Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
ANTHONYJA MICHAELA COLLINSA,
predstavljeni 8. junija 2023 [1]

Zadeva C-178/22

Neznani posamezniki
ob udeležbi
Procura della Repubblica presso il Tribunale di Bolzano

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Tribunale di Bolzano (sodišče v Bolzanu, Italija))

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Zaupnost komunikacij – Ponudniki elektronskih komunikacijskih storitev – Direktiva 2002/58/ES – Člena 1(3) in 15(1) – Listina Evropske unije o temeljnih pravicah – Členi 7, 8, 11 in člen 52(1) – Zahteva državnega tožilstva za dostop do podatkov zaradi preiskave in pregona velike tatvine mobilnega telefona – Opredelitev pojma ‚hudo kaznivo dejanje‘, ki upravičuje hud poseg v temeljne pravice – Obseg predhodnega nadzora, da se zagotovi upoštevanje zahteve glede hudih kaznivih dejanj – Načelo sorazmernosti“

I. Uvod

1. Procura della Repubblica presso il Tribunale di Bolzano (državno tožilstvo pri sodišču v Bolzanu, Italija; v nadaljevanju: državno tožilstvo (Bolzano)) od Tribunale di Bolzano (sodišče v Bolzanu, Italija) zahteva odobritev dostopa do podatkov, ki jih ponudniki elektronskih komunikacijskih storitev hranijo na podlagi nacionalne zakonodaje, ki med drugim omogoča sledenje in identifikacijo vira in cilja komunikacije z mobilnega telefona.

2. V okviru navedene zahteve Tribunale di Bolzano (sodišče v Bolzanu) Sodišče prosi za razlago člena 15(1) Direktive 2002/58/ES. [2] Navedena določba državam članicam omogoča uvedbo zakonodajnih izjem od obveznosti iz navedene direktive, [3] da se zagotovi zaupnost elektronskih komunikacij. V sodbi v zadevi Prokuratuur [4] je Sodišče ugotovilo, da dostop do podatkov, ki omogoča natančno sklepanje o uporabnikovem zasebnem življenju, v okviru ukrepov, sprejetih

[1] Jezik izvirnika: angleščina.

[2] Direktiva 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, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514, in popravek v UL 2013, L 241, str. 9), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11, in popravek v UL 2013, L 241, str. 9).

[3] Glej člen 5 Direktive 2002/58. Varstvo zaupnosti elektronskih komunikacij, ki ga zagotavlja člen 5(1) Direktive 2002/58, se uporablja za ukrepe vseh oseb, razen uporabnikov, ne glede na to, ali gre za javne ali zasebne osebe. Sodba z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 36 in navedena sodna praksa).

[4] Sodba z dne 2. marca 2021, Prokuratuur (Pogoji dostopa do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2021:152; v nadaljevanju: sodba v zadevi Prokuratuur).

na podlagi člena 15(1) Direktive 2002/58, pomeni hud poseg v temeljne pravice in načela iz členov 7, 8 in 11 ter člena 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).[5] Takega posega ni mogoče odobriti zaradi preprečevanja, preiskovanja, odkrivanja in pregona „kaznivih dejanj na splošno“. Odobri se lahko le v postopkih, povezanih z bojem proti „hudemu kriminalu“[6], zanj pa mora veljati predhodni preizkus sodišča ali neodvisnega upravnega organa, da se zagotovi skladnost z navedeno zahtevo.[7] Tribunale di Bolzano (sodišče v Bolzanu) je prosilo Sodišče, naj pojasni dva vidika sodbe v zadevi Prokuratuur: pojem „hudega kriminala [kaznivega dejanja]“ ter obseg predhodnega preizkusa, ki ga mora opraviti sodišče na podlagi določbe nacionalne zakonodaje, ki od sodišča zahteva odobritev dostopa do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev.

II. Pravni okvir

A. Pravo Evropske unije

3. Člen 5 Direktive 2002/58 z naslovom „Zaupnost sporočil“ določa:

„1. Države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Zlasti prepovejo vsem osebam razen uporabnikom, da poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1). […]

[…]“.

4. Člen 6 Direktive 2002/58 z naslovom „Podatki o prometu“ določa:

„1. Podatki o prometu, ki se nanašajo na naročnike in uporabnike in ki jih je ponudnik javnega komunikacijskega omrežja ali javno razpoložljive elektronske komunikacijske storitve obdelal in shranil, morajo biti izbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila, kar ne vpliva na odstavke 2, 3 in 5 tega člena in [člen] 15(1).

[…]

5. Obdelava podatkov o prometu mora biti v skladu z odstavki 1, 2, 3 in 4 omejena na osebe, ki delujejo pod nadzorom ponudnikov javnih komunikacijskih omrežij in javno razpoložljivih elektronskih komunikacijskih storitev in ki skrbijo za zaračunavanje ali upravljanje prometa, se odzivajo na povpraševanje 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.

[…]“.

[5] Ne glede na obdobje, za katero se zahteva dostop do podatkov, in količino ali vrsto podatkov, ki so na voljo za navedeno obdobje.

[6] Ali za preprečevanje resnih groženj javni varnosti. Glej sodbo v zadevi Prokuratuur, točke 35, 39 in 45. Glej tudi sodbi z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 56), in z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 140).

[7] Sodba v zadevi Prokuratuur, točke od 48 do 52.

5. Člen 9 Direktive 2002/58 z naslovom „Podatki o lokaciji razen podatkov o prometu“ določa:

„1. Kadar se podatki o lokaciji, razen podatkov o prometu, ki se nanašajo na uporabnike ali naročnike javnih komunikacijskih omrežij ali javno razpoložljivih elektronskih komunikacijskih storitev, dajo obdelovati, se smejo takšni podatki obdelati šele potem, ko postanejo anonimni ali s privolitvijo uporabnikov ali naročnikov in to v obsegu in trajanju, ki sta potrebna za izvedbo storitve z dodano vrednostjo. Ponudnik storitve mora pred pridobitvijo njihove privolitve obvestiti uporabnike ali naročnike o vrsti podatkov v zvezi z lokacijo, razen podatkov o prometu, ki bodo obdelani, o namenih in trajanju obdelave in ali bodo podatki poslani tretji osebi za namen izvedbe storitve z dodano vrednostjo. Uporabnikom ali naročnikom je treba dati možnost, da kadar koli umaknejo privolitev za obdelavo podatkov o lokaciji, razen podatkov o prometu.

[…]“.

6. Člen 15(1) Direktive 2002/58 določa:

„Države članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen [sorazmeren] ukrep znotraj demokratične družbe za zaščito državne [nacionalne] varnosti (to je [d]ržavne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj [kaznivih dejanj] ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive 95/46/ES[8]. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje Skupnosti [Unije], vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji.“

B. Nacionalna zakonodaja

7. Člen 132(3) decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (zakonska uredba št. 196 z dne 30. junija 2003 o zakoniku o varstvu osebnih podatkov),[9] kakor je bila nazadnje spremenjena s členom 1 decreto-legge 30 settembre 2021 n. 132 – Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23 novembre 2021 n. 178 (uredba z zakonsko močjo št. 132 z dne 30. septembra 2021,[10] s spremembami preoblikovana v zakon št. 178 z dne 23. novembra 2021)[11] (v nadaljevanju: člen 132(3) zakonske uredbe št. 196/2003) določa:

„3. če obstaja dovolj indicev za kaznivo dejanje, za katero je po zakonu zagrožena kazen dosmrtnega zapora ali najvišja zaporna kazen najmanj 3 let, določena v skladu s členom 4 [Codice di procedura penale (zakonik o kazenskem postopku)], ali kaznivo dejanje grožnje in nadlegovanja ali vznemirjanja oseb po telefonu, če so grožnje ali vznemirjanje hudi, se podatki, če so upoštevni za ugotovitev dejanskega stanja, pridobijo v zakonsko določenem roku za hrambo [to je 24 mesecev od datuma komunikacije], potem ko sodišče na zahtevo državnega tožilstva ali na

[8] Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355).

[9] Redni dodatek št. 123 h GURI št. 174 z dne 29. julija 2003, str. 11.

[10] GURI št. 234 z dne 30. septembra 2021, str. 1.

[11] GURI št. 284 z dne 29. novembra 2021, st. 1.

predlog zagovornika obtoženca, preiskovanca ali oškodovanca ali drugih strank izda dovoljenje z obrazloženim sklepom;

[…]

3c Podatkov, pridobljenih s kršitvijo določb odstavkov 3 ali 3a, ni mogoče uporabiti.“

8. Člen 4 zakonika o kazenskem postopku z naslovom „Pravila za določanje pristojnosti“ določa:

„Pristojnost sodišča se ugotavlja glede na kazen, ki je po zakonu zagrožena za vsako storitev ali poskus kaznivega dejanja. Ne upoštevajo se nadaljevana kazniva dejanja, povratništvo in okoliščine kaznivega dejanja, razen obteževalnih okoliščin, za katera je po zakonu zagrožena drugačna kazen od tiste za navadno kaznivo dejanje in tistih s posebnim učinkom.“

9. Po navedbah predložitvenega sodišča lahko državno tožilstvo preganja kaznivo dejanje velike tatvine po uradni dolžnosti.[12] V skladu s členom 625 Codice penale (kazenski zakonik) je za veliko tatvino zagrožena posebna zaporna kazen od dveh do šestih let in globa od 927 EUR do 1500 EUR. Člen 624 kazenskega zakonika določa, da je za navadno tatvino, ki se lahko preganja na predlog oškodovanca, zagrožena zaporna kazen od šestih mesecev do treh let in globa od 154 EUR do 516 EUR.

III. Spora o glavni stvari in vprašanje za predhodno odločanje

10. Državno tožilstvo (Bolzano) je začelo dva kazenska postopka proti neznanim storilcem zaradi velike tatvine mobilnega telefona na podlagi členov 624 in 625 kazenskega zakonika.[13] Za identifikacijo storilca je tožilstvo na podlagi člena 132(3) zakonske uredbe št. 196/2003 od predložitvenega sodišča zahtevalo „[…] dovoljenje za pridobitev vseh podatkov, ki jih imajo telekomunikacijske družbe, s sredstvi za sledenje in lokalizacijo (zlasti podatke o uporabnikih in po možnosti kode IMEI klicanih/kličočih številk, obiskana/dosežena spletna mesta, čas in trajanje klica/povezave ter navedbo zadevnih celic in/ali repetitorjev, podatke o uporabnikih in kode IMEI pošiljateljev/prejemnikov sporočil SMS ali MMS in, če je mogoče, podatke o zadevnih imetnikih) v zvezi z dohodnimi in izhodnimi telefonskimi pogovori/komunikacijami in opravljenimi povezavami, tudi med gostovanjem, ter tudi tistimi, ki niso obračunani (neodgovorjeni klici) od datuma tatvine do datuma obravnave zahteve“.

11. Predložitveno sodišče dvomi, da je člen 132(3) zakonske uredbe št. 196/2003 skladen s členom 15(1) Direktive 2002/58, kot je bil razložen v sodbi v zadevi Prokuratuur. Predložitveno sodišče navaja, da je Corte suprema di cassazione (vrhovno kasacijsko sodišče, Italija)[14] 7. septembra 2021 ugotovilo, da imajo nacionalna sodišča določeno polje proste presoje pri opredelitvi, katera kazniva dejanja pomenijo „resn[o] grožnj[o] nacionalni varnosti ali druge oblike hudega kriminala“, zato se sodba v zadevi Prokuratuur ne uporablja neposredno za nacionalna sodišča. Na podlagi sodbe Corte suprema di cassazione (vrhovno kasacijsko sodišče) je italijanski zakonodajalec sprejel uredbo z zakonsko močjo št. 132 z dne 30. septembra 2021,

[12] V skladu z italijanskim pravom velja tatvina, ki jo obravnava predložitveno sodišče, za „veliko“ tatvino.

[13] Prva tatvina je bila storjena 27. oktobra 2021 (referenčna štev. RGNR 9228/2021). Druga je bila storjena 20. novembra 2021 (referenčna štev. RGNR 9794/2021). Tatvini mobilnih telefonov sta bili storjeni v Bolzanu, lastnika telefonov pa sta tatvino prijavila Carabinieri (policiji).

[14] Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

katere člen 132(3) za namene pridobitve telefonskih evidenc huda kazniva dejanja opredeljuje med drugim kot kazniva dejanja, za katera je po zakonu zagrožena „najvišja zaporna kazen najmanj treh let“.

12. Po navedbah predložitvenega sodišča glede na prag za opredelitev hudega kaznivega dejanja iz člena 132(3) zakonske uredbe št. 196/2003 v to skupino spadajo tudi kazniva dejanja, ki nimajo hudih družbenih posledic in se lahko preganjajo le na predlog oškodovanca.[15] Dostop do telefonskih evidenc je torej na podlagi navedene določbe mogoče pridobiti zaradi tatvine predmeta minimalne vrednosti, kot je mobilni telefon ali kolo. Zato prag iz člena 132(3) zakonske uredbe št. 196/2003 ne upošteva načela sorazmernosti v skladu s členom 52(1) Listine, ki določa, da je treba vsekakor upoštevati sorazmernost med težo preiskovanega kaznivega dejanja in omejitvijo uživanja temeljne pravice. Pregon takih blagih kaznivih dejanj ne upravičuje omejevanja uživanja temeljnih pravic do zasebnega življenja, varstva osebnih podatkov ter svobode izražanja in obveščanja.[16]

13. Predložitveno sodišče pojasnjuje, da imajo italijanska sodišča zelo omejeno polje proste presoje glede zavrnitve dostopa do telefonskih evidenc, saj morajo tak dostop odobriti, „če obstaja dovolj indicev za kaznivo dejanje“ in je taka odobritev „upoštevn[a] za ugotovitev dejanskega stanja“. Sodišča zlasti nimajo pristojnosti presojati teže kaznivih dejanj, ki so predmet preiskave. To presojo je opravil že zakonodajalec, ko je na splošno in brez razlikovanja med različnimi vrstami kaznivih dejanj določil, da je treba odobriti dostop do telefonskih evidenc med drugim pri preiskavi vseh kaznivih dejanj, za katera je najvišja zagrožena zaporna kazen najmanj treh let.

14. V teh okoliščinah je Tribunale di Bolzano (sodišče v Bolzanu) prekinilo odločanje in Sodišču v predhodno odločanje predložilo naslednje vprašanje:

„Ali člen 15(1) [Direktive 2002/58] nasprotuje nacionalni zakonodaji v členu 132 [zakonske uredbe št. 196/2003, ki] v veljavni različici določa:

‚Če obstaja dovolj indicev za kaznivo dejanje, za katero je po zakonu zagrožena kazen dosmrtnega zapora ali najvišja zaporna kazen najmanj treh let, določena v skladu s členom 4 zakonika o kazenskem postopku, ali kaznivo dejanje grožnje in nadlegovanja ali vznemirjanja oseb po telefonu, če so grožnje, nadlegovanje ali vznemirjanje hudi, se podatki, če so upoštevni za ugotovitev dejanskega stanja, pridobijo, potem ko sodišče na zahtevo državnega tožilstva ali na predlog zagovornika obtoženca, preiskovanca ali oškodovanca ali drugih strank izda dovoljenje z obrazloženim sklepom‘?“

IV. Postopek pred Sodiščem

15. Pisna stališča so predložile češka in estonska vlada, Irska, francoska, italijanska, ciprska, madžarska, nizozemska, avstrijska in poljska vlada ter Evropska komisija.

[15] V skladu z navedbami predložitvenega sodišča „[se na primer] kaznivo dejanje kršitve nedotakljivosti stanovanja […] po členu 614 kazenskega zakonika kaznuje z zaporno kaznijo od enega do štirih let. Zakonsko določena kazen omogoča pridobitev seznamov telefonskih klicev tudi pri drugih kaznivih dejanjih, ki se preganjajo samo na predlog stranke, ker ne povzročajo hudih družbenih posledic, in sicer pri kaznivih dejanjih iz člena 633 kazenskega zakonika (nezakonito zasedanje zemljišč in zgradb: zaporna kazen od enega do treh let in globa od 103 EUR do 1032 EUR) ali člena 640 kazenskega zakonika (mala goljufija: zaporna kazen od šestih mesecev do treh let in globa od 51 EUR do 1032 EUR).“

[16] Glej člene 7, 8 in 11 Listine.

16. Navedene zainteresirane strani in državno tožilstvo (Bolzano) so svoja stališča ustno predstavili na obravnavi 21. marca 2023, na kateri so tudi odgovarjali na vprašanja Sodišča.

V. Presoja

A. Dopustnost

17. Italijanska vlada in Irska trdita, da del predloga za sprejetje predhodne odločbe ni dopusten. Glede na opis dejanskega stanja v predložitveni odločbi je bila zahteva za dostop vložena v okviru preiskave velike tatvine mobilnih telefonov. Irska poudarja, da lahko državno tožilstvo navedeno kaznivo dejanje preganja po uradni dolžnosti. Iz te pristojnosti izhaja, da navedeno kaznivo dejanje zaradi svoje narave in posledic vpliva na družbo na splošno. Predlog za sprejetje predhodne odločbe je torej hipotetičen v delu, v katerem se nanaša tudi na kazniva dejanja, ki se lahko preganjajo le na predlog posameznika. Italijanska vlada navaja, da se predložitveno sodišče sklicuje na več kaznivih dejanj, ki niso upoštevna v zadevah, ki ju obravnava. Italijanska vlada in Komisija trdita, da je v nasprotju s sklicem v predložitveni odločbi na „najvišj[o] zaporn[o] kazen najmanj treh let“ iz člena 625 kazenskega zakonika za kaznivo dejanje velike tatvine zagrožena zaporna kazen od dveh do šestih let. Komisija zato predlaga, naj Sodišče preoblikuje vprašanje. Tudi francoska vlada predlaga, naj Sodišče preoblikuje vprašanje. Meni, da čeprav lahko Sodišče razlaga določbe prava Unije, pa ni pristojno za presojo skladnosti določb nacionalne zakonodaje s pravom Unije.

18. Predložitveno sodišče s svojim vprašanjem dobesedno prosi Sodišče, naj presodi o skladnosti določbe nacionalne zakonodaje s pravom Unije. To pa samo po sebi še ne pomeni, da predložitvenemu sodišču ni mogoče zagotoviti razlage prava Unije, v tem primeru člena 15(1) Direktive 2002/58, na podlagi katere bo lahko samo odločilo o skladnosti katerega koli zadevnega nacionalnega pravila, ki ga obravnava, z navedeno določbo.[17]

19. Iz predložitvene odločbe jasno izhaja, da je državno tožilstvo (Bolzano) dostop do podatkov zahtevalo med drugim zaradi preiskave in pregona dveh primerov kaznivih dejanj velike tatvine mobilnega telefona na podlagi člena 625 kazenskega zakonika. V navedenih okoliščinah sklici v predložitveni odločbi na druga kazniva dejanja, med njimi na člen 624 kazenskega zakonik (navadna tatvina),[18] niso upoštevni za odločitev o zahtevah, o katerih mora odločiti predložitveno sodišče.[19] V delu, v katerem se vprašanje za predhodno odločanje nanaša na zahtevo državnega tožilstva (Bolzano) za dostop do podatkov z namenom preiskave kaznivih dejanj velike tatvine, ne gre za hipotetično vprašanje. V skladu s tem bom svojo oceno uporabe člena 132(3) zakonske uredbe št. 196/2003 omejil na dejansko stanje, kot ga opisuje predložitveno sodišče in ki se nanaša na veliko tatvino mobilnih telefonov.

[17] Glej po analogiji sodbo z dne 17. marca 2021, Consulmarketing (C-652/19, EU:C:2021:208, točka 33). V skladu z uveljavljeno sodno prakso na podlagi člena 267 PDEU Sodišče nacionalnemu sodišču zagotovi odgovor, ki slednjemu omogoči odločitev v zadevi, ki jo obravnava. Zato lahko Sodišče preoblikuje predložena vprašanja. Sodba z dne 25. julija 2018, Dyson (C-632/16, EU:C:2018:599, točka 47 in navedena sodna praksa).

[18] Za kaznivo dejanje navadne tatvine je zagrožena zaporna kazen od šestih mesecev do treh let, zato spada na področje člena 132(3) zakonske uredbe št. 196/2003.

[19] V zvezi z vprašanjem, ali iz navedenih sklicev izhaja, da se je mogoče sklicevati na člen 132(3) zakonske uredbe št. 196/2003 pri preiskavi kaznivih dejanj, ki se ne štejejo za huda, glej točke od 35 do 39 teh sklepnih predlogov.

B. Vsebinska presoja

1. Uvodne ugotovitve

20. Ta predložitvena odločba izhaja iz zahteve državnega tožilstva (Bolzano) za dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev. Ne nanaša pa se na hrambo navedenih podatkov ali njeno zakonitost na podlagi (med drugim) člena 15(1) Direktive 2002/58.[20] Podatki vključujejo vhodna in izhodna sporočila (komunikacijo)[21], poslana/prejeta z ukradenimi mobilnimi telefoni, in podatke o lokaciji.[22] Čeprav podatki ne vključujejo vsebine sporočil (komunikacije), omogočajo natančno sklepanje o zasebnem življenju oseb, na katere se podatki nanašajo; ob tem se zdi, da dostop do teh podatkov pomeni „hud“ poseg v njihove temeljne pravice.[23] Poseg, ki je posledica takega dostopa do podatkov, lahko upravičuje cilj[24] iz prvega stavka člena 15(1) Direktive 2002/58, torej preprečevanje, preiskovanje, odkrivanje in pregon „hudih kriminalnih [kaznivih] dejanj“, vendar ne kaznivih dejanj na splošno. Sodišče pri razlagi člena 15(1) Direktive 2002/58 povezuje resnost posega v temeljne pravice oseb s težo preiskovanega kaznivega dejanja.[25]

2. Pristojnost držav članic, da opredelijo „huda kazniva dejanja“

21. Direktiva 2002/58 ureja dejanja ponudnikov elektronskih komunikacijskih storitev v zvezi z obdelavo osebnih podatkov.[26] Člen 1(3) s področja uporabe Direktive 2002/58 izrecno izključuje dejavnosti države na posebnih področjih, kot so javna varnost, obramba, državna varnost in kazensko pravo. Dejavnosti, na katere se nanaša člen 15(1) Direktive 2002/58, se v veliki meri prekrivajo s tistimi iz člena 1(3) navedene direktive in vključujejo dejavnosti države na področju kazenskega prava, ki so izrecno izključene s področja uporabe Direktive 2002/58.[27]

[20] Predlog za sprejetje predhodne odločbe torej temelji na predpostavki, da je hramba zahtevanih podatkov zakonita. Hramba podatkov, na katere se nanaša Direktiva 2002/58, in dostop do njih sta ločena posega v temeljne pravice, ki jih zagotavljajo členi 7, 8 in 11 Listine, zato ju je na podlagi člena 52(1) Listine treba utemeljiti ločeno. Glej v tem smislu sodbo z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, EU:C:2022:258, točka 47). Točke od 29 do 33 sodbe v zadevi Prokuratuur vsebujejo pregled pravil o hrambi takih podatkov.

[21] Člen 2(d) Direktive 2002/58 določa, da „‚sporočilo‘ (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve […]“.

[22] Člen 2(c) Direktive 2002/58 določa, da „‚podatki o lokaciji‘ pomenijo vsakršne podatke, […] ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve“.

[23] Sodba v zadevi Prokuratuur, točki 34 in 35. Glej po analogiji sodbo z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točke od 59 do 62). Nacionalno sodišče mora oceniti, ali dostop do zadevnih podatkov pomeni „hud“ poseg v temeljne pravice oseb, na katere se taki podatki nanašajo. Ti sklepni predlogi temeljijo na predpostavki, da je poseg, ki je posledica dostopa do podatkov, opisanih v točki 10 teh sklepnih predlogov, hud.

[24] Seznam ciljev v členu 15(1) Direktive 2002/58 je izčrpen. Sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točka 90).

[25] Glej v tem smislu sklepne predloge generalnega pravobranilca H. Saugmandsgaarda Øeja v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točke od 79 do 82 in navedena sodna praksa). V zvezi s ciljem boja proti kriminalu se lahko dostop načeloma odobri le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so bile tako ali drugače udeležene pri takem kaznivem dejanju. Sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, EU:C:2022:258, točka 105).

[26] Glej v tem smislu člen 3 Direktive 2002/58, ki določa, da se direktiva uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev. Glej tudi sodbo z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točki 70 in 74), ter po analogiji sklepne predloge generalnega pravobranilca M. Szpunarja v zadevi La Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju) (C-470/21, EU:C:2022:838, točka 38).

[27] Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 97).

Zato obstaja jasna povezava med dejavnostmi države, ki jih člen 1(3) Direktive 2002/58 izključuje s področja uporabe navedene direktive, in zakonodajnimi ukrepi, ki jih države članice lahko sprejmejo na podlagi člena 15(1) navedene direktive. [28]

22. Ne glede na navedeno jasno povezavo je Sodišče dosledno ugotavljalo, da ker člen 15(1) Direktive 2002/58 izrecno pooblašča države članice, da lahko sprejmejo v njem opisane ukrepe nacionalne zakonodaje, taki ukrepi spadajo na področje uporabe navedene direktive. Iz navedene sodne prakse izhaja, da pojem „dejavnosti“, vključno z „dejavnost[m]i države na področju kazenskega prava“ iz člena 1(3) Direktive 2002/58 ne vključuje zakonskih ukrepov, na katere se nanaša člen 15(1) navedene direktive. [29]

23. Pojem „kriminalna [kazniva] dejanja“ ni opredeljen niti v členu 2 Direktive 2002/58, ki vsebuje več opredelitev pojmov za uporabo navedene direktive, niti v nobeni drugi določbi Direktive 2002/58, vključno s členom 15(1). Direktiva 2002/58 ne vsebuje seznama „kriminalnih [kaznivih] dejanj“. [30] Ta pojem tudi ni opredeljen v sodni praksi o razlagi člena 15(1) Direktive 2002/58. [31]

24. Kljub neobstoju takih opredelitev pa Direktiva 2002/58 ne določa, da vsaka država članica opredeli „kriminalna [kazniva] dejanja“ v skladu s svojim nacionalnim pravom. [32] V skladu z ustaljeno sodno prakso Sodišča iz načela enotne uporabe prava Unije in načela enakosti izhaja, da je treba za določitev pomena in obsega pojmov v določbah prava Unije, ki se nikjer izrecno ne nanašajo na pravo držav članic, te pojme v vsej Uniji običajno razlagati neodvisno in enotno. V okviru razlage člena 15(1) Direktive 2002/58 je mogoče pojem „kriminalna [kazniva] dejanja“ vsaj načeloma razumeti kot avtonomen pojem prava Unije, ki ga je treba razlagati enotno v vseh državah članicah. [33]

25. Vendar 10 držav članic, ki so Sodišču predložile stališča, in Komisija enoglasno menijo, da lahko vsaka država članica opredeli „kriminalna [kazniva] dejanja“, vključno s hudimi kaznivimi dejanji, na katere se nanaša člen 15(1) Direktive 2002/58 s sklicevanjem na nacionalno zakonodajo.

26. Iz razlogov, navedenih v nadaljevanju, se strinjam z navedenimi stališči.

[28] Za zaščito državne varnosti, obrambe, javne varnosti ter preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema.

[29] Sodbi z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 98), in z dne 6. oktobra 2020, Privacy International (C-623/17, EU:C:2020:790, točka 38 in navedena sodna praksa).

[30] Glej za primerjavo člen 2(2) Okvirnega sklepa Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL, posebna izdaja v slovenščini, poglavje 19, zvezek 6, str. 34, in popravek v UL 2018, L 25, str. 88), kakor je bil spremenjen z Okvirnim sklepom Sveta 2009/299/PNZ z dne 26. februarja 2009 (UL 2009, L 81, str. 24), v katerem so navedena kazniva dejanja, ki so razlog za predajo osebe na podlagi evropskega naloga za prijetje, ter Prilogo II k Direktivi (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL 2016, L 119, str. 132), v kateri so navedena „huda kazniva dejanja“, kakor so opredeljena v členu 3(9) navedene direktive.

[31] Direktiva 2002/58 se ne sklicuje na „splošna kazniva dejanja“, „huda kazniva dejanja“ ali „kriminal“. Sodišče se v svoji sodni praksi sklicuje na navedene pojme, ne da bi jih opredelilo ali opredelilo kakršna koli merila, kako naj jih opredelijo nacionalni zakonodajalci. Glej na primer sodbi z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točki 115 in 125), in z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točke 54, 56 in 63). Glej v zvezi s tem tudi točko 45 sodbe v zadevi Prokuratuur.

[32] Glej za primerjavo člen 1(1) Direktive 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58 (UL 2006, L 105, str. 54), ki določa, da „je [namen te direktive] uskladiti določbe držav članic glede obveznosti ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij glede hrambe določenih podatkov, ki jih pridobivajo ali obdelujejo, da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, *kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic*“ (moj poudarek). Sodišče je s sodbo z dne 8. aprila 2014, Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238) razglasilo Direktivo 2006/24 za neveljavno.

[33] Glej po analogiji sodbo z dne 7. septembra 2022, Staatssecretaris van Justitie en Veiligheid (Narava pravice do prebivanja na podlagi člena 20 PDEU) (C-624/20, EU:C:2022:639, točki 19 in 20).

27. Prvič, Sodišče je predhodno ugotovilo, da v okviru člena 15(1) Direktive 2002/58 velja, da države članice same opredelijo svoje bistvene varnostne interese in sprejmejo ustrezne ukrepe, da zagotovijo svojo notranjo in zunanjo varnost.[34] Čeprav tega ni izrecno navedlo, se zdi, da je Sodišče sprejelo stališče, da pojem „državna [nacionalna] varnost“ iz člena 15(1) Direktive 2002/58 ni avtonomen pojem prava Unije, kljub temu, da ne obstaja opredelitev tega pojma ali kakršen koli izrecen sklic na pravo držav članic.[35] Ne vidim razloga, zakaj se ta pristop ne bi mogel uporabiti glede pristojnosti držav članic za opredelitev pojmov „kriminalna [kazniva] dejanja“ ali „huda kazniva dejanja“ za namene člena 15(1) Direktive 2002/58. Pojme „kriminalna [kazniva] dejanja“, „javna varnost“ in „državna [nacionalna] varnost“ iz navedene določbe je mogoče šteti za *noscitur a sociis*, saj se zdi, da je zakonodajalec Unije želel, da se vsak od njih obravnava podobno, tudi glede opredelitve njihovega pomena.[36]

28. Drugič, člen 4(2) PEU določa, da mora Evropska unija spoštovati nacionalno identiteto držav članic, ki je neločljivo povezana z njihovimi temeljnimi političnimi in ustavnimi strukturami. Preambula k Listini potrjuje tudi, da Unija prispeva k ohranjanju in razvijanju skupnih vrednot, pri tem pa med drugim spoštuje tudi raznolikosti kultur in tradicij evropskih narodov. Opredelitev kaznivega dejanja in kazni[37] odraža nacionalno občutljivost in tradicije, ki se močno razlikujejo, ne le med državami članicami, ampak tudi v času, skladno z družbenimi spremembami.[38]

29. V zvezi s tem je mogoče ugotoviti, da države članice pri opredelitvi kaznivih dejanj in kazni upoštevajo zelo različne dejavnike in v različni meri. Ocena „teže“ posameznega kaznivega dejanja, ki jo opravi država članica, se pogosto, če ne celo neizogibno, odraža v višini zagrožene kazni. Višina prostostne kazni je lahko določena na podlagi analize številnih dejavnikov, vključno s „težo“ kaznivega dejanja samega po sebi in relativno glede na druga kazniva dejanja. Predstavljeni niso bili nobeni razlogi, zakaj države članice ne bi smele izvrševati te pristojnosti ali celo zakaj bi moral v specifičnih okoliščinah te zadeve drugačen pristop veljati za opredelitev pojmov „kriminalna [kazniva] dejanja“, „huda kazniva dejanja“ ali „kazniva dejanja na splošno“.

30. Pristojnost držav članic na področju kazenskega prava ne posega v pristojnost Evropske unije, da v nekaterih primerih na primer določi minimalna pravila glede opredelitve kaznivih dejanj in sankcij na področju posebno hudih oblik kriminala s čezmejnimi posledicami zaradi narave ali

[34] Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točki 99 in 136).

[35] Poleg tega člen 4(2) PEU določa, da nacionalna varnost ostaja v izključni pristojnosti vsake države članice. Dejstvo, da je nacionalni ukrep sprejet za varstvo nacionalne varnosti, še ne pomeni, da se pravo Unije ne uporablja in da države članice nimajo nobenih obveznosti glede zagotavljanja skladnosti z njim. Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točki 99 in 135).

[36] Čeprav ima cilj zaščite nacionalne varnosti prednost pred bojem proti hudim kaznivim dejanjem, zato je z njim mogoče upravičiti hujše posege v temeljne pravice, ta cilj ne posega v pravico držav članic opredeliti pojma „kriminalna [kazniva] dejanja“ ali „huda kazniva dejanja“. Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 136).

[37] Ter olajševalnih in obteževalnih okoliščin.

[38] Generalni pravobranilec H. Saugmandsgaard Øe je menil, da kazenska zakonodaja in predpisi kazenskega postopka spadajo v pristojnost držav članic, čeprav lahko na pravni red teh držav kljub temu vplivajo določbe prava Unije, sprejete na tem področju, tudi na podlagi člena 83(2) PDEU. Zato ne obstaja splošna določba, ki bi vsebovala usklajeno opredelitev pojma „hudo kaznivo dejanje“. Sklepni predlogi v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točka 95). Generalni pravobranilec G. Pitruzzella je navedel, da bi bilo treba opredelitev pojma „hudo kaznivo dejanje“ prepustiti državam članicam. Glede na nacionalne pravne sisteme je namreč isto kaznivo dejanje lahko kaznovano bolj ali manj strogo. Tudi opredelitev obteževalnih okoliščin se lahko po državah članicah razlikuje. Sklepni predlogi v zadevi Prokuratuur (Pogoji dostopa do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2020:18, točki 91 in 92). V nasprotju s tem pa je generalni pravobranilec M. Szpunar menil, da „je treba pojem ‚hud kriminal‘ razlagati samostojno. Ne more biti odvisen od njegovega pojmovanja v posameznih državah članicah, saj bi v tem primeru omogočili izogibanje zahtevam člena 15(1) Direktive 2002/58 glede na to, ali države članice boj proti hudemu kriminalu pojmujejo široko ali ozko.“ Sklepni predlogi v zadevi *La* Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju) (C-470/21, EU:C:2022:838, točka 74).

učinkov teh dejanj ali zaradi posebne potrebe po skupnem boju proti njim.[39] Vendar zakonodajalec Unije ni določil pravil glede opredelitve kaznivih dejanj v členu 15(1) Direktive 2002/58.[40] Kot je bilo že navedeno,[41] iz besedila člena 1(3) Direktive 2002/58 izhaja, da zakonodajalec Unije s sprejetjem navedene direktive ni nameraval izvrševati nobenih pristojnosti na področju kazenskega prava.

31. Ta dva razloga zadoščata za razlago, zakaj – ne glede na to, da ukrepi nacionalne zakonodaje, sprejeti na podlagi člena 15(1) Direktive 2002/58 za preiskovanje in pregon kaznivih dejanj, spadajo na področje uporabe navedenega ukrepa – države članice ohranijo pristojnost opredelitve pojma „kriminalna [kazniva] dejanja“, vključno s „hudimi kaznivimi dejanji“, in določitve kazni za taka ravnanja.[42]

3. Standard nadzora izvrševanja možnosti iz člena 15(1) Direktive 2002/58 glede odstopanja od načela zaupnosti

32. Sodišče je poudarilo, da je treba možnost odstopanja[43] od, med drugim, načela zaupnosti iz člena 5(1) Direktive 2002/58 razlagati ozko, da ne postane splošno pravilo, saj bi se sicer tej določbi v veliki meri odvzel pomen.[44] Pri izvrševanju navedene možnosti je torej treba med drugim upoštevati načeli enakovrednosti[45] in učinkovitosti.[46] Prav tako mora biti skladno s splošnimi načeli prava Unije, vključno z načelom sorazmernosti,[47] ter s členi 7, 8 in 11[48] in členom 52(1) Listine.[49] Cilj boja proti hudim kaznivim dejanjem je treba vedno uravnotežiti z uživanjem temeljnih pravic, na katere vplivajo. Pravice iz členov 7, 8 in 11 Listine niso absolutne in uveljavljati jih je treba glede na njihovo vlogo v družbi.[50] Člen 52(1) Listine torej določa, da morajo omejitve uresničevanja navedenih pravic, kakor jih določa zakon, spoštovati

[39] Člen 83(1), prvi pododstavek, PDEU. Glej tudi sodbo z dne 21. oktobra 2021, Okrazhna prokuratura – Varna (C-845/19 in C-863/19, EU:C:2021:864, točka 32).

[40] Glej po analogiji sodbo v zadevi Prokuratuur, točki 41 in 42. Sodišče je navedlo, da se lahko ob neobstoju pravil EU o tem vprašanju ter v skladu z načelom procesne avtonomije, „načeloma le z nacionalnim pravom določijo pravila za dopustnost in presojo – v okviru kazenskega postopka, ki se vodi zoper osumljence kaznivih dejanj – informacij in dokazov, pridobljenih s splošno in neselektivno hrambo teh podatkov, ki je v nasprotju s pravom Unije“. Pravna podlaga za Direktivo 2002/58 je člen 114 PDEU (prej člen 95 PES) in ne na primer člen 83(1), prvi pododstavek, PDEU. V nasprotju s tem sta pravna podlaga Direktive 2016/781 točka (d) člena 82(1), drugi pododstavek, PDEU (pravosodno sodelovanje v kazenskih zadevah) in točka (a) člena 87(2) PDEU (policijsko sodelovanje).

[41] Glej točko 21 teh sklepnih predlogov.

[42] Glej po analogiji sodbo z dne 23. oktobra 2007, Komisija/Svet (C-440/05, EU:C:2007:625, točke 66, 70 in 71 ter navedena sodna praksa). Glej tudi sodbo z dne 28. aprila 2011, El Dridi (C-61/11 PPU, EU:C:2011:268, točka 53).

[43] Člen 15(1) Direktive 2002/58 določa, da države članice „lahko sprejmejo“ zakonske ukrepe, ki omejujejo nekatere pravice in obveznosti, ki jih določa navedena direktiva.

[44] Sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točka 89). Generalni pravobranilec H. Saugmandsgaard Øe je menil, da „čeprav ima vsaka država članica možnost presoditi, kateri je ustrezen prag kazni za ugotovitev obstoja hudega kaznivega dejanja, pa ima tudi dolžnost, da tega praga glede na običajno višino kazni, ki se uporabljajo v tej državi, ne določi tako nizko, da bi se izjeme od prepovedi shranjevanja in uporabe osebnih podatkov, ki so predvidene v zadevnem členu 15(1), spremenile v načela […]“. Sklepni predlogi v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točka 114).

[45] Ni ničesar, kar bi kazalo na to, da zadevno italijansko pravo ni skladno s tem načelom.

[46] Sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, EU:C:2022:258, točka 127).

[47] Glej tudi uvodno izjavo 11 Direktive 2002/58.

[48] Glej tudi uvodno izjavo 2 Direktive 2002/58.

[49] Sodbi z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točka 89), in z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točke od 111 do 113). Glej tudi sklepne predloge generalnega pravobranilca H. Saugmandsgaarda Øeja v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točke od 116 do 120). V sodbi z dne 8. marca 2022, Bezirkshauptmannschaft Hartberg-Fürstenfeld (Neposredni učinek) (C-205/20, EU:C:2022:168, točka 31), je Sodišče opozorilo, da načelo sorazmernosti zavezuje države članice pri izvajanju prava Unije. V tem okviru morajo države članice zagotoviti skladnost s členom 49(3) Listine, kadar določajo kazenske sankcije, tudi če ne obstaja zakonodaja EU, ki harmonizira navedene sankcije.

[50] Člen 52(1) Listine. Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 120).

bistveno vsebino teh pravic, v skladu z načelom sorazmernosti pa mora biti njihovo uresničevanje potrebno in mora dejansko izpolnjevati cilje v splošnem interesu, ki jih priznava Evropska unija, ali potrebo po varstvu pravic in svoboščin drugih. Ukrepi nacionalne zakonodaje, sprejeti na podlagi člena 15(1) Direktive 2002/58, morajo torej dejansko in strogo ustrezati enemu od ciljev iz navedene določbe. Temeljiti morajo na objektivnih merilih, biti pravno zavezujoči ter določati jasna in natančna pravila, iz katerih izhajajo materialni in procesni pogoji, pod katerimi morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do podatkov. [51]

33. Da se zagotovi polno upoštevanje teh pogojev v praksi, mora biti dostop pristojnih nacionalnih organov do shranjenih podatkov načeloma [52] podvržen predhodnemu nadzoru sodišča ali neodvisnega upravnega organa [53], na podlagi obrazložene zahteve navedenih organov in ob obveščanju zadevnih oseb. [54] Iz ustaljene sodne prakse izhaja, da mora sodišče ali neodvisen upravni organ pri izvajanju navedenega predhodnega nadzora upoštevati različne interese in pravice ter poiskati pravično ravnovesje med zahtevami preiskave in potrebo po zagotavljanju temeljnih pravic do zasebnosti in varstva osebnih podatkov zadevnih oseb. [55]

34. V obravnavani zadevi člen 132(3) zakonske uredbe št. 196/2003 določa pogoje, na podlagi katerih mora nacionalno sodišče na zahtevo državnega tožilstva ponudnikom elektronskih komunikacijskih storitev odrediti, naj državnemu tožilstvu omogočijo dostop do podatkov. Ni sporno, [56] da člen 132(3) zakonske uredbe št. 196/2003 jasno določa okoliščine in pogoje, v katerih lahko nacionalno sodišče ponudnikom elektronskih komunikacijskih storitev odredi, naj omogočijo tak dostop. Vendar predložitveno sodišče meni, da je prag zagrožene „najvišje zaporne kazni najmanj treh let“ prenizek, saj vključuje tudi kazniva dejanja, kot je navadna tatvina, ki nimajo hudih družbenih posledic.

35. Čeprav člen 132(3) zakonske uredbe št. 196/2003 potencialno vključuje veliko različnih kaznivih dejanj, Sodišče v obravnavani zadevi ne razpolaga z nobenimi dokazi, da je obseg uporabe tega člena tako širok, da bi dostop do podatkov, ki ga omogoča, postal pravilo in ne izjema. [57] Zdi se, da prag najvišje zaporne kazni najmanj treh let v navedeni določbi ni prenizek. [58] Za primerjavo, člen 3, točka 9, Direktive 2016/681 [59] opredeljuje „hudo kaznivo dejanje“ kot „kazniva dejanja iz Priloge II, ki se po nacionalnem pravu države članice kaznujejo z zaporno

[51] Sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točke od 117 do 119). Glej tudi sodbo z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točke 110 in od 129 do 133).

[52] Člen 132(3a) zakonske uredbe št. 196/2003 na primer določa posebna pravila glede dostopa do podatkov v nujnih primerih. Generalni pravobranilec M. Szpunar je v sklepnih predlogih v zadevi La Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju) (C-470/21, EU:C:2022:838, točke od 99 do 105) navedel, da je predhodni nadzor potreben le, če gre za posebej resno vmešavanje v zasebno življenje uporabnikov elektronskih komunikacijskih storitev. Predhodni nadzor je potreben, ker gre v obravnavanem postopku za hud poseg zaradi vrste podatkov, do katerih zahteva dostop državno tožilstvo.

[53] Zahteva glede predhodnega nadzora ne izhaja iz Direktive 2002/58, ampak se je oblikovala v sodni praksi: sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točki 120 in 121 ter navedena sodna praksa).

[54] Sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točki 120 in 121).

[55] Sodba v zadevi Prokuratuur, točka 52.

[56] To mora preveriti predložitveno sodišče.

[57] Glej presojo v sklepnih predlogih generalnega pravobranilca H. Saugmandsgaarda Øeja v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točke od 116 do 120). To mora presoditi predložitveno sodišče.

[58] Dejstvo, da se opredelitve kaznivih dejanj in sistem kazni med državami članicami razlikujejo, samo po sebi še ne vpliva na sorazmernost zakonodaje. Glej po analogiji sodbo z dne 8. julija 2010, Sjöberg in Gerdin (C-447/08 in C-448/08, EU:C:2010:415, točka 38).

[59] Direktiva 2016/681 se nanaša na prenos in obdelavo podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj.

kaznijo oziroma ukrepom odvzema prostosti z najvišjo zagroženo kaznijo najmanj treh let.“ [60] Vendar je Sodišče ugotovilo, da ker se člen 3(9) Direktive 2016/681 ne nanaša na najnižjo možno zagroženo kazen, temveč na najvišjo možno zagroženo kazen, ni izključeno, da se „podatki PNR lahko obdelujejo zaradi boja proti kaznivim dejanjem, ki – čeprav izpolnjujejo merilo iz te določbe v zvezi s pragom teže – ob upoštevanju posebnosti nacionalnega kazenskega sistema ne spadajo med huda kazniva dejanja, ampak med splošna kazniva dejanja“. [61]

36. Kazen treh let iz člena 132(3) zakonske uredbe št. 196/2003 se nanaša na najvišjo zagroženo kazen in se torej lahko uporablja za kazniva dejanja, kot je navadna tatvina. [62] Zato je treba preučiti, kako se člen 132(3) zakonske uredbe št. 196/2003 uporablja v praksi. Zdi se, da člen 132(3) zakonske uredbe št. 196/2003 vzpostavlja dva različna standarda predhodnega nadzora nacionalnega sodišča, odvisno od vrste kaznivih dejanj, ki se preiskujejo, vendar mora to preveriti predložitveno sodišče.

37. Prvi od navedenih standardov nadzora zahteva, [63] da nacionalna sodišča državnemu tožilstvu odobrijo dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, če so taki podatki upoštevni za ugotovitev dejanskega stanja in če obstaja dovolj indicev za kaznivo dejanje grožnje in nadlegovanja ali vznemirjanja oseb po telefonu, če so grožnje ali vznemirjanje hudi. Nacionalno sodišče mora torej opraviti individualno presojo teže zadevnega kaznivega dejanja in preveriti, ali preiskava in pregon navedenega kaznivega dejanja upravičujeta omejevanje splošnih pravic iz členov 7, 8 in 11 Listine ter posebnih pravic iz členov 5, 6 in 9 Direktive 2002/58. Ta standard zahteva individualno presojo v posamezni zadevi, ali je poseg v navedene pravice glede na cilj boja proti kriminalu, ki je v javnem interesu, sorazmeren.

38. V nasprotju s tem drugi od navedenih standardov nadzora, ki je upošteven v obravnavanem postopku, od nacionalnih sodišč zahteva, [64] da državnemu tožilstvu odobrijo dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, če so taki podatki upoštevni za ugotovitev dejanskega stanja in če obstaja dovolj indicev za kaznivo dejanje, za katero je po zakonu med drugim zagrožena najvišja zaporna kazen najmanj treh let. V tem primeru je vloga nacionalnega sodišča omejena na preverjanje navedenih objektivnih zahtev, pri čemer sodišče

[60] Sodišče je ugotovilo, da so zahteve, ki izhajajo iz navedene določbe in se nanašajo na naravo in težo kazni, ki se uporabi, načeloma takšne, da lahko omejijo uporabo sistema, vzpostavljenega z Direktivo 2016/681, na dovolj resna kazniva dejanja, da lahko upravičijo poseganje v temeljne pravice, določene v členih 7 in 8 Listine. Sodba z dne 21. junija 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, točka 150).

[61] Sodišče je torej ugotovilo, da morajo države članice zagotoviti, da je sistem, vzpostavljen z Direktivo 2016/681, omejen na boj proti hudim kaznivim dejanjem, ne splošnim. Sodba z dne 21. junija 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, točki 151 in 152). Predmet in področje uporabe Direktive 2016/681, ki med drugim določa izmenjavo podatkov PNR med državami članicami, se ne prekriva s predmetom in področjem uporabe Direktive 2002/58. Iz tega sledi, da je treba določbe navedenih direktiv presojati ločeno. Glede na to in v nasprotju s stališčem v zvezi s členom 15(1) Direktive 2002/58, je pojem „hudega kaznivega dejanja“ iz Direktive 2016/681 avtonomen pojem prava Unije. V zvezi s tem glej tudi uvodno izjavo 12 in člen 3(9) Direktive 2016/681 ter Prilogo II k tej direktivi.

[62] Glej po analogiji sodbo z dne 21. junija 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, točka 151).

[63] Besedilo v izvirniku se glasi „i dati sono acquisiti“.

[64] Iz uporabe povednega naklona v členu 132(3) zakonske uredbe št. 196/2003 („i dati sono acquisiti“) je mogoče sklepati, da nacionalno sodišče odobri dostop do zadevnih podatkov, če so izpolnjeni objektivni pogoji, ki jih nalaga določba, vendar mora to preveriti predložitveno sodišče.

nima nobene možnosti opraviti individualne presoje interesov v posamezni zadevi.[65] Nadzor, ki ga nacionalno sodišče opravi na podlagi člena 132(3) zakonske uredbe št. 196/2003, torej nima nobene zveze z dejanskimi okoliščinami zadeve, ki jo obravnava.

39. Čeprav nacionalna sodišča morda niso pristojna za nadzor opredelitve kaznivih dejanj ali njihove teže, kot jo je določil zakonodajalec,[66] pa morajo kljub temu biti pristojna za individualno presojo, ali je odobritev dostopa v skladu z zakonskimi ukrepi, sprejetimi na podlagi člena 15(1) Direktive 2002/58, do občutljivih podatkov, ki omogočajo natančno sklepanje o uporabnikovem zasebnem življenju – kar torej pomeni hud poseg v temeljne pravice iz členov 7, 8, 11 in člena 52(1) Listine – sorazmerna.

40. Iz tega sledi, da se z ukrepi, sprejetimi na podlagi člena 15(1) Direktive 2002/58, ne sme omogočati dostopa do občutljivih podatkov, razen če (i) zadevno kaznivo dejanje presega prag resnosti, ki ga vnaprej določi nacionalni zakonodajalec, in (ii) sodišče ali drug neodvisni upravni organ na podlagi individualne presoje ali nadzora potrdi, da je v posamezni zadevi poseg v temeljne pravice, ki je posledica takega dostopa, sorazmeren s ciljem boja proti kriminalu v javnem interesu. V nekaterih primerih pa se dostop do takih podatkov ne odobri, tudi če kaznivo dejanje presega prag resnosti iz nacionalne zakonodaje.

41. Kaznivo dejanje velike tatvine iz obravnavane zadeve se v nacionalni zakonodaji šteje za „hudo“, saj je zanj med drugim zagrožena zaporna kazen od dveh do šestih let, zato presega prag resnosti iz člena 132(3) zakonske uredbe št. 196/2003.[67] Zdi se, da italijanska sodišča pri uporabi ukrepov, sprejetih na podlagi člena 15(1) Direktive 2002/58, nimajo pristojnosti preverjati opredelitve velike tatvine kot „hudega kaznivega dejanja“ v smislu nacionalne zakonodaje. Če prag, določen v nacionalni zakonodaji, ni presežen, predložitveno sodišče torej ne sme odobriti dostopa do zahtevanih podatkov.[68]

42. Če je pogoj praga iz nacionalne zakonodaje izpolnjen, mora predložitveno sodišče na podlagi člena 15(1) Direktive 2002/58 preveriti, ali je glede na vse okoliščine posamezne zadeve poseg v temeljne pravice, ki je posledica omogočanja dostopa do občutljivih podatkov, sorazmeren s ciljem boja proti takemu kaznivemu dejanju v javnem interesu. V zvezi s tem mora predložitveno sodišče upoštevati vse upoštevne pravice in interese, med drugim tudi škodo na premoženjskih pravicah žrtev, ki jih zagotavlja člen 17 Listine, in dejstvo, da lahko mobilni telefoni vsebujejo izredno občutljive informacije o lastnikovem zasebnem in poklicnem življenju ali finančnem položaju.[69] Dostop do zadevnih podatkov je lahko edini učinkovit način, ki je na voljo za preiskavo in pregon zadevnih kaznivih dejanj, da se zagotovi, da neznani storilci ne ostanejo nekaznovani. Upoštevati je treba tudi pravice tretjih oseb[70].

[65] Na obravnavi so se stališča državnega tožilstva (Bolzano) in italijanske vlade glede vloge nacionalnega sodišča in obsega predhodnega nadzora na podlagi člena 132(3) zakonske uredbe št. 196/2003 razlikovala. Medtem ko je državno tožilstvo (Bolzano) trdilo, da mora nacionalno sodišče, preden odobri dostop do takih podatkov, opraviti individualni preizkus sorazmernosti odobritve navedenega dostopa, je italijanska vlada poudarila, da nacionalno sodišče v skladu s členom 101 Costituzione della Repubblica Italiana (ustava Italijanske republike) in člena 1 kazenskega zakonika zavezuje načelo zakonitosti in ne more uporabiti kreativne razlage prava (kot je to poimenovala italijanska vlada). Predložitveno sodišče mora zagotoviti razlago določb nacionalnega prava, ki se uporabljajo.

[66] Razen če to dovoljuje nacionalno pravo in v skladu z, med drugim, členom 49 Listine.

[67] Najvišja zaporna kazen najmanj treh let.

[68] Člen 52(1) Listine določa, da mora biti kakršno koli omejevanje uresničevanja pravice, ki jo priznava Listina, predpisano z zakonom. Iz tega izhaja, da nacionalna sodišča načeloma zavezuje nacionalna zakonodaja, ki vsebuje take omejitve.

[69] Mobilni telefoni lahko vsebujejo fotografije, podatke o zdravju, bančne izpiske, gesla itd. Tatvina mobilnega telefona lahko torej pomeni poseg v digitalno identiteto lastnika, učinki tega pa lahko znatno presežejo izgubo denarne vrednosti telefona. Predložitveno sodišče bi moralo torej upoštevati tudi morebitno škodo na pravicah žrtve, med drugim na podlagi členov 7, 8 in 17 Listine.

[70] Kot so žrtve domnevnega kaznivega dejanja.

43. V zvezi s pravicami tretjih oseb iz dokumentov predložitvenega sodišča izhaja,[71] da je državno tožilstvo (Bolzano) zahtevalo dostop do podatkov v zvezi s komunikacijami iz ukradenih mobilnih telefonov od 29. oktobra 2021 naprej (glede prve tatvine, ki je bila storjena 27. oktobra 2021)[72] in od 20. novembra 2021 naprej (glede druge tatvine, ki je bila storjena na navedeni datum).[73] Iz teh datumov izhaja, da zahteve za dostop do podatkov v zelo omejeni meri posegajo v pravice žrtev, ki jih med drugim zagotavljajo členi 7, 8 in 11 Listine.[74] Italijanska vlada je v pisnih stališčih tudi navedla, da se nacionalni postopek nanaša izključno na podatke, ki bi pripomogli k identifikaciji storilca oziroma storilcev zadevnih tatvin. Če bi se odkrili klici tretjim osebam, ki niso povezane s tatvino, oziroma klici takih oseb, bi se taki podatki v skladu s členom 269 zakonika o kazenskem postopku uničili.[75] Nazadnje, člen 132(3c) zakonske uredbe št. 196/2003 določa, da se podatkov, pridobljenih v nasprotju z odstavkoma 3 ali 3a navedene zakonske uredbe, ne sme uporabiti.[76]

VI. Predlog

44. Glede na navedeno predlagam, da Sodišče na vprašanje, ki mu ga je Tribunale di Bolzano (sodišče v Bolzanu, Italija) postavilo v postopku predhodnega odločanja, odgovori:

Člen 15(1) Direktive 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), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, ter člene 7, 8, 11 in člen 52(1) Listine Evropske unije o temeljnih pravicah

je treba razlagati tako, da

ne nasprotujejo nacionalni zakonodaji, ki sodišču nalaga, naj državnemu tožilstvu odobri dostop do podatkov, ki jih zakonito hranijo ponudniki elektronskih komunikacijskih storitev in ki omogočajo natančno sklepanje o uporabnikovem zasebnem življenju, če so taki podatki upoštevni za ugotovitev dejanskega stanja in če obstaja dovolj indicev, da je bilo storjeno hudo kaznivo dejanje, kot ga opredeljuje nacionalna zakonodaja, za katero je zagrožena najvišja zaporna kazen najmanj treh let. Pred odobritvijo dostopa mora nacionalno sodišče opraviti individualno presojo, ali je poseg v temeljne pravice, ki ga pomeni tak dostop, sorazmeren, med drugim, glede na težo konkretnega kaznivega dejanja in dejansko stanje.

71 To mora preveriti predložitveno sodišče.

72 Sklicna št. RGNR 9228/2021.

73 Sklicna št. RGNR 9794/2021.

74 Čeprav se podatki lahko nanašajo na komunikacijo z žrtvijo po datumu tatvine, pa se dejansko ne nanašajo na komunikacijo žrtve ali na njene podatke o lokaciji.

75 Po navedbah italijanske vlade člen 269(2) zakonika o kazenskem postopku v različici, ki se uporablja, določa, da „[…] se zapisi hranijo do izreka pravnomočne sodbe. Vendar lahko zainteresirane stranke z namenom varovanja zaupnosti od sodnika, ki je odobril prestrezanje, zahtevajo uničenje zapisov, ki niso vključeni v spis“ (saj niso upoštevni). Čeprav dostop do podatkov, ki se nanašajo na nedolžne tretje osebe, ni omejen, pa se zdi, da nacionalna zakonodaja omejuje uporabo navedenih podatkov, kar mora preveriti predložitveno sodišče.

76 V predložitveni odločbi ni pojasnjen niti natančen pomen te določbe niti njena uporaba v praksi.