



Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 30. aprila 2024*

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Zaupnost komunikacij – Ponudniki elektronskih komunikacijskih storitev – Direktiva 2002/58/ES – Člen 15(1) – Členi 7, 8 in 11 ter člen 52(1) Listine Evropske unije o temeljnih pravicah – Dostop do teh podatkov, ki ga zahteva pristojni nacionalni organ za pregon kaznivih dejanj tatvin z obteževalnimi okoliščinami – Opredelitev pojma ‚hudo kaznivo dejanje‘, katerega pregon lahko upraviči resen poseg v temeljne pravice – Pristojnost držav članic – Načelo sorazmernosti – Obseg predhodnega nadzora sodišča nad zahtevami za dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev“

V zadevi C-178/22,

katere predmet je predlog za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki ga je vložil Giudice delle indagini preliminari presso il Tribunale di Bolzano (preiskovalni sodnik sodišča v Bolzanu, Italija) z odločbo z dne 20. februarja 2022, ki je na Sodišče prispela 8. marca 2022, v kazenskih postopkih zoper

neznane osebe,

ob udeležbi

Procura della Repubblica presso il Tribunale di Bolzano,

SODIŠČE (veliki senat),

v sestavi K. Lenaerts, predsednik, L. Bay Larsen, podpredsednik, A. Arabadjiev, predsednik senata, A. Prechal, K. Jürimäe, predsednici senatov, T. von Danwitz in Z. Csehi, predsednika senatov, J.-C. Bonichot, S. Rodin, P. G. Xuereb (poročevalec), D. Gratsias, sodniki, M. L. Arastey Sahún, sodnica, in M. Gavalec, sodnik,

generalni pravobranilec: A. M. Collins,

sodni tajnik: C. Di Bella, administrator,

na podlagi pisnega postopka in obravnave z dne 21. marca 2023,

* Jezik postopka: italijanščina.

ob upoštevanju stališč, ki so jih predložili:

- za Procura della Repubblica presso il Tribunale di Bolzano F. Iovene, sostituto procuratore della Repubblica,
- za italijansko vlado G. Palmieri, agentka, skupaj s S. Faracijem, avvocato dello Stato,
- za češko vlado A. Edelmannová, O. Serdula, M. Smolek, T. Suchá in J. Vlácil, agenti,
- za estonsko vlado M. Kriisa, agentka,
- za Irsko M. Browne, Chief State Solicitor, A. Joyce in M. Tierney, agenta, skupaj z D. Fennellyjem, BL,
- za francosko vlado A. Daniel, A.-L. Desjonquères, B. Fodda in J. Illouz, agenti,
- za ciprsko vlado E. Neophytou, agentka,
- za madžarsko vlado Zs. Biró-Tóth in M. Z. Fehér, agenta,
- za nizozemsko vlado M. K. Bulterman, A. Hanje in J. Langer, agenti,
- za avstrijsko vlado A. Posch, J. Schmoll, C. Gabauer, K. Ibili in E. Samoilova, agenti,
- za poljsko vlado B. Majczyna, D. Lutostańska in J. Sawicka, agenti,
- za Evropsko komisijo S. L. Kaléda, H. Kranenborg, L. Malferrari in F. Wilman, agenti,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 8. junija 2023

izreka naslednjo

Sodbo

- 1 Predlog za sprejetje prehodne odločbe se nanaša na razlago člena 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) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11) (v nadaljevanju: Direktiva 2002/58), glede na člene 7, 8 in 11 ter člen 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).
- 2 Ta predlog je bil vložen v okviru predložitve zadeve Giudice delle indagini preliminari presso il Tribunale di Bolzano (preiskovalni sodnik sodišča v Bolzanu, Italija) s strani Procura della Repubblica presso il Tribunale di Bolzano (državno tožilstvo pri sodišču v Bolzanu, Italija) (v nadaljevanju: državno tožilstvo), da bi mu ta sodnik dovolil dostop do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, za identifikacijo storilcev dveh tatvin mobilnih telefonov z obteževalnimi okoliščinami.

Pravni okvir

Pravo Unije

Direktiva 2002/58

3 V uvodnih izjavah 2 in 11 Direktive 2002/58 je navedeno:

„(2) Ta direktiva uveljavlja spoštovanje temeljnih pravic in upošteva načela, priznana zlasti z [Listino]. Zlasti pa želi ta direktiva zagotoviti popolno spoštovanje pravic, določenih v členih 7 in 8 [te listine].

[...]

(11) Ta direktiva, tako kot Direktiva [Evropskega parlamenta in Sveta] 95/46/ES [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)], ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red Skupnosti. Zato ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito javne varnosti, obrambe, državne varnosti (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve državne varnosti) in izvajanje kazenske zakonodaje. Ta direktiva torej ne vpliva na zmožnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so potrebni iz katerega koli od teh namenov ter v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin[, podpisano v Rimu 4. novembra 1950], kakor jo razlaga Evropsko sodišče za človekove pravice v svojih sodbah. Taki ukrepi morajo biti ustrezni, dosledno sorazmerni z namenom in potrebni v demokratični družbi ter predmet primernih zaščitnih ukrepov v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.“

4 Člen 2 te direktive, naslovljen „Opredelitve“, določa:

„Razen če je drugače določeno, se uporabijo opredelitve pojmov iz Direktive [95/46] in Direktive 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva) [(UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 349)].

Uporabijo se tudi naslednje opredelitve pojmov:

- (a) ‚uporabnik‘ pomeni vsako fizično osebo, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev;
- (b) ‚podatki o prometu‘ pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila;

- (c) ‚podatki o lokaciji‘ pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve;
- (d) ‚sporočilo‘ (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve. To ne vključuje nobenih podatkov, prenesenih javnosti kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da podatek povezati s prepoznavnim naročnikom ali uporabnikom, ki ga prejme;

[...].“

5 Člen 5 navedene direktive, naslovljen „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). Ta odstavek ne preprečuje tehničnega shranjevanja, ki je potrebno za prenos sporočila, brez vpliva na načelo zaupnosti.

[...]

3. Države članice zagotovijo, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo [95/46], med drugim o namenih obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.“

6 Člen 6 iste direktive, naslovljen „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).

2. Podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave, se lahko obdelujejo. Taka obdelava je dovoljena samo do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila.

3. Za namen trženja elektronskih komunikacijskih storitev ali zagotovitve storitev z dodano vrednostjo lahko ponudnik javno razpoložljive elektronske komunikacijske storitve obdelava podatke iz odstavka 1 v obsegu in trajanju, ki sta potrebna za takšne storitve ali trženje, če naročnik ali uporabnik, na katerega se podatki nanašajo, v to prej privoli. Uporabnikom ali naročnikom je dana možnost, da kadar koli umaknejo privolitev v obdelavo podatkov o prometu.

[...]

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.

[...]“

- 7 Člen 9 Direktive 2002/58, naslovljen „Podatki o lokaciji razen podatkov o prometu“, v odstavku 1 določa:

„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. [...]“

- 8 Člen 15 te direktive, naslovljen „Uporaba nekaterih določb Direktive [95/46]“, v odstavku 1 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 ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]. 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, vključno s tistimi iz člena 6(1) in (2) [PEU].“

Italijansko pravo

Zakonska uredba št. 196/2003

- 9 Člen 132(3) decreto legislativo n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (zakonska uredba št. 196 o zakoniku na področju varstva osebnih podatkov glede določb za prilagoditev nacionalnega prava Uredbi (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) z dne 30. junija 2003 (redni dodatek h GURI št. 174 z dne 29. julija 2003) v različici, ki se uporablja za spor o glavni stvari (v nadaljevanju: zakonska uredba št. 196/2003), določa:

„Če v zakonsko določenem obdobju hrambe 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 [codice di procedura penale (zakonik 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.“

10 Odstavek 3a tega člena določa:

„Če so izpolnjeni razlogi za nujnost in je mogoče utemeljeno šteti, da bi odlašanje hudo škodovalo preiskavi, državno tožilstvo odredi pridobitev podatkov z obrazloženim sklepom, ki se nemudoma in najpozneje v 48 urah posreduje pristojnemu sodišču za redno izdajo dovoljenja. Sodišče v naslednjih 48 urah odloči o potrditvi z obrazloženim sklepom.“

11 Nazadnje, v skladu z odstavkom 3c navedenega člena „[p]odatkov, pridobljenih s kršitvijo določb odstavkov 3 in 3a, ni mogoče uporabiti.“

Kazenski zakonik

12 Člen 624 codice penale (kazenski zakonik), naslovljen „Tatvina“, določa:

„Kdor si prilasti tujo premično stvar tako, da jo odtuji od njenega imetnika, da bi zase ali za drugega pridobil premoženjsko korist, se kaznuje z zaporom od šest mesecev do treh let in denarno kaznijo od 154 do 516 EUR.

[...]

Kaznivo dejanje se kaznuje na predlog oškodovanca, razen če je izpolnjen eden ali več pogojev iz člena 61(7) in člena 625.“

13 Člen 625, prvi odstavek, kazenskega zakonika, naslovljen „Obteževalne okoliščine“, določa:

„Dejanje iz člena 624 se kaznuje z zaporom od dveh do šest let in z denarno kaznijo od 927 do 1500 EUR:

[...]

2) če storilec uporabi silo na stvari ali kakršno koli goljufivo sredstvo;

3) če ima storilec pri sebi orožje ali droge, ne da jih uporabi;

4) če gre za tatvino, storjeno na posebno predrzen način;

5) če dejanje storijo tri osebe ali več, ali celo ena sama, zamaskirana v policista ali se izdaja za policista ali zamaskirana v javnega uradnika ali osebo, ki opravlja javno funkcijo, ali se izdaja zanjo;

6) če se dejanje nanaša na prtljago potnikov v katerem koli vozilu, na postajah, na letališčih ali na peronih, v hotelih ali katerem koli obratu za prodajo živil ali pijač;

7) če se dejanje nanaša na stvari, ki so v pisarnah ali javnih ustanovah, ali ki so zasežene ali zarubljene, ali ki so zaradi nujnosti ali običajev ali namembnosti dostopne javnosti, ali ki so namenjene javni službi ali javnim interesom, obrambi ali čaščenju;

7a) če se dejanje nanaša na kovinske dele ali druge materiale, odstranjene z infrastruktur, namenjenih oskrbi z energijo, prevozne ali telekomunikacijske storitve ali druge javne storitve, ki jih opravljajo javni ali zasebni subjekti v okviru javne koncesije;

8) če se dejanje nanaša na tri ali več glav živine v čredi ali goveda ali kopitarjev, tudi če niso v čredi;

8a) če je dejanje storjeno v sredstvih javnega prevoza;

8c) če je dejanje storjeno zoper osebo, ki v tistem trenutku uporablja ali ki bo uporabila storitve kreditne institucije, poštne urada ali bankomata.“

Zakonik o kazenskem postopku

14 Člen 4 zakonika o kazenskem postopku, naslovljen „Pravila za določanje pristojnosti“, določa:

„Pristojnost se ugotavlja glede na kazni, ki je po zakonu zagrožena za storitev ali poskus kaznivega dejanja. Ne upoštevajo se nadaljevanje, ponovitev in okoliščine kaznivega dejanja, razen obteževalnih okoliščin, za katere je po zakonu zagrožena drugačna kazni od tiste za navadno kaznivo dejanje, in okoliščin s posebnim učinkom.“

15 Člen 269(2) tega zakonika določa:

„[...] zapisi se hranijo do izdaje pravnomočne sodbe. Vendar lahko zadevne osebe zaradi varstva zaupnosti – kadar dokumenti niso nujni za postopek – pri sodišču, ki je dovolilo ali potrdilo prestrezanje, zaprosijo za uničenje zapisov.“

Spor o glavni stvari in vprašanje za predhodno odločanje

16 Državno tožilstvo je na podlagi dveh ovadb, vloženih glede kaznivih dejanj tatvin mobilnega telefona, storjenih 27. oktobra oziroma 20. novembra 2021, na podlagi členov 624 in 625 kazenskega zakonika začelo kazenska postopka proti neznanim storilcem za kazniva dejanja tatvine z obteževalnimi okoliščinami.

17 Državno tožilstvo je, da bi identificiralo storilce teh tatvin, na podlagi člena 132(3) zakonske uredbe št. 196/2003 7. decembra oziroma 30. decembra 2021 pri Giudice delle indagini preliminari presso il Tribunale di Bolzano (preiskovalni sodnik sodišča v Bolzanu), ki je predložitveno sodišče, vložilo zahteve za dovoljenje, da pri vseh telefonskih družbah pridobi telefonske evidence v zvezi z ukradenima telefonoma. Ti zahteve sta se nanašali na „vse podatke[, ki jih imajo telefonske družbe,] s sredstvi za sledenje in lokalizacijo (zlasti na naročnike in po možnosti klicane/kličoče kode [glede mednarodne identitete mobilne opreme (IMEI)], obiskana/dosežena spletna mesta, čas in trajanje klica/povezave ter navedbo zadevnih celic in/ali repetitorjev, naročnike in kode IMEI [naprav] pošiljateljev/prejemnikov sporočil SMS ali MMS

in, če je mogoče, podatke o zadevnih imetnikih) telefonskih pogovorov/komunikacij in opravljenih povezav, tudi med gostovanjem, dohodnih in izhodnih ter tudi tistih, ki niso obračunane (neodgovorjeni klici) od datuma tatvine do datuma priprave zahtev“.

- 18 Predložitveno sodišče dvomi, da je člen 132(3) zakonske uredbe št. 196/2003 skladen s členom 15(1) Direktive 2002/58, kot ga je Sodišče razložilo v sodbi z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2021:152).
- 19 Opozarja, da je na podlagi točke 45 navedene sodbe nacionalne določbe, ki javnim organom dovoljujejo dostop do telefonskih evidenc, ki zajemajo vse podatke o prometu ali lokaciji, iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju zadevnega uporabnika, ob upoštevanju načela sorazmernosti, določenega v členu 52(1) Listine, in teže posega v temeljne pravice do zasebnosti, varstva osebnih podatkov ter svobode izražanja in obveščanja, kot so zagotovljene v členih 7, 8 oziroma 11 Listine, mogoče upravičiti samo, če gre za pregon hudih kaznivih dejanj, kot so resne grožnje javne varnosti, ki se razume kot varnost države, in druge oblike hudega kriminala.
- 20 Glede tega predložitveno sodišče navaja, da je Corte suprema di cassazione (vrhovno kasacijsko sodišče, Italija) v sodbi št. 33116 z dne 7. septembra 2021 menilo, da glede na razlagalno polje proste presoje pri opredelitvi, katera kazniva dejanja pomenijo resno grožnjo javni varnosti ali druge oblike hudega kriminala, v smislu sodne prakse Sodišča, ta sodna praksa ni imela značilnosti, ki se zahtevajo za to, da jo nacionalna sodišča uporabljajo neposredno. Zato naj bi italijanski zakonodajalec spremenil člen 132(3) zakonske uredbe št. 196/2003, tako da bi se kot huda kazniva dejanja, zaradi katerih se lahko pridobijo telefonske evidence, opredelila kazniva dejanja, ki se po zakonu kaznujejo z najvišjo zaporno kaznijo „najmanj treh let“.
- 21 Po mnenju predložitvenega sodišča je ta prag treh let, od katerega dalje najvišja zaporna kazen za kaznivo dejanje upravičuje, da se v primeru tega kaznivega dejanja lahko sporočajo telefonske evidence javnim organom, tak, da bi bilo te evidence mogoče sporočiti tem organom za pregon kaznivih dejanj, ki nimajo hudih družbenih posledic in se lahko preganjajo le na predlog oškodovanca, med drugim tatvine majhne vrednosti, kot je tatvina mobilnega telefona ali kolesa.
- 22 Z zadevno nacionalno določbo naj bi bilo tako kršeno načelo sorazmernosti, določeno v členu 52(1) Listine, ki zahteva, da se resnost kaznivega dejanja uravnoteži s temeljnimi pravicami, v katere se posega za pregon kaznivega dejanja. To načelo naj bi namreč nasprotovalo temu, da se poseg v temeljne pravice, zagotovljene s členi 7, 8 in 11 Listine, upraviči s pregonom kaznivega dejanja, kot je tatvina.
- 23 Predložitveno sodišče pojasnjuje, da imajo italijanska sodišča zelo omejeno polje proste presoje glede zavrnitve dovoljenja za pridobitev telefonskih evidenc, saj je treba na podlagi zadevne določbe dovoljenje dati, če obstaja „dovolj indicev za kaznivo dejanje“ in če so zaproseni podatki „upoštevni za ugotovitev dejanskega stanja“. Italijanska sodišča naj torej ne bi imela polja proste presoje glede konkretne teže kaznivega dejanja, ki je predmet preiskave. To presojo naj bi dokončno opravil italijanski zakonodajalec, ko je določil, da je treba dovoljenje za pridobitev podatkov dati med drugim za vsa kazniva dejanja, ki se kaznujejo z zaporno kaznijo najmanj treh let.

- 24 V teh okoliščinah je Giudice delle indagini preliminari presso il Tribunale di Bolzano (preiskovalni sodnik sodišča v Bolzanu) prekinil odločanje in Sodišču v predhodno odločanje predložil to vprašanje:

„Ali člen 15(1) [Direktive 2002/58] nasprotuje nacionalni zakonodaji v členu 132[(3) zakonske uredbe št. 196/2003, ki] [...] določa:

„3. Če v zakonsko določenem obdobjem hrambe 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 upoštevnosti 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.““

Dopustnost predloga za sprejetje predhodne odločbe

- 25 Italijanska vlada in Irska menita, da predlog za sprejetje predhodne odločbe deloma ni dopusten. Navajata, da je državno tožilstvo na podlagi člena 132(3) zakonske uredbe št. 196/2003 zahteva za dostop do podatkov, ki jih hranijo ponudniki elektronskih telekomunikacijskih storitev, vložilo za pregon kaznivih dejanj tatvin mobilnih telefonov z obteževalnimi okoliščinami. Predložitveno sodišče pa naj bi Sodišče spraševalo tudi, ali člen 15(1) Direktive 2002/58 nasprotuje nacionalni določbi, ki dovoljuje pridobitev dostopa do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, za pregon drugih kaznivih dejanj, zajetih s členom 132(3) zakonske uredbe št. 196/2003, od tistih iz postopka v glavni stvari, kakršna sta navadna tatvina ali hudo nadlegovanje po telefonu. Zato naj bi bil predlog za sprejetje predhodne odločbe hipotetičen v delu, v katerem se nanaša na druga kazniva dejanja.
- 26 Glede tega je treba opozoriti, da je v skladu z ustaljeno sodno prakso v okviru sodelovanja med Sodiščem in nacionalnimi sodišči, ki ga določa člen 267 PDEU, le nacionalno sodišče, ki odloča o sporu in ki mora prevzeti odgovornost za sodno odločbo, ki bo izdana, pristojno, da ob upoštevanju posebnosti zadeve presodi potrebo po predhodni odločbi, da bi lahko izdalo sodbo, in tudi upoštevnost vprašanj, ki jih postavi Sodišču. Zato je Sodišče, kadar se predložena vprašanja nanašajo na razlago prava Unije, načeloma dolžno odločiti (sodba z dne 21. marca 2023, Mercedes-Benz Group (Odgovornost proizvajalcev vozil, opremljenih z odklopnimi napravami), C-100/21, EU:C:2023:229, točka 52 in navedena sodna praksa).
- 27 Iz tega sledi, da za vprašanja, ki se nanašajo na pravo Unije, velja domneva upoštevnosti. Sodišče lahko zavrne odločanje o vprašanju nacionalnega sodišča za predhodno odločanje samo, če je očitno, da zahtevana razlaga prava Unije nima nobene zveze z dejanskim stanjem ali predmetom spora o glavni stvari, če je problem hipotetičen ali če Sodišče nima na voljo dejanskih in pravnih elementov, ki so potrebni, da bi lahko na postavljena vprašanja dalo koristne odgovore (sodba z dne 21. marca 2023, Mercedes-Benz Group (Odgovornost proizvajalcev vozil, opremljenih z odklopnimi napravami), C-100/21, EU:C:2023:229, točka 53 in navedena sodna praksa).
- 28 Vprašanje za predhodno odločanje pa s tem, da je v njem v celoti citiran člen 132(3) zakonske uredbe št. 196/2003, čeprav ne razlikuje med vrstami kaznivih dejanj, za katera se uporablja ta določba, nujno zajema kazniva dejanja tatvin z obteževalnimi okoliščinami, za katera sta bili v postopku v glavni stvari vloženi zahtevi za dovoljenje za dostop do osebnih podatkov.

29 Zato to vprašanje ni hipotetično in je torej dopustno.

Vprašanje za predhodno odločanje

- 30 Kot je francoska vlada navedla v pisnih stališčih, je Sodišče z vprašanjem, ki ga je postavilo predložitveno sodišče, kakor je formulirano, zaproseno, naj odloči o skladnosti člena 132(3) zakonske uredbe št. 196/2003 s členom 15(1) Direktive 2002/58.
- 31 V zvezi s tem je treba opozoriti, da v okviru postopka iz člena 267 PDEU Sodišče ni pristojno za odločanje niti o razlagi določb nacionalnih zakonov in drugih predpisov niti o skladnosti takih določb s pravom Unije. Iz ustaljene sodne prakse je namreč razvidno, da lahko Sodišče v okviru predloga za sprejetje predhodne odločbe na podlagi člena 267 PDEU razlaga pravo Unije le v mejah pristojnosti, ki so dodeljene Uniji (sodba z dne 14. decembra 2023, Getin Noble Bank (Zastaralni rok za zahtevke za vračilo), C-28/22, EU:C:2023:992, točka 53 in navedena sodna praksa).
- 32 Iz ustaljene sodne prakse pa je razvidno, da mora Sodišče, če so bila vprašanja neprimerno oblikovana ali če presegajo okvir nalog, ki jih ima v skladu s členom 267 PDEU, iz vseh elementov, ki jih je predložilo nacionalno sodišče, in zlasti iz obrazložitve predložitvene odločbe izluščiti elemente prava Unije, ki jih je treba razložiti ob upoštevanju predmeta spora. S tega vidika mora Sodišče po potrebi preoblikovati vprašanja, ki so mu bila predložena (sodba z dne 14. decembra 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, točka 20 in navedena sodna praksa).
- 33 Poleg tega lahko Sodišče presodi, da je treba upoštevati določbe prava Unije, na katere se nacionalno sodišče v besedilu svojega vprašanja ni sklicevalo (sodba z dne 17. novembra 2022, Harman International Industries, C-175/21, EU:C:2022:895, točka 31 in navedena sodna praksa).
- 34 Glede na navedeno je treba šteti, da predložitveno sodišče z vprašanjem v bistvu sprašuje, ali je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8 in 11 ter na člen 52(1) Listine razlagati tako, da nasprotuje nacionalni določbi, ki nacionalnemu sodišču, ki v okviru predhodnega nadzora, opravljenega na obrazloženo zahtevo po dostopu do vseh podatkov o prometu ali podatkov o lokaciji, iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju uporabnika elektronskega komunikacijskega sredstva in ki jih hranijo ponudniki elektronskih komunikacijskih storitev, pri čemer je to zahtevo vložil pristojni nacionalni organ v okviru kazenske preiskave, nalaga, naj ta dostop dovoli, če se zahteva za preiskovanje kaznivih dejanj, ki se po nacionalnem pravu kaznujejo z najvišjo zaporno kaznijo najmanj treh let, pod pogojem, da obstaja dovolj indicov za taka kazniva dejanja in da so ti podatki upoštevní za ugotovitev dejanskega stanja.
- 35 Uvodoma je treba spomniti, da je Sodišče glede pogojev, pod katerimi se lahko na podlagi zakonodajnega ukrepa, sprejetega na podlagi člena 15(1) Direktive 2002/58, javnim organom zaradi preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj dovoli dostop do podatkov o prometu in lokaciji, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, razsodilo, da je tak dostop mogoče dovoliti le, če so ti ponudniki te podatke hranili na način, ki je v skladu s to direktivo (glej v tem smislu sodbo z današnjega dne, La Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju), C-470/21, točka 65 in navedena sodna praksa). Razsodilo je tudi, da ta člen 15(1) glede na člene 7, 8 in 11 ter na člen 52(1) Listine nasprotuje zakonodajnim ukrepom, ki preventivno določajo splošno in neselektivno hrambo podatkov

o prometu in podatkov o lokaciji (sodba z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, EU:C:2021:152, točka 30 in navedena sodna praksa).

- 36 Spomniti je treba tudi na sodno prakso Sodišča, v skladu s katero se lahko resen poseg v temeljne pravice, določene v členih 7 in 8 Listine, ki je posledica dostopa javnih organov do vseh podatkov o prometu ali lokaciji, iz katerih so lahko razvidne informacije o komunikacijah uporabnika elektronskega komunikacijskega sredstva ali o lokaciji uporabljene terminalske opreme in iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju posameznikov, na katere se nanašajo osebni podatki, upraviči samo s ciljema boja proti hudemu kriminalu in preprečevanja hudih nevarnosti za javno varnost, ne da bi lahko drugi dejavniki, povezani s sorazmernostjo zahteve za dostop, kot je trajanje obdobja, za katero se zahteva dostop do takih podatkov, učinkovali tako, da bi bilo mogoče tak dostop upravičiti s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno (glej v tem smislu sodbo z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, EU:C:2021:152, točka 35 in navedena sodna praksa).
- 37 Predložitveno sodišče z vprašanjem v bistvu želi izvedeti, ali je tak resen poseg mogoče dovoliti za kazniva dejanja, kakršna so ta iz nacionalne ureditve iz postopka v glavni stvari.
- 38 Najprej, glede vprašanja, ali je dostop, kakršen je ta iz postopka v glavni stvari, mogoče opredeliti kot resen poseg v temeljne pravice, zagotovljene s členoma 7 in 8 Listine, je treba navesti, da je državno tožilstvo za identifikacijo storilcev domnevnih tatvin, ki so podlaga za ta spor, pri predložitvenem sodišču na podlagi člena 132(3) zakonske uredbe št. 196/2003 za vsakega od zadevnih mobilnih telefonov vložilo zahtevo za dovoljenje za pridobitev vseh podatkov, ki jih imajo telefonske družbe in se pridobijo s sredstvi za sledenje in lokalizacijo telefonskih pogovorov in komunikacij ter povezav, opravljenih s temi telefoni. Ti zahtevi sta se nanašali, natančneje, na naročnike in kode IMEI klicanih/kličočih naprav, obiskana/dosežena spletna mesta, čas in trajanje klicev in povezav, navedbo zadevnih celic ali repetitorjev ter naročnike in kode IMEI pošiljateljcev/prejemnikov sporočil SMS ali MMS.
- 39 Na podlagi dostopa do take celote podatkov o prometu ali lokaciji je očitno mogoče natančno sklepati o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraj stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi teh oseb in družbeni krogi, v katerih se gibljejo (glej v tem smislu sodbo z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, EU:C:2021:152, točka 36 in navedena sodna praksa). Poseg v temeljne pravice, zagotovljene s členoma 7 in 8 Listine, ki je posledica dostopa do takih podatkov, je torej očitno mogoče opredeliti kot resen.
- 40 Kot je razvidno iz točke 39 sodbe z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2021:152), take presoje ni mogoče ovreči zgolj zato, ker sta se zadevni zahtevi za dostop do podatkov o prometu ali podatkov o lokaciji nanašali le na kratka obdobja – manj kot dva meseca, ki sta pretekla od datumov domnevnih tatvin mobilnih telefonov do datumov, ko sta bili napisani ti zahtevi – saj sta se navedeni zahtevi nanašali na celoto teh podatkov, iz katerih so lahko razvidne natančne informacije o zasebnem življenju oseb, ki so uporabljale zadevna telefona.
- 41 Za presojo obstoja resnega posega v pravice, zagotovljene s členoma 7 in 8 Listine, prav tako ni upoštevana okoliščina, da podatki, do katerih dostop je zahtevalo državno tožilstvo, niso podatki lastnikov zadevnih mobilnih telefonov, ampak podatki oseb, ki so komunicirale med sabo

z uporabo teh telefonov po njihovih domnevnih tatvinah. Iz člena 5(1) Direktive 2002/58 namreč izhaja, da se načelna obveznost zagotavljanja zaupnosti elektronskih komunikacij in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev, nanaša na komunikacije, ki jih opravijo uporabniki tega omrežja. V členu 2(a) te direktive pa je pojem „uporabnik“ opredeljen kot vsaka fizična oseba, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev.

- 42 Zato glede na sodno prakso, navedeno v točki 36 te sodbe, velja, da kadar je poseg v temeljne pravice, ki je posledica dostopa do podatkov, kakršen je ta iz postopka v glavni stvari, očitno mogoče opredeliti kot resen, ga je mogoče upravičiti samo s ciljema boja proti hudemu kriminalu in preprečevanja hudih nevarnosti za javno varnost.
- 43 Dalje, čeprav je treba v nacionalnem pravu določiti pogoje, pod katerimi morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom odobriti dostop do podatkov, ki jih imajo, mora taka ureditev določati jasna in natančna pravila, ki urejajo obseg in pogoje uporabe takega dostopa. Tak dostop se sme v razmerju do cilja boja proti kriminalu načeloma odobriti le za podatke oseb, ki so osumljene vpletenosti v hudo kaznivo dejanje. Za to, da se v praksi zagotovi polno upoštevanje teh pogojev, ki zagotavljajo, da se poseganje omeji na to, kar je nujno potrebno, je bistveno, da sodišče ali neodvisen upravni organ pred dostopom pristojnih nacionalnih organov do hranjenih podatkov – razen v ustrezno utemeljenih nujnih primerih – opravi predhodni nadzor (glej v tem smislu sodbo z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, EU:C:2021:152, točke od 48 do 51).
- 44 Nazadnje, glede opredelitve pojma „hudo kaznivo dejanje“ je iz sodne prakse razvidno, da če Unija ne sprejema zakonodaje na tem področju, kazenska zakonodaja in pravila kazenskega postopka spadajo v pristojnost držav članic. Vendar morajo te to pristojnost izvrševati ob spoštovanju prava Unije (glej v tem smislu sodbo z dne 26. februarja 2019, Rimševičs in ECB/Latvija, C-202/18 in C-238/18, EU:C:2019:139, točka 57 in navedena sodna praksa).
- 45 Glede tega je treba opozoriti, da opredelitev kaznivih dejanj, olajševalnih in obteževalnih okoliščin ter sankcij odraža tako družbene realnosti kot pravne tradicije, ki se razlikujejo ne le med državami članicami, ampak tudi v času. Te realnosti in tradicije pa so precej pomembne za določitev kaznivih dejanj, ki se štejejo za huda.
- 46 Zato je ob upoštevanju razdelitve pristojnosti med Unijo in državami članicami na podlagi Pogodbe DEU ter pomembnih razlik, ki obstajajo med pravnimi sistemi držav članic na področju kazenskih zadev, treba ugotoviti, da morajo za uporabo člena 15(1) Direktive 2002/58 „huda kazniva dejanja“ opredeliti države članice.
- 47 Vendar morajo države članice pri opredelitvi „hudih kaznivih dejanj“ spoštovati zahteve, ki izhajajo iz tega člena 15(1) glede na člene 7, 8 in 11 ter člen 52(1) Listine.
- 48 Glede tega je treba opozoriti, da člen 15(1) Direktive 2002/58 s tem, da državam članicam omogoča, da sprejmejo zakonodajne ukrepe, katerih namen je „omejiti obseg“ pravic in obveznosti, določenih zlasti v členih 5, 6 in 9 te direktive, kot so tiste, ki izhajajo iz načel zaupnosti komunikacij in prepovedi hrambe s tem povezanih podatkov, določa izjemo od splošnega pravila, določenega zlasti v teh členih 5, 6 in 9, in ga je zato treba v skladu z ustaljeno sodno prakso razlagati ozko. Taka določba torej ne more upravičiti tega, da odstopanje od

načelne obveznosti zagotavljanja zaupnosti elektronskih komunikacij in z njimi povezanih podatkov postane pravilo, sicer bi se členu 5 navedene direktive v veliki meri odvzel njegov pomen (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 40).

- 49 Poleg tega je iz člena 15(1), tretji stavek, Direktive 2002/58 razvidno, da morajo ukrepi, ki jih države članice sprejmejo na podlagi te določbe, spoštovati splošna načela Unije, med katerimi je načelo sorazmernosti, in zagotoviti spoštovanje temeljnih pravic, zagotovljenih s členi 7, 8 in 11 Listine (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 42).
- 50 Iz tega sledi, da države članice ne smejo izkriviti pojma „hudo kaznivo dejanje“ in posledično pojma „hud kriminal“ s tem, da za uporabo tega člena 15(1) v ta pojma vključijo kazniva dejanja, ki glede na prevladujoče družbene razmere v zadevni državi članici očitno niso huda, tudi če je zakonodajalec te države članice določil, da se kaznujejo z najvišjo zaporno kaznijo treh let.
- 51 Zlasti zaradi preverjanja neobstoja takega izkrivljanja je bistveno, da kadar dostop pristojnih nacionalnih organov do shranjenih podatkov zajema tveganje za resen poseg v temeljne pravice osebe, na katero se nanašajo osebni podatki, sodišče ali neodvisen upravni organ nad tem dostopom opravi predhodni nadzor (glej v tem smislu sodbo z današnjega dne, La Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju), C-470/21, točke od 124 do 131).
- 52 V obravnavanem primeru je iz predložitvene odločbe razvidno, da člen 132(3) zakonske uredbe št. 196/2003 določa pogoje, pod katerimi lahko sodišče, ki odloča o obrazloženi zahtevi javnega organa, odobri dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev. V tej določbi so opredeljena kazniva dejanja, zaradi pregona katerih je mogoče odobriti dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, s sklicevanjem na najvišjo zaporno kazen najmanj treh let. Za ta dostop določa dva pogoja, in sicer da obstaja „dovolj indicev za kaznivo dejanje“ in da so ti podatki „upoštevni za ugotovitev dejanskega stanja“.
- 53 Predložitveno sodišče pa se sprašuje, ali iz te določbe izhajajoča opredelitev „hudih kaznivih dejanj“, zaradi pregona katerih je mogoče odobriti dostop do podatkov, ni preširoka, saj zajema kazniva dejanja, ki nimajo hudih družbenih posledic.
- 54 Glede tega je treba, prvič, navesti, da opredelitev – v skladu katero so „huda kazniva dejanja“, zaradi pregona katerih je mogoče odobriti dostop, tista, za katera je zagrožena najvišja zaporna kazen vsaj v zakonsko določenem trajanju – temelji na objektivnem merilu. To je skladno z zahtevo, v skladu s katero se mora zadevna nacionalna zakonodaja pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom odobri dostop do zadevnih podatkov, opreti na objektivna merila (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 105 in navedena sodna praksa).
- 55 Drugič, iz sodne prakse, navedene v točki 48 te sodbe, je razvidno, da opredelitev, ki je v nacionalnem pravu določena za „huda kazniva dejanja“, zaradi katerih je mogoče dovoliti dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev in iz katerih je mogoče natančno sklepati o zasebnem življenju posameznikov, na katere se nanašajo osebni podatki, ne sme biti tako široka, da bi dostop do teh podatkov postal prej pravilo kot izjema.

Tako ne more zajemati velike večine kaznivih dejanj, kar bi veljalo, če bi bil prag, nad katerim najvišja zaporna kazen, s katero se kaznuje kaznivo dejanje, upravičuje to, da bi se to dejanje opredelilo kot hudo kaznivo dejanje, določen prenizko.

- 56 Vendar se prag, določen s sklicevanjem na najvišjo zaporno kazen treh let, s tega vidika ne zdi prenizek (glej v tem smislu sodbo z dne 21. junija 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, točka 150).
- 57 Res je sicer, da kadar opredelitev „hudih kaznivih dejanj“, za katera je mogoče zahtevati dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, ni določena s sklicevanjem na najnižjo možno zagroženo kazen, ampak na najvišjo možno zagroženo kazen, ni izključeno, da je dostop do podatkov, ki pomeni resen poseg v temeljne pravice, mogoče zahtevati za pregon kaznivih dejanj, ki v resnici ne spadajo v hud kriminal (glej po analogiji sodbo z dne 21. junija 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, točka 151).
- 58 Vendar določitev praga, nad katerim najvišja zaporna kazen, s katero se kaznuje neko kaznivo dejanje, upravičuje, da se to dejanje opredeli kot hudo kaznivo dejanje, ni nujno v nasprotju z načelom sorazmernosti.
- 59 Na eni strani je očitno tako v primeru določbe, kakršna je ta iz postopka v glavni stvari, ker se – kot je razvidno iz predložitvene odločbe – na splošno nanaša na dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, ne da bi bila natančneje določena narava teh podatkov. Tako ta določba očitno zajema med drugim primere, v katerih dostopa ni mogoče opredeliti kot resen poseg, saj se ne nanaša na celoto podatkov, iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju posameznikov, na katere se nanašajo osebni podatki.
- 60 Na drugi strani mora biti sodišče ali neodvisen upravni organ v okviru predhodnega nadzora, opravljenega na obrazloženo zahtevo po dostopu, pooblaščen, da zavrne ali omeji ta dostop, kadar ugotovi, da je poseg v temeljne pravice, ki bi ga pomenil tak dostop, resen, tudi če je očitno, da zadevno kaznivo dejanje dejansko ne spada v hud kriminal (glej po analogiji sodbo z dne 21. junija 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, točka 152).
- 61 Sodišče ali organ, zadolžen za nadzor, mora imeti namreč možnost zagotoviti pravično ravnotežje med legitimnimi interesi, povezanimi s potrebami preiskave v okviru boja proti kriminalu, na eni strani ter temeljnimi pravicami do spoštovanja zasebnega življenja in varstva osebnih podatkov posameznikov, do katerih podatkov se dostopa, na drugi strani (sodba z današnjega dne, *La Quadrature du Net in drugi* (Osebni podatki in boj proti ponarejanju), C-470/21, točka 125 in navedena sodna praksa).
- 62 Natančneje, to sodišče ali ta organ mora v okviru preizkusa sorazmernosti zadevnega posega v temeljne pravice osebe, na katero se nanaša zahteva za dostop, imeti možnost izključiti tak dostop, kadar se navedeni dostop zahteva v okviru pregona kaznivega dejanja, ki očitno ni hudo, v smislu točke 50 te sodbe.
- 63 Iz zgoraj navedenega sledi, da je treba na vprašanje za predhodno odločanje odgovoriti, da je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8 in 11 ter na člen 52(1) Listine razlagati tako, da ne nasprotuje nacionalni določbi, ki nacionalnemu sodišču, ki v okviru predhodnega nadzora, opravljenega na obrazloženo zahtevo po dostopu do vseh podatkov o prometu ali podatkov o lokaciji, iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju uporabnika elektronskega komunikacijskega sredstva in ki jih hranijo ponudniki elektronskih komunikacijskih

storitev, pri čemer je to zahtevo vložil pristojni nacionalni organ v okviru kazenske preiskave, nalaga, naj ta dostop dovoli, če se navedeni dostop zahteva za preiskovanje kaznivih dejanj, ki se po nacionalnem pravu kaznujejo z najvišjo zaporno kaznijo najmanj treh let, s pridržkom da obstaja dovolj indicev za taka kazniva dejanja in da so ti podatki upoštevni za ugotovitev dejanskega stanja, vendar pod pogojem, da je to sodišče pooblaščen, da navedeni dostop zavrne, če se ta dostop zahteva v okviru preiskave v zvezi s kaznivim dejanjem, ki glede na prevladujoče družbene razmere v zadevni državi članici očitno ni hudo.

Stroški

- 64 Ker je ta postopek za stranke v postopku v glavni stvari ena od stopenj v postopku pred predložitvenim sodiščem, to odloči o stroških. Stroški za predložitev stališč Sodišču, ki niso stroški omenjenih strank, se ne povrnejo.

Iz teh razlogov je Sodišče (veliki senat) razsodilo:

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, glede na člene 7, 8 in 11 ter na člen 52(1) Listine Evropske unije o temeljnih pravicah

je treba razlagati tako, da

ne nasprotuje nacionalni določbi, ki nacionalnemu sodišču, ki v okviru predhodnega nadzora, opravljenega na obrazloženo zahtevo po dostopu do vseh podatkov o prometu ali podatkov o lokaciji, iz katerih bi bilo mogoče natančno sklepati o zasebnem življenju uporabnika elektronskega komunikacijskega sredstva in ki jih hranijo ponudniki elektronskih komunikacijskih storitev, pri čemer je to zahtevo vložil pristojni nacionalni organ v okviru kazenske preiskave, nalaga, naj ta dostop dovoli, če se navedeni dostop zahteva za preiskovanje kaznivih dejanj, ki se po nacionalnem pravu kaznujejo z najvišjo zaporno kaznijo najmanj treh let, s pridržkom da obstaja dovolj indicev za taka kazniva dejanja in da so ti podatki upoštevni za ugotovitev dejanskega stanja, vendar pod pogojem, da je to sodišče pooblaščen, da navedeni dostop zavrne, če se ta dostop zahteva v okviru preiskave v zvezi s kaznivim dejanjem, ki glede na prevladujoče družbene razmere v zadevni državi članici očitno ni hudo.

Podpisi