je zahtevala samo pisno zahtevo policije za pridobitev podatkov o tem, kdo komunicira, se je informacijski pooblaščenki zdela problematična z vidika ustavnosti.

27. Dne 13. februarja 2014 je ustavno sodišče zavrnilo pritožnikovo pritožbo z obrazložitvijo, da njegove ustavne pravice niso bile kršene. Odločba ustavnega sodišča je bila sprejeta s sedmimi glasovi proti dvema. Sodnici J. Sovdat in D. Jadek Pensa sta napisali odklonilni ločeni mnenji. Odločba je bila vročena pritožniku 11. marca 2014.

1. Odločba ustavnega sodišča

28. Ustavno sodišče je v izhodišču poudarilo, da je poleg vsebine komunikacij 37. člen Ustave RS varuje tudi podatke o prometu, to je vse podatke, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju. Menilo je, da IP-naslovi spadajo med podatke o prometu. Vendar je ustavno sodišče sklenilo, da se je pritožnik, ki na noben način ni skrival IP-naslova, prek katerega je dostopal do interneta, zavestno javno izpostavljal in ni mogel upravičeno pričakovati zasebnosti. Posledično podatki v zvezi z identiteto uporabnika IP-naslova niso bili zaščiteni kot komunikacijska zasebnost v skladu s 37. členom ustave, temveč samo kot informacijska zasebnost v skladu z 38. členom ustave, zato v pritožnikovem primeru ni bila potrebna odredba sodišča za njihovo razkritje.

29. Najpomembnejši deli odločbe ustavnega sodišča so naslednji (kot je prevedeno v angleščino na spletni strani ustavnega sodišča):

> **"Presoja očitkov, ki se nanašajo na pridobitev IP-naslova pritožnika s strani švicarske policije**
>
> 11. Ustava v drugem odstavku 37. člena zagotavlja višjo raven varstva kot 8. člen Konvencije o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju EKČP), saj za vsak poseg v pravico do komunikacijske zasebnosti zahteva odredbo sodišča ... Pravica do komunikacijske zasebnosti iz prvega odstavka 37. člena Ustave v prvi vrsti varuje vsebino posredovanega sporočila. ... Poleg vsebine sporočila pa so varovani tudi okoliščine in dejstva, povezani s komunikacijo. V skladu s takšnim stališčem je ustavno sodišče z odločbo št. Up-106/05 z dne 2. oktobra 2008 (Uradni list RS, št. 100/08, in OdlUS XVII, 84) varstvo 37. člena Ustave razširilo tudi na tiste podatke o telefonskih klicih, ki po svoji naravi pomenijo sestavni del komunikacije, kar pomeni, da tovrstnih podatkov ni mogoče pridobiti brez odredbe sodišča. Navedena odločitev se sicer nanaša na telefonsko komunikacijo, a je mogoče enak zaključek smiselno uporabiti tudi za druge vrste komuniciranja na daljavo. Ključni ustavnosodni test, po katerem ustavno sodišče presoja, ali določena komunikacija uživa varstvo iz 37. člena Ustave, je upravičeno pričakovanje zasebnosti.

12. Komunikacija prek interneta načeloma poteka v anonimni obliki, kar je ključno za svoboden razvoj osebnosti, za svobodo govora in izražanja idej ter posledično za razvoj svobodne in demokratične družbe. Komunikacijska zasebnost, varovana s strogimi pogoji iz drugega odstavka 37. člena Ustave, je torej zelo pomembna človekova pravica, ki zaradi tehnološkega napredka in s tem naraščajočih možnosti nadzora vse bolj pridobiva pomen. Zajema upravičeno pričakovanje posameznika, da ga država tudi pri njegovem sporazumevanju prek sodobnih komunikacijskih poti pusti pri miru in da se mu ni treba zagovarjati za to, kar naredi, reče, napiše ali misli. V primeru suma storitve kaznivega dejanja pa mora imeti policija možnost, da identificira posameznike, ki so sodelovali pri določeni komunikaciji, povezani z domnevnim kaznivim dejanjem, saj so storilci prav zaradi omenjene načelne anonimnosti na internetu težje izsledljivi. Pod kakšnimi pogoji sme policija opravljati preiskovalna dejanja in ali zanje potrebuje odredbo sodišča, pa je odvisno od tega, ali gre za poseg v pravico do komunikacijske zasebnosti.

13. Kot je bilo že izpostavljeno, 37. člen Ustave poleg vsebine komunikacije varuje tudi podatke o prometu. Podatki o prometu so kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega obračunavanja. To pomeni, da je IP-naslov prometni podatek. Ustavno sodišče mora zato odgovoriti na vprašanje, ali je pritožnik na njem upravičeno pričakoval zasebnost.

14. Pri presoji o tem je treba tehtati dva elementa: pričakovanje zasebnosti na IP-naslovu ter upravičenost tega pričakovanja, pri čemer mora biti slednje takšno, da ga je družba pripravljena sprejeti kot upravičeno. Pritožnik je v tej zadevi z drugimi uporabniki mreže Razorback komuniciral tako, da so si s pomočjo programa E-mule medsebojno izmenjavali različne datoteke, med njimi tudi takšne, ki so vsebovale otroško pornografijo. Glede na splošno anonimnost uporabnikov interneta in tudi glede na vsebino datotek ustavno sodišče ne dvomi, da je pritožnik pričakoval, da bo njegova komunikacija ostala zasebna, gotovo pa je pričakoval tudi, da ne bo razkrita njegova identiteta. Vprašati se je torej treba, ali je bilo takšno pričakovanje zasebnosti upravičeno. Pritožnik ni izkazal, da bi bil IP-naslov, prek katerega je dostopal do interneta, kakorkoli prikrit, torej drugim uporabnikom neviden, oziroma da bi bil dostop do omrežja Razorback (in s tem do vsebine datotek) na kakršenkoli način omejen, npr. z gesli ali drugimi orodji. ... Nasprotno pa je v pritožnikovem primeru do spornih datotek lahko dostopal kdorkoli, ki je bil zainteresiran za njihovo izmenjavo, pritožnik pa ni izkazal, da bi bil njegov IP-naslov kakorkoli prikrit oziroma nedostopen za druge uporabnike te mreže. To vodi v zaključek, da je šlo za odprto komunikacijo z vnaprej nedoločenim krogom neznancev, ki po vsem svetu uporabljajo internet in ki so pokazali interes za izmenjavo določenih datotek, hkrati pa uporabnikom te mreže dostop do IP-naslovov drugih uporabnikov ni bil omejen. Zato po presoji ustavnega sodišča pritožnikovo pričakovanje zasebnosti ni bilo upravičeno; kar namreč oseba zavestno izpostavi javnosti, pa čeprav z domačega računalnika in iz zavetja svojega doma, ne more biti predmet varstva 37. člena Ustave. Glede na navedeno izpodbijano stališče Vrhovnega sodišča ne vzbuja ustavnopravnih pomislekov. Pridobitev podatka o pritožnikovem dinamičnem IP-naslovu ob upoštevanju vseh okoliščin konkretnega primera namreč ne pomeni posega v njegovo pravico do komunikacijske zasebnosti iz prvega odstavka 37. člena Ustave in zato odredba sodišča za njegovo pridobitev ni bila potrebna. Pritožnik se je namreč s svojim ravnanjem sam odpovedal svoji zasebnosti in zato glede nje ni mogel imeti upravičenega pričakovanja zasebnosti.

...

Presoja očitkov, ki se nanašajo na pridobitev podatka o uporabniku določenega IP-naslova

16. Pritožnik nasprotuje tudi stališču Vrhovnega sodišča, da policija z zaprosilom na podlagi tretjega odstavka 149.b člena ZKP od operaterja ni pridobivala podatkov o prometu, temveč izključno podatke o konkretnem uporabniku določenega komunikacijskega sredstva.

17. V obravnavani zadevi je policija na podlagi tretjega odstavka 149.b člena ZKP[20] dne 7. 6. 2006 na operaterja naslovila zaprosilo za posredovanje podatkov o uporabniku, ki mu je bil dne 20. februarja 2006 ob 13.28 uri dodeljen IP-naslov 195.210.223.200. Kot odgovor je prejela podatke o uporabnikovem imenu, priimku ter naslovu, čas komunikacije, določen na sekundo natančno, pa je bil že znan. Policija je nato na podlagi prvega odstavka 149.b člena ZKP dne 14. decembra 2006 pridobila odredbo preiskovalnega sodnika, na njeni podlagi pa je operater posredoval še prometne podatke. Glavno vprašanje, na katero mora v tem delu odločbe odgovoriti ustavno sodišče, torej je, ali pridobitev podatkov o identiteti uporabnika določenega IP-naslova sodi v domet komunikacijske zasebnosti.

18. V skladu s stališčem ustavnega sodišča iz odločbe št. Up-106/05, 37. člen Ustave varuje tudi prometne podatke, torej podatke o tem, npr. kdo, kdaj, s kom in kako pogosto je komuniciral. Identiteta komunicirajočega posameznika je torej eden od pomembnih vidikov komunikacijske zasebnosti, zato je treba za njeno razkritje pridobiti odredbo sodišča v skladu z drugim odstavkom 37. člena Ustave. Kljub takšnemu stališču pa po presoji ustavnega sodišča očitki pritožnika o kršitvi 37. člena Ustave v obravnavani zadevi niso utemeljeni. Pritožnik se je namreč s svojim ravnanjem, ko je javno razkril tako svoj IP-naslov kot tudi vsebino svoje komunikacije, sam odrekel varovanju svoje zasebnosti in se zato v primeru razkritja identitete nanjo ne more več sklicevati. Ker se je s tem odrekel tudi upravičenemu pričakovanju zasebnosti, podatki o identiteti uporabnika IP-naslova niso več uživali varstva z vidika komunikacijske zasebnosti, temveč zgolj z vidika informacijske zasebnosti iz 38. člena Ustave. Tako policija s pridobitvijo podatkov o imenu, priimku in naslovu uporabnika dinamičnega IP-naslova, prek katerega je komuniciral pritožnik, ni posegla v njegovo komunikacijsko zasebnost in zato za razkritje identitete ni potrebovala odredbe sodišča. Glede na navedeno izpodbijano stališče Vrhovnega sodišča ni v neskladju s 37. členom Ustave, očitki pritožnika v tem delu pa niso utemeljeni."

2. Odklonilno ločeno mnenje sodnice J. Sovdat

30. Sodnica J. Sovdat je pozdravila odstopanje stališča ustavnega sodišča od stališča Vrhovnega sodišča, da zadevne informacije niso spadale med prometne podatke. Vendar bi po njenem mnenju policija, ki je želela pridobiti identifikacijo naročnika, morala zahtevati odredbo sodišča. Poudarila je, da je stališče ustavnega sodišča nakazovalo, da je varovanje zasebnosti prometnih podatkov vedno odvisno od varovanja vsebine komunikacije. Skladno s tem so bili prometni podatki določene komunikacije varovani, dokler je bila varovana vsebina te komunikacije. Posledično posameznik ne more biti deležen ločenega in neodvisnega varovanja prometnih podatkov. Sodnica Sovdat se ni strinjala s tem mnenjem ob poudarjanju, da se pritožnik ni pojavil v javnosti s svojim imenom, temveč samo prek številk dinamičnega IP-naslova.

31. Sodnica Sovdat se je strinjala z informacijsko pooblaščenko, da policije ni zanimalo lastništvo naprave, temveč "identiteta uporabnika, ki je komuniciral in ravno zato, ker je z nekom komuniciral". Podprla je stališče

informacijske pooblaščenke, da "sama vsebina komunikacije nima posebne vrednosti, če ne vemo, kdo je komuniciral s kom". Poudarila je tudi, da v skladu z 166. in 168. členom Zakona o elektronskih komunikacijah (v nadaljevanju "ZEKom-1", glej 39. odstavek spodaj) operater policiji ne sme posredovati podatkov, ki jih hrani, brez odredbe sodišča. V primerjavi s tretjim odstavkom 149.b člena ZKP je ZEKom-1 nedvomno kasnejši in je torej odločitev večine v nasprotju z že doseženo ravnjo varstva pravic.

3. Odklonilno ločeno mnenje sodnice D. Jadek Pensa

32. Sodnica D. Jadek Pensa je trdila, da so ustavna jamstva, določena v 37. členu ustave, namenjena krepitvi pričakovanja zasebnosti na tem področju in preprečevanju nesorazmernega poseganja in zlorabe moči izvršilne veje oblasti.

33. Glede pritožnikovega pričakovanja spletne anonimnosti je sodnica D. Jadek Pensa trdila, da nobena od javno razkritih informacij, ki jih je razkril pritožnik, ni razkrila njegove identitete. Po njenem mnenju je anonimnost preprečila policiji, da bi določeno komunikacijo povezala z določeno osebo – tj., da bi povezala dinamični IP-naslov in posameznika z njegovim imenom in naslovom. Nadalje je trdila, da bi bilo treba vprašanje, ali bi način pritožnikovega komuniciranja lahko pripeljal do sklepa, da njegova pričakovanja zasebnosti niso bila objektivno upravičena, obravnavati ob upoštevanju vseh okoliščin, vključno s takrat veljavnim zakonom. Pojasnila je, da je bila v ZEKom (2. točka prvega odstavka 103. člena, prvi odstavek 104. člena in 107. člen ZEKom – glej 37odstavek spodaj) operaterjem naložena dolžnost izbrisa podatkov o prometu takoj, ko niso bili več potrebni za posredovanje sporočil. Poleg tega je 107. člen ZEKom določal, da se je v nedotakljivost zaupnosti komunikacij smelo posegati samo na podlagi odredbe pristojnega organa. Dopis s policije ponudniku internetnih storitev ni mogel veljati za takšno odredbo. Torej tudi če bi tretji odstavek 149. b člena ZKP lahko razlagali, da omogoča policiji, da zahteva informacije o naročniku interneta, se za področje, ki ga je urejal ZEKom, ne bi smel uporabiti, saj je ZEKom izrecno določal, da ureja "zaščito tajnosti in zaupnosti elektronskih komunikacij." Sicer bi bil pravni red dvoličen. Sodnica je sklenila, da veljavni pravni okvir torej ni mogel pripeljati do sklepa, da pritožnik kot razumno in zadostno obveščen posameznik, ne bi bil mogel pričakovati zasebnosti; tj. da ne bi bil mogel pričakovati varstva njegove anonimnosti.

34. Sodnica Jadek Pensa je nadaljevala z obrazložitvijo nevtralnosti podatkov o prometu, kot je podatek o uporabniku določenega dinamičnega IP-naslova:

> "9. Prometni podatek – dinamični IP-naslov, ki je bil v določenem trenutku naključno dodeljen – kot razumem, razkriva način uporabe interneta na nekem računalniku, ker je neločljivo navezan na specifično povezavo. ... To pa zato, ker šele oba podatka skupaj sporočata o načinu uporabe interneta v neanonimizirani obliki, to je o načinu uporabe

interneta v povezavi z identificirano osebo. Ta bistvena okoliščina po mojem mnenju negira pojmovanje o nevtralnosti podatka o konkretnem uporabniku storitev za določen (znan) dinamični IP-naslov, ki ga je policija iskala pri operaterju. Namreč, nevtralnosti podatka v smislu zanikanja njegove sposobnosti, da ne sporoča čisto nič več kot le ime in priimek ter naslov neke osebe (ki ima z operaterjem sklenjeno naročniško razmerje). Ravno zato, ker je ta podatek neločljivo navezan na prav določeno komunikacijo, se prometni podatek pripisuje k polju varstva komunikacijske zasebnosti.

10. Četudi je operater policiji sporočil "le" podatke, ki identificirajo določeno osebo, s katero ima sklenjeno naročniško razmerje, ji je s tem, kot razumem, v resnici sporočil (poenostavljeno) podatke o prometu v elektronskem komunikacijskem omrežju za to osebo. Tudi policija je, kot sem že obrazložila, hotela izvedeti več kot le ime in priimek nekega sklenitelja pogodbe. Ker je, kot razumem, poizvedovala po prometnem podatku, ki se povezuje z določeno osebo, bi bila morala postopati skladno prvemu odstavku 149.b člena ZKP in pridobiti odredbo preiskovalnega sodnika."

II. UPOŠTEVANI DOMAČA ZAKONODAJA IN PRAKSA

A. Ustava

35. 37. in 38. člen ustave zagotavljata varstvo tajnosti pisem in drugih občil ter osebnih podatkov, in sicer:

37. člen

"Zagotovljena je tajnost pisem in drugih občil.

Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države."

38. člen

"Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi."

B. Zakon o kazenskem postopku

36. 149. b člen Zakona o kazenskem postopku (Uradni list RS, št. 8/06) je v poglavju o urejanju ukrepov, ki jih sprejme policija v predkazenskih postopkih, določal:

"(1) Če so podani razlogi za sum, da je bilo storjeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o prometu v elektronskem komunikacijskem omrežju, lahko preiskovalni sodnik na obrazložen

predlog državnega tožilca odredi operaterju elektronskega komunikacijskega omrežja, da mu sporoči 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.

(2) Predlog in odredba morata biti pisna in morata vsebovati podatke, ki omogočajo identifikacijo komunikacijskega sredstva za elektronski komunikacijski promet, utemeljitev razlogov, časovno obdobje, za katerega se podatki zahtevajo, ter ostale pomembne okoliščine, ki narekujejo uporabo ukrepa.

(3) Če so podani razlogi za sum, da je bilo storjeno, oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o lastniku ali uporabniku določenega komunikacijskega sredstva za elektronski komunikacijski promet, ki niso objavljeni v naročniških imenikih in o času, v katerem je tako sredstvo bilo oziroma je v uporabi, lahko policija od operaterja elektronskega komunikacijskega omrežja zahteva, da ji na njeno pisno zahtevo, tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči te podatke.

(4) Operater elektronskih komunikacijskih omrežij svoji stranki ali tretji osebi ne sme razkriti, da je ali da bo določene podatke posredoval preiskovalnemu sodniku (prvi odstavek tega člena) ali policiji (prejšnji odstavek)."

C. Zakon o elektronskih komunikacijah

37. V času pridobivanja spornih podatkov (to je avgusta 2006) je veljal Zakon o elektronskih komunikacijah (ZEKom) (Uradni list RS, št. 43/04 in 86/04, v nadaljevanju ZEKom). Ta zakon je med drugim prenos Direktive 2002/58/ES (glej 56 spodaj). Pomembne so bile naslednje določbe:

1. člen

Vsebina zakona

"Ta zakon ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev ... določa pravice uporabnikov ... ureja varovanje tajnosti in zaupnosti elektronskih komunikacij ter ureja druga vprašanja, povezana z elektronskimi komunikacijami."

3. člen

Uporabljeni izrazi

"Izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:

...

25. Podatki o prometu so kateri koli podatki, obdelani za namen prenosa komunikacije po elektronskem komunikacijskem omrežju ali zaradi njegovega zaračunavanja.

..."

103. člen

Zaupnost komunikacij

"(1) Zaupnost komunikacij se nanaša na:

1. vsebino komunikacij;

2. podatke o prometu in lokacijske podatke, povezane s komunikacijo iz prejšnje točke tega odstavka;

3. dejstva in okoliščine v zvezi s prekinitvijo povezave ali s tem, da povezava ni bila vzpostavljena.

(2) Operater in vsakdo, ki sodeluje pri zagotavljanju in izvajanju njegove dejavnosti, je dolžan varovati zaupnost komunikacij tudi po prenehanju opravljanja dejavnosti, pri kateri jo je bil dolžan varovati.

(3) Zavezanci iz prejšnjega odstavka smejo pridobiti informacije o komunikacijah iz prvega odstavka tega člena le v obsegu, ki je nujno potreben za izvajanje določenih javnih komunikacijskih storitev, in smejo te informacije uporabljati ali posredovati drugim le zaradi izvajanja teh storitev.

(4) Če morajo operaterji v skladu s prejšnjim odstavkom pridobiti informacije o vsebini komunikacij, posneti ali shraniti komunikacije in z njimi povezane podatke o prometu iz pododstavka (3) zgoraj, morajo o tem ob sklenitvi naročniške pogodbe oziroma ob začetku izvajanja javne komunikacijske storitve seznaniti uporabnika, informacije o vsebini komunikacije oziroma komunikacijo pa zbrisati takoj, ko je to tehnično izvedljivo in ko to ni več potrebno za izvedbo določene javne komunikacijske storitve.

(5) Vse oblike nadzora oziroma prestrezanja, kot so poslušanje, prisluškovanje, snemanje, shranjevanje in posredovanje komunikacij iz prvega odstavka tega člena so prepovedane, razen če je to dovoljeno v skladu s prejšnjim odstavkom ali v skladu s 107. členom tega zakona oziroma, če je takšna oblika nadzora oziroma prestrezanja nujno potrebna za prenos sporočil (npr. faksimilna sporočila, elektronska pošta, elektronski predali, glasovna pošta, storitev SMS).

..."

104. člen

Podatki o prometu

"(1) Podatki o prometu, ki se nanašajo na naročnike in uporabnike ter jih je operater obdelal in shranil, morajo biti izbrisani ali spremenjeni tako, da se ne dajo povezati z določeno ali določljivo osebo, takoj ko niso več potrebni za prenos sporočil.

(2) Ne glede na določbo prejšnjega odstavka lahko operater do popolnega plačila storitve, vendar najdlje do preteka zastaralnega roka, hrani in obdeluje podatke o prometu, ki jih potrebuje za obračun in za plačila v zvezi z medomrežnim povezovanjem.

(3) Izvajalec javne komunikacijske storitve lahko zaradi trženja elektronskih komunikacijskih storitev ali izvajanja storitev z dodano vrednostjo obdeluje podatke iz prvega odstavka tega člena v obsegu in trajanju, potrebnem za takšno trženje ali storitve, samo na podlagi predhodnega soglasja naročnika ali uporabnika, na katerega se ti podatki nanašajo. Naročniki oziroma uporabniki morajo biti pri tem predhodno obveščeni o vrstah podatkov o prometu, ki se obdelujejo, in trajanju takšne obdelave pred pridobitvijo soglasja. Uporabnik ali naročnik ima pravico, da kadar koli prekliče to soglasje.

(4) Izvajalec storitve mora za namene iz drugega odstavka tega člena v splošnih pogojih določiti, katere prometne podatke se bo hranilo, obdelovalo in koliko časa, ter izjaviti, da se bo z njimi ravnalo v skladu z zakonom, ki ureja varstvo osebnih podatkov.

(5) Podatke o prometu smejo v skladu s prejšnjimi odstavki tega člena obdelovati le osebe, ki pod nadzorstvom operaterja skrbijo za zaračunavanje ali upravljanje prometa, odgovarjajo na vprašanja porabnikov, odkrivajo prevare, tržijo elektronske komunikacijske storitve ali zagotavljajo storitve z dodano vrednostjo, pri čemer mora biti ta obdelava omejena na to, kar je potrebno za namene takšnih dejavnosti.

Ne glede na določbe prvega, drugega, tretjega in petega odstavka tega člena operater na pisno zahtevo pristojnega organa, ki jo ta poda z namenom reševanja sporov, zlasti sporov v zvezi z medsebojnim povezovanjem ali zaračunavanjem, in v skladu z veljavno zakonodajo, tega seznani s podatki o prometu."

107. člen

Zakonito prestrezanje komunikacij

"... (2) Operater je dolžan omogočiti zakonito prestrezanje komunikacij na določeni točki javnega komunikacijskega omrežja takoj, ko prejme prepis tistega dela izreka odredbe pristojnega organa, v katerem je navedba točke ... na kateri naj se izvaja zakonito prestrezanje komunikacij, ter drugi podatki, povezani z načinom, obsegom in trajanjem tega ukrepa."

38. Nadaljnje spremembe ZEKom, in sicer ZEKom-A, ki so začele veljati 28. novembra 2006, to je potem, ko so bili že sprejeti izpodbijani ukrepi v obravnavani zadevi (Uradni list RS, št. 129/06) so urejale hranjenje prometnih podatkov za namene, *inter alia*, kazenskih postopkov. To je vključevalo podatke, potrebne za identifikacijo vira komunikacije, kot sta ime in naslov naročnika, ki mu je bil dodeljen IP-naslov, podatke potrebne za identifikacijo namembnega naslova komunikacij ter podatke, potrebne za identifikacijo datuma, časa in trajanja komunikacij (107.a in 107.b člen). V tem pogledu ni bilo razlikovanj med statičnim in dinamičnim IP-naslovom. Nadalje je sprememba, ki jo je uvedel 107.č člen določala, da je operater dolžan omogočiti dostop do hranjenih podatkov ali jih posredovati takoj oz. najkasneje v treh dneh potem, ko prejme prepis "odredbe" "pristojnega organa". 107. e člen spremenjenega zakona je določal, da "sodišče, ki je odredilo dostop do podatkov, vodi zbirne podatke o odredbah o dostopu do podatkov in posredovanja hranjenih podatkov". Urejal je tudi postopek poročanja o dostopu do hranjenih podatkov – od sodišč do Ministrstva za pravosodje in potem od ministrstva do Evropske komisije.

39. Dne 20. decembra 2012 je bil sprejet novi Zakon o elektronskih komunikacijah (ZEKom–1) (Uradni list RS, št. 109/2012). Njegova 166. in 168. člen določata:

166. člen

Posredovanje hranjenih podatkov pristojnim organom

"(1) Operater mora takoj oziroma brez nepotrebnega odlašanja posredovati hranjene podatke od trenutka prejema prepisa tistega dela izreka odredbe pristojnega organa, v katerem je navedba vseh potrebnih podatkov o obsegu dostopa.

...

(4) Operater osebam, ki jih odredba iz prvega odstavka tega člena zadeva, ali tretjim osebam ne sme razkriti te odredbe in da je ali da bo hranjene podatke na podlagi tega člena posredoval pristojnemu organu.

...

(7) Informacijski pooblaščenec nadzira izpolnitev obveznosti operaterjev iz tega člena, kar ne posega v pristojnosti nadzora s strani pristojnih organov na podlagi drugih zakonov."

168. člen

Podatki o odredbah o dostopu do podatkov in posredovanja podatkov

"(1) Sodišče, ki je odredilo dostop do podatkov, vodi zbirne podatke o odredbah o dostopu do podatkov in posredovanja podatkov, hranjenih na podlagi 166. člena tega zakona, ki obsegajo:

1. število zadev, v katerih je bil odrejen dostop do hranjenih podatkov,

2. navedbo dneva ali časovnega obdobja, za katero so bili podatki zahtevani, dneva, ko je pristojni organ izdal odredbo o dostopu do podatkov in dneva posredovanja podatkov,

3. število zadev, v katerih odredbe za dostop do podatkov ni bilo mogoče izvršiti.

(2) Pristojno sodišče posreduje zbirne podatke iz prejšnjega odstavka za tekoče leto ministrstvu, pristojnemu za pravosodje, najkasneje do 31. januarja naslednje leto.

(3) Ministrstvo, pristojno za pravosodje, na podlagi prejetih zbirnih podatkov vseh sodišč najpozneje do 20. februarja vsako leto pripravi skupno poročilo o dostopu do hranjenih podatkov za preteklo leto in ga pošlje ministrstvu, ki jih takoj posreduje Evropski komisiji in komisiji državnega zbora, ki je pristojna za nadzor obveščevalnih in varnostnih služb.

(4) Minister, pristojen za pravosodje, po predhodnem mnenju predsednika Vrhovnega sodišča Republike Slovenije, izda navodilo z obrazci za poročanje po tem členu."

D. Zakon o varstvu osebnih podatkov

40. Ko je Slovenija postala članica Evropske unije, je Državni zbor Republike Slovenije na seji 15. julija 2004 sprejel Zakon o varstvu osebnih podatkov (Uradni list št. 86/04) na podlagi Direktive 95/46/ES (glej 53 spodaj). Zakon v zvezi s tem določa:

1. člen

Vsebina zakona

"S tem zakonom se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice (v nadaljnjem besedilu: posameznik) pri obdelavi osebnih podatkov."

6. člen

Pomen izrazov

"V tem zakonu uporabljeni izrazi imajo naslednji pomen:

1. Osebni podatek – je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

2. Posameznik – je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

...

18. Anonimiziranje – je takšna sprememba oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa.

19. Občutljivi osebni podatki – so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, ..."

41. 2. člen Zakona o varstvu osebnih podatkov je določal, da se osebni podatki obdelujejo zakonito in pošteno. 8. člen je določal, da se osebni podatki lahko obdelujejo le, če to določa zakon ali na podlagi osebne privolitve zadevnega posameznika. V skladu z 12. členom so se osebni podatki lahko obdelovali brez druge zakonite pravne podlage, če je bilo to nujno potrebno za varovanje življenja ali telesa posameznika.

42. Zakon o varstvu osebnih podatkov je tudi določal, da se podatki lahko zbirajo samo za določene in zakonite namene in se jih v skladu s tem lahko obdeluje (16. člen) ter samo, če je to potrebno za dosego tega namena (21. člen). Potem jih je treba zbrisati, uničiti, blokirati ali anonimizirati (prav tam). Zakon je tudi določal ukrepe in postopke, ki jih morajo sprejeti izvajalci in pogodbeni obdelovalci za varovanje osebnih podatkov in preprečenje nenamernega ali namernega nepooblaščenega uničenja podatkov, njihove spremembe, izgube ali nepooblaščene obdelave (24. in 25. člen).

E. Kazenski zakonik

43. 187. člen Kazenskega zakonika, ki je tedaj veljal, je prepovedoval prikazovanje pornografskih vsebin osebam, mlajšim od štirinajst let, ter izdelavo in razširjanje pornografskega gradiva, ki prikazuje mladoletne osebe. Zadevna določba se glasi:

"...

(2) Kdor zlorabi mladoletno osebo za izdelavo slik, avdiovizualnih ali drugih predmetov pornografske vsebine, ali jo uporabi za pornografsko predstavo, se kaznuje za zaporom od šestih mesecev do petih let.

(3) Enako se kaznuje kdor proizvede, razširi, proda, uvozi, izvozi ali drugače ponudi pornografsko gradivo, ki prikazuje mladoletne osebe, ali kdor poseduje tako gradivo z namenom proizvodnje, razširjanja, prodaje, uvoza, izvoza ali drugačnega ponujanja.

..."

F. Odločba ustavnega sodišča št. Up-106/05 z dne 2. oktobra 2008

44. Zadeva št. Up-106/05 je obravnavala pritožnika, ki je bil obsojen zaradi neupravičene proizvodnje prepovedanih drog in prometa z njimi na podlagi podatkov (seznama telefonskih številk in besedilnih sporočil), pridobljenih z njegove kartice SIM brez odredbe sodišča. Pritožnik se je pritožil, da je njegova obsodba temeljila na nezakonito pridobljenih dokazih, saj je policija brez odredbe sodišča spremljala njegovo komunikacijo po mobilnem telefonu. Ustavno sodišče je ugodilo pritožbi in odpravilo sodbe nižjih sodišč.

45. Ustavno sodišče je ugotovilo, da ne samo, da je bila varovana vsebina komunikacij, temveč so bile varovane tudi okoliščine in dejstva, povezana s komunikacijo, vključno s podatki, shranjenimi v spominu telefona, ki so bili sestavni del komunikacijske zasebnosti. Zato sta pomenila pridobitev podatkov o zadnjih opravljenih in neodgovorjenih klicih ter vpogled v vsebino sporočila SMS vpogled v vsebino in okoliščine komunikacije ter s tem poseg v pravico iz prvega odstavka 37. člena ustave. Sodišče je poudarilo, da je v skladu z drugim odstavkom 37. člena ustave tak poseg dopusten, če so izpolnjeni naslednji pogoji: (1) je poseg določen v zakonu, (2) poseg z odločbo dovoli sodišče, (3) je določno omejen čas izvajanja posega in (4) je poseg nujen za uvedbo ali potek kazenskega postopka ali varnost države.

III. UPOŠTEVANO MEDNARODNO PRAVO

A. Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov

46. Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (ki je bila na voljo za podpis od 28. januarja 1981, ETS št. 108, v nadaljnjem besedilu: konvencija) so ratificirale vse članice Sveta Evrope in je za Slovenijo začela veljati 1. septembra 1994. 1. člen določa predmet in namen te konvencije, ki "je zagotoviti na ozemlju vsake pogodbenice vsakemu posamezniku ne glede na državljanstvo in prebivališče spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj (‘zaščita podatkov‘)." Konvencija iz leta 1981 med drugim ščiti posameznika pred zlorabo in velja za vso obdelavo podatkov v javnem in zasebnem sektorju, kot je na primer obdelava

podatkov, ki jo izvajajo organi sodstva in kazenskega pregona. V 2. členu so "osebni podatki" katera koli informacija, ki se nanaša na določenega ali določljivega posameznika. 5. člen zahteva, da so osebni podatki, ki se avtomatsko obdelujejo, pridobljeni in obdelani pošteno in zakonito.

B. Konvencija o kibernetski kriminaliteti

47. Konvencijo o kibernetski kriminaliteti (ki je bila na voljo za podpis od 23. novembra 2001 in je začela veljati 1. julija 2004, ETS št. 185, v nadaljnjem besedilu: Konvencija o kibernetski kriminaliteti) je za Slovenijo začela veljati 1. januarja 2005.

48. Konvencija o kibernetski kriminaliteti je prva mednarodna pogodba o kaznivih dejanjih, storjenih prek interneta, in je na voljo za pristop vsem državam. Od držav med drugim zahteva, da kot kaznivo dejanje opredelijo otroško pornografijo.

49. Za namene Konvencije o kibernetski kriminaliteti 1. člen določa, da so "podatki o prometu" "vsi računalniški podatki o komuniciranju s pomočjo računalniškega sistema, ustvarjeni z računalniškim sistemom, ki je bil del komunikacijske verige, in nakazujejo izvor, cilj, pot, čas, datum, obseg, trajanje ali vrsto take storitve." Njeno razlagalno poročilo dalje, v ustreznem delu, določa (30. odstavek), kot se glasi:

> "'Izvor' se nanaša na telefonsko številko, naslov internetnega protokola (IP), ali podobno identifikacijo komunikacijske naprave, ki ji operater nudi storitve. 'Cilj' se nanaša na primerljivo navedbo komunikacijskih naprav, ki so jim komunikacije posredovane. Izraz 'vrsta povezanih storitev' se nanaša na vrsto storitev, ki se uporabljajo znotraj omrežja, tj. prenos datotek, elektronska pošta ali neposredno sporočanje."

50. V skladu s Konvencijo o kibernetski kriminaliteti so organom oblasti za boj proti v njej naštetim kaznivim dejanjem na voljo:

> **18. člen – Odredba za predložitev podatkov**
>
> "1. Pogodbenica sprejme potrebne zakonodajne in druge ukrepe, s katerimi pristojne organe pooblasti:
>
> ...
>
> b) zahtevati od ponudnika storitev na njenem ozemlju, da predloži podatke o naročnikih v zvezi s storitvami, ki jih ta ponudnik storitev poseduje ali upravlja.
>
> 2. Pooblastila in postopki iz tega člena se uporabljajo v skladu z določbami iz 14. in 15. člena.
>
> 3. V tem členu izraz 'podatki o naročniku' pomeni vse podatke v obliki računalniških podatkov ali kateri koli drugi obliki, v kateri jih hrani ponudnik storitev in ki se nanašajo na naročnike njegovih storitev in jih ni mogoče šteti za podatke o prometu ali vsebinske podatke in iz katerih je mogoče ugotoviti:
>
> a) vrsto uporabljene komunikacijske storitve, v ta namen uporabljene tehnične rešitve in trajanje storitve;

b) identiteto naročnika, poštni ali geografski naslov, telefonsko ali drugo številko za dostop, podatke o zaračunavanju in plačevanju, ki so na razpolago na podlagi pogodbe ali sporazuma o opravljanju storitev;

c) vsako drugo informacijo o kraju namestitve komunikacijske opreme, ki je na razpolago na podlagi pogodbe ali sporazuma o opravljanju storitev."

20. člen – Zbiranje podatkov o prometu v dejanskem času

"1. Pogodbenica sprejme potrebne zakonodajne in druge ukrepe, s katerimi pristojne organe pooblasti, da:

a) s pomočjo uporabe tehničnih sredstev na njenem ozemlju zbirajo ali zapisujejo, in

b) zahtevajo od ponudnika storitev v okviru njegovih tehničnih zmožnosti:

i) s pomočjo uporabe tehničnih sredstev na njenem ozemlju zbirajo ali zapisujejo, ali

ii) sodelovanje in pomoč pristojnim organom pri zbiranju ali zapisovanju

podatkov o prometu v dejanskem času, povezanih z določenimi komunikacijami, posredovanimi z računalniškim sistemom na njenem ozemlju.

...

4. Pooblastila in postopki iz tega člena se uporabljajo v skladu z določbami iz 14. in 15. člena."

21. člen – Prestrezanje vsebinskih podatkov

"1.Pogodbenica sprejme potrebne zakonodajne in druge ukrepe, sorazmerne z obsegom resnih kaznivih dejanj, kot jih bo opredelilo notranje pravo, s katerimi pristojne organe pooblasti, da:

a) s pomočjo uporabe tehničnih sredstev na njenem ozemlju zbirajo ali zapisujejo, in

b) zahtevajo od ponudnika storitev v okviru njegovih tehničnih zmožnosti:

i) zbiranje ali zapisovanje s pomočjo tehničnih sredstev na njenem ozemlju ali

ii) sodelovanje in pomoč pristojnim organom pri zbiranju ali zapisovanju

vsebinskih podatkov določenih sporočil v dejanskem času, ki se prenašajo s pomočjo računalniškega sistema na njenem ozemlju.

...

4. Pooblastila in postopki iz tega člena se uporabljajo v skladu z določbami iz 14. in 15. člena."

51. V zvezi z odredbo za predložitev podatkov, Razlagalno poročilo h Konvenciji o kibernetski kriminaliteti (Budimpešta, 23. november 2001, ETS št. 185) navaja, da so med preiskavo kaznivega dejanja podatki o naročniku potrebni predvsem v dveh primerih. Prvič, za ugotovitev katere storitve in povezane tehnične ukrepe je uporabnik uporabljal ali jih uporablja, kot na primer vrsta uporabljene telefonske storitve, vrsta drugih povezanih storitev (na primer preusmeritev klicev, glasovna pošta) ali telefonska številka ali drug tehnični naslov (na primer e-poštni naslov). Drugič, če je tehnični naslov znan, so podatki o naročniku potrebni za pomoč pri ugotavljanju identitete zadevne osebe. V skladu z Razlagalnim poročilom odredba za predložitev

podatkov zagotavlja manj vsiljiv in manj invaziven ukrep, ki ga organi kazenskega pregona lahko uporabijo namesto ukrepov, kot sta prestrezanje vsebinskih podatkov in zbiranje podatkov o prometu v dejanskem času, ki morajo biti ali so lahko omejeni samo na težja kazniva dejanja.

52. Konvencija o kibernetski kriminaliteti zahteva, da zgoraj navedeni ukrepi, ki jih predpisujejo 18., 20. in 21. člen, upoštevajo pogoje, določene v 14. in 15. členu, ki se v ustreznem delu glasijo:

14. člen – Obseg procesnih določb

"1. Pogodbenice sprejmejo potrebne zakonodajne in druge ukrepe, s katerimi določijo pooblastila in postopke, namenjene izvajanju posebnih kazenskih postopkov ali odkrivanju kaznivih dejanj, opredeljenih v tem oddelku.

..."

15. člen – Pogoji in zaščitne določbe

"1. Pogodbenice zagotovijo, da se za vzpostavitev, uveljavitev in uporabo pooblastil in postopkov, predvidenih v tem oddelku, uporabljajo pogoji in zaščitne določbe v skladu z notranjim pravom, kar bo zagotovilo primerno varovanje človekovih pravic in temeljnih svoboščin, vključno s pravicami, ki izhajajo iz Konvencije Sveta Evrope o varstvu človekovih pravic in temeljnih svoboščin iz leta 1950, Mednarodnega pakta Združenih narodov o državljanskih in političnih pravicah iz leta 1966 in drugih mednarodnih dokumentov o varstvu človekovih pravic, ki vključujejo načelo sorazmernosti.

2. Ti pogoji in zaščitne določbe naj glede na vrsto postopka ali pooblastila, kadar je to primerno, *inter alia*, vsebujejo sodni ali drug neodvisen nadzor, razloge, ki utemeljujejo uporabo in omejitev obsega in trajanja takega pooblastila ali postopka."

IV. UPOŠTEVANO PRAVO EVROPSKE UNIJE

A. Direktiva 95/46/ES in Uredba (EU) 2016/679

53. Odstavek a prve točke 2. člena Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL 1995 L 281, str. 31, v nadaljevanju besedila: Direktiva o varstvu podatkov) določa, da "osebni podatek" pomeni "katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo ("posameznik, na katerega se nanašajo osebni podatki")". Poleg tega je v skladu z zgoraj navedeno določbo "določljiva oseba" tista "oseba, ki jo je mogoče posredno ali neposredno določiti, še zlasti s pomočjo identifikacijske številke ali enega ali več dejavnikov, značilnih za njeno fizično, fiziološko, mentalno, ekonomsko, kulturno ali socialno identiteto". Direktiva o varstvu podatkov ne velja za področje policije in kazenskega pravosodja.

54. Uvodna izjava 26 navaja, da je pri ugotavljanju, ali je posameznik določljiv, "treba upoštevati vsa sredstva, za katera se razumno pričakuje, da

se jih uporabi ... za identifikacijo navedenega posameznika"; načela varstva podatkov ne veljajo za podatke, ki so spremenjeni v anonimne tako, da posameznik, na katerega se osebni podatki nanašajo, ni več določljiv.

55. Uredba (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 2016 L 119/1, str. 1) je začela veljati 24. maja 2016. Ko bo začela učinkovati (25. maja 2018), bo nadomestila Direktivo o varstvu podatkov. Njen 4. člen določa, da je "določljivi posameznik" tisti "posameznik, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator ...". Uvodna izjava 26 nadalje navaja, da bi bilo pri ugotavljanju, ali se za ta sredstva lahko razumno pričakuje, da bodo uporabljena za identifikacijo posameznika, "treba upoštevati vse objektivne dejavnike, kot so stroški identifikacije in čas, potreben zanjo, ter pri tem upoštevati razpoložljivo tehnologijo in tehnološki razvoj v času obdelave." Nadalje razlaga, da "načel varstva podatkov zato ne bi smeli uporabljati za anonimizirane informacije, in sicer informacije, ki niso povezane z določenim ali določljivim posameznikom, ali osebne podatke, ki so bili anonimizirani na tak način, da posameznik, na katerega se nanašajo osebni podatki, ni ali ni več določljiv."

B. Direktiva 2002/58/ES

56. Poleg tega je bila posebej za področje elektronskih komunikacij 12. julija 2002 sprejeta Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L št. 201, str. 37). Ta ne velja za področje policije in kazenskega pravosodja, temveč usklajuje določbe držav članic, potrebne za zagotovitev enakovredne stopnje zaščite temeljnih pravic in svoboščin in zlasti pravice do zasebnosti v zvezi z obdelavo osebnih podatkov v sektorju elektronskih komunikacij. 2. člen določa opredelitev izraza "uporabnik", ki pomeni "vsako fizično osebo, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev". Nato opredeli izraz "podatki o prometu" kot "katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila". Poleg tega opredeli izraz "sporočilo (komunikacija)" kot "vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve".

C. Okvirni sklep Sveta Evropske unije 2008/977/PNZ in Direktiva (EU) 2016/680

57. Namen Okvirnega sklepa Sveta Evropske unije 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L št. 350, str. 60, v nadaljevanju besedila: Okvirni sklep o varstvu osebnih podatkov), je zagotavljanje varstva osebnih podatkov posameznikov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij. Okvirni sklep o varstvu osebnih podatkov večinoma temelji na načelih in opredelitvah iz konvencije iz leta 1981 in Direktive o varstvu podatkov.

58. Direktiva (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 2016 L 119, str. 89) ureja način ravnanja pristojnih organov, kot so policija in kazenski sodni organi, s podatki za namene, *inter alia*, preiskave in pregona kaznivih dejanj. Prva točka 3. člena vsebuje enako opredelitev izraza "določljivi posameznik" in uvodna izjava 21 enako razlago glede sredstev identifikacije kot Splošna uredba o varstvu podatkov (glej 55 zgoraj). Poleg tega 4. člen določa, da se osebni podatki obdelujejo, *inter alia,* zakonito in pošteno. Tretja točka 1. člena določa, da lahko države članice določijo višjo raven varnostnih ukrepov od tiste, ki jo določa direktiva.

59. Direktiva nadomešča Okvirni sklep 2008/977/PNZ, in sicer z začetkom veljavnosti 6. maja 2018.

D. Izbrane odločitve Sodišča Evropske unije

60. Glede koncepta "osebnih podatkov" v skladu z odstavkom a 2. člena Direktive o varstvu podatkov je Sodišče Evropske unije (SEU) v sodbi z dne 24. novembra 2011 v zadevi *Scarlet Extended,* C-70/10, EU:C:2011:771, 51. odstavek, ugotovilo da so IP-naslovi uporabnikov "varovani osebni podatki, ker omogočajo, da se ti uporabniki natančno določijo".

61. Sodišče Evropske unije je v sodbi z dne 19. oktobra 2016 v zadevi *Breyer,* C-582/14, EU:C:2016:779 obravnavalo posebne lastnosti dinamičnih IP-naslovov. Ugotovilo je naslednje:

> "[15] IP-naslovi so zaporedja številk, ki se dodelijo omrežno povezanim računalnikom za omogočanje njihove komunikacije z dostopom do interneta. Pri dostopu do spletnega mesta se IP-naslov kličočega računalnika posreduje strežniku, na katerem je to spletno mesto shranjeno. To je potrebno za zagotavljanje prenosa priklicanih podatkov do pravega prejemnika.

> [16] Poleg tega je iz predložitvene odločbe in spisa Sodišča razvidno, da ponudniki dostopa do interneta računalnikom internetnih uporabnikov dodelijo bodisi ‘statičen’ IP-naslov bodisi ‘dinamičen’ IP-naslov, torej naslov, ki se spreminja ob vsaki naknadni povezavi. Drugače kakor statični IP-naslovi dinamični IP-naslovi ne omogočajo povezave prek datotek, dostopnih javnosti, med danim računalnikom in fizičnim priključkom na omrežje, ki ga uporablja ponudnik dostopa do interneta."

62. Sodišče Evropske unije je bilo mnenja, da dinamični IP-naslov ni bil podatek v zvezi z "določenim posameznikom", saj tak naslov ni neposredno razkril identitete posameznika, ki je bil lastnik računalnika, s katerega se je dostopalo do spletnega mesta, ali druge osebe, ki je mogoče uporabljala ta računalnik (prav tam, 38. odstavek). Sodišče Evropske unije je v nadaljevanju odločalo, ali je lahko IP- naslov, ki ga je v tej zadevi zabeležil ponudnik storitev spletnih medijev, obravnavan kot podatek v zvezi z "določljivim posameznikom", smiselno po odstavku a 2. člena Direktive o varstvu podatkov. V ta namen je Sodišče Evropske unije, opirajoč se na uvodno izjavo 26, preučilo, ali je v obravnavani zadevi možnost ponudnika storitev spletnih medijev, da kombinira zadevni dinamični IP-naslov z dodatnimi podatki, ki jih ima, pomenila sredstva, za katera se pričakuje, da bodo uporabljena za identifikacijo posameznika, na katerega se nanašajo osebni podatki (41. in 45. odstavek). V zvezi s tem vprašanjem je Sodišče Evropske unije sklenilo:

> "[49] Glede na navedeno je treba na prvo vprašanje odgovoriti, da je treba člen 2(a) Direktive 95/46 razlagati tako, da dinamični IP-naslov, ki ga je ponudnik storitev spletnih medijev zabeležil ob dostopu neke osebe do spletnega mesta, ki jo ta ponudnik daje na voljo javnosti, glede tega ponudnika pomeni osebni podatek v smislu te določbe, če ima na voljo pravna sredstva, ki mu omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki, z dodatnimi informacijami, ki jih ima na voljo ponudnik dostopa do interneta tega posameznika."

V. PRIMERJALNO PRAVO

A. Ustavno sodišče Zvezne republike Nemčije

63. Pritožnik se je skliceval na sodbo Ustavnega sodišča Zvezne republike Nemčije z dne 24. januarja 2012, BVerfG, 1 BvR 1299/05. Ustavno sodišče Zvezne republike Nemčije je delno podprlo pritožbe v zvezi, *inter alia*, ročnim pridobivanjem podatkov o dinamičnem IP-naslovu, ki so ga hranili ponudniki telekomunikacijskih storitev.

64. V skladu s 113. členom Zakona o telekomunikacijah so morali ponudniki telekomunikacijskih storitev na zahtevo pristojnih agencij (vključno z agencijami za odkrivanje in pregon) zagotoviti informacije o določenih zbranih podatkih, za namene, *inter alia,* pregona kaznivih dejanj ali kršitev predpisov. Izpodbijana zakonska določba je bila oblikovana, da bi po možnosti omogočala dodelitev vseh telekomunikacijskih številk zadevnim naročnikom (in poleg tega na koncu, po možnosti njihovim uporabnikom).

Kakor je ugotovilo Ustavno sodišče Zvezne republike Nemčije, določba ni določala posebnega praga kršitve, ki bi njen obseg natančneje opredelil. Namesto tega je vedno dopuščala informacije v posameznem primeru, če je bilo to nujno za izvedbo zgoraj navedenih nalog. Ustavno sodišče Zvezne republike Nemčije je bilo mnenja, da to samo po sebi ni protiustavno. Vendar pa je bilo vprašanje, ki se je tudi zastavilo, ali je izpodbijana določba zajemala tudi informacije o lastniku dinamičnega IP-naslova. Na začetku je Ustavno sodišče Zvezne republike Nemčije obravnavalo povezavo med podatki o naročniku in prej obstoječo informacijo o vsebini, ki bi ji jo lahko pripisali. Ugotovilo je naslednje (113. odstavek, citat iz prevoda, ki je na voljo na spletni strani Ustavnega sodišča Zvezne republike Nemčije):

> " ... tajnost telekomunikacij [prvi odstavek 10. člena Temeljnega zakona] ne varuje zaupnosti v okoliščinah vsake telekomunikacijske storitve, kot je na primer dodelitev telekomunikacijskih številk, ki jih ponudnik storitev dodeljuje posameznim naročnikom."

65. Ustavno sodišče Zvezne republike Nemčije je nadaljevalo s seznanitvijo z razliko med statičnim in dinamičnim IP-naslovom in ugotovilo (115. in 116. odstavek):

> " ... dodelitev statičnega IP-naslova določenemu naročniku – natančneje, internetnega vmesnika naročniku – praviloma prinese tudi posredno informacijo o določenem telekomunikacijskem dogodku, ki vključuje zadevno osebo, saj so ti naslovi, čeprav so statični, registrirani in postanejo sredstvo za prepoznavo posameznika, in sicer skoraj izključno v povezavi z določenimi komunikacijskimi dogodki. Vendar pa je tudi tu posredovanje informacij v tej zvezi kot takšno omejeno izključno na abstraktno dodelitev številke in naročnika.
>
> ... Nasprotno pa je zadeva drugačna, če so dinamični IP-naslovi dodeljeni določenim osebam, saj so ti naslovi še zlasti tesno povezani z določenimi telekomunikacijskimi dogodki. Ta dodelitev spada na področja varstva iz prvega odstavka 10. člena Temeljnega zakona. Vendar pa tudi to ne izhaja samodejno iz dejstva, da je dodelitev dinamičnega IP-naslova nujno vedno povezana z določenim telekomunikacijskim dogodkom, o katerem zato posredno tudi zagotavlja informacije. Tudi v tej povezavi se informacija sama po sebi le navezuje na podatke, ki so abstraktno dodeljeni naročniku. Torej se bistveno ne razlikuje od dodelitve statičnega IP-naslova. Vendar pa tukaj uporaba prvega odstavka 10. člena Temeljnega zakona temelji na dejstvu, da če telekomunikacijska podjetja identificirajo dinamični IP-naslov, morajo narediti vmesni korak, v katerem raziščejo ustrezne podatke o povezavah njihovih strank, torej morajo dostopati do posebnih telekomunikacijskih dogodkov. Za te telekomunikacijske povezave, ki jih ponudniki storitev hranijo individualno, velja tajnost telekomunikacij, ne glede na to, ali jih morajo ponudniki storitev hraniti na voljo v skladu z zakonsko predpisano dolžnostjo ... ali pa jih hranijo na podlagi pogodbe. Če zakonodaja telekomunikacijskim podjetjem nalaga dolžnost dostopa do teh podatkov in njihovega ocenjevanja v interesu države zaradi opravljanja njenih nalog, je to kršenje prvega odstavka 10. člena Temeljnega zakona. To je ne samo v primeru, če morajo ponudniki storitev sami predložiti podatke o povezavah, temveč tudi, če morajo uporabiti podatke kot predhodno vprašanje za informacije."

66. Ustavno sodišče Zvezne republike Nemčije je sklenilo, da je prvi odstavek 113. člena Zakona o telekomunikacijah toliko kršil prvi odstavek

10. člena Temeljnega zakona, kolikor je bil podlaga za zagotavljanje informacij o dinamičnih IP-naslovih.

67. Poleg tega, čeprav Ustavno sodišče Zvezne republike Nemčije ni ugotovilo, da bi bilo samodejno pridobivanje podatkov (12. člen Zakona o telekomunikacijah) v zvezi s statičnim IP-naslovom protiustavno, pa je do takšne ugotovitve prišlo ob omejeni rabi teh naslovov v naslednjem kontekstu (160. in 161. odstavek):

> "... Dodelitev statičnih IP-naslovov, katerih dodelitev je zdaj v praksi v vsakem primeru javno dostopna, je v bistvu omejeno na institucije in velike uporabnike. Možnost pridobivanja teh številk v teh okoliščinah nima velike teže.
>
> Vendar pa bi lahko 112. člen Zakona o telekomunikacijah] dobil bistveno večjo težo kršitve, če bi se statični IP-naslovi v prihodnosti – na primer na temelju internetnega protokola različice 6 – začeli širše uporabljati kot podlaga za internetno komunikacijo. Teža kršitve identifikacije IP-naslova primarno ni odvisna – celo če bi v tem primeru veljale številne temeljne pravice – od tega, ali je IP-naslov tehnično dinamičen ali statičen, temveč od dejanskega pomena dolžnosti informiranja v zvezi s tem. Če pa so v praksi statični IP-naslovi dodeljeni tudi širokemu obsegu posameznikov, to lahko mogoče pomeni, da so naslovi internetnih uporabnikov v širokem obsegu, ali vsaj v veliki meri, opredeljeni in da so komunikacijski dogodki na internetu deanonimizirani ne samo za omejeno časovno obdobje, temveč za stalno. Ta daljnosežna možnost deanonimizacije komunikacije na internetu sega prek učinka klasičnega telefonskega imenika ... Za prizadeto osebo teža dodelitve IP-naslova naročniku ne more biti enakovredna teži identifikacije telefonske številke, ker prva od obeh omenjenih omogoča dostop do informacij, obseg in vsebina katerih sta bistveno daljnosežnejša ... Glede na te povečane informacijske možnosti bi bila splošna možnost identifikacije IP-naslovov ustavno dopustna samo v skladu z večjimi omejitvami ..."

B. Kanadsko vrhovno sodišče

68. Zadeva *R proti Spencer* (2014 SCC 43, [2014] 2 S.C.R. 212) je obravnavala pridobitev brez predhodnega sodnega pooblastila, podatkov o naročniku v zvezi s pritožnikovo sestro, povezanih z dinamičnim IP-naslovom, ki jih je policija pridobila v zvezi s spletno izmenjavo datotek z otroško pornografijo. Na podlagi podatkov o naročniku, ki jih je policija prejela od ponudnika internetnih storitev, je policija pridobila nalog za preiskavo zoper pritožnika. Pritožnik je zahteval izključitev dokazov, najdenih na njegovem računalniku, češ da so dejanja policije pri pridobivanju njegovega naslova od ponudnika internetnih storitev brez predhodnega sodnega pooblastila vodila do neutemeljene preiskave, ki je bila v nasprotju s Kanadsko listino pravic in svoboščin. Sodbo Vrhovnega sodišča Kanade z dne 13. junija 2014, ki je bila v dobro pritožnika, je izdal sodnik Judge Cromwell.

69. Ob sklicevanju na preteklo sodno prakso o tem vprašanju je sodba ugotovila, da je upravičeno pričakovanja standardov zasebnosti prej normativ kot pa enostaven opis in da je neizogibno "obremenjeno z vrednostnimi sodbami, ki so bile napisane z neodvisnega vidika razumnega in obveščenega

posameznika, ki je bil zaskrbljen zaradi dolgoročnih posledic vladnega ukrepa za zaščito zasebnosti" (18. odstavek). Vrhovno sodišče Kanade je v nasprotju z mnenjem obravnavnega sodnika ugotovilo, da je bilo pritožnikovo subjektivno pričakovanje zasebnosti utemeljeno z dejstvom, da je uporabljal omrežno povezavo za prenos občutljivih podatkov. Sodba je v nadaljevanju opredelila, ali je bilo pritožnikovo subjektivno pričakovanje zasebnosti upravičeno. V ta namen je sodba preučila dve okoliščini: naravo obravnavanega interesa zasebnosti ter zakonski in pogodbeni okvir, ki ureja razkritje podatkov o naročniku s strani ponudnika internetnih storitev. V zvezi s prvim je sodnik Cromwell sprejel naslednje sklepe:

> "[31] Zato je jasno, da je pri določanju predmeta preiskave treba upoštevati tendenco informacij, iskanih za podporo sklepanju v zvezi z drugimi osebnimi podatki.
>
> [36] ... Analiza obravnava zasebnost področja ali stvari, ki se preiskuje, in vplivu iskanja na njegov cilj, ne na zakonitost ali nezakonitost iskanih predmetov ...
>
> [41] Obstaja tudi tretji koncept informacijske zasebnosti, ki je še zlasti pomembna v zvezi z uporabo interneta. To je razumevanje zasebnosti kot anonimnosti. Moje mnenje je, da mora koncept zasebnosti, ki jo potencialno varuje 8. člen [pravica do varnosti pred neutemeljeno preiskavo ali zasegom], vključevati to razumevanje zasebnosti.
>
> [50] ... V okoliščinah te zadeve je bila zahteva policije za povezavo določenega IP-naslova s podatki o naročniku dejansko zahteva, da se za določeno osebo (ali omejeno število oseb v primeru skupnih internetnih storitev) ugotovi povezava s posebnimi spletnimi dejavnostmi. Ta vrsta zahteve vključuje vidik anonimnosti interesa informacijske zasebnosti s poizkusom povezati osumljenca z anonimno izvajanimi spletnimi dejavnostmi, dejavnostmi, ki jih je Sodišče v drugih okoliščinah spoznalo za tiste, ki vključujejo bistvene interese zasebnosti ...
>
> [51] Zato zaključujem, da policijska zahteva Shawu (ponudniku internetnih storitev) za podatke o naročniku, ki ustrezajo posebej opazovani anonimni internetni dejavnosti, vključuje visoko raven informacijske zasebnosti. S sklepom, ki ga je izdal Caldwell J. A., se strinjam v naslednji točki:
>
> > ...razumen in obveščen posameznik, zaskrbljen zaradi varstva zasebnosti, bi pričakoval, da bodo njegove dejavnosti na njegovem računalniku, uporabljanem v njegovem domu, zasebne ... Po moji presoji ni pomembno, da so se osebni atributi razkritih informacij nanašali na sestro g. Spencerja, ker je bil g. Spencer osebno in neposredno izpostavljen posledicam ravnanja policije v tem primeru. Kot tako je ravnanje policije *prima facie* zadevalo pravico do osebne zasebnosti g. Spencerja in v tem pogledu je bil njegov interes za zasebnost razkritih informacij neposreden in oseben ..."

70. Sodba je tudi odgovorila na zaskrbljenost organov sodnega pregona glede tega, da bi priznanje pravice od spletne anonimnosti vzpostavilo kriminalu prijazen internet. Ob priznanju, da te zaskrbljenosti ni mogoče obravnavati zlahka, je sodnik Cromwell pojasnil, da priznanja interesa ni mogoče enačiti s pravico do anonimnosti in da se je, na primer, v zadevnem primeru zdelo jasno, da bi bila policija zlahka dobila odredbo za predložitev podatkov o naročniku.

71. Glede vprašanja, ali je bilo pričakovanje zasebnosti upravičeno ob upoštevanju zadevnih pogodbenih in zakonskih določb, je sodba ugotovila, da je za zbiranje, uporabo in razkritje osebnih podatkov s strani ponudnika internetnih storitev o njegovih naročnikih veljal Zakon o varstvu osebnih podatkov in o elektronskih dokumentih (PIPEDA), ki je osebne podatke, ki so jih hranile organizacije, ki so se ukvarjale s poslovno dejavnostjo, varoval pred razkritjem brez vedenja ali pristanka osebe, na katero so se nanašali. Sodba je ugotovila:

> "[62] Člen 7(3) (*c*.1)(ii) omogoča razkritje brez pristanka vladne ustanove, če je ta ustanova utemeljila svoje *zakonsko upravičenje* za pridobitev informacij. Vprašanje pa je, ali je obstajalo takšno zakonsko upravičenje, ki je deloma odvisno od tega, ali je obstajalo upravičeno pričakovanje zasebnosti glede naročniških podatkov ali ne. *Zakona o varstvu osebnih podatkov in elektronskih dokumentov* (*PIPEDA)* zato ni mogoče uporabiti za primerjavo z obstojem upravičenega pričakovanja zasebnosti... Ker je namen *Zakona o varstvu osebnih podatkov in elektronskih dokumentov (PIPEDA)* vzpostavitev predpisov, ki urejajo, med drugim, razkritje "osebnih podatkov na način, ki priznava pravico do zasebnosti posameznikov v zvezi z njihovimi osebnimi podatki" (3. člen), bi bilo utemeljeno, da bi uporabnik interneta pričakoval, da enostavna zahteva policije ne bo sprožila obveznosti razkritja osebnih podatkov ali izničila splošne prepovedi razkritja osebnih podatkov brez soglasja v skladu z *Zakonom o varstvu osebnih podatkov in elektronskih dokumentov (PIPEDA)."*

72. Sodba je v nadaljevanju ugotovila, da zahteva policije ni imela zakonskega upravičenja in da je bila torej informacija pridobljena protiustavno. Sodišče ni hotelo delati vzporednic z drugimi rednimi policijskimi poizvedbami, kot je na primer razgovor z žrtvijo kaznivega dejanja. Ob sklicevanju na zadevo *R. proti Duarte*, [1990] 1 S.C.R. 30 je ugotovilo:

> "[67] ... V zadevi *Duarte* je Sodišče razlikovalo med osebo, ki je ponovila razgovor z osumljencem policiji, in policijo, ki je pridobila avdio posnetek tega razgovora. Sodišče je odločilo, da ne gre za nevarnost 'tveganja, da bo nekdo ponovil naše besede, temveč da je veliko bolj zahrbtna nevarnost v dopuščanju državi, da po svoji neomejeni lastni presoji snema in prenaša naše besede'... Podobno je v tem primeru policija zahtevala od ponudnika internetnih storitev razkritje podatkov o naročniku, ki je bilo dejansko zahteva, povezati g. Spencerja s točno določeno spletno dejavnostjo, ki jo je policija opazovala, in je tako vključevala veliko pomembnejši interes zasebnosti, kot je enostavno vprašanje, ki ga policija zastavi v teku preiskave."

PRAVO

I. ZATRJEVANA KRŠITEV 8. ČLENA KONVENCIJE

73. Pritožnik se je pritožil, da je bila kršena njegova pravica do zasebnosti, ker je (i) ponudnik internetnih storitev domnevno nezakonito ohranil njegove osebne podatke in (ii) je policija pridobila podatke o naročniku, povezane z

njegovim dinamičnim IP-naslovom, in posledično samovoljno brez odredbe sodišča pridobila njegovo identiteto s kršenjem 8. člena konvencije, ki se glasi:

> "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."

A. Sprejemljivost

1. Glede očitane nezakonite hrambe osebnih podatkov s strani ponudnika spletnih storitev

74. Vlada je trdila, da se pritožnik pred domačimi sodišči ni ugovarjal, da je ponudnik spletnih storitev nezakonito hranil njegove osebne podatke. Posledično domača sodišča niso obravnavala tega vprašanja v izpodbijanih odločbah. Vlada je nadalje trdila, da bi lahko pritožnik za odškodnino tožil ponudnika internetnih storitev, ki je bil zasebni subjekt, v pravdnem postopku. Tako ali drugače, ta del pritožbe bi bilo po mnenju vlade treba razglasiti za nesprejemljivega zaradi neizčrpanja notranjepravnih sredstev.

75. Poleg tega je vlada trdila, da pritožnik ni mogel trditi, da je bil žrtev zatrjevane kršitve 8. člena v zvezi s hrambo osebnih podatkov, saj se ti podatki niso nanašali nanj, temveč na naročnika internetnih storitev, ki je bil njegov oče.

76. Pritožnik je trdil, da je ponudnik internetnih storitev hranil njegove osebne podatke skoraj šest mesecev, ne da bi za to dejanje imel jasno zakonsko podlago, in je tako kršil 8. člen konvencije. V svoji vlogi, predloženi 15. oktobra 2015, je pritožnik trdil, da ni vložil svoje pritožbe na Sodišče zato, ker ponudnik internetnih storitev ni varoval tajnosti njegovih osebnih podatkov, ali ker jih je hranil prek zakonsko določenega roka, temveč ker je država pridobila in uporabila zadevne podatke v kazenskem postopku proti njemu. Zatrjeval je, da je ves čas kazenskih postopkov trdil, da so se sodišča opirala na nezakonito pridobljena dokazna sredstva.

77. Sodišče ugotavlja, da je vlada pritožniku izpodbijala status žrtve v zvezi s to pritožbo. Vendar je Sodišče mnenja, da mu ni treba obravnavati teh ugovorov, saj je ta del pritožbe v vsakem primeru nesprejemljiv iz naslednjih razlogov:

78. Sodišče ugotavlja, da je namen prvega odstavka 35. člena državam pogodbenicam zagotoviti možnost, da preprečijo ali odpravijo proti njim navedene kršitve, še preden se njihove navedbe predložijo institucijam konvencije. To pravilo je pomemben vidik načela, da je s konvencijo vzpostavljen sistem zaščite podrejen domačim sistemom varovanja človekovih pravic. Tako je treba pritožbo, predvideno za naknadno vložitev

pri Sodišču, najprej vložiti pri ustreznem domačem organu – vsaj glede bistvenega – ter v skladu s formalnimi zahtevami in roki, ki jih določa domača zakonodaja (glej, med drugimi sodbami, Sejdović *proti Italiji* [VS], št. 56581/00, 43.– 44. odstavek, ESČP 2006-II).

79. V zadevnem primeru se je pritožnik v pritožbi Sodišču pritožil, ker je po njegovem zatrjevanju ponudnik internetnih storitev hranil njegove osebne podatke. Vendar pa glede tega ni izčrpal domačih pravnih sredstev, saj glede tega ni ugovarjal – vsaj vsebinsko – v domačih postopkih.

80. Pritožbo je v tem delu zato treba zavrniti kot nesprejemljivo v skladu s prvim in četrtim odstavkom 35. člena konvencije.

2. Glede razkritja podatkov o naročniku

81. Vlada je trdila, da pritožnik ni mogel trditi, da je bil žrtev, saj so se podatki o naročniku, ki jih je ponudnik internetnih storitev razkril policiji, nanašali na njegovega očeta.

82. Pritožnik je to stališče izpodbijal. Trdil je, da je bila kršena njegova zasebnost, ne naročnikova, in da ni sporno vprašanje lastništva, temveč pravica do zasebnosti.

83. Sodišče pripominja, da je to vprašanje tesno povezano z utemeljenostjo pritožbe in se zato pridružuje vladnemu ugovoru glede utemeljenosti.

84. Sodišče ugotavlja, da ta pritožba ni očitno neutemeljena po točki a tretjega odstavka 35. člena konvencije. Prav tako ugotavlja, da ni nesprejemljiva niti iz katerih koli drugih razlogov. Torej jo je treba razglasiti za sprejemljivo.

B. Utemeljenost

1. Navedbe strank

(a) Pritožnik

85. Pritožnik se je skliceval na opredelitev osebnih podatkov iz konvencije iz leta 1981 (glej 46. odstavek zgoraj) in trdil, da je pridobitev podatkov brez odredbe sodišča (glej 7. odstavek zgoraj) pripeljala do njegove identifikacije.

86. Trdil je tudi, da se kljub temu, da je razkril vsebino svoje komunikacije nedoločljivi javnosti, ni odrekel svoji pravici do zasebnosti v zvezi s podatki o prometu (vodenje evidence klicnih številk), to je podatki v zvezi s trajanjem in časom uporabe interneta in podatki v zvezi s tem, kdo je uporabljal internet in na katero spletno stran je dostopal v času te uporabe. Po njegovem mnenju so bili ti podatki ločeno varovani v okviru koncepta zasebnega življenja, ki vključuje zasebnost komunikacij in informacijsko zasebnost.

87. V tej zvezi je navedel, da bi moralo biti priznano bistveno razlikovanje med statičnim in dinamičnim IP-naslovom. Medtem ko bi bilo mogoče videti podobnost med statičnim IP-naslovom, ki je bil stalno dodeljen napravi, in telefonsko številko, pa je bil dinamični IP-naslov dodeljen vsakokrat, ko je računalnik dostopil do interneta. Ob sklicevanju na sodbo Ustavnega sodišča Zvezne republike Nemčije z dne 24. januarja 2012 (glej 63. odstavek zgoraj) je pritožnik zatrjeval, da se z izbiro dinamičnega IP-naslova, kakor je to v obravnavani zadevi storil naročnik, človek odloči za skrito identiteto, saj so bili za identifikacijo računalnika, ki se je uporabljal za dostop do interneta, potrebni dodatni podatki, in torej tudi za identifikacijo naročnika. Po njegovem mnenju je zato dinamični IP-naslov spadal v področje podatkov o prometu (vodenje evidence klicnih številk), za katere je veljal prvi odstavek 149. b člena.

88. Pritožnik je nadalje poudaril, da so bili podatki o vsebini komunikacije pridobljeni brez vključitve slovenskih organov oblasti. Slovenski organi oblasti bi za pridobitev teh podatkov potrebovali odredbo sodišča, vendar so se temu sicer nujnemu koraku izognili tako, da so zahtevali podatke o naročniku na podlagi tretjega odstavka 149. b člena ZKP. Glede dopisa je pritožnik zatrjeval, da v času, ko je slovenska policija pridobila podatke, ki so povezovali njegov IP-naslov z njegovo identiteto, zakon, ki je urejal dostop do teh podatkov, ni bil jasen (*lex certa*) in zato zakonitost, ki jo zahteva drugi odstavek 8. člena, ni bila izpolnjena. Predvsem so bile v času posega (avgust 2006) določbe domačega zakona glede tega vprašanja nasprotujoče. Ustava v drugem odstavku 37. člena za vsak poseg v pravico do komunikacijske zasebnosti zahteva odredbo sodišča. ZEKom je določal, da morajo podatki o prometu ostati tajni in da se komunikacija ne sme prestrezati samo na podlagi odredbe pristojnega organa. V domačem pravnem sistemu bi bila to lahko samo odredba sodišča ali, teoretično, odredba preiskovalnega sodnika. Kakor koli že, v skladu s 107. členom je bilo mogoče samo "prestrezati" podatke, ne pa določenih podatkov izročiti. Poleg tega so morali ponudniki izbrisati shranjene podatke v skladu s 104. členom, kakor hitro jih niso več potrebovali zaradi zaračunavanja. Po drugi strani pa sta prvi in tretji odstavek 149. b člena ZKP določala različne pogoje za dostopanje do podatkov in ni bilo jasno, kakšna je razlika med njima pri njuni pri uporabi. Zaradi te nejasnosti v domači zakonodaji ni mogoče reči, da je bila pravica do zasebnosti zadostna pravna zaščita pred samovoljnim poseganjem javnih organov.

89. Po pritožnikovem mnenju je bil ZEKom *lex specialis* glede na ZKP in ni omogočal posredovanja osebnih podatkov policiji. V takšnem položaju pravne praznine bi bilo treba ustavo uporabiti neposredno, ta pa je jasno zahtevala odredbo sodišča za posredovanje teh podatkov.

(b) Vlada

90. Vlada je pojasnila, da so statični IP-naslovi osebni podatki in da je kot osebne podatke treba šteti tudi dinamični IP-naslovi, skratka, da to niso podatki o prometu. Edina razlika med obojimi navedenimi je bila, da je statični IP-naslov ostal naročnikov tako dolgo, dokler ni zamenjal ponudnika internetnih storitev, medtem ko je bil novi dinamični IP-naslov dodeljen vsakokrat, ko je naročnik dostopal do interneta. V zvezi z obema je ponudnik internetnih storitev hranil podatke o času uporabe določenega IP-naslova.

91. Vlada je trdila, da se je preiskava osredotočila na pritožnika šele po zasegu in pregledu računalnikov in šele potem, ko so bili zaslišani tisti, ki so živeli na naslovu naročnika. Tako je postala povezava med naročnikom in pritožnikom očitna šele po hišni preiskavi, ki pa je bila opravljena na podlagi veljavne odredbe sodišča.

92. Ob priznanju, da je bil IP-naslov osebni podatek, saj je omogočal identifikacijo posameznika, pa je vlada poudarila, da je bila izbira vsakega posameznega uporabnika, ali bo uporabil spletno stran, ki je omogočala razkritje osebnih podatkov in/ali vsebine komunikacije nedoločljivemu in neomejenemu krogu posameznikov. Vlada je trdila, da pritožnik ni trdil, da je skrival IP-naslov, ki ga je uporabljal za dostop do programa za izmenjavo datotek. Ker je razkritje IP-naslova pomenilo razkritje podatkov o naročniku, uporabnik ni pokazal namena ohraniti svoje identitete zasebne ali skrito in njegova pravica do zasebnega življenja tako v obravnavanem primeru ni bila prizadeta.

93. Vlada je trdila, da pritožnik ni mogel pričakovati, da podatki o naročniku, povezani z dinamičnim IP-naslovom, ne bodo predani policiji. Po vladnem mnenju so bili izpodbijani ukrepi zakoniti in sorazmerni s ciljem varovanja integritete otrok, ki so v skladu s konvencijo kot posebej ogroženi posamezniki imeli posebno zaščito.

94. Vlada je za primerjavo navedla primer, ko je osumljenca med vožnjo posnela videonadzorna kamera. V takšnem primeru so osumljenčeva fotografija in njegove registrske tablice zadoščali za njegovo identifikacijo. Podobno bi morali v obravnavanem primeru sklepati, da je bil v času, ko je policija dobila dinamični IP-naslov in čas njegove uporabe, osumljenec identificiran na podlagi teh podatkov. Zato je vlada trdila, da so domača sodišča pravilno uporabila tretji odstavek 149. b člena namesto prvega odstavka 149. b člena, saj se je slednji nanašal na podatke o prometu, in ne na podatke o lastniku ali uporabniku komunikacijske naprave.

2. Presoja Sodišča

(a) Uvodne ugotovitve in obseg presoje Sodišča

95. Sodišče najprej ugotavlja posebnost obravnavane zadeve, ki zadeva razkritje podatkov o naročniku, povezanih z dinamičnim IP-naslovom. Sodišče je seznanjeno z obsežno zakonodajo in sodno prakso v zvezi z

varovanjem osebnih podatkov in zasebnostjo elektronskih komunikacij v Evropski uniji in se bo oprlo nanju in na drugo ustrezno gradivo primerjalnega prava pri presoji nekaterih tehničnih vprašanj v zvezi z obravnavanim primerom. Kadar je to ustrezno, bo upoštevalo tudi pravne doktrine, vzpostavljene v njih.

96. V uvodnem delu Sodišče nadalje ugotavlja, da je IP-naslov enkratna številka, dodeljena vsaki napravi v omrežju, ki omogoča napravam, da med seboj komunicirajo. Za razliko od statičnega IP-naslova, ki je trajno dodeljen določenemu omrežnemu vmesniku določene naprave, dinamični IP-naslov ponudnik internetnih storitev začasno dodeli napravi, običajno vsakokrat, ko se naprava poveže z internetom (glej odstavke 61, 87. in 90.) IP-naslov omogoča opredelitev določenih podrobnosti, kot sta na primer ponudnik internetnih storitev, na katerega je uporabnik priključen, in širša fizična lokacija, ki je najverjetnejša lokacija ponudnika internetnih storitev. Večini dinamičnih IP-naslovov je tako mogoče slediti do ponudnika internetnih storitev in ne do določenega računalnika. Za pridobitev imena in naslova naročnika, ki uporablja dinamični IP-naslov, se od ponudnika internetnih storitev običajno zahteva, da poišče te podatke in v ta namen pregleda zadevne podatke o povezavah svojih naročnikov (glej odstavka 61. in 65.)

97. V obravnavani zadevi je podatke o dinamičnem IP-naslovu in času, kdaj je bil dodeljen, zbrala švicarska policija, ki je spremljala uporabnike določenega internetnega omrežja, ki je vključevalo vsebine z otroško pornografijo. Podatke so poslali slovenski policiji, ki je od ponudnika internetnih storitev pridobila ime in naslov naročnika z zadevnim dinamičnim IP-naslovom – pritožnikovega očeta (glej 6. in 7. odstavek zgoraj).

98. Vlada je trdila, da se v tej zadevi 8. člen konvencije ne uporablja, ker pritožnik ni bil neposredno prizadet zaradi izpodbijanega ukrepa in tudi če bi bil prizadet, se je prostovoljno odrekel svoji pravici do zasebnosti z izmenjavo zadevnih datotek (glej 92. in 93. odstavek zgoraj). Da bi odgovorilo na ta vprašanja, mora Sodišče preučiti, ali je pritožnik ali kateri koli drug posameznik, ki uporablja internet, upravičeno pričakoval, da bo njegova sicer javna spletna dejavnost ostala anonimna (glej 115. do 118. odstavek zgoraj).

99. V tej zvezi Sodišče ponavlja, da je spolna zloraba nedvomno odvratno hudodelstvo, s hudimi posledicami na njegove žrtve. Otroci in drugi ranljivi posamezniki so upravičeni do državnega varovanja v obliki učinkovitega odvračanja od teh hudih posegov v bistveni vidik njihovega zasebnega življenja in da to varovanje vključuje nujo po prepoznanju kršiteljev in njihovo privedbo pred sodišče (glej *K. U. proti Finski*, št. 2872/02, 46. odstavek, ESČP 2008-V). Vendar pa je treba na vprašanja, ki jih je zastavila vlada v zvezi z uporabo 8. člena, odgovoriti neodvisno od zakonitosti ali nezakonitosti obravnavane dejavnosti kakor tudi brez poseganja v zahteve konvencije, da morajo države članice zagotavljati varovanje ranljivih

posameznikov, kakor je med drugim poudarjeno v zadevi *K.U. proti Finski* (navedena zgoraj).

(b) Uporaba 8. člena

(i) Povzetek ustreznih načel

100. Sodišče znova opozarja, da je zasebno življenje širok pojem, ki ga ni mogoče v celoti opredeliti. 8. člen varuje, *inter alia,* pravico do identitete in osebnega razvoja ter pravico do vzpostavljanja in krepitve odnosov z drugimi ljudmi in zunanjim svetom. Med posameznikom in drugimi ljudmi je območje interakcije, in to celo v javnem kontekstu, ki lahko spada na področje "zasebnega življenja" (glej zadeva *Uzun proti Nemčiji*, št. 35623/05, 43. odstavek, ECHR 2010-VI (povzetki)).

101. Obstajajo številni dejavniki, ki so pomembni pri preučitvi, ali je posameznikovo zasebno življenje prizadeto zaradi ukrepov, ki se izvajajo zunaj njegovega doma ali zasebnih prostorov. Sodišče je za ugotovitev, ali je pojma "zasebno življenje" in "korespondenca" primerno uporabiti, ob več priložnostih preučilo, ali so posamezniki upravičeno pričakovali, da bo njihova zasebnost spoštovana in varovana (glej *Bărbulescu proti Romuniji* [GC], št. 61496/08, 73. točka, ECHR 2017, in *Copland proti Združenemu kraljestvu*, št. 62617/00, 41. do 42. točka, ECHR 2007-I). V tej zvezi je Sodišče navedlo, da je upravičeno pričakovanje zasebnosti bistveni, čeprav ne nujno odločilni dejavnik (glej *Bărbulescu,* navedena zgoraj, 73. točka)

102. Glede osebnih podatkov je Sodišče poudarilo, da se izraz "zasebno življenje" ne sme ozko razlagati. Ugotovilo je, da široka razlaga ustreza tisti iz konvencije iz leta 1981, namen katere je "zagotoviti na ozemlju vsake pogodbenice vsakemu posamezniku ... spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj (1. člen). Ti osebni podatki so opredeljeni kot "katera koli informacija, ki se nanaša na določenega ali določljivega posameznika" (2. člen) (glej *Amann proti Švici* [GC], št. 27798/95, 65. odstavek, ESČP 2000-II; glej tudi 46. odstavek zgoraj).

103. Iz uveljavljene sodne prakse izhaja, da če so zbiranje podatkov o določenem posamezniku, obdelava ali uporaba osebnih podatkov ali objava zadevnega gradiva presegali način ali stopnjo, kakor sta običajno predvidena, to vzbudi zaskrbljenost glede zasebnosti (glej *Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski*[GC], št. 931/13, 136. člen, ESČP 2017 (povzetki)). 8. člen konvencije tako določa pravico do oblike informacijske samoodločitve, ki posameznikom omogoča, da se zanesejo na svojo pravico do zasebnosti glede podatkov, ki se jih, čeprav nevtralne, zbira, obdeluje in kolektivno razširja in to v obliki ali na način, ki bi lahko prizadela njihove pravice iz 8. člena (prav tam, 137. odstavek).

104. Pred tem je Sodišče preučilo informacije, kot so na primer podatki o vodenju evidence klicnih številk na klicanih telefonskih številkah (glej zadevo *Malone proti Združenemu kraljestvu*, 2. avgust 1984, 84. odstavek, serija A št. 82), osebne podatke, povezane s telefonom, elektronsko pošto in uporabo interneta (glej zadevo *Copland*, navedena zgoraj, 41. in 43. odstavek), informacije, ki so jih organi sodnega pregona shranili na kartici v zvezi z dejstvi, ki se nanašajo na poslovne odnose pritožnika (glej zadevo *Amann*, navedena zgoraj, 66. odstavek), in informacije javnega značaja, ki so jih oblasti shranile o pritožnikov daljni preteklosti (glej *Rotaru proti Romuniji* [GC], št. 28341/95, 43. in 44. odstavek, ESČP 2000-V), ki spadajo na področje uporabe 8. člena.

105. Poleg tega je Sodišče pred tem v zadevi *Delfi AS proti Estoniji* ([GC] št. 64569/09, 147. odstavek, ESČP 2015) priznalo pomen spletne anonimnosti ob ugotovitvi, da je bila ta dolgo sredstvo za izogibanje povračilnim ukrepom in neželeni pozornosti. Kot takšna lahko pomembno spodbuja prosti pretok idej in informacij, vključno in zlasti prek interneta. Hkrati pa Sodišče ne pozablja enostavnosti, obsega in hitrosti razširjanja informacij prek interneta in dolgotrajnosti učinkov razkritja informacij, kar lahko bistveno poslabša učinke nezakonitega govora prek interneta v primerjavi s klasičnimi mediji (prav tam).

106. V zgoraj navedeni zadevi je Sodišče preučilo tudi različne stopnje anonimnosti, vključene v spletno dejavnost, in ugotovilo naslednje (prav tam, 148. odstavek):

> "Sodišče ugotavlja, da so na internetu možne različne stopnje anonimnosti. Internetni uporabnik je lahko za širšo javnost anonimen, medtem ko je določljiv za ponudnika storitev prek računa ali podatkov za stik, ki so lahko nepreverjeni ali pa je zanje potrebna neka vrsta preverjanja, ki obsega omejeno preverjanje (na primer z aktivacijo računa prek elektronskega poštnega naslova ali računa družabnega omrežja) za zagotovitev avtentikacije, ali pa uporabo elektronskih osebnih izkaznic ali podatkov za preverjanje istovetnosti pri spletnem bančništvu, ki omogočajo varnejšo identifikacijo uporabnika. Ponudnik storitev lahko omogoči visoko stopnjo anonimnosti za svoje uporabnike, v tem primeru se od uporabnikov sploh ne zahteva, da se identificirajo in jim je mogoče slediti le v omejenem obsegu prek informacij, ki so jih shranili ponudniki dostopa do interneta. Razkritje teh informacij bi običajno zahtevalo odredbo preiskovalnih ali sodnih organov in bi zanjo veljali strogi pogoji. V nekaterih primerih je mogoče vseeno potrebna za razkritje in sodni pregon storilcev."

(ii) Uporaba zgoraj navedenih načel pri obravnavani zadevi

(α) Značilnosti vpletenih interesov

107. Vlada ni ugovarjala, da se podatki o naročniku načeloma nanašajo na osebne podatke (glej 90. in 92. odstavek zgoraj). Takšen sklep izhaja tudi iz opredelitev, ki jih vsebujejo konvencija iz leta 1981, zakonodaja Evropske unije in tudi domača zakonodaja, namenjena njihovemu izvajanju (glej 40, 46, 53 in 57 zgoraj).

108. Poleg tega Sodišče ugotavlja, da 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, na katera se sklicuje vlada (glej 94. odstavek, zgoraj). V resnici se zdi, da bi za identifikacijo naročnika, ki mu je bil določen dinamični IP-naslov dodeljen ob določenem času, moral ponudnik internetnih storitev dostopati do shranjenih podatkov, ki se nanašajo na določene telekomunikacijske dogodke (glej, na primer, 29., 61., 65. in 95. odstavek zgoraj). Uporaba teh shranjenih podatkov bi že sama po sebi lahko vzbudila pomisleke glede posega v zasebnosti (glej 103. odstavek zgoraj).

109. Prav tako Sodišče ne more spregledati določenega konteksta, v katerem so v obravnavani iskali podatke o naročniku. Edini namen pridobitve podatkov o naročniku je bila identifikacija določene osebe, ki je stala za neodvisno zbrano vsebino razkritih podatkov, ki jih je ta oseba dala v skupno rabo. V tej zvezi Sodišče ugotavlja, da je med posameznikom in drugimi ljudmi območje interakcije, ki lahko spada na področje "zasebnega življenja" (glej 100. odstavek zgoraj). Podatki o teh dejavnostih vključujejo vidik zasebnosti takrat, ko je povezan z določenim ali določljivim posameznikom ali se mu pripisuje (za sklic na prepoznavnost, čeprav v nekoliko drugačnem kontekstu, glej *Peck proti Združenemu kraljestvu*, št. 44647/98, 62. odstavek, ESČP 2003-I, in zadevo *J. S. proti Združenemu kraljestvu* (dec.), št. 445/10, 70. in 72. odstavek, 3. marec 2015). Zato mora biti tisto, kar bi se zdelo obrobna informacija, ki jo išče policija, torej ime in naslov naročnika, v primeru, kakršen je zadevni, obravnavano kot neločljivo povezano z ustrezno, prej obstoječo vsebino, ki razkriva podatke (glej odklonilna ločena mnenja ustavnih sodnikov, navedena v 31. in 34. odstavku; primerjaj tudi s stališčem kanadskega vrhovnega sodišča, navedenim v 69. in 72. odstavku, in stališčem Ustavnega sodišča Zvezne republike Nemčije, navedenim v 64. in 65. odstavku zgoraj). Odločiti drugače bi pomenilo zanikati potrebno varstvo informacij o osebi, ki bi lahko veliko razkrile o spletni dejavnosti posameznika, vključno z občutljivimi podrobnostmi njegovih ali njenih interesov, prepričanj in intimnega življenja.

110. Glede na zgoraj navedene premisleke Sodišče ugotavlja, da se obravnavana zadeva nanaša na vprašanja zasebnosti, ki lahko vključujejo varovanje v skladu z 8. členom.

(β) Ali je bil pritožnik identificiran z izpodbijanim ukrepom

111. Zatem mora Sodišče obravnavati vladno trditev, da so podatki o naročniku, ki jih je pridobila policija, razkrili samo ime in naslov pritožnikovega očeta, ne pa pritožnika (glej 91. odstavek zgoraj). V zvezi s tem Sodišče ugotavlja, da je splošno sprejeto, da se opredelitev osebnih podatkov nanaša na informacije v zvezi z ne samo določenimi, temveč tudi določljivimi posamezniki (glej 40., 47., 53., 54., 55. in 58. odstavek, zgoraj).

112. V obravnavanem kontekstu je bil pritožnik nedvomno uporabnik zadevnih internetnih storitev (glej 56. odstavek zgoraj), policija pa je spremljala njegovo spletno dejavnost. Sodišče nadalje ugotavlja, da je pritožnik uporabljal internet, kakor kaže s svojim računalnikom na svojem domu. To, da pritožnikovo ime ni bilo omenjeno v podatkih o naročniku, ki jih je pridobila policija, nima velikega pomena. V resnici ni neobičajno, da ima eno gospodinjstvo eno samo naročnino za internetne storitve, ki jih uporablja več družinskih članov. Dejstvo, da niso osebno naročeni na internetno storitev, ne vpliva na njihova pričakovanja glede zasebnosti, ki so neposredno vključena, ko so razkriti podatki o naročniku, ki se nanašajo na njihovo zasebno uporabo interneta.

113. Jasno je, da je bil namen izpodbijanega ukrepa, to je, da je policija brez odredbe sodišča pridobila podatke o naročniku, povezane z dinamičnim IP-naslovom, ki ga je zagotovila švicarska policija (glej 7. odstavek zgoraj), povezati računalniško uporabo z lokacijo in morda tudi osebo. Podatki o naročniku, ki so vsebovali tudi naslov, so policiji omogočili, da je identificirala bivališče, od koder so bile narejene zadevne internetne povezave. To jo je pripeljalo do pritožnika kot osumljenega uporabnika omrežja Razorback.

114. Ob upoštevanju zgoraj navedenega in tega, da domača sodišča niso zavrnila zadeve zaradi tega, ker pritožnik ni bil naročnik zadevne internetne storitve, Sodišče sklepa, da to dejstvo ne more biti prepreka za uporabo 8. člena v obravnavani zadevi. V skladu s tem zavrača vladni ugovor glede tega, da pritožnika ni mogoče šteti kot žrtev (glej 83. odstavek zgoraj).

(γ) Ali je pritožnik upravičeno pričakoval zasebnost

115. Da bi ugotovilo, ali se pojem "zasebno življenje" uporablja za obravnavani primer, mora Sodišče preučiti, ali je s stališča javne dostopnosti obravnavanega omrežja pritožnik upravičeno pričakoval, da bo njegova zasebnost spoštovana in varovana (glej 101. odstavek zgoraj). V tej zvezi sta slovensko ustavno sodišče in tožena vlada (glej 14. in 18. odstavek odločbe ustavnega sodišča, navedena v 29. odstavku zgoraj; glej tudi 92. odstavek zgoraj) ugotovila, da je pomembno, da je pritožnik sodeloval v omrežju Razorback, do katerega dostop ni bil omejen. Bila sta mnenja, da je s svojo spletno dejavnostjo dinamični IP-naslov vede izpostavljal javnosti in ga z njo povezoval. Zato po njunem mnenju njegovo pričakovanje zasebnosti ni bilo legitimno in bi celo morali šteti, da se ji je odpovedal (prav tam).

116. Sodišče enako kot ustavno sodišče dopušča, da je pritožnik pri izmenjavi datotek s pornografsko vsebino prek omrežja Razorback pričakoval s svojega subjektivnega vidika, da bo dejavnost ostala zasebna in da njegova identiteta ne bo razkrita (glej 14. odstavek odločbe ustavnega sodišča, navedene v 29. odstavku zgoraj). Vendar pa drugače kot ustavno sodišče Sodišče meni, da dejstvo, da ni skril svojega dinamičnega IP-naslova kljub ob domnevi, da je to sploh mogoče storiti, ne more biti odločujoče pri

presoji, ali je bilo njegovo pričakovanje zasebnosti upravičeno z objektivnega stališča. V tej zvezi Sodišče ugotavlja, da vprašanje nedvomno ni, ali bi bil pritožnik lahko upravičeno pričakoval, da bo svoj dinamični IP-naslov ohranil zaseben, temveč, ali je lahko upravičeno pričakoval zasebnost v zvezi s svojo identiteto.

117. Sodišče je pred tem že potrdilo anonimnostni vidik spletne zasebnosti (glej zadevo *Delfi AS*, navedena v 105. odstavku zgoraj, glej tudi 12. odstavek odločbe ustavnega sodišča, naveden v 29. zgoraj), v zvezi s spletno dejavnostjo, pri kateri uporabniki sodelujejo, ne da bi bili nujno določljivi. Ta anonimnostno pojmovanje zasebnosti je pomemben dejavnik, ki ga je treba upoštevati v tej presoji. Predvsem pa ni bilo zatrjevano, da je pritožnik kadarkoli razkril svojo identiteto v zvezi z obravnavano spletno dejavnostjo (glej v tej povezavi odklonilno ločeno mnenje sodnice Jadek Pensa, navedeno v 33. odstavku zgoraj33), ali da bi na primer identificiral določeni ponudnik spletnih storitev prek računa ali kontaktnih podatkov. Njegova spletna dejavnost je zato vključevala visoko stopnjo anonimnosti (glej zadevo *Delfi AS*, navedena v 105odstavku zgoraj, 148. odstavek), kar potrjuje 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 podatke preveril na zahtevo policije.

118. Na koncu Sodišče ugotavlja, da sta veljavni pravni in zakonodajni okvir lahko tudi ustrezna, čeprav ne nujno odločilna dejavnika pri določanju upravičenega pričakovanja zasebnosti (glej, na primer, *J. S. proti Združenemu kraljestvu* (dec.), navedeno zgoraj, 70. odstavek, in *Peev proti Bolgariji*, št. 64209/01, 39. odstavek, 26. julij 2007). V obravnavani zadevi nobena od strank ni predložila informacij o pogodbenih pogojih, na podlagi katerih so bile pritožnikovemu očetu nudene internetne storitve. Glede zakonodajnega okvira Sodišče meni, da zadošča ugotovitev, da 37. člen ustave zagotavlja zasebnost korespondence in komunikacij in zahteva, da kakršenkoli poseg v to pravico temelji na odredbi sodišča (glej 35. odstavek zgoraj). Zato 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.

(δ) Sklep

119. Zaradi vseh zgoraj navedenih razlogov Sodišče sklepa, da pritožnikov interes, da bi bila njegova identiteta v zvezi z njegovo spletno dejavnostjo varovana, spada v obseg pojma "zasebno življenje" in da se zato za to pritožbo uporablja 8. člen.

(c) Izpolnjevanje 8. člena

(i) Ali je prišlo do posega

120. Ob upoštevanju zgoraj navedenega sklepa, da je bila prizadeta pritožnikova pravica do spoštovanja njegovega zasebnega življenja, kot jo jamči prvi odstavek 8. člena, Sodišče nadalje ugotavlja, da sta zahteva policije, predana ponudniku internetnih storitev, in njena uporaba podatkov o naročniku, ki je pripeljala do identifikacije pritožnika, povzročili poseg v te njegove pravice (glej, *mutatis mutandis*, zadeva *Rotaru*, navedena zgoraj, 46. odstavek, in zadeva *Uzun*, navedena zgoraj, 52. odstavek). Glede na navedeno Sodišče meni, da ni treba ugotoviti, ali je obravnavani ukrep povzročil tudi poseg v pritožnikove pravice do spoštovanja njegove korespondence.

121. Sodišče mora zato preučiti, ali je bil poseg v pritožnikove pravice do zasebnosti v skladu z zahtevami drugega odstavka 8. člena, z drugimi besedami, ali je bil "v skladu z zakonom", usmerjen k enemu ali več zakonitim ciljem, določenim v tem odstavku, in "potreben v demokratični družbi", da se doseže ali dosežejo obravnavani cilj ali cilji.

(ii) Ali je bil poseg v skladu z zakonom

122. Sodišče ugotavlja, da izraz "v skladu z zakonom" v pomenu drugega odstavka 8. člena najprej zahteva, da morajo imeti izpodbijani ukrepi podlago v domači zakonodaji. Drugič, domača zakonodaja mora biti zadevni osebi dostopna. Tretjič, prizadeta oseba mora biti sposobna predvideti posledice, ki jih domača zakonodaja predvideva za določeno ravnanje, in četrtič, domača zakonodaja mora biti v skladu z načeli pravne države (glej, med številnimi drugimi zadevami, zadeva *Rotaru*, navedena zgoraj, 52. odstavek; *Liberty in drugi proti Združenemu kraljestvu*, št. 58243/00, 59. odstavek, 1. julij 2008; in *Sallinen in drugi proti Finski*, št. 50882/99, 76. odstavek, 27. september 2005).

123. Sodišče tudi ponovno poudarja, da je naloga domačih oblasti, zlasti sodišč, predvsem ta, da razlagajo in uporabljajo domače pravo. Vendar mora Sodišče preveriti, ali način, na katerega se razlaga in uporablja domača zakonodaja, ustvarja posledice, ki so v skladu z načeli konvencije, kakor je razložena ob upoštevanju sodne prakse Sodišča (glej *Cocchiarella proti Italiji* [GC], št. 64886/01, 81. in 82. odstavek, ESČP 2006-V).

124. V obravnavanem primeru pod pogojem, da ima policijska pridobitev podatkov o naročniku, povezanih z zadevnim dinamičnim IP-naslovom, podlago v domači zakonodaji zaradi tretjega odstavka 149. b člena ZKP, če bi policija lahko pridobila informacije o lastniku ali uporabniku določenih sredstev elektronske komunikacije od ponudnika internetnih storitev (glej 36odstavek zgoraj), mora Sodišče preučiti, ali je bil ta zakon dostopen in predviden ter v skladu z načeli pravne države.

125. Sodišče ugotavlja, da obravnavana zadeva ne sproža nobenih vprašanj glede dostopnosti zakona. Glede drugih zahtev Sodišče ponovno ugotavlja, da je nacionalno pravilo "predvidljivo", če je oblikovano z zadostno natančnostjo, da kateremu koli posamezniku omogoča – če je to potrebno z ustreznim nasvetom – uravnavati svoje ravnanje (glej zadevo *Rotaru*, navedena zgoraj, 55. odstavek in načela, ki so v njej povzeta). Poleg tega usklajenost z načeli pravne države zahteva, da domača zakonodaja zagotavlja ustrezno varstvo pred samovoljnim poseganjem v pravice po 8. členu (glej *mutatis mutandis*, zadevo *Amann*, navedena zgoraj, 76.–77. odstavek, *Bykov proti Rusiji* [GC], št. 4378/02, 76. odstavek, 10. marec 2009; glej tudi *Weber in Saravia proti Nemčiji* (dec.), št. 54934/00, 94. odstavek, ESČP 2006-XI; in zadevo *Liberty in drugi*, navedeno zgoraj, 62. odstavek). Sodišče se mora zato prepričati tudi, da proti zlorabi obstajajo ustrezna in učinkovita jamstva. Ta presoja je odvisna od vseh okoliščin zadeve, kot so vrsta, obseg in trajanje možnih ukrepov, razlogi, ki so potrebni, da se jih odredi, organi, pristojni za njihovo dovoljenje, izvajanje in nadzor ter vrsta pravnega sredstva, ki ga določa domača zakonodaja (glej *Association for European Integration and Human Rights* in *Ekimdzhiev proti Bolgariji*, št. 62540/00, 77. odstavek, 28. junij 2007, s sklicevanjem na *Klass in drugi proti Nemčiji*, 6. september 1978, 50. odstavek, serija A št. 28, in zadevo *Uzun*, navedena zgoraj, 63. odstavek).

126. Ob upoštevanju določenega konteksta Sodišče poudarja, da Konvencija o kibernetski kriminaliteti obvezuje države članice, da sprejmejo ukrepe, kot sta zbiranje podatkov v realnem času in izdaja odredb za predložitev podatkov, ki so na voljo organom oblasti v boju proti, *inter alia*, kaznivim dejanjem, povezanim z otroško pornografijo (glej 47. In 51. odstavek zgoraj). Vendar v skladu s 15. členom zadevne konvencije za te ukrepe "veljajo pogoji in zaščitne določbe, določeni v okviru domačega prava (države pogodbenice]", in morajo "glede na vrsto zadevnega postopka ali pooblastila, kadar je to primerno, *inter alia*, vsebovati sodni ali drug neodvisni nadzor, razloge, ki utemeljujejo uporabo in omejitev obsega ter trajanje takega pooblastila ali postopka" (glej 52. odstavek zgoraj).

127. V obravnavani zadevi Sodišče ugotavlja, da je tretji odstavek 149. b člena ZKP (glej 36odstavek zgoraj), na katerega se opirajo domači organi oblasti, obravnaval zahtevo po podatkih o lastniku ali uporabniku določenih sredstev elektronske komunikacije. Ni pa vseboval posebnih določb glede zveze med dinamičnim IP-naslovom in podatki o naročniku. Sodišče nadalje ugotavlja, da ustava v 37. členu za vsak poseg v pravico do komunikacijske zasebnosti zahteva odredbo sodišča (glej 35. odstavek zgoraj). Poleg tega ZEKom (glej 37. odstavek zgoraj), ki je posebej urejal tajnost in zaupnost elektronske komunikacije v tistem času, ni predvideval možnosti, da bi se do podatkov o naročniku in povezanih podatkov o prometu dostopalo in se jih posredovalo za namene kazenskih postopkov. Določal je, da so elektronske komunikacije, vključno s povezanimi podatki o prometu, zaupne in bi jih

ponudnik internetnih storitev kot take moral varovati (glej 37odstavek zgoraj). Določal je nadalje, da ponudnik internetnih storitev ne sme posredovati podatkov o prometu drugim, če ni to nujno za zagotavljanje storitev, razen če je zakonito prestrezanje komunikacij odredil pristojni organ (glej 103. člen ZEKom, naveden v 37. odstavku zgoraj). Torej najmanj, kar je bilo, zakonodaja ni bila koherentna glede ravni varovanja interesa zasebnosti uporabnikov.

128. Glede na navedeno bi Sodišče nedopustno poseglo v vlogo državnih sodišč, če bi poskušalo oblastno izjaviti, kateri nacionalni zakon bi moral prevladati v obravnavani zadevi. Namesto tega mora obravnavati argumentacijo domačih sodišč. V tej zvezi tako Sodišče ugotavlja, da je bilo ustavno sodišče mnenja, da "je [bila] identiteta komunicirajočega posameznika eden od pomembnih vidikov komunikacijske zasebnosti" in da je bilo treba za njeno razkritje pridobiti odredbo sodišča v skladu z drugim odstavkom 37. člena ustave (glej 18. odstavek odločbe ustavnega sodišča, naveden v 29 odstavku zgoraj). Natančneje, v skladu z razlago ustavnega sodišča, ki je bila usklajena s predhodno ugotovitvijo sodne prakse, da podatki o prometu, kakor so opredeljeni v domači zakonodaji, spadajo v okvir varstva 37. člena ustave (prav tam), je razkritje podatkov o naročniku, povezanih z določenim dinamičnim IP-naslovom, načeloma zahtevalo odredbo sodišča in jih ni bilo mogoče pridobiti z enostavno pisno zahtevo policije.

129. Sodišče ugotavlja, da je bil v resnici edini razlog, da je ustavno sodišče zavrnilo pritožnikovo pritožbo – zaradi odobritve razkritja podatkov o naročniku brez odredbe sodišča – predvidevanje, da se je pritožnik "odrekel upravičenemu pričakovanju zasebnosti" (glej 18. odstavek odločbe ustavnega sodišča, naveden v 29. odstavku zgoraj). Vendar pa je ob upoštevanju svojih ugotovitev glede na uporabo 8. člena Sodišče mnenja, da stališče ustavnega sodišča glede tega vprašanja ni združljivo z obsegom pravic do zasebnosti v skladu s konvencijo (glej 115. – 118. odstavek zgoraj). Ob upoštevanju ugotovitve ustavnega sodišča, da "identiteto komunicirajočega posameznika" varuje 37. člen ustave (glej 128. odstavek zgoraj) in sklepa Sodišča, da je pritožnik upravičeno pričakoval, da bo njegova identiteta v zvezi s spletno dejavnostjo ostala zasebna (glej 115. - 118. odstavek zgoraj), je bila v obravnavanem primeru potrebna odredba sodišča. Poleg tega nič v domači zakonodaji ni preprečevalo policiji, da bi jo pridobila, glede na to, da je nekaj mesecev po pridobitvi podatkov o naročniku, v času katerih očitno niso bili v zadevi narejeni nobeni preiskovalni koraki, zahtevala in pridobila odredbo sodišča, kakor se zdi vsaj deloma, za iste podatke, kot so bili tisti, ki jih je že imela (glej 8. odstavek zgoraj). Opiranje domačih organov oblasti na tretji odstavek 149. b člena ZKP je bilo torej očitno neustrezno in kar je še pomembnejše, omogočalo ni skoraj nobenega varstva pred samovoljnim posegom.

130. V tej zvezi Sodišče ugotavlja, da se zdi, da v tistem času ni bilo predpisa, ki bi določal pogoje za hrambo podatkov, pridobljenih v skladu s tretjim odstavkom 149. b člena ZKP, in nobenih varoval proti zlorabi s strani državnih uradnikov v postopkih za dostop do podatkov in sporočanje teh podatkov. Glede zadnjega navedenega bi lahko policija, ki je imela na voljo podatke o določeni spletni dejavnosti, identificirala avtorja samo s tem, da bi od ponudnika internetnih storitev zahtevala, naj poišče te podatke. Poleg tega se je izkazalo, da v tistem času ni bilo neodvisnega nadzora nad uporabo teh policijskih pooblastil, kljub dejstvu, da so ta pooblastila, kakor so jih razlagala domača sodišča, prisilila ponudnika internetnih storitev, da je pridobil shranjene podatke o povezavah in omogočil policiji, da je povezala velik del informacij o spletni dejavnosti z določenim posameznikom brez njegovega pristanka (glej 108. in 109. odstavek zgoraj).

131. Sodišče nadalje ugotavlja, da je kmalu potem, ko je bil proti pritožniku sprejet izpodbijani ukrep, Državni zbor sprejel spremembe k ZEKom (glej 38. odstavek zgoraj, kakor tudi ustrezne določbe poznejšega novega zakona, navedenega v 39.) Te spremembe so, me drugim, določale predpise o hrambi podatkov v zvezi z izvorom komunikacij, to je, *inter alia*, ime in naslov naročnika, ki mu je bil določeni IP-naslov dodeljen, ter postopek za dostop do njih in njihovo posredovanje. Vendar pa to ni vplivalo na pritožnikov položaj.

132. Ob upoštevanju zgoraj navedenega Sodišče meni, da je zakon, na katerem je temeljil izpodbijani ukrep, to je pridobitev podatkov o naročniku s strani policije, povezanih z obravnavanim dinamičnim IP-naslovom (glej 7. odstavek zgoraj), ki so ga domača sodišča uporabila, nejasen in ni dajal zadostnih varoval proti samovoljnemu poseganju v pravice iz 8. člena.

133. V teh okoliščina Sodišče ugotavlja, da poseg v pritožnikove pravice do spoštovanja njegove zasebnosti ni bil "v skladu z zakonom", kot to zahteva drugi odstavek 8. člena konvencije. Posledično ni potrebno, da Sodišče preuči, ali je imel izpodbijani ukrep legitimen cilj in ali je bil sorazmeren.

134. Ob preučitvi zgoraj navedenega Sodišče razsoja, da je bil kršen 8. člen konvencije.

II. UPORABA 41. ČLENA KONVENCIJE

135. 41. člen konvencije določa:

> "Če Sodišče ugotovi, da je prišlo do kršitve konvencije ali njenih protokolov, in če notranje pravo visoke pogodbenice dovoljuje le delno zadoščenje, Sodišče oškodovani stranki, če je potrebno, nakloni pravično zadoščenje."

A. Škoda

136. Pritožnik je zahteval 32.000 evrov (EUR) za nepremoženjsko škodo, ki so vključevali 7.000 EUR za stisko, ki jo je utrpel zaradi sojenja proti

njemu, 15.000 EUR, ker je bil neupravičeno zaprt, in 10.000 EUR za stigmatizacijo v družbi zaradi obsodbe.

137. Vlada je trdila, da je bil zahtevek pritožnika za nepremoženjsko škodo neutemeljen in pretiran. Nadalje je trdila, da ni bilo povezave med kršitvijo 8. člena in obravnavano zadevo ter zatrjevano nepremoženjsko škodo in pritožnikovo kazensko obsodbo ter kaznijo zapora. Tudi če bi bili obravnavani podatki izključeni iz dosjeja, se pritožnik ne bi mogel izogniti kazenskemu postopku. Poleg tega je vlada trdila, da ker je pritožnik priznal, da bi lahko zahteval obnovo postopka, če bi bila kršitev ugotovljena, zato bi morala zadoščati deklarativna sodba Sodišča s katero bi ugotovilo kršitev.

138. Sodišče je mnenja, da je ugotovitev kršitve zadostno pravično zadoščenje za vso nepremoženjsko škodo, ki jo je utrpel pritožnik.

B. Stroški in izdatki

139. Pritožnik je tudi zahteval 4.335,50 EUR za stroške in izdatke, ki so nastali pred domačimi sodišči, in 2.600 EUR za stroške in izdatke, ki so nastali pred Sodiščem in davek na dodano vrednost (DDV). Trdil je, da sta bili ti vsoti izračunani na podlagi uradne odvetniške tarife.

140. Vlada je trdila, da so stroški, povrnitev katerih je pritožnik zahteval v zvezi z njegovim zastopanjem v domačih postopkih, vključevali DDV. Vključevali so tudi stroške pravnega mnenja, in sicer 2.000 EUR, ki očitno ni bilo izdelano za namene zastopanja v domačih postopkih. Glede zahtevka v zvezi s postopkom pred Sodiščem je vlada trdila, da je bil pretiran. Poleg tega razen računa za zgoraj navedeno pravno mnenje pritožnik ni predložil nobenega dokaza, da je imel stroške zaradi pravnega zastopanja.

141. V skladu s sodno prakso Sodišča je pritožnik upravičen do povrnitve stroškov in izdatkov samo, če dokaže, da so ti dejansko nastali in bili neizogibni ter da je njihov znesek razumen. Sodišče ob upoštevanju razpoložljivih dokumentov in navedenih meril v obravnavani zadevi meni, da je razumno prisoditi 922 EUR za stroške in izdatke v domačih postopkih in 2.600 EUR za postopke pred Sodiščem. Zato je pritožniku za stroške in izdatke treba priznati skupaj 3.522 EUR.

C. Zamudne obresti

142. Po mnenju Sodišča je primerno, da zamudne obresti temeljijo na mejni posojilni obrestni meri Evropske centralne banke, ki se ji dodajo tri odstotne točke.

IZ TEH RAZLOGOV SODIŠČE

1. *odloča* s šestimi glasovi proti enemu, da se združi odločanje o utemeljenosti pritožbe z ugovorom vlade glede tega, da pritožnika ni mogoče šteti za žrtev razkritja podatkov o naročniku po 8. členu konvencije, ter *ga zavrne;*

2. z večino glasov *razglaša*, da je pritožba glede razkritja podatkov o naročniku po 8. členu konvencije sprejemljiva, preostali del pritožbe pa nesprejemljiv;

3. *razsoja* s šestimi glasovi proti enemu, da je bil kršen 8. člen konvencije;

4. soglasno *razsoja*, da je ugotovitev kršitve zadostno pravično zadoščenje za nepremoženjsko škodo pritožnika;

5. *razsoja* s šestimi glasovi proti enemu,
   a) da mora tožena država pritožniku v treh mesecih od dne, ko postane sodba v skladu z drugim odstavkom 44. člena konvencije pravnomočna, plačati 3.522 EUR (tri tisoč petsto dvaindvajset evrov) za stroške in izdatke ter morebitni davek, obračunan pritožniku;
   b) da se za navedeni znesek od dneva poteka treh mesecev do plačila obračunajo linearne obresti po stopnji, ki je enaka stopnji mejne posojilne obrestne mere Evropske centralne banke, za vse zamujeno obdobje z dodanimi tremi odstotnimi točkami;

6. soglasno *zavrača* preostali del zahtevka pritožnika za pravično zadoščenje.

Sestavljeno v angleškem jeziku in 24. aprila 2018 poslano v pisni obliki v skladu z drugim in tretjim odstavkom 77. člena Poslovnika Sodišča.

Andrea Tamietti	Ganna Yudkivska
namestnik sodnega tajnika	predsednica

V skladu z drugim odstavkom 45. člena konvencije in drugim odstavkom 74. člena Poslovnika Sodišča sta tej sodbi priloženi naslednji ločeni mnenji:

a) pritrdilno ločeno mnenje sodnice G. Yudkivske, ki se mu je pridružil sodnik M. Bošnjak;

b) odklonilno ločeno mnenje sodnika F. Vehabovića.

G. Y.
A. N. T.

PRITRDILNO LOČENO MNENJE SODNICE YUDKIVSKE, KI SE MU JE PRIDRUŽIL SODNIK M. BOŠNJAK

Strinjam se z izidom sodbe kakor tudi z metodologijo, ki jo je uporabila večina. Vendar pa me preseneča očitna težavnost, s katero je bil dosežen sklep o obstoju poseganja v tej zadevi in zlasti zelo previden pristop k upravičenemu pričakovanju zasebnosti v 115.–118. odstavku.

Obravnavana zadeva je bila enkratna priložnost za razjasnitev obsega upravičenega pričakovanja zasebnosti v digitalni dobi, kjer se osupljiva količina informacij o našem zasebnem življenju z lahkoto razpošilja naokoli brez našega nadzora. "Civilizacija je napredek v smeri družbe zasebnosti", je izjavila Ayn Rand[1]. Sodobna realnost pa je, da zasebnost postaja vse bolj cenjena vrednota, ki zahteva vsak dan večje varstvo. Nešteti učenjaki so že razglasili "smrt", "konec" ali "uničenje" zasebnosti.[2] Pogosto slišimo, da bi za zaščito zasebnosti v sodobnem času morali ponovno preučiti zastarelo pojmovanje zasebnosti kot zgolj tajnosti in narediti korak v smeri pravne zaščite zaupanja in zaupnosti ter pravice do nadzora nad razširjanjem in uporabo informacij.[3] Kot sodnikom nam je zaupana naloga, da v zadevah, kot je obravnavana, ponovno presodimo paradigmo zasebnosti.

V tej zadevi se je Sodišče prvič poglobilo v preučevanje internetnega protokola in oblik dodeljevanja IP-naslovov, in sicer statičnega in dinamičnega – do obsega, ki je bil v teh okoliščinah potreben. V zadevi Benedik obravnavamo dinamični IP-naslov, tj. naključno dodeljevanje novih IP-naslovov iz množice naslovov, dodeljenih ponudniku internetnih storitev vsakokrat, ko se uporabnik priključi na internet. Danes je dodeljevanje dinamičnih IP-naslovov najbolj običajna oblika za uporabnike interneta in zato bodo sklepi Sodišča glede zasebnosti v obravnavani zadevi vplivali na veliko večino uporabnikov interneta po vsej Evropi.

Postalo je običajno, da se v razpravah o zasebnosti opozarja, da pravni pojem zasebnosti ni bil jasen, dokler Samuel D. Warren in Louis D. Brandeis nista že leta 1890 objavila njunega odmevnega članka "Pravica do zasebnosti". Tisto, kar je vredno omembe, je, da ju je spodbudila zaskrbljenost, da bodo sodobne tehnologije, in sicer nedavno izumljena prenosna kamera in skokovit razvoj tiskanih medijev, razkrila neželene podrobnosti o življenju navadnih ljudi: "Takojšnje fotografije in časopisna podjetja so vdrla v nedotakljiv prostor zasebnega in domačega življenja; in

1. Ayn Rand, The Fountainhead.
2. Glej Daniel Solove, “Speech, Privacy and Reputation on the Internet” (Govor, zasebnost in ugled na internetu") pri: Saul Levmore in Martha Nussbaum, urednika, The Offensive Internet (Žaljivi internet): Speech, Privacy, and Reputation, (Govor, zasebnost in ugled na internetu") Cambridge, Mass.: Harvard University Press, 2011, z nadaljnjimi sklicevanji.
3. Prav tam, str. 20 in 22.

številne mehanske naprave grozijo, da bodo uresničile prerokbo, da 'kar se šepeta v sobici, bo razglašeno s streh hiš'."[4]

Od takrat je vsak razvoj obstoječih tehnologij in nastanek novih sprožil ponovno preučitev doktrine zasebnosti in njenih upravičenih pričakovanj: od zaskrbljenosti glede spremljanja telefonskih pogovorov na začetku 20. stoletja do široke razprave o množičnem nadzoru, zbiranju in predelavi metapodatkov na začetku 21. stoletja. Že leta 1966 je sodnik William Douglas v svojem odklonilnem ločenem mnenju v zadevi *Osborn proti Združenim državam* opozoril: "Hitro vstopamo v dobo brez zasebnosti, kjer je vsakdo lahko ves čas nadzorovan; kjer ni skrivnosti pred vlado".[5] Tehnične možnosti, ki danes obstajajo, so veliko bolj invazivne, kot bi si sodnik Douglas pred približno petdesetimi leti sploh lahko zamišljal. Široka razširjenost interneta pomeni samo novo stopnjo jakosti glede stare težave.

Pojem "upravičeno pričakovanje zasebnosti" je Sodišče uporabilo v več zadevah, vključno z obravnavano, vendar je ta pojem prišel k nam z Vrhovnega sodišča Združenih držav, kjer so ga uporabili v zadevi *Katz proti Združenim državam*[6], ki je obravnavala FBI-jevo uporabo prisluškovalnih naprav za prejemanje pogovorov o nezakonitih igrah na srečo, ki jih je osumljenec opravil iz javne telefonske govorilnice. Kakor je ugotovilo vrhovno sodišče, "nič manj kakor posameznik v poslovni pisarni, prijateljevem stanovanju ali taksiju, se lahko oseba v telefonski govorilnici zanese na varstvo četrtega amandmaja. Tisti, ki zaseda telefonsko govorilnico, zapre vrata za seboj in plača uporabnino, ki mu omogoča, da naredi klic, je gotovo upravičen predvidevati, da besede, ki jih izreče v telefonsko slušalko, ne bodo objavljene svetu."

Pritrdilno ločeno mnenje sodnika Harlana je bilo tisto, ki je uvedlo ta posebni koncept: napisal je, da "razume pravilo, ki je izviralo iz predhodnih odločitev, kot pravilo z dvojno zahtevo": Prvič, da je oseba "pokazala dejansko (subjektivno) pričakovanje zasebnosti", in drugič, da je družba pripravljena priznati, da je to pričakovanje (objektivno) upravičeno. Ta preizkus je bil pozneje citiran v sodni praksi vrhovnega sodišča v zvezi s četrtim amandmajem.

Koncept "upravičenega pričakovanja zasebnosti" je to Sodišče prvič uporabilo v zadevi *Halford proti Združenemu kraljestvu*[7]. V omenjeni zadevi je Sodišče sklenilo, da je policist upravičeno pričakoval zasebnost telefonskih klicev, opravljenih na delovnem mestu, ob odsotnosti kakršnega koli opozorila, da bi bili ti klici lahko prestreženi. Sodišče se je sklicevalo na isti

4. Warren & Brandeis, the Right to Privacy (Pravica do zasebnosti), 4 HARV. L. REV. 193 (1890).
5. Katz Osborn proti Združenim državam, 385 ZDA 323 (1966).
6. Zadeva Katz proti Združenim državam, 389 ZDA 347 (1967).
7. Zadeva *Halford proti Združenemu kraljestvu*, 25. junij 1997, *Reports of Judgments and Decisions* 1997-III (*Poročila o sodbah in sklepih* 1997-III.)

koncept deset let pozneje v zadevi *Copland proti Združenemu kraljestvu*[8], ob ugotovitvi, da je ob odsotnosti kakršnega koli opozorila uslužbenka visokošolske ustanove upravičeno pričakovala zasebnost elektronskih sporočil, ki jih je poslala s svojega poštnega naslova visokošolske ustanove.

Nedavno je bil koncept omenjen pred velikim senatom v zadevi *Bărbulescu proti Romuniji*[9]. Zadeva je obravnavala odpoved, ki jo je dobil pritožnik potem, ko je bila nadzorovana njegova elektronska komunikacija, večinoma prek računa Yahoo Messenger, za katerega je bilo pritožniku naročeno, naj ga ustvari za komuniciranje s strankami. Ugotovljeno je bilo, da je med delovnim časom uporabljal internet za svoje osebne namene in s tem kršil interni poslovnik. Sodišče je vprašanje, ali je pritožnik upravičeno pričakoval zasebnost, pustilo odprto, ne glede na jasna navodila delodajalca, naj se vzdrži vseh osebnih dejavnosti na delovnem mestu, ker "delodajalčeva navodila ne morejo zmanjšati zasebnega družbenega življenja na delovnem mestu na ničlo."

Obravnavana zadeva sproža vprašanje upravičenega pričakovanja zasebnosti, kadar gre za podatke o prometu (vodenje evidence klicnih številk ali metapodatke), in obžalujem, da je Sodišče izpustilo priložnost za zavzetje jasnega stališče glede tega. Zanimiva razprava o tej temi je na Ustavnem sodišču Slovenije (glej 28.–34. odstavek sodbe) ostala neobravnavana.

Podobne razprave potekajo v ameriškem sodstvu. V skladu z izvornim konceptom ustavnega prava Združenih držav se je vrhovno sodišče jasno opredelilo, da medtem ko se lahko reče, da je pričakovanje zasebnosti upravičeno v zvezi z vsebino, pa takšnega pričakovanja ni, ko gre za metapodatke (podatke o prometu). Pred približno štiridesetimi leti je vrhovno sodišče v zadevi *Smith proti Marylandu*[10] obravnavalo ravnanje z metapodatki telefonskih družb, ki so imele podatke o klicanih telefonskih številkah in trajanju pogovorov. Ugotovilo je, da "je preveč domnevati, da imajo telefonski naročniki v takšnih okoliščinah kakršna koli splošna pričakovanja, da bodo številke, ki jih kličejo, ostale tajne." Zato v skladu s tem konceptom posameznik nima upravičenega pričakovanja zasebnosti glede te vrste informacij.

Ameriška sodišča so razlagala, da "doktrina tretje osebe", vzpostavljena v zadevi *Smith,* velja za IP-naslove, ter odločila, da uporabniki interneta ne morejo upravičeno pričakovati zasebnosti pri njihovih IP-naslovih, saj so jih prostovoljno predali tretjim osebam – uporabnikovemu ponudniku internetnih storitev in ponudnikom spletnih storitev[11], z ugotovitvijo, da "sam

8. Zadeva *Copland proti Združenemu kraljestvu*, št. 62617/00, ESČP 2007-I.
9. GC, št. 61496/08, ESČP 2017 (povzetki).
10. Zadeva Smith proti Marylandu, 442 ZDA 735 (1979).
11. Glej Alexandra D. Vesalga, Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data, (Alexandra D. Vesalga, Lokacija, lokacija, lokacija: Posodobitev Zakona o zasebnosti elektronskih komunikacij za zaščito podatkov o geolokaciji) 43 GOLDEN GATE U.L.REV. 459(2013),

dostop do omrežja sam po sebi ne odpravi pričakovanj zasebnosti"[12] in da "imajo posamezniki upravičena pričakovanja zasebnosti glede vsebine njihovih računalnikov"[13]. Ne glede na to je leta 2008 sodišče višje stopnje v New Jerseyu sprejelo sodbo v zadevi *država proti Reid*, [14]z obrazložitvijo, da "posamezniki potrebujejo naslov ponudnika internetnih storitev za dostop do interneta. Vendar ko uporabniki brskajo po spletu v zasebnosti svojih domov, z razlogom pričakujejo, da so njihova dejanja zaupna. Mnogi se ne zavedajo, da njihov numerični IP-naslov lahko zabeležijo spletne strani, ki jih obiskujejo. Bolj napredni uporabniki vedo, da edinstveni niz številk sam po sebi zunanjemu svetu razkriva malo, če sploh kaj. Samo ponudnik internetnih storitev lahko prevede IP-naslov v uporabnikovo ime."

Sodišče v New Jerseyu je potem nadaljevalo z izjemno pomembnim preoblikovanjem vzorca zasebnosti, ki so ga spodbudile sodobne internetne dejavnosti: "... medtem ko dekodirani IP-naslovi ne razkrivajo vsebine internetnih komunikacij, pa podatki o naročniku lahko veliko povedo o posamezniku. S celotnim navajanjem IP-naslovov je mogoče slediti posameznikovi uporabi interneta... Takšne informacije lahko razkrijejo intimne podrobnosti o posameznikovih osebnih zadevah na enak način, kot ga razkrijejo zapisi klicev na telefonskem računu. Čeprav so lahko vsebine internetnih komunikacij celo bolj razkrivajoče, pa obe vrsti informacij vključujeta interese zasebnosti".

Po mojem mnenju je to ključni izziv, ki ga je treba jasno artikulirati – podatki o prometu ali metapodatki se danes zbirajo veliko širše kot podatki o vsebini (dejanski vsebini komunikacij) in takšno poseganje je treba "vnaprej vzpostaviti z zakonom in ga določiti izrecno, izčrpno, natančno in jasno ter vsebinsko in postopkovno" z opredelitvijo "vzrokov in pogojev, ki bodo državi omogočali prestrezanje komunikacij posameznikov, zbiranje podatkov o komunikacijah ali "metapodatkov" ali uvedbo njihovega nadzora ali spremljanja, ki vdira na področja, na katerih upravičeno pričakujejo zasebnost."[15] Resolucija Parlamentarne skupščine Sveta Evrope o množičnem nadzoru (PACE Resolution on Mass Surveillance)[16] je pozvala države članice Sveta Evrope "naj zagotovijo, da njihova domača zakonodaja omogoča zbiranje in analizo osebnih podatkov (*vključno s tako imenovanimi metapodatki*) samo s pristankom zadevne osebe, ali potem, ko je bila izdana

---

s sklicevanjem na zadeve Združene države proti Bynum, 604 F.3d 161, 164 & n.2 (4th Cir. 2010); Združene države proti Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); Združene države proti Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008), itd.

12. Zadeva Združene države proti Heckenkamp, 482 F.3d 1 142, 1 146 (9th Cir. 2007).
13. Zadeva Združene države proti Howe, 2011 WL 2160472 at. 7 (W. D. N . Y. 27. maj, 2011).
14. Zadeva Država proti Reid, 945 A.2d 26, 28 (N. J. 2008).
15. Urad posebnega poročevalca za svobodo izražanja medameriške komisije za človekove pravice, svobodo izražanja in internet (31. december 2013).
16. Resolucija Parlamentarne skupščine Sveta Evrope (PACE) o množičnem nadzoru 2045 (21. april 2015).

odredba sodišča na podlagi utemeljenega suma, da je ciljna oseba vpletena v kriminalno delovanje ...".

Zdi se, da je sprejeto, da je bilo zbiranje metapodatkov razumljeno (in je še vedno) kot manj vsiljivo od zbiranja vsebin. V predinternetni dobi leta 1984 je Evropsko sodišče za človekove pravice odločilo, da medtem ko je zbiranje vsebin večje poseganje kot zbiranje metapodatkov, pa je zbiranje metapodatkov še vedno poseganje po 8. členu. To je bil primer v zadevi *Malone proti Združenemu kraljestvu*[17], kjer je policija uporabila sredstva, ki so beležila številke, klicane z določenega telefona, kakor tudi čas in trajanje vsakega klica – brez prestrezanja pogovorov. Vlada je trdila, da zbiranje takšnih informacij ni pomenilo poseganja v pravice, ki jih jamči 8. člen.

Sodišče je v zadevi *Malone* ugotovilo, da "ne sprejema …, da uporaba podatkov, pridobljenih z vodenjem evidence klicnih številk, kakšne koli so že okoliščine in nameni, ne more sprožiti vprašanja na podlagi 8. člena", saj so bile klicane številke "sestavni del komunikacije po telefonu" in je izročitev teh podatkov s strani ponudnika telefonskih storitev policiji brez naročnikovega pristanka pomenila poseganje v pravico, ki jo jamči 8. člen (zadeva *Malone*, 84. odstavek).

To mnenje bi moralo biti danes bistveno okrepljeno. Stališče, da metapodatki ne potrebujejo enake ravni varstva kot vsebinski podatki, je razrahljano, saj je soočeno z realnostjo sedanjosti: zdaj je toliko oblik metapodatkov – od telefonskih klicev, elektronske pošte, spletnih naprav, ki pokažejo vašo zgodovino iskanja, do Googlovih zemljevidov, ki prikazujejo vašo lokacijo, itd.; in če se vsi ti podatki združijo, se dobi izrazito prodoren portret zadevne osebe, ki odkriva njeno osebne in poklicne odnose, etnični izvor, politična nagnjenja, verska prepričanja, članstvo v različnih skupinah, finančni položaj, zgodovino nakupov ali bolezni in tako naprej. Da bi pridobili te podatke, se nam ni treba mučiti s poslušanjem pogovorov ali branjem pisem kot v dobrih starih časih. Ta točka je bila poudarjena v resoluciji Sveta Združenih narodov za človekove pravice o pravici do zasebnosti v digitalni dobi, ki je ugotovila, da "medtem ko metapodatki mogoče zagotavljajo koristi, pa lahko določene vrste metapodatkov, ko so združene, odkrijejo osebne podatke, ki niso lahko nič manj občutljivi kot dejanska vsebina komunikacij in lahko dajo vpogled v posameznikovo obnašanje, socialne odnose, osebna nagnjenja in identiteto"[18].

V svoji knjigi "Data and Goliath" ("Podatki in Goljat")[19], posebej posvečeni "zlati dobi nadzora", vodilni strokovnjak za varnost navaja zelo zanimiv primer poskusa, opravljenega na univerzi v Stanfordu, v katerem je

17. Zadeva *Malone proti Združenemu kraljestvu*, 2. avgust 1984, serija A št. 82.
18. Resolucija Sveta Združenih narodov za človekove pravice o pravici do zasebnosti v digitalni dobi, ZN Doc. A/HRC/34/L.7/Rev.1 (22. marec 2017).
19. Bruce Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" ("Podatki in Goljat: Skrite bitke za zbiranje vaših podatkov in nadzorovanje vašega sveta"), New York, N. Y.: W. W. Norton & Company, 2015.

preiskoval telefonske metapodatke mnogih ljudi in med njimi zlahka prepoznal – samo z uporabo podatkov o prometu njihovih različnih telefonskih klicev – žrtev srčnega napada, osebo, ki je doma gojila marihuano, in nosečnico, ki je načrtovala splav.

Zbiranje in združevanje več vrst varovanih podatkov iz različnih virov ustvarja nova tveganja za človekove pravice, pred katerimi si to Sodišče ne more zatiskati oči, glede na to, da skoraj vse, kar počnemo, pušča digitalni odtis.

Pritožnik v obravnavani zadevi je tako kot vsi drugi uporabniki interneta užival anonimnost, saj je dinamični IP-naslov lahko povezan s posameznikovo identiteto samo, če ga ponudnik storitev posebej razkrije po predložitvi ustrezne zahteve. Zato ne sme biti dvoma, da so bila njegova pričakovanja zasebnosti popolnoma legitimna, ne glede na zaničevanja vredno nezakonitost njegovih dejavnosti, kot je pojasnjeno v 99. odstavku (če bi bil poseg v skladu z zakonom, bi Sodišče nadaljevalo z nadaljnjo preiskavo njegove ustreznosti in vrsta kaznivega dejanja bi bila ustrezno preučena).

Glede na navedeno menim, da bi Sodišče moralo nedvomno ugotoviti, da so glede na tehnično anonimnost IP-naslovov pričakovanja uporabnikov interneta pri brskanju po spletu v zvezi z zasebnostjo upravičena. Nadaljnja obdelava teh metapodatkov se sme izvajati samo v skladu z zakonom, ki ustreza zahtevam glede kakovosti, kot je navedeno zgoraj.

Varstvo zasebnosti je ključni dosežek evropske politične in pravne kulture, ne nazadnje zato, ker je bilo oblikovana na izkušnjah grozot nacističnega in komunističnega režima. Dolgoročno bo zasebnost ostala temeljna pravica samo tako dolgo, dokler jo bo družba branila, in bo izginila, ko jo bo družba prenehala razumeti kot temeljno vrednoto. Upravičeno pričakujemo, da bo naša zasebnost varovana tudi na spletu. Naša temeljna pravica, imeti nadzor nad tem, kako se predstavljamo zunanjemu svetu, je bistvena in to stališče bi moralo Sodišče krepiti.

ODKLONILNO LOČENO MNENJE SODNIKA VEHABOVIĆA

Nisem glasoval z večino, ki je ugotovila, da je bil kršen 8. člen konvencije v zvezi s pritožnikovim upravičenim pričakovanjem zasebnosti in poseganjem v pritožnikove pravice v skladu z 8. členom konvencije.

Podatki, ki jih je 7. avgusta 2006 razkril ponudnik internetnih storitev (ISP), niso bili podatki o prometu ali osebni podatki v zvezi s pritožnikom; bila sta naslov in ime pritožnikovega očeta, ki je bil naročnik internetnih storitev. Glede na to dejstvo se zdi, da pritožnik ni mogel trditi, da je bil žrtev, saj so se podatki o naročniku, ki jih je ponudnik internetnih storitev razkril policiji, nanašali na njegovega očeta, ki pa v tej zadevi ni pritožnik, kot je poudarila vlada.

Utemeljeni sum prenosa datotek, ki so vključevale otroško pornografijo, ki je kaznivo dejanje, je od lokalnih organov oblasti zahteval nadaljnjo preiskavo, in podatki v zvezi s pritožnikom, to je podatki o prometu, ki so se nanašali na internetne dejavnosti, izvajane s tega IP-naslova, so bili razkriti policiji 14. decembra 2006 potem, ko je okrožno sodišče izdalo odredbo, ki je od ponudnika internetnih storitev zahtevala razkritje osebnih podatkov naročnika in podatkov o prometu, povezanih z zadevnim IP-naslovom. Poleg zgoraj navedenega je 12. januarja 2007 preiskovalni sodnik Okrožnega sodišča v Kranju izdal nalog za hišno preiskavo in šele potem je bil pritožnik povezan z obravnavanimi podatki o prometu in šele od tedaj pritožnik lahko zatrjuje, da je bil žrtev.

Po mojem mnenju pridobljeni IP-naslov, ki je pripeljal do naslova in imena pritožnikovega očeta, ne zadošča, da bi se kvalificiral kot osebni podatek pritožnika, saj ni razkril identitete in podatkov o prometu ne pritožnika ne njegovega očeta.

Ob številnih priložnostih se je Sodišče sklicevalo na Konvencijo o varstvu podatkov, ki v 2. členu osebne podatke opredeljuje kot katero koli informacijo, ki se nanaša na določenega ali določljivega posameznika (glej *Satakunnan Markkinapörssi Oy in Satamedia Oy* proti Finski, 931/13, 133. odstavek, in *Amann* proti Švici 27798/95, 65. odstavek). Lokalne oblasti niso prejele podatkov o pritožniku; pritožnik ni bil določen ali določljiv posameznik, preden je bila izdana odredba sodišča, ki je bila podlaga za ugotovitev Sodišča o kršenju 8. člena konvencije. Zato se ne strinjam z ugotovitvijo večine, da je šlo za poseg v pravico pritožnika po prvem odstavku 8. člena konvencije.

V zvezi z upravičenim pričakovanjem zasebnosti se ne strinjam, da bi bilo treba upoštevati subjektivno pritožnikovo pričakovanje zasebnosti, kadar gre za obravnavo kaznivega delovanja. V skoraj vseh zadevah storilci kaznivih dejanj ne želijo, da bi drugi vedeli za njihova dejanja. Ta vrsta pričakovanja zasebnosti ne bi bila upravičena, če temelji na nezakoniti ali kakor v tem primeru kaznivi pobudi. Pričakovanje skrivanja kaznivega delovanja ne bi

smelo veljati za upravičeno. Pri drugem vprašanju v zvezi z upravičenim pričakovanjem zasebnosti je pritožnik izmenjeval datoteke, ki so vključevale otroško pornografijo (kar je senat, po mojem mnenju, namenoma izpustil iz 115. odstavka), prek javnega omrežnega računa, ki je bil viden drugim. Pritožnik je zato vedel, ali bi moral vedeti, da njegova dejanja niso anonimna. Pritožnik v času v času storitve kršitve ni imel namena skrivati svoje kršitve.

Poleg tega je bilo Sodišče v številnih zadevah, v katerih je bila ugotovljena kršitev, mnenja, da je preprečevanje kaznivih dejanj legitimen cilj. Na primer v zadevi *Nada proti Švici* je Sodišče odločilo, da "se ni zdelo, da bi pritožnik zanikal, da so bile sporne omejitve naložene zaradi uresničevanja legitimnih ciljev. Sodišče je ugotovilo, da so si te omejitve prizadevale za uresničitev enega ali več legitimnih ciljev, navedenih v drugem odstavku 8. člena; prvič, prizadevale so si preprečiti kazniva dejanja" (*Nada proti Švici,* 10593/08, 174. odstavek). Tudi v zadevi *S. in Marper proti Združenemu kraljestvu*"se Sodišče strinja z vlado, da je cilj hrambe prstnih odtisov in podatkov o DNA legitimni namen odkrivanja in torej preprečevanje kaznivih dejanj. Medtem ko je izvorno jemanje teh podatkov imelo za cilj povezovanje določene osebe z določenim kaznivim dejanjem, ki ga je bila osumljena, pa ima njihova hramba širši namen pomoči pri identifikaciji prihodnjih storilcev kaznivih dejanj" (glej *S. in Marper proti Združenemu kraljestvu*, 30562/04 30566/04, 100. odstavek). Zato se ne strinjam z ugotovitvijo večine, da je v obravnavani zadevi šlo za poseg v pravice pritožnika po prvem odstavku 8. člena konvencije.