



Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 20. septembra 2022 *

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Zaupnost sporočil – Ponudniki elektronskih komunikacijskih storitev – Splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji – Direktiva 2002/58/ES – Člen 15(1) – Listina Evropske unije o temeljnih pravicah – Členi 6, 7, 8 in 11 ter člen 52(1) – Člen 4(2) PEU“

V združenih zadevah C-793/19 in C-794/19,

katerih predmet sta predloga za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki ju je vložilo Bundesverwaltungsgericht (zvezno upravno sodišče, Nemčija) z odločbama z dne 25. septembra 2019, ki sta na Sodišče prispeli 29. oktobra 2019, v postopkih

Bundesrepublik Deutschland, ki jo zastopa Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

proti

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

SODIŠČE (veliki senat),

v sestavi K. Lenaerts, predsednik, A. Arabadjiev, predsednik senata, A. Prechal, predsednica senata, S. Rodin, I. Jarukaitis, predsednika senatov, in I. Ziemele, predsednica senata, T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (poročevalec), N. Piçarra, sodniki, L. S. Rossi, sodnica, in A. Kumin, sodnik,

generalni pravobranilec: M. Campos Sánchez-Bordona,

sodni tajnik: D. Dittert, vodja oddelka,

na podlagi pisnega postopka in obravnave z dne 13. septembra 2021,

ob upoštevanju stališč, ki so jih predložili:

– za Bundesrepublik Deutschland, ki jo zastopa Bundesnetzagentur für Elektrizität Gas, Telekommunikation, Post und Eisenbahnen, C. Mögelin, agent,

* Jezik postopka: nemščina.

- za SpaceNet AG M. Bäcker, Rechtsanwalt,
- za Telekom Deutschland GmbH T. Mayen, Rechtsanwalt,
- za nemško vlado J. Möller, F. Halibi, M. Hellmann, D. Klebs in E. Lankenau, agenti,
- za dansko vlado M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen in M. Søndahl Wolff, agenti,
- za estonsko vlado, A. Kalbus in M. Kriisa, agentki,
- za Irsko A. Joyce in J. Quaney, agenta, skupaj z D. Fennellyjem, BL, in P. Gallagherjem, SC,
- za špansko vlado L. Aguilera Ruiz, agent,
- za francosko vlado A. Daniel, D. Dubois, J. Illouz, E. de Moustier in T. Stéhelin, agenti,
- za ciprsko vlado I. Neophytou, agentka,
- za nizozemsko vlado M. K. Bulterman, A. Hanje in C. S. Schillemans, agentke,
- za poljsko vlado B. Majczyna, D. Lutostańska in J. Sawicka, agenti,
- za finsko vlado A. Laine in M. Pere, agentki,
- za švedsko vlado H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson in H. Shev, agentke,
- za Evropsko komisijo G. Braun, S. L. Kalèda, H. Kranenborg, M. Wasmeier in F. Wilman, agenti,
- za Evropskega nadzornika za varstvo podatkov A. Buchta, D. Nardi, N. Stolič in K. Ujazdowski, agenti,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 18. novembra 2021

izreka naslednjo

Sodbo

- 1 Predloga za sprejetje prehodne odločbe se nanašata 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) v povezavi s členi od 6 do 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina) in členom 4(2) PEU.

- 2 Ta predloga sta bila vložena v okviru sporov med Bundesrepublik Deutschland (Zvezna republika Nemčijo), ki jo zastopa Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (zvezna agencija za omrežja električne energije, plina, telekomunikacij, pošte in železnic, Nemčija), ter družbama SpaceNet AG (zadeva C-793/19) in Telekom Deutschland GmbH (zadeva C-794/19) v zvezi z obveznostjo, naloženo tema družbama, da hranita podatke o prometu in podatke o lokaciji v zvezi s telekomunikacijami svojih strank.

Pravni okvir

Pravo Unije

Direktiva 95/46/ES

- 3 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) je bila z učinkom od 25. maja 2018 razveljavljena z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1).
- 4 Člen 3(2) Direktive 95/46 je določal:

„Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

- med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI Pogodbe o Evropski uniji, in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,
- s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti.“

Direktiva 2002/58

- 5 V uvodnih izjavah 2, 6, 7 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 navedene listine.

[...]

- (6) Internet spreminja tradicionalne tržne strukture, ker ponuja skupno, globalno infrastrukturo za dobavo široke izbire elektronskih komunikacijskih storitev. Javno dostopne elektronske komunikacijske storitve prek interneta odpirajo nove možnosti uporabnikom, pa tudi nova tveganja za njihove osebne podatke in zasebnost.

(7) V primeru javnih komunikacijskih omrežij je treba sprejeti posebne zakone in druge predpise, s katerimi se zavarujejo temeljne pravice in svoboščine fizičnih oseb ter zakoniti interesi pravnih oseb, zlasti v zvezi s čedalje večjo zmogljivostjo samodejnega shranjevanja in obdelave podatkov, ki se nanašajo na naročnike in uporabnike.

[...]

(11) Ta direktiva, tako kot Direktiva [95/46], 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.“

6 Člen 1 te direktive, naslovljen „Področje in cilj“, določa:

„1. Ta direktiva določa uskladitev [harmonizacijo] določb držav članic, ki je potrebna za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v Skupnosti.

2. Določbe te direktive podrobno opredeljujejo in dopolnjujejo Direktivo [95/46] za namene, navedene v odstavku 1. Razen tega predvidevajo varstvo zakonitih interesov naročnikov, ki so pravne osebe.

3. Ta direktiva se ne uporablja za dejavnosti, ki so zunaj obsega [Pogodbe DEU], kot na primer tiste, zajete v Oddelkih V in VI Pogodbe [EU] in v vsakem primeru za dejavnosti v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo) ter dejavnosti države na področju kazenskega prava.“

7 Člen 2 navedene 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;

[...]“

- 8 Člen 3 Direktive 2002/58, naslovljen „Storitve“, določa:

„Ta direktiva se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Skupnosti, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave.“

- 9 Člen 5 te 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.“

10 Člen 6 Direktive 2002/58, 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 člena 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 privolitve 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.

[...]“

11 Člen 9 te direktive, 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. [...]“

12 Člen 15 Direktive 2002/58, 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 [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 [kaznivih] 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 [hrambo] 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].“

Nemško pravo

TKG

- 13 Člen 113a(1), prvi stavek, Telekommunikationsgesetz (zakon o telekomunikacijah) z dne 22. junija 2004 (BGBl. 2004 I, str. 1190) v različici, ki se uporablja za spor o glavni stvari (v nadaljevanju: TKG), določa:

„Obveznosti v zvezi s shranjevanjem, uporabo in varnostjo podatkov o prometu, opredeljene v členih od 113b do 113g, se nanašajo na operaterje, ki končnim uporabnikom zagotavljajo javno dostopne telekomunikacijske storitve.“

- 14 Člen 113b TKG določa:

„(1) Operaterji, omenjeni v členu 113a(1), morajo podatke shranjevati na državnem ozemlju na naslednji način:

1. podatke iz odstavkov 2 in 3 deset tednov,
2. podatke o lokaciji iz odstavka 4 štiri tedne.

(2) Ponudniki javno dostopnih telefonskih storitev shranjujejo:

1. klicano telefonsko številko ali kakšno drugo identiteto kličočega priključka in priključka v zvezi ter pri preklapljanju ali preusmeritvi klicev klicano telefonsko številko ali kakšno drugo identiteto vsakega naslednjega udeležene priključka,
2. datum in čas začetka in konca povezave z navedbo časovnega pasu,
3. podatke o uporabljeni storitvi, kadar se lahko v okviru telefonske storitve uporabljajo različne storitve,
4. v primeru storitev mobilne telefonije tudi
 - (a) mednarodno identiteto naročnika mobilne telefonije za kličoči in klicani priključek,
 - (b) mednarodno identiteto kličočega in klicanega telefonskega terminala,
 - (c) datum in čas prve aktivacije storitve z navedbo časovnega pasu, če se storitve plačujejo vnaprej,
5. v primeru internetne telefonije tudi naslove IP (internetnega protokola) kličočega in klicanega priključka ter dodeljene identifikacijske številke.

Prvi pododstavek se smiselno uporablja

1. v primeru komunikacije po SMS, večpredstavnostnem ali podobnem sporočilu; v tem primeru se navedbe iz prvega pododstavka, točka 2, nadomestijo s časom pošiljanja in prejema sporočila;
2. za neodgovorjene klice ali klice, ki niso bili uspešni zaradi posredovanja upravljavca omrežja [...].

(3) Ponudniki javno dostopnih storitev dostopa do interneta shranjujejo

1. naslov IP, dodeljen naročniku za uporabo interneta,
2. jasno identifikacijo povezave, ki omogoča dostop do interneta, in dodeljeno identifikacijsko številko,
3. datum in čas začetka in konca uporabe interneta z dodeljenega naslova IP, z navedbo časovnega pasu.

(4) Če se uporabljajo storitve mobilne telefonije, je treba shranjevati oznako telefonskih celic, ki se uporabljajo na začetku komunikacije s strani kličočega in klicanega priključka. V zvezi s storitvami dostopa do interneta, ki so dostopne javnosti, je treba v primeru mobilne uporabe shranjevati oznako telefonske celice, ki se uporabi na začetku internetne povezave. Prav tako je treba shranjevati podatke, iz katerih sta razvidna zemljepisna lega in glavna smer sevanja anten, ki pokrivajo posamezno telefonsko celico.

(5) Vsebina komunikacije, podatki o obiskanih spletnih straneh in podatki o storitvah elektronske pošte se v skladu s to določbo ne smejo shranjevati.

(6) Podatki, ki so podlaga za komunikacije iz člena 99(2), se v skladu s to določbo ne smejo shranjevati. To smiselno velja za telefonske komunikacije, ki izvirajo od subjektov iz člena 99(2). Člen 99(2), od drugega do sedmega stavka, se uporablja smiselno.

[...]

15 Komunikacije iz člena 99(2) TKG, na katere napotuje člen 113b(6) TKG, so komunikacije z osebami, organi in organizacijami socialne ali verske narave, ki klicateljem, ki ostanejo načeloma anonimni, ponujajo izključno ali predvsem storitve telefonske pomoči v primerih psihološke ali socialne stiske in za katere oziroma za zaposlene katerih v zvezi s tem veljajo posebne obveznosti varovanja zaupnosti. Odstopanje iz člena 99(2), drugi in četrti stavek, TKG je pogojeno z vpisom klicanih priključkov na seznam, ki ga vodi zvezna agencija za omrežja električne energije, plina, telekomunikacij, pošte in železnic, potem ko imetniki številčk dokažejo svojo nalogo s predložitvijo potrdila, ki ga izda javnopravna institucija, organizacija ali ustanova.

16 Člen 113c(1) in (2) TKG določa:

„(1) Podatki, shranjeni na podlagi člena 113b, se lahko

1. posredujejo organu pregona, če ta zahteva razkritje na podlagi zakonske določbe, ki ga pooblašča za zbiranje podatkov iz člena 113b za pregon posebej hudih kaznivih dejanj;
2. posredujejo organu za varnost dežel, če ta zahteva razkritje na podlagi zakonske določbe, ki ga pooblašča za zbiranje podatkov iz člena 113b za preprečevanje konkretne nevarnosti za telesno nedotakljivost, življenje ali svobodo osebe ali pa za obstoj zvezne države ali zvezne dežele;

[...]

(2) Podatke, shranjene na podlagi člena 113b, lahko tisti, za katere veljajo obveznosti, določene v členu 113a(1), uporabljajo samo za namene, določene v odstavku 1.“

17 Člen 113d TKG določa:

„Naslovnik obveznosti iz člena 113a(1) mora zagotoviti, da so podatki, ki se shranjujejo v skladu s členom 113b(1) na podlagi obveznosti hrambe, pred nedovoljeno seznanitvijo z njimi in njihovo uporabo zaščiteni s tehničnimi in organizacijskimi ukrepi, skladnimi s stanjem tehnike. Ti ukrepi vključujejo zlasti:

1. uporabo posebej varnega postopka šifriranja,
2. shranjevanje v prostorih za shranjevanje, ki so ločeni od tistih, ki se uporabljajo za tekoče operativne naloge,
3. shranjevanje z visoko ravno varstva pred kibernetскими napadi v informacijskih sistemih za obdelavo podatkov, ki niso povezani z internetom,
4. omejitev dostopa do naprav, ki se uporabljajo za obdelavo podatkov, na osebe, ki imajo posebno pooblastilo naslovnika obveznosti, in
5. obveznost, da sta pri dostopu do podatkov udeleženi vsaj dve osebi, ki ju je naslovnik obveznosti za to posebej pooblastil.“

18 Člen 113e TKG določa:

„(1) Naslovnik obveznosti iz člena 113a(1) mora zagotoviti, da se za namene nadzora nad varstvom podatkov zabeleži vsak dostop do in zlasti branje, kopiranje, spreminjanje, brisanje in blokiranje podatkov, ki se na podlagi obveznosti hrambe shranjujejo v skladu s členom 113b(1). Zabeležiti je treba

1. čas dostopa,
2. osebe, ki dostopajo do podatkov,
3. predmet in naravo dostopa.

(2) Zabeleženi podatki se ne smejo uporabljati za druge namene kot za nadzor varstva podatkov.

(3) Naslovnik obveznosti iz člena 113a(1) mora zagotoviti, da se zabeleženi podatki izbrišejo po enem letu.“

19 Zvezna agencija za omrežja električne energije, plina, telekomunikacij, pošte in železnic je za zagotovitev posebej visoke ravni varstva in kakovosti podatkov na podlagi člena 113f(1) TKG pripravila sklop zahtev, ki ga je treba v skladu s členom 113f(2) TKG nenehno ocenjevati in po potrebi prilagajati. Člen 113g TKG zahteva, da se v izjavo o varnostni politiki, ki jo mora podati naslovnik obveznosti, vključijo posebni varnostni ukrepi.

StPO

- 20 Člen 100g(2), prvi stavek, Strafprozessordnung (zakonik o kazenskem postopku, v nadaljevanju: StPO) določa:

„Če nekatera dejstva utemeljujejo sum, da je nekdo kot storilec ali sosterilec storil eno od posebej hudih kaznivih dejanj iz drugega stavka, ali če je v primerih, v katerih je poskus kaznivega dejanja kazniv, poskusil storiti tako kaznivo dejanje in je kaznivo dejanje prav tako v obravnavanem primeru posebej hudo, se lahko podatki o prometu, shranjeni v skladu s členom 113b [TKG], zberejo, če bi bilo preiskovanje dejstev ali ugotavljanje kraja, kjer je preiskovana oseba, na druge načine pretirano oteženo ali neizvedljivo in če je zbiranje podatkov sorazmerno s pomembnostjo zadeve.“

- 21 Člen 101a(1) StPO določa, da je za zbiranje podatkov o prometu v skladu s členom 100g StPO potrebno dovoljenje sodnika. V skladu s členom 101a(2) StPO mora obrazložitev odločbe vsebovati bistvene preudarke v zvezi z nujnostjo in primernostjo ukrepa v posameznem primeru. Člen 101a(6) StPO določa obveznost obveščanja udeležencev zadevne telekomunikacije.

Spora o glavni stvari in vprašanje za predhodno odločanje

- 22 Družbi SpaceNet in Telekom Deutschland zagotavljata javno dostopne storitve dostopa do interneta v Nemčiji. Zadnjenavedena družba zagotavlja v Nemčiji tudi javno dostopne telefonske storitve.
- 23 Ti ponudnici storitev sta pri Verwaltungsgericht Köln (upravno sodišče v Kölnu, Nemčija) izpodbijali obveznost, ki jima je naložena s členom 113a(1) v povezavi s členom 113b TKG, da od 1. julija 2017 dalje hranita podatke o prometu in podatke o lokaciji v zvezi s telekomunikacijami svojih strank.
- 24 Verwaltungsgericht Köln (upravno sodišče v Kölnu) je v sodbah z dne 20. aprila 2018 odločilo, da družbi SpaceNet in Telekom Deutschland nista dolžni hraniti podatkov o prometu v zvezi s telekomunikacijami strank, ki jim zagotavljata dostop do interneta, iz člena 113b(3) TKG in da družba Telekom Deutschland poleg tega ni dolžna hraniti podatkov o prometu v zvezi s telekomunikacijami strank, ki jim zagotavlja dostop do javno dostopnih telefonskih storitev, iz člena 113b(2), prvi in drugi stavek, TKG. To sodišče je namreč ob upoštevanju sodbe z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), štelo, da je ta obveznost hrambe v nasprotju s pravom Unije.
- 25 Zvezna republika Nemčija je zoper ti sodbi vložila reviziji pri Bundesverwaltungsgericht (zvezno upravno sodišče, Nemčija), ki je predložitveno sodišče.
- 26 Navedeno sodišče meni, da je vprašanje, ali je obveznost hrambe, ki je naložena s členom 113a(1) v povezavi s členom 113b TKG, v nasprotju s pravom Unije, odvisno od razlage Direktive 2002/58.
- 27 Predložitveno sodišče v zvezi s tem navaja, da je Sodišče v sodbi z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), že dokončno odločilo, da ureditve, ki se nanašajo na hrambo podatkov o prometu in podatkov o lokaciji ter na dostop nacionalnih organov do teh podatkov, načeloma spadajo na področje uporabe Direktive 2002/58.

- 28 Predložitveno sodišče poleg tega navaja, da je obveznost hrambe, ki se obravnava v postopku v glavni stvari – ker omejuje pravice, ki izhajajo iz člena 5(1), člena 6(1) in člena 9(1) Direktive 2002/58 – lahko utemeljena le na podlagi člena 15(1) te direktive.
- 29 V zvezi s tem opozarja, da iz sodbe z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), izhaja, da je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki za boj proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev.
- 30 Po mnenju predložitvenega sodišča pa nacionalna ureditev iz postopka v glavni stvari tako kot nacionalne ureditve iz zadev, v katerih je bila izdana zgoraj navedena sodba, ne zahteva nobenega razloga za hrambo podatkov niti kakršne koli povezave med hranjenimi podatki in kaznivim dejanjem ali tveganjem za javno varnost. Ta nacionalna ureditev naj bi namreč določala splošno hrambo brez razloga in brez osebnega, časovnega in geografskega razlikovanja za večino upoštevanih podatkov o prometu v zvezi s telekomunikacijami.
- 31 Predložitveno sodišče kljub temu meni, da ni mogoče izključiti možnosti, da je obveznost hrambe, ki se obravnava v postopku v glavni stvari, upravičena na podlagi člena 15(1) Direktive 2002/58.
- 32 Na prvem mestu, navaja, da v nasprotju z nacionalnimi ureditvami iz zadev, v katerih je bila izdana sodba z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), nacionalna ureditev iz postopka v glavni stvari ne zahteva shranjevanja vseh podatkov o prometu, ki se nanašajo na telekomunikacije vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev. Ne le, da naj bi bila iz obveznosti hrambe izključena vsebina komunikacij, temveč naj se podatki o obiskanih spletnih straneh, podatki o storitvah elektronske pošte in podatki, na katerih temeljijo komunikacije do ali z določenimi priključki, ki so socialne ali verske narave – kot izhaja iz člena 113b(5) in (6) TKG – ne bi smeli shranjevati.
- 33 To sodišče, na drugem mestu, navaja, da je v členu 113b(1) TKG določeno, da se podatki o lokaciji hranijo štiri tedne, podatki o prometu pa deset tednov, medtem ko je Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL 2006, L 105, str. 54), na kateri so temeljile nacionalne ureditve, obravnavane v zadevah, v katerih je bila izdana sodba z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), določala obdobje hrambe od šestih mesecev do dveh let.
- 34 Predložitveno sodišče meni, da izključitev nekaterih komunikacijskih sredstev oziroma nekaterih kategorij podatkov in omejitev trajanja hrambe sicer ne zadostujeta za odpravo vsakršnega tveganja, da se ugotovi popoln profil zadevnih oseb, vendar naj bi bilo to tveganje v okviru izvajanja nacionalne zakonodaje iz postopka v glavni stvari vsaj znatno zmanjšano.
- 35 Na tretjem mestu, ta ureditev naj bi vsebovala stroge omejitve glede varstva hranjenih podatkov in dostopa do njih. Na eni strani naj bi tako zagotavljala učinkovito varstvo hranjenih podatkov pred tveganji zlorab ter pred vsakršnim nezakonitim dostopom do teh podatkov. Na drugi strani naj bi

se hranjeni podatki lahko uporabljali le za boj proti hudim kaznivim dejanjem oziroma za preprečevanje konkretne nevarnosti za telesno nedotakljivost, življenje ali svobodo osebe oziroma za obstoj zvezne države ali dežele.

- 36 Na četrtem mestu, razlaga člena 15(1) Direktive 2002/58 v smislu splošne nezdržljivosti vsakršne hrambe podatkov brez razloga s pravom Unije naj bi lahko bila v navzkrižju z obveznostjo ukrepanja držav članic, ki izhaja iz pravice do varnosti iz člena 6 Listine.
- 37 Predložitveno sodišče, na petem mestu, meni, da bi razlaga člena 15 Direktive 2002/58 v smislu, da ta nasprotuje splošni hrambi podatkov, znatno omejila manevrski prostor nacionalnega zakonodajalca na področju pregona kaznivih dejanj in javne varnosti, ki naj bi v skladu s členom 4(2) PEU ostalo v izključni pristojnosti vsake države članice.
- 38 Predložitveno sodišče, na šestem mestu, meni, da je treba upoštevati sodno prakso Evropskega sodišča za človekove pravice, in poudarja, da je to razsodilo, da člen 8 Evropske konvencije o varstvu človekovih pravic in svoboščin (v nadaljevanju: EKČP) ne nasprotuje nacionalnim določbam, ki predvidevajo množično prestrezanje čezmejnega pretoka podatkov, ob upoštevanju groženj, s katerimi se trenutno soočajo številne države, in tehnoloških orodij, ki jih teroristi in storilci kaznivih dejanj zdaj lahko uporabljajo pri nezakonitih ravnanjih.
- 39 V teh okoliščinah je Bundesverwaltungsgericht (zvezno upravno sodišče) prekinilo odločanje in Sodišču v predhodno odločanje predložilo to vprašanje:

„Ali je treba člen 15 Direktive [2002/58] glede na člene 7, 8, 11 in 52(1) [Listine] na eni strani ter glede na člen 6 [Listine] in glede na člen 4 [PEU] na drugi strani razlagati tako, da nasprotuje nacionalni ureditvi, ki ponudnike javno dostopnih elektronskih komunikacijskih storitev zavezuje, da hranijo podatke o prometu in lokaciji končnega uporabnika teh storitev, če

- (1) se za to obveznost ne zahteva noben poseben razlog v krajevnem, časovnem ali prostorskem smislu,
- (2) obveznost hrambe pri opravljanju javno dostopne telefonske storitve – vključno s prenosom SMS, večpredstavnostnih ali podobnih sporočil ter neodgovorjenimi ali neuspešnimi klici – vključuje naslednje podatke:
 - (a) klicano telefonsko številko ali kakšno drugo identiteto kličočega in klicanega priključka ter pri preklapljanju ali preusmeritvi klicev klicano telefonsko številko ali kakšno drugo identiteto vsakega naslednjega udeleženega priključka,
 - (b) datum in čas od začetka do konca zveze oziroma – pri prenosu SMS, večpredstavnostnega ali podobnega sporočila – čas pošiljanja in prejema sporočila z navedbo dejanskega časovnega pasu,
 - (c) podatke o uporabljeni storitvi, če se lahko v okviru telefonske storitve uporabljajo različne storitve,
 - (d) v primeru storitve mobilne telefonije pa še
 - (i) mednarodno identiteto naročnika mobilne telefonije za kličoči in klicani priključek,
 - (ii) mednarodno identiteto kličočega in klicanega telefonskega terminala,
 - (iii) datum in čas prve aktivacije storitve z navedbo dejanskega časovnega pasu, če se storitve plačujejo vnaprej,
 - (iv) identiteto celic, ki so bile uporabljene pri začetku povezave s kličočim in klicanim priključkom,

- (e) v primeru internetne telefonije tudi naslove IP kličočega in klicanega priključka ter dodeljenega uporabniškega imena,
- (3) obveznost hrambe pri opravljanju javno dostopne storitve dostopa do interneta vključuje naslednje podatke:
- (a) naslov IP, ki je dodeljen naročniku za uporabo interneta,
 - (b) enolični identifikator priključka, ki omogoča dostop do interneta, ter dodeljeno uporabniško ime,
 - (c) datum in čas začetka in konca uporabe interneta pod dodeljenim naslovom IP in navedbo dejanskega časovnega pasu,
 - (d) v primeru mobilne uporabe identiteto celic, ki so bile uporabljene pri začetku internetne povezave,
- (4) se naslednji podatki ne smejo hraniti:
- (a) vsebina komunikacije,
 - (b) podatki o obiskanih spletnih straneh,
 - (c) podatki o storitvah elektronske pošte,
 - (d) podatki, na katerih temeljijo komunikacije z ali do določenih priključkov oseb, organov in organizacij na socialnih ali cerkvenih področjih,
- (5) hramba za podatke o lokaciji, torej identifikacija uporabljenih celic, znaša štiri tedne, za ostale podatke pa deset tednov,
- (6) je zagotovljeno učinkovito varstvo hranjenih podatkov pred tveganji zlorabe in pred vsakim nezakonitim dostopom ter
- (7) se hranjeni podatki smejo uporabljati samo za pregon posebej hudih kaznivih dejanj in za boj proti konkretni nevarnosti za telesno nedotakljivost, življenje ali svobodo osebe ali za obstoj zvezne države ali zvezne dežele, razen naslova IP, ki se dodeli naročniku za uporabo interneta in katerega uporaba je dopustna v okviru informacije o podatkih o naročniškem razmerju za pregon vseh kaznivih dejanj, za preprečevanje nevarnosti za javno varnost in red ter za izvajanje nalog obveščevalnih služb?“

Postopek pred Sodiščem

- 40 S sklepom predsednika Sodišča z dne 3. decembra 2019 sta bili zadevi C-793/19 in C-794/19 združeni za pisni in ustni del postopka ter izdajo sodbe.
- 41 S sklepom predsednika Sodišča z dne 14. julija 2020 je bil postopek v združenih zadevah C-793/19 in C-794/19 na podlagi člena 55(1)(b) Poslovnika Sodišča prekinjen do razglasitve sodbe v zadevi La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18).
- 42 Potem ko je Sodišče 6. oktobra 2020 izdalo sodbo v zadevi La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791), je predsednik Sodišča 8. oktobra 2020 odredil nadaljevanje postopka v združenih zadevah C-793/19 in C-794/19.
- 43 Predložitveno sodišče, ki mu je sodno tajništvo posredovalo navedeno sodbo, je navedlo, da vztraja pri svojem predlogu za sprejetje predhodne odločbe.

- 44 V zvezi s tem je to predložitveno sodišče najprej ugotovilo, da se obveznost hrambe iz ureditve v postopku v glavni stvari nanaša na manjše število podatkov in krajše trajanje hrambe od tistega, ki je določeno v nacionalnih ureditvah, obravnavanih v zadevah, v katerih je bila izdana 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). Zaradi teh posebnosti naj bi bila možnost, da bi bilo na podlagi hranjenih podatkov mogoče izpeljati zelo natančne ugotovitve glede zasebnega življenja oseb, katerih podatki se hranijo, manjša.
- 45 Nato je predložitveno sodišče vnovič navedlo, da nacionalna ureditev iz postopka v glavni stvari zagotavlja učinkovito varstvo hranjenih podatkov pred tveganji zlorabe in nezakonitim dostopom.
- 46 Nazadnje je poudarilo, da ostajajo negotovosti glede vprašanja združljivosti hrambe naslovov IP, ki jo določa nacionalna ureditev iz postopka v glavni stvari, s pravom Unije zaradi neskladja med točkama 155 in 168 sodbe 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). Predložitveno sodišče tako meni, da ta sodba vsebuje negotovost v zvezi z vprašanjem, ali Sodišče za hrambo naslovov IP zahteva razlog za hrambo, ki je povezan s ciljem zaščite nacionalne varnosti, boja proti hudemu kriminalu ali preprečevanja resnih groženj javni varnosti, kot naj bi bilo razvidno iz točke 168 navedene sodbe, ali pa je hramba naslovov IP dovoljena tudi brez konkretnega razloga, pri čemer je zgolj uporaba hranjenih podatkov omejena z navedenimi cilji, kot naj bi bilo razvidno iz točke 155 iste sodbe.

Vprašanje za predhodno odločanje

- 47 Predložitveno sodišče želi z vprašanjem za predhodno odločanje v bistvu izvedeti, ali je treba člen 15(1) Direktive 2002/58 ob upoštevanju členov od 6 do 8 in 11 ter 52(l) Listine in člena 4(2) PEU razlagati tako, da nasprotuje nacionalnemu zakonskemu ukrepu, ki z nekaterimi izjemami od ponudnikov javno dostopnih elektronskih komunikacijskih storitev za namene, ki so navedeni v členu 15(1) te direktive, zlasti pa za pregon hudih kaznivih dejanj oziroma za preprečevanje konkretnega tveganja za nacionalno varnost, zahteva splošno in neselektivno hrambo večine podatkov o prometu in podatkov o lokaciji končnih uporabnikov teh storitev, pri čemer določa večtedensko obdobje hrambe ter pravila za zagotovitev učinkovitega varstva hranjenih podatkov pred tveganji zlorabe in pred vsakršnim nezakonitim dostopom do teh podatkov.

Uporaba Direktive 2002/58

- 48 Glede trditev Irske ter francoske, nizozemske, poljske in švedske vlade, da nacionalna ureditev iz postopka v glavni stvari – ker je bila sprejeta zlasti zaradi zaščite nacionalne varnosti – ne spada na področje uporabe Direktive 2002/58, zadostuje spomniti, da nacionalna ureditev, ki od ponudnikov elektronskih komunikacijskih storitev zahteva, da hranijo podatke o prometu in podatke o lokaciji med drugim zaradi zaščite nacionalne varnosti in boja proti kriminalu, kot je ta iz postopka v glavni stvari, spada na področje uporabe Direktive 2002/58 (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 104).

Razlaga člena 15(1) Direktive 2002/58

Pregled načel, ki izhajajo iz sodne prakse Sodišča

- 49 V skladu z ustaljeno sodno prakso je treba pri razlagi določbe prava Unije upoštevati ne le njeno besedilo, ampak tudi sobesedilo in cilje, ki se uresničujejo z ureditvijo, katere del je, ter zlasti zgodovino nastanka te ureditve (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 32 in navedena sodna praksa).
- 50 Iz samega besedila člena 15(1) Direktive 2002/58 je razvidno, da se lahko zakonski ukrepi, ki jih ta direktiva dovoljuje državam članicam, v skladu s pogoji, ki jih določa, nanašajo le na „omejitev obsega“ pravic in obveznosti, določenih zlasti v členih 5, 6 in 9 Direktive 2002/58 (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 33).
- 51 Glede sistema, ki ga vzpostavlja ta direktiva in katerega del je njen člen 15(1), je treba opozoriti, da morajo države članice v skladu s členom 5(1), prvi in drugi stavek, navedene direktive s svojo nacionalno zakonodajo zagotoviti zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Zlasti morajo prepovedati 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) iste direktive (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 34).
- 52 V zvezi s tem je Sodišče že razsodilo, da člen 5(1) Direktive 2002/58 določa načelo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu ter med drugim zahteva, da se načeloma vsem, razen uporabnikom, prepove shranjevanje teh komunikacij in podatkov brez privolitve uporabnikov (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 107, in z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 35).
- 53 Ta določba odraža cilj, ki ga je imel zakonodajalec Unije pri sprejetju Direktive 2002/58. Iz obrazložitve Predloga direktive Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (COM(2000) 385 final), na podlagi katerega je bila sprejeta Direktiva 2002/58, namreč izhaja, da je zakonodajalec Unije želel „še naprej zagotavljati visoko raven varstva osebnih podatkov in zasebnosti za vse elektronske komunikacijske storitve ne glede na tehnologijo, ki se uporablja“. Namen te direktive je, kot izhaja med drugim iz njenih uvodnih izjav 6 in 7, zavarovati uporabnike elektronskih komunikacijskih storitev pred tveganji za njihove osebne podatke in zasebnost, ki izhajajo iz novih tehnologij in zlasti čedalje večje zmogljivosti samodejnega shranjevanja podatkov in obdelave. Natančneje, kot je navedeno v uvodni izjavi 2 te direktive, je namen zakonodajalca Unije zlasti zagotoviti popolno spoštovanje pravic, navedenih v členih 7 in 8 Listine, ki se nanašata na varstvo zasebnega življenja in varstvo osebnih podatkov (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 36 in navedena sodna praksa).
- 54 Zakonodajalec Unije je s sprejetjem Direktive 2002/58 te pravice tako konkretiziral, zato lahko uporabniki elektronskih komunikacijskih sredstev načeloma utemeljeno pričakujejo, da bodo njihova sporočila in z njimi povezani podatki, če ne privolijo v nasprotno, ostali anonimni in jih

ne bo mogoče hraniti (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 109, in z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 37).

- 55 Člen 6 Direktive 2002/58 glede obdelave in shranjevanja podatkov o prometu, ki se nanašajo na naročnike in uporabnike, s strani ponudnikov elektronskih komunikacijskih storitev v odstavku 1 določa, da morajo biti ti podatki izbrisani ali predelani v anonimne, potem ko niso več potrebni za prenos sporočila, v odstavku 2 pa pojasnjuje, da se podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave, lahko obdelujejo le do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila. Glede podatkov o lokaciji, ki niso podatki o prometu, člen 9(1) navedene direktive določa, da se smejo takšni podatki obdelati le pod določenimi pogoji in šele po tem, ko postanejo anonimni, oziroma s privolitvijo uporabnikov ali naročnikov.
- 56 Zato Direktiva 2002/58 ni omejena na to, da dostop do takih podatkov ureja z jamstvi, katerih namen je preprečevanje zlorab, temveč določa zlasti tudi načelo prepovedi njihovega shranjevanja s strani tretjih oseb (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 39).
- 57 Ker člen 15(1) Direktive 2002/58 državam članicam omogoča, da sprejmejo zakonske 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 sporočil in prepovedi hrambe s tem povezanih podatkov, navedenih v točki 52 te sodbe, je s to določbo postavljena izjema od splošnega pravila, določenega zlasti v teh členih 5, 6 in 9, in jo 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 ter zlasti od prepovedi shranjevanja teh podatkov, ki je določena v členu 5 navedene direktive, postane pravilo, sicer bi se zadnjenavedeni določbi v veliki meri odvzel njen pomen (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 40 in navedena sodna praksa).
- 58 V zvezi s cilji, s katerimi je mogoče upravičiti omejitev pravic in obveznosti, določenih med drugim v členih 5, 6 in 9 Direktive 2002/58, je Sodišče že razsodilo, da so cilji iz člena 15(1), prvi stavek, te direktive naštetih izčrpno, tako da mora zakonski ukrep, sprejet na podlagi te določbe, dejansko in strogo ustrezati enemu od teh ciljev (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 41 in navedena sodna praksa).
- 59 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 prava Unije, med katerimi je načelo sorazmernosti, in zagotoviti spoštovanje temeljnih pravic, zagotovljenih z Listino. V zvezi s tem je Sodišče že razsodilo, da se z obveznostjo, ki jo država članica z nacionalno ureditvijo naloži ponudnikom elektronskih komunikacijskih storitev, da hranijo podatke o prometu, zato da se, če je to potrebno, pristojnim nacionalnim organom omogoči dostop do teh podatkov, postavljajo vprašanja v zvezi s spoštovanjem ne le členov 7 in 8 Listine, ampak tudi člena 11 Listine, ki se nanaša na svobodo izražanja, glede na to, da je ta svoboda eden od glavnih temeljev demokratične in pluralistične družbe ter je del vrednot, na katerih v skladu s členom 2 PEU temelji Evropska unija (glej v tem smislu sodbo z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točki 42 in 43 ter navedena sodna praksa).

- 60 V zvezi s tem je treba pojasniti, da hramba podatkov o prometu in podatkov o lokaciji kot taka pomeni po eni strani odstopanje od prepovedi iz člena 5(1) Direktive 2002/58, ki vsakomur razen uporabnikom prepoveduje shranjevanje teh podatkov, ter po drugi strani poseganje v temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov, ki sta določeni v členih 7 in 8 Listine, pri čemer ni pomembno, ali so zadevne informacije o zasebnem življenju občutljive, ali so bile zadevne osebe zaradi tega poseganja morda oškodovane in ali se bodo shranjeni podatki pozneje uporabili (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 44 in navedena sodna praksa).
- 61 Ta ugotovitev je še toliko bolj utemeljena, ker lahko podatki o prometu in podatki o lokaciji razkrijejo informacije o veliko vidikih zasebnega življenja zadevnih oseb, vključno z občutljivimi informacijami, kot so spolna usmerjenost, politična mnenja, verska, filozofska, družbena ali druga prepričanja in zdravstveno stanje, poleg tega pa taki podatki uživajo posebno varstvo v pravu Unije. Na podlagi navedenih podatkov, obravnavanih kot celota, je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega bivanja, dnevne ali druge poti, dejavnosti, družbeni stiki teh oseb in socialna okolja, ki jih obiskujejo. Natančneje, ti podatki so sredstva za ugotavljanje profila zadevnih oseb, kar je z vidika pravice do spoštovanja zasebnega življenja informacija, ki je prav tako občutljiva kot sama vsebina komunikacij (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 45 in navedena sodna praksa).
- 62 Zato lahko na eni strani hramba podatkov o prometu in podatkov o lokaciji za policijske namene posega v pravico do spoštovanja komunikacij, določeno v členu 7 Listine, in odvrča uporabnike elektronskih komunikacijskih sredstev od uresničevanja svobode izražanja, ki je zagotovljena s členom 11 Listine, ti odvrčilni učinki pa so še toliko resnejši, kolikor večja sta število in raznovrstnost hranjenih podatkov. Na drugi strani, glede na to, da se s splošnim in neselektivnim ukrepom hrambe lahko neprekinjeno shranjuje velika količina podatkov in da so informacije, ki se lahko zagotovijo s temi podatki, občutljive, že samo shranjevanje navedenih podatkov s strani ponudnikov elektronskih komunikacijskih storitev pomeni tveganje zlorabe in nezakonitega dostopa (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 46 in navedena sodna praksa).
- 63 Vendar se v členu 15(1) Direktive 2002/58, ki državam članicam dopušča, da omejijo pravice in obveznosti iz točk od 51 do 54 te sodbe, odraža dejstvo, da pravice iz členov 7, 8 in 11 Listine niso absolutne, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi. Kot namreč izhaja iz člena 52(1) Listine, ta dopušča omejitve pri uresničevanju teh pravic, če so te omejitve predpisane z zakonom, če spoštujejo bistveno vsebino navedenih pravic, če so ob upoštevanju načela sorazmernosti potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih. Tako razlaga člena 15(1) Direktive 2002/58 v povezavi z Listino zahteva tudi upoštevanje pomembnosti pravic, določenih s členi 3, 4, 6 in 7 Listine, ter pomembnosti ciljev zaščite nacionalne varnosti in boja proti hudemu kriminalu, s čimer se pripomore k varstvu pravic in svoboščin drugih (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 48 in navedena sodna praksa).
- 64 Kar posebej zadeva učinkovit boj proti kaznivim dejanjem, katerih žrtve so zlasti mladoletniki in druge ranljive osebe, pa je treba upoštevati dejstvo, da lahko pozitivne obveznosti za javne organe izhajajo iz člena 7 Listine, da se tako sprejmejo pravni ukrepi za zavarovanje zasebnega in družinskega življenja. Take obveznosti lahko izhajajo iz navedenega člena 7 tudi v zvezi

- z varstvom stanovanja in komunikacij, iz členov 3 in 4 pa v zvezi z varstvom telesne in duševne celovitosti oseb ter prepovedjo mučenja in nečloveškega in ponižujočega ravnanja (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 49 in navedena sodna praksa).
- 65 Ob upoštevanju teh različnih pozitivnih obveznosti je treba torej uskladiti različne zadevne legitimne interese in pravice ter vzpostaviti pravni okvir, ki bo to uskladitev omogočal (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 50 in navedena sodna praksa).
- 66 V tem okviru iz samega besedila člena 15(1), prvi stavek, Direktive 2002/58 izhaja, da lahko države članice sprejmejo ukrep, ki odstopa od načela zaupnosti, ki je navedeno v točki 52 te sodbe, kadar je tak ukrep „potrben, primeren in ustrezen [sorazmeren] [...] znotraj demokratične družbe“, pri čemer je v uvodni izjavi 11 te direktive navedeno, da mora biti tak ukrep „dosledno“ sorazmeren z zastavljenim ciljem.
- 67 V zvezi s tem je treba opozoriti, da varstvo temeljne pravice do spoštovanja zasebnega življenja v skladu z ustaljeno sodno prakso Sodišča zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno. Poleg tega cilja v splošnem interesu ni mogoče uresničevati brez upoštevanja dejstva, da ga je treba uskladiti s temeljnimi pravicami, na katere se nanaša ukrep, in sicer z uravnoteženjem cilja v splošnem interesu na eni strani ter zadevnih pravic na drugi strani (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 52 in navedena sodna praksa).
- 68 Natančneje, iz sodne prakse Sodišča je razvidno, da je treba možnost za države članice, da utemeljijo omejitev pravic in obveznosti, določenih zlasti s členi 5, 6 in 9 Direktive 2002/58, presoati tako, da se oceni teža posega, ki ga pomeni taka omejitev, in preveri, ali je pomembnost cilja splošnega interesa, ki se uresničuje s to omejitvijo, v sorazmerju s to težo (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 53 in navedena sodna praksa).
- 69 Za izpolnitev zahteve po sorazmernosti mora ureditev določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, kar zadeva njihove osebne podatke, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe. Ta ureditev mora biti zakonsko zavezujoča v nacionalnem pravu, v njej pa mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno. Nujnost obstoja takih jamstev je toliko pomembnejša, če se osebni podatki obdelujejo samodejno, zlasti kadar obstaja veliko tveganje nezakonitega dostopa do teh podatkov. Te ugotovitve veljajo še posebej, kadar gre za varstvo te posebne kategorije osebnih podatkov, ki so občutljivi podatki (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 54 in navedena sodna praksa).
- 70 Tako mora nacionalna zakonodaja, ki določa hrambo osebnih podatkov, vedno ustrezati objektivnim merilom, ki vzpostavljajo povezavo med podatki, ki jih je treba hraniti, in zastavljenim ciljem (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 55 in navedena sodna praksa).

- 71 Glede ciljev splošnega interesa, s katerimi je mogoče utemeljiti ukrep, sprejet na podlagi člena 15(1) Direktive 2002/58, iz sodne prakse Sodišča, zlasti iz sodbe 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), izhaja, da v skladu z načelom sorazmernosti obstaja hierarhija med temi cilji glede na to, kako so pomembni, in da mora biti pomembnost cilja, ki ga tak ukrep uresničuje, povezana z resnostjo posega, ki iz njega izhaja (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 56).
- 72 V zvezi z zaščito nacionalne varnosti, katere pomembnost presega pomembnost drugih ciljev iz člena 15(1) Direktive 2002/58, je Sodišče tako ugotovilo, da ta določba v povezavi s členi 7, 8 in 11 ter 52(1) Listine ne nasprotuje zakonskim ukrepom, s katerimi je v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero se ponudnikom elektronskih komunikacijskih storitev naloži splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, pri čemer je sklep o tej odredbi lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni, in je navedeni sklep mogoče izdati le za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je v primeru nadaljnje obstoja te grožnje mogoče podaljšati (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 58 in navedena sodna praksa).
- 73 Kar zadeva cilj preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, je Sodišče opozorilo, da je v skladu z načelom sorazmernosti mogoče zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti utemeljiti resne posege v temeljne pravice, določene s členoma 7 in 8 Listine, kakršne pomeni hramba podatkov o prometu in podatkov o lokaciji. Torej je mogoče s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno utemeljiti izključno posege v navedene temeljne pravice, ki po naravi niso resni (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 59 in navedena sodna praksa).
- 74 V zvezi s ciljem boja proti hudemu kriminalu je Sodišče razsodilo, da nacionalna zakonodaja, ki za to določa splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, presega meje tistega, kar je nujno potrebno, in je ni mogoče šteti za upravičeno v demokratični družbi. Glede na občutljivost informacij, ki jih je mogoče razbrati iz podatkov o prometu in podatkov o lokaciji, je namreč njihova zaupnost bistvena za pravico do spoštovanja zasebnega življenja. Torej je ob upoštevanju na eni strani odvrtilnih učinkov, ki jih lahko ima hramba teh podatkov na uresničevanje temeljnih pravic, določenih s členoma 7 in 11 Listine, na kateri se nanaša točka 62 te sodbe, na drugi strani pa teže posega, ki ga pomeni taka hramba, v demokratični družbi nujno, da je tak poseg – kot to določa sistem, vzpostavljen z Direktivo 2002/58 – izjema, ne pa pravilo, ter da teh podatkov ni mogoče hraniti sistematično in neprekinjeno. Ta ugotovitev velja tudi v zvezi s ciljem boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti ter veliko pomembnostjo, ki jima jo je treba priznati (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 65 in navedena sodna praksa).

75 Nasprotno pa je Sodišče pojasnilo, da člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine ne nasprotuje zakonskim ukrepom, ki za boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti določajo:

- ciljno hrambo podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije oseb, na katere se nanašajo osebni podatki, ali geografsko merilo, za obdobje, ki je časovno omejeno na to, kar je nujno potrebno, vendar ga je mogoče podaljšati;
- splošno in neselektivno hrambo naslovov IP, dodeljenih viru povezave, za obdobje, ki je časovno omejeno na to, kar je nujno potrebno;
- splošno in neselektivno hrambo podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev in
- uporabo odredbe, ki se ponudnikom elektronskih komunikacijskih storitev naloži s sklepom pristojnega organa, ki je predmet učinkovitega sodnega nadzora, da za določen čas izvedejo takojšnjo hrambo (quick freeze) podatkov o prometu in podatkov o lokaciji, ki jih imajo ti ponudniki storitev,

če je s temi ukrepi z jasnimi in natančnimi pravili zagotovljeno, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe (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 168, in z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 67).

Ukrep, ki določa splošno in neselektivno hrambo večine podatkov o prometu in podatkov o lokaciji za obdobje več tednov

76 Ob upoštevanju teh načelnih preudarkov je treba preučiti značilnosti nacionalne ureditve iz postopka v glavni stvari, ki jih je izpostavilo predložitveno sodišče.

77 Na prvem mestu, v zvezi z obsegom hranjenih podatkov je iz predložitvene odločbe razvidno, da se obveznost hrambe, ki je določena s to ureditvijo, v okviru zagotavljanja telefonskih storitev nanaša zlasti na podatke, potrebne za prepoznanje vira in cilja komunikacije, datum in čas začetka in konca klica oziroma – v primeru SMS, večpredstavnostnega ali podobnega sporočila – čas pošiljanja in prejema sporočila ter v primeru mobilne uporabe identiteto celic, ki so bile uporabljene pri začetku povezave s kličočim in klicanim priključkom. V okviru zagotavljanja storitev dostopa do interneta obveznost hrambe med drugim vključuje naslov IP, dodeljen naročniku, datum in čas začetka in konca uporabe interneta z dodeljenega naslova IP ter v primeru mobilne uporabe identiteto celic, ki so bile uporabljene pri začetku internetne povezave. Hranijo se tudi podatki, iz katerih sta razvidna zemljepisna lega in glavna smer sevanja anten, ki pokrivajo posamezno celico.

78 Čeprav nacionalna ureditev iz postopka v glavni stvari izključuje obveznost hrambe vsebine komunikacije in podatkov o obiskanih spletnih straneh ter zahteva hrambo ID celice le pri začetku povezave, je treba ugotoviti, da je to v bistvu veljalo tudi za nacionalne ureditve, s katerimi je bila prenesena Direktiva 2006/24 in ki so bile obravnavane v zadevah, v katerih je bila izdana 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). Kljub tem omejitvam pa je Sodišče v tej sodbi ugotovilo, da je bilo na podlagi

kategorij podatkov, hranjenih v skladu z navedeno direktivo in temi nacionalnimi ureditvami, mogoče priti do zelo natančnih ugotovitev o zasebnem življenju zadevnih oseb, kot so vsakodnevne navade, kraji stalnega ali začasnega bivanja, dnevne ali druge poti, dejavnosti, družbeni stiki teh oseb in socialna okolja, ki jih obiskujejo, ter, natančneje, da so ti podatki sredstvo za ugotavljanje profila teh oseb.

- 79 Poleg tega je treba ugotoviti, da ureditev iz postopka v glavni stvari sicer ne zajema podatkov o obiskanih spletnih straneh, vendar določa hrambo naslovov IP. Ker pa je te naslove IP mogoče uporabiti zlasti za izčrpno sledenje brskanju, ki ga je opravil uporabnik interneta, in torej njegovim spletnim dejavnostim, ti podatki omogočajo ugotavljanje njegovega podrobnega profila. Tako hramba in analiza navedenih naslovov IP, ki sta potrebni za tako sledenje, pomenita resna posega v temeljne pravice uporabnika interneta, določene s členoma 7 in 8 Listine (glej v tem smislu 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, točka 153).
- 80 Poleg tega – in kot je družba SpaceNet navedla v svojem pisnem stališču – predstavljajo podatki v zvezi s storitvami elektronske pošte, na katere se obveznost, ki je določena v ureditvi iz postopka v glavni stvari, sicer ne nanaša, le zelo majhen del zadevnih podatkov.
- 81 Kot je generalni pravobranilec v bistvu navedel v točki 60 sklepnih predlogov, se obveznost hrambe, ki je določena v nacionalni ureditvi iz postopka v glavni stvari, nanaša na zelo širok nabor podatkov o prometu in podatkov o lokaciji, ki v bistvu ustreza tistim, glede katerih je bila izoblikovana ustaljena sodna praksa, na katero je bilo opozorjeno v točki 78 te sodbe.
- 82 Poleg tega je nemška vlada v odgovor na vprašanje, postavljeno na obravnavi, pojasnila, da je bilo na seznam oseb, organov oziroma organizacij na socialnih ali cerkvenih področjih, katerih podatki glede elektronskih komunikacij se v skladu s členom 99(2) in členom 113b(6) TKG ne shranjujejo, vključenih le 1300 subjektov, kar očitno predstavlja majhen delež vseh uporabnikov telekomunikacijskih storitev v Nemčiji, katerih podatki so zajeti z obveznostjo hrambe, ki je določena z nacionalno ureditvijo iz postopka v glavni stvari. Tako se med drugim shranjujejo podatki uporabnikov, ki so zavezani varovanju poklicne skrivnosti, kot so odvetniki, zdravniki in novinarji.
- 83 Iz predložitvene odločbe torej izhaja, da se hramba podatkov o prometu in podatkov o lokaciji, ki je določena s to nacionalno ureditvijo, nanaša na skoraj vse osebe, ki tvorijo prebivalstvo, ne da bi se te – četudi posredno – znašle v položaju, ki bi lahko pripeljal do kazenskega pregona. Ta ureditev prav tako nalaga splošno hrambo brez razloga in brez osebnega, časovnega in geografskega razlikovanja za večino upoštevnih podatkov o prometu in podatkov o lokaciji, katerih obseg v bistvu ustreza obsegu hranjenih podatkov iz zadev, na podlagi katerih se je izoblikovala sodna praksa, navedena v točki 78 te sodbe.
- 84 Zato ob upoštevanju sodne prakse, navedene v točki 75 te sodbe, obveznosti hrambe podatkov, kot je ta iz postopka v glavni stvari, v nasprotju s trditvami nemške vlade ni mogoče šteti za ciljno usmerjeno hrambo podatkov.
- 85 Na drugem mestu, v zvezi s trajanjem hrambe podatkov je iz člena 15(1), drugi stavek, Direktive 2002/58 razvidno, da je obdobje hrambe, določeno z nacionalnim ukrepom, ki nalaga splošno in neselektivno obveznost hrambe podatkov, sicer eden od pomembnih dejavnikov pri ugotavljanju, ali pravo Unije nasprotuje takemu ukrepu, saj se z navedenim stavkom zahteva, da je to obdobje „določeno“.

- 86 V obravnavanem primeru pa so ta obdobja, ki v skladu s členom 113b(1) TKG znašajo štiri tedne za podatke o lokaciji in deset tednov za druge podatke, res bistveno krajša od tistih, ki so bila določena v nacionalnih ureditvah o naložitvi splošne in neselektivne obveznosti hrambe, ki jih je Sodišče preučilo v sodbah z dne 21. decembra 2016, *Tele2 Sverige* ter *Watson* in drugi (C-203/15 in C-698/15, EU:C:2016:970), 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), in z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi (C-140/20, EU:C:2022:258).
- 87 Vendar, kot izhaja iz sodne prakse, navedene v točki 61 te sodbe, teža posega izhaja iz tveganja, da bi bilo na podlagi shranjenih podatkov, obravnavanih kot celota, zlasti glede na njihovo število in raznolikost, mogoče priti do zelo natančnih ugotovitev o zasebnem življenju osebe ali oseb, katerih podatki so bili shranjeni, in, natančneje, da bi bili ti sredstvo za ugotavljanje profila zadevne osebe ali oseb, kar je prav tako občutljiva informacija z vidika pravice do spoštovanja zasebnega življenja kot sama vsebina komunikacij.
- 88 Zato hramba podatkov o prometu ali lokaciji, iz katerih bi bile lahko razvidne informacije o komunikacijah, ki jih je uporabnik opravil z uporabo elektronskih komunikacijskih sredstev, ali o lokaciji uporabljene terminalske opreme, vsekakor pomeni resen poseg, ne glede na trajanje obdobja hrambe, količino ali naravo hranjenih podatkov, če je na podlagi navedenega nabora podatkov mogoče priti do zelo natančnih ugotovitev o zasebnem življenju zadevne osebe ali oseb (v zvezi z dostopom do takih podatkov glej sodbo z dne 2. marca 2021, *Prokuratuur* (Pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, EU:C:2021:152, točka 39).
- 89 V zvezi s tem je mogoče tudi s hrambo omejene količine podatkov o prometu ali podatkov o lokaciji oziroma s hrambo teh podatkov za kratko obdobje priti do zelo natančnih informacij o zasebnem življenju uporabnika elektronskega komunikacijskega sredstva. Poleg tega je količino razpoložljivih podatkov in zelo natančne informacije o zasebnem življenju zadevne osebe, ki iz teh podatkov izhajajo, mogoče presojati šele po tem, ko se navedeni podatki pregledajo. Do posega, ki je posledica hrambe navedenih podatkov, pa nujno pride pred možnostjo vpogleda v podatke in informacije, ki iz njih izhajajo. Tako se presoja teže posega, ki ga pomeni hramba, nujno opravi glede na tveganje, ki ga neka kategorija hranjenih podatkov na splošno predstavlja za zasebno življenje zadevnih oseb, ne da bi bilo treba tudi vedeti, ali so informacije o zasebnem življenju, ki izhajajo iz teh podatkov, v konkretnem primeru občutljive ali ne (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 40).
- 90 Kot je razvidno iz točke 77 te sodbe in kot je bilo potrjeno na obravnavi, je v obravnavanem primeru na podlagi nabora podatkov o prometu in podatkov o lokaciji, ki se hranijo deset tednov oziroma štiri tedne, mogoče priti do zelo natančnih ugotovitev o zasebnem življenju oseb, katerih podatki se shranjujejo, kot so vsakodnevne navade, kraji stalnega ali začasnega bivanja, dnevne ali druge poti, dejavnosti, družbeni stiki teh oseb in socialna okolja, ki jih obiskujejo, ter, natančneje, ugotoviti profil navedenih oseb.
- 91 Na tretjem mestu, v zvezi z jamstvi, določenimi z nacionalno ureditvijo iz postopka v glavni stvari, katerih namen je varstvo hranjenih podatkov pred tveganji zlorabe in pred vsakršnim nezakonitim dostopom, je treba navesti, da sta hramba teh podatkov in dostop do njih, kot izhaja iz sodne prakse, na katero je bilo opozorjeno v točki 60 te sodbe, ločena posega v temeljne pravice, zagotovljene s členoma 7 in 11 Listine, za katera je potrebna ločena utemeljitev na podlagi njenega člena 52(1). Iz tega izhaja, da nacionalna zakonodaja, ki zagotavlja polno spoštovanje pogojev, ki izhajajo iz sodne prakse, s katero je bila Direktiva 2002/58 razlagana na področju dostopa do

hranjenih podatkov, sama po sebi ne more niti omejiti niti odpraviti resnega posega, ki bi izhajal iz splošne hrambe teh podatkov, ki je določena s to nacionalno zakonodajo, v pravice, zagotovljene s členoma 5 in 6 te direktive in s temeljnimi pravicami, ki jih ta člena konkretizirata (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 47).

- 92 Na četrtem in zadnjem mestu, v zvezi s trditvijo Evropske komisije, da je posebej hud kriminal mogoče enačiti z grožnjo za nacionalno varnost, je Sodišče že presodilo, da cilj ohranitve nacionalne varnosti ustreza ključnemu interesu, ki je zaščititi bistvene funkcije države in temeljne interese družbe, ter vključuje preprečevanje in kaznovanje dejavnosti, ki lahko resno destabilizirajo temeljne ustavne, politične, gospodarske ali družbene strukture države ter zlasti neposredno ogrozijo družbo, prebivalstvo ali državo kot tako, kot so teroristična dejanja (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 61 in navedena sodna praksa).
- 93 Za razliko od kriminala, tudi posebej hudega, mora biti grožnja za nacionalno varnost resnična in sedanja ali vsaj predvidljiva, kar predpostavlja nastanek dovolj konkretnih okoliščin, da se lahko upraviči splošen in neselektiven ukrep hrambe podatkov o prometu in podatkov o lokaciji za določen čas. Taka grožnja se torej po svoji naravi, resnosti in posebnosti okoliščin, ki jo sestavljajo, razlikuje od splošnega in stalnega tveganja nastanka napetosti ali nemirov, tudi hudih, ki bi ogrozili javno varnost, ali tveganja hudih kaznivih dejanj (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 62 in navedena sodna praksa).
- 94 Kriminala, tudi če je zelo hud, torej ni mogoče enačiti z grožnjo za nacionalno varnost. S takim enačenjem bi lahko bila namreč uvedena vmesna kategorija med nacionalno in javno varnostjo, da bi se za slednjo uporabile zahteve, ki veljajo za prvo (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 63).

Ukrepi, ki določajo ciljno hrambo, takojšnjo hrambo ali hrambo naslovov IP

- 95 Več vlad, med njimi tudi francoska, poudarja, da le splošna in neselektivna hramba omogoča učinkovito doseganje ciljev ohranitvenih ukrepov, pri čemer je nemška vlada v bistvu pojasnila, da take ugotovitve ni mogoče ovreči z dejstvom, da lahko države članice uporabijo ukrepe ciljne hrambe in takojšnje hrambe, navedene v točki 75 te sodbe.
- 96 V zvezi s tem je treba, na prvem mestu, poudariti, da učinkovitost kazenskega pregona na splošno ni odvisna od enega samega preiskovalnega instrumenta, temveč od vseh preiskovalnih instrumentov, ki jih imajo pristojni nacionalni organi za to na voljo (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 69).
- 97 Na drugem mestu, člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine, kot je razložen v sodni praksi, navedeni v točki 75 te sodbe, državam članicam omogoča, da zaradi boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti sprejmejo ne le ukrepe za ciljno hrambo in takojšnjo hrambo, temveč tudi ukrepe, ki določajo splošno in neselektivno hrambo podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev na eni strani in naslovov IP, dodeljenih viru povezave, na drugi strani (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 70).

- 98 Glede tega ni sporno, da hramba podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev lahko prispeva k boju proti hudemu kriminalu, če ti podatki omogočajo identifikacijo oseb, ki so ta sredstva uporabile v okviru priprave ali izvršitve dejanja, ki spada v hud kriminal (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 71).
- 99 Direktiva 2002/58 pa ne nasprotuje splošni hrambi podatkov o civilni identiteti zaradi boja proti kriminalu na splošno. V teh okoliščinah je treba pojasniti, da niti ta direktiva niti noben drug akt prava Unije ne nasprotuje nacionalni zakonodaji, katere cilj je boj proti hudemu kriminalu in v skladu s katero je pridobitev elektronskega komunikacijskega sredstva, kot je predplačljiva kartica SIM, pogojena s preverjanjem uradnih dokumentov, iz katerih je razvidna identiteta kupca, in z registracijo informacij, ki iz tega izhajajo, s strani prodajalca, zato mora prodajalec, če je to potrebno, pristojnim nacionalnim organom omogočiti dostop do teh informacij (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 72).
- 100 Poleg tega je treba opozoriti, da je splošna hramba naslovov IP vira povezave hud poseg v temeljne pravice, določene v členih 7 in 8 Listine, ker je na podlagi teh naslovov IP mogoče ugotoviti podrobnosti o zasebnem življenju uporabnika zadevnega elektronskega komunikacijskega sredstva, in ima lahko odvratilni učinek na uresničevanje svobode izražanja, zagotovljene v členu 11 Listine. Vendar je Sodišče v zvezi s to hrambo ugotovilo, da je treba za potrebno uskladitev zadevnih pravic in zakonitih interesov, ki se zahteva s sodno prakso, navedeno v točkah od 65 do 68 te sodbe, upoštevati dejstvo, da je v primeru kaznivega dejanja, storjenega na spletu, in zlasti v primeru pridobitve, razširjanja, prenosa ali dajanja na voljo na spletu otroške pornografije v smislu člena 2(c) Direktive 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL 2011, L 335, str. 1), naslov IP lahko edino preiskovalno sredstvo, ki omogoča identifikacijo osebe, ki ji je bil v času storitve tega kaznivega dejanja ta naslov dodeljen (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 73).
- 101 V takih okoliščinah sicer drži, da bi se zakonski ukrep, ki določa hrambo naslovov IP vseh fizičnih oseb, ki so lastniki terminalske opreme, ki omogoča dostop do interneta, nanašal na osebe, ki na prvi pogled v smislu sodne prakse, navedene v točki 70 te sodbe, nimajo nikakršne zveze z zastavljenimi cilji, ter da imajo uporabniki interneta v skladu z ugotovitvami iz točke 54 te sodbe pravico v skladu s členoma 7 in 8 Listine pričakovati, da njihova identiteta načeloma ne bo razkrita, vendar zakonski ukrep, ki določa splošno in neselektivno hrambo zgolj naslovov IP, dodeljenih viru povezave, načeloma ni v nasprotju s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine, če je za to možnost določeno strogo spoštovanje materialnih in postopkovnih pogojev, ki morajo urejati uporabo teh podatkov (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 155).
- 102 Ob upoštevanju resnosti posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga pomeni ta hramba, je mogoče navedeni poseg razen z zaščito nacionalne varnosti upravičiti zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti. Poleg tega trajanje hrambe ne sme biti daljše od tega, kar je nujno potrebno z vidika zastavljenega cilja. Nazadnje, pri tovrstnem ukrepu je treba določiti stroge pogoje in jamstva glede uporabe teh podatkov, zlasti s sledenjem, kar zadeva komunikacije in dejavnosti, ki so jih zadevne osebe opravile prek spleta (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 156).

- 103 Tako v nasprotju s tem, kar je poudarilo predložitveno sodišče, med točkama 155 in 168 sodbe 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), ni neskladij. Kot je generalni pravobranilec v bistvu poudaril v točkah 81 in 82 sklepnih predlogov, je iz te točke 155 v povezavi s točko 156 in točko 168 navedene sodbe jasno razvidno, da je mogoče splošno hrambo naslovov IP, dodeljenih viru povezave, razen z zaščito nacionalne varnosti utemeljiti zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti, ne glede na to, ali so zadevne osebe lahko vsaj posredno povezane z zastavljenimi cilji.
- 104 Na tretjem mestu, v zvezi z zakonskimi ukrepi, ki določajo ciljno in takojšnjo hrambo podatkov o prometu in podatkov o lokaciji, je iz nekaterih pomislekov, ki so jih države članice izrazile glede takih ukrepov, razvidno ožje razumevanje obsega teh ukrepov od tistega, ki je bil upoštevan v sodni praksi, navedeni v točki 75 te sodbe. Čeprav morajo biti namreč v skladu s tem, na kar je bilo opozorjeno v točki 57 te sodbe, ti ukrepi hrambe izjema v sistemu, vzpostavljenem z Direktivo 2002/58, ta direktiva v povezavi s temeljnimi pravicami, določenimi v členih 7, 8 in 11 ter 52(1) Listine, za možnost izdaje odredbe, s katero se nalaga ciljna hramba, ne določa pogoja, da so vnaprej znani kraji, ki bi lahko bili prizorišče hudega kaznivega dejanja, ali osebe, osumljene, da so vpletene v tako dejanje. Prav tako navedena direktiva ne zahteva, da mora biti odredba, s katero se nalaga takojšnja hramba, omejena na osumljence, ki so bili identificirani pred izdajo take odredbe (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 75).
- 105 Prvič, v zvezi s ciljno hrambo je Sodišče razsodilo, da člen 15(1) Direktive 2002/58 ne nasprotuje nacionalni zakonodaji, ki temelji na objektivnih elementih, na podlagi katerih je mogoče identificirati na eni strani osebe, katerih podatki o prometu in podatki o lokaciji lahko, vsaj posredno, izkažejo zvezo s hudimi kaznivimi dejanji, tako ali drugače prispevajo k boju proti hudemu kriminalu ali preprečijo resno nevarnost za javno varnost ali nevarnost za nacionalno varnost (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 76 in navedena sodna praksa).
- 106 Sodišče je v zvezi s tem pojasnilo, da čeprav se lahko ti objektivni elementi spreminjajo glede na ukrepe, ki so bili sprejeti za preprečevanje, preiskovanje, odkrivanje in pregon hudih kaznivih dejanj, so lahko osebe, na katere se ti ukrepi nanašajo, med drugim tiste, ki so bile v okviru nacionalnih postopkov, ki se uporabljajo, in na podlagi objektivnih in nediskriminatornih elementov predhodno opredeljene kot osebe, ki predstavljajo grožnjo javni varnosti ali nacionalni varnosti zadevne države članice (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 77).
- 107 Države članice imajo tako zlasti možnost sprejeti ukrep hrambe za osebe, zoper katere zaradi take identifikacije poteka preiskava ali drugi tekoči nadzorni ukrepi ali vpis v nacionalno kazensko evidenco, v kateri je navedena prejšnja obsodba za huda kazniva dejanja, ki lahko pomenijo visoko nevarnost ponovitve kaznivih dejanj. Kadar pa taka identifikacija temelji na objektivnih in nediskriminatornih elementih, opredeljenih v nacionalnem pravu, je ciljno usmerjena hramba, ki se nanaša na tako identificirane osebe, utemeljena (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, C-140/20, EU:C:2022:258, točka 78).
- 108 Na drugi strani lahko ukrep ciljne hrambe podatkov o prometu in podatkov o lokaciji glede na izbiro nacionalnega zakonodajalca in ob strogem spoštovanju načela sorazmernosti temelji tudi na geografskem merilu, kadar pristojni nacionalni organi na podlagi objektivnih in nediskriminatornih elementov menijo, da na enem ali več geografskih območjih obstaja položaj,

za katerega je značilno visoko tveganje za pripravo ali izvršitev hudih kaznivih dejanj. Taka območja so lahko zlasti kraji, za katere je značilno veliko število hudih kaznivih dejanj, kraji, posebej izpostavljeni storitvi hudih kaznivih dejanj, kot so kraji ali infrastrukture, ki jih redno obiskuje zelo veliko ljudi, ali strateški kraji, kot so letališča, železniške postaje, pomorska pristanišča ali cestninska območja (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 79 in navedena sodna praksa).

- 109 Poudariti je treba, da lahko v skladu s to sodno prakso pristojni nacionalni organi za območja, navedena v prejšnji točki, sprejmejo ukrep ciljne hrambe, ki temelji na geografskem merilu, kot je zlasti povprečna stopnja kriminala na geografskem območju, ne da bi morali imeti na voljo konkretne indice o pripravi ali izvrševanju hudih kaznivih dejanj na zadevnih območjih. Ker lahko ciljna hramba, ki temelji na takem merilu, glede na zadevna huda kazniva dejanja in položaj zadevnih držav članic prizadene hkrati kraje, za katere je značilno veliko število hudih kaznivih dejanj, in kraje, ki so posebej izpostavljeni storitvi takih dejanj, načeloma tudi ni taka, da bi povzročila diskriminacijo, saj merilo povprečne stopnje hudega kriminala samo po sebi nima nobene povezave s potencialno diskriminatornimi elementi (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 80).
- 110 Poleg tega ukrep ciljne hrambe, ki se nanaša na prostore ali infrastrukturo, ki jo redno obiskuje zelo veliko oseb, ali strateške kraje, kot so letališča, železniške postaje, pomorska pristanišča ali območja cestnin, pristojnim organom predvsem omogoča, da zberejo podatke o prometu in zlasti podatke o lokaciji vseh oseb, ki v danem trenutku uporabljajo elektronsko komunikacijsko sredstvo na enem od teh krajev. Tako lahko tak ukrep ciljne hrambe navedenim organom omogoči, da z dostopom do tako shranjenih podatkov pridobijo informacije o navzočnosti teh oseb na krajih ali geografskih območjih, na katera se ta ukrep nanaša, in o potovanjih teh oseb med njimi ali znotraj njih ter da zaradi boja proti hudemu kriminalu na podlagi tega ugotavljajo navzočnost in dejavnosti teh oseb na teh krajih ali geografskih območjih v danem trenutku v obdobju hrambe (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 81).
- 111 Poudariti je še treba, da se geografska območja, na katera se nanaša taka ciljna hramba, lahko in glede na okoliščine primera morajo spreminjati glede na razvoj pogojev, ki so utemeljevali njihovo izbiro, s čimer se je zlasti mogoče odzvati na razvoj boja proti hudemu kriminalu. Sodišče je namreč že razsodilo, da trajanje ukrepov ciljne hrambe, opisanih v točkah od 105 do 110 te sodbe, ne sme biti daljše od trajanja, ki je nujno potrebno z vidika zastavljenega cilja in okoliščin, ki jih upravičujejo, kar pa ne vpliva na morebitno podaljšanje zaradi nadaljnega obstoja potrebe po taki hrambi (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 151, in z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 82).
- 112 V zvezi z možnostjo določitve drugih razlikovalnih meril, ki niso osebno ali geografsko merilo za izvedbo ciljne hrambe podatkov o prometu in podatkov o lokaciji, ni mogoče izključiti, da je mogoče upoštevati druga objektivna in nediskriminatorna merila, da se zagotovi, da je obseg ciljne hrambe omejen na najnujnejše, in vsaj posredno povezavo med dejanji hudega kriminala in osebami, katerih podatki se hranijo. Ker se člen 15(1) Direktive 2002/58 nanaša na zakonodajne ukrepe držav članic, morajo taka merila določiti države članice, ne pa Sodišče, pri čemer seveda s tem ni mogoče ponovno uvesti splošne in neselektivne hrambe podatkov o prometu in podatkov o lokaciji (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 83).

- 113 Kot je generalni pravobranilec poudaril v točki 50 sklepnih predlogov, morebitni obstoj težav pri natančni opredelitvi primerov in pogojev, pod katerimi se lahko opravi ciljna hramba, nikakor ne more upravičiti tega, da države članice s tem, da izjemo spremenijo v pravilo, določijo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 84).
- 114 Drugič, v zvezi s takojšnjo hrambo podatkov o prometu in podatkov o lokaciji, ki jih ponudniki elektronskih komunikacijskih storitev obdelujejo in hranijo na podlagi členov 5, 6 in 9 Direktive 2002/58 ali na podlagi zakonskih ukrepov, sprejetih na podlagi člena 15(1) te direktive, je treba opozoriti, da je treba take podatke, odvisno od primera, načeloma izbrisati ali preoblikovati v anonimne ob izteku zakonskih rokov, v katerih morata biti v skladu z nacionalnimi določbami, s katerimi je prenesena navedena direktiva, opravljena njihova obdelava in hramba. Vendar je Sodišče odločilo, da lahko med to obdelavo in hrambo nastanejo položaji, ko je treba te podatke shraniti dlje od navedenih rokov, da se tako razjasnijo huda kazniva dejanja ali posegi v nacionalno varnost, in sicer tako v položaju, ko je bilo ta kazniva dejanja ali te posege že mogoče ugotoviti, kot tudi v položaju, ko je mogoče po objektivni preučitvi vseh upoštevnihih okoliščin na njihov obstoj razumno sumiti (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 85).
- 115 V takem položaju lahko države članice ob upoštevanju potrebne uskladitve med zadevnimi pravicami in legitimnimi interesi, na katero se nanašajo točke od 65 do 68 te sodbe, v zakonodaji, sprejeti na podlagi člena 15(1) Direktive 2002/58, določijo možnost, da se s sklepom pristojnega organa, ki je predmet učinkovitega sodnega nadzora, ponudnikom elektronskih komunikacijskih storitev odredi, da za določen čas izvedejo takojšnjo hrambo podatkov o prometu in podatkov o lokaciji, ki jih imajo na voljo (sodbi z dne 6. oktobra 2020, Quadrature du Net in drugi, C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 163, in z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 86).
- 116 Ker se namen take takojšnje hrambe ne ujema več z nameni, za katere so bili podatki prvotno zbrani in shranjeni, in ker mora biti v skladu s členom 8(2) Listine kakršna koli obdelava podatkov izvedena za določene namene, morajo države članice v svoji zakonodaji navesti namen, za katerega je takojšnjo hrambo podatkov mogoče izvesti. Ob upoštevanju resnosti posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga lahko taka hramba pomeni, je mogoče ta poseg upravičiti zgolj z bojem proti hudemu kriminalu in *a fortiori* z zaščito nacionalne varnosti, če sta ta ukrep in dostop do tako hranjenih podatkov v mejah nujno potrebnega, kot so navedene v točkah od 164 do 167 sodbe 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) (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 87).
- 117 Sodišče je pojasnilo, da tovrstni ukrep hrambe ne sme biti omejen na podatke oseb, za katere je bilo predhodno ugotovljeno, da ogrožajo javno varnost ali nacionalno varnost zadevne države članice, ali oseb, ki so dejansko osumljene storitve hudega kaznivega dejanja ali ogrožanja nacionalne varnosti. Ob upoštevanju okvira, izoblikovanega s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine, ter preudarkov, navedenih v točki 70 te sodbe, je namreč po mnenju Sodišča mogoče tak ukrep glede na izbiro nacionalnega zakonodajalca in ob upoštevanju meja tega, kar je nujno potrebno, razširiti na podatke o prometu in podatke o lokaciji v zvezi s še drugimi osebami, ki niso osumljene načrtovanja ali storitve hudega kaznivega dejanja ali napada na nacionalno varnost, če lahko ti podatki na podlagi objektivnih in nediskriminatornih ciljev pripomorejo k razjasnitvi takega kaznivega dejanja ali takega napada na nacionalno varnost, na primer podatki o žrtvi tega dejanja in o njenem socialnem ali poklicnem

okolju (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 165, in z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 88).

- 118 Tako lahko zakonski ukrep dovoljuje uporabo odredbe za ponudnike elektronskih komunikacijskih storitev, da opravijo takojšnjo hrambo podatkov o prometu in podatkov o lokaciji med drugim oseb, s katerimi je bila žrtev pred nastankom resne grožnje javni varnosti ali storitvijo hudega kaznivega dejanja v stiku prek svojih elektronskih komunikacijskih sredstev (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 89).
- 119 Tako takojšnjo hrambo je v skladu s sodno prakso Sodišča, navedeno v točki 117 te sodbe, in pod enakimi pogoji, kot so navedeni v tej točki, mogoče razširiti tudi na določena geografska območja, kot so kraji izvršitve in priprave kaznivega dejanja ali ogrožanja zadevne nacionalne varnosti. Pojasniti je treba, da so lahko predmet takega ukrepa še podatki o prometu in podatki o lokaciji, ki se nanašajo na kraj, kjer je oseba, ki bi bila potencialno žrtev hudega kaznivega dejanja, izginila, če ta ukrep in dostop do tako shranjenih podatkov spoštujeta meje nujno potrebnega za boj proti hudemu kriminalu ali zaščito nacionalne varnosti, kot so navedene v točkah od 164 do 167 sodbe 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) (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 90).
- 120 Poleg tega je treba pojasniti, da člen 15(1) Direktive 2002/58 ne nasprotuje temu, da pristojni nacionalni organi odredijo ukrep takojšnje hrambe že v prvi fazi preiskave, ki se nanaša na resno grožnjo za javno varnost ali morebitno hudo kaznivo dejanje, in sicer od trenutka, ko lahko ti organi v skladu z ustreznimi določbami nacionalnega prava začnejo tako preiskavo (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 91).
- 121 Glede raznolikosti ukrepov hrambe podatkov o prometu in podatkov o lokaciji iz točke 75 te sodbe je treba pojasniti, da se ti različni ukrepi glede na izbiro nacionalnega zakonodajalca in ob spoštovanju meja tega, kar je nujno potrebno, lahko uporabljajo skupaj. V teh okoliščinah člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8, in 11 ter 52(1) Listine, kakor je razložen v sodni praksi iz sodbe 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), ne nasprotuje kombinaciji teh ukrepov (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 92).
- 122 Na četrtem in zadnjem mestu, poudariti je treba, da sorazmernost ukrepov, sprejetih na podlagi člena 15(1) Direktive 2002/58 v skladu z ustaljeno sodno prakso, kot je bila povzeta v 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), zahteva spoštovanje ne le zahtev primernosti in nujnosti, ampak tudi zahteve po sorazmernosti teh ukrepov glede na cilj, ki se uresničuje (sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána* in drugi, C-140/20, EU:C:2022:258, točka 93).
- 123 V tem okviru je treba spomniti, da je Sodišče v točki 51 sodbe z dne 8. aprila 2014, *Digital Rights Ireland* in drugi (C-293/12 in C-594/12, EU:C:2014:238), presodilo, da čeprav je boj proti hudemu kriminalu bistvenega pomena za zagotavljanje javne varnosti in čeprav je njegova učinkovitost lahko v velikem obsegu odvisna od uporabe sodobnih preiskovalnih tehnik, tak cilj v splošnem interesu, čeprav je temeljnega pomena, sam po sebi ne more upravičiti tega, da se ukrep splošne

in neselektivne hrambe podatkov v zvezi s prometom in podatkov o lokaciji, kakršen je ta, ki je bil določen z direktivo 2006/24, šteje za nujni ukrep (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 94).

- 124 Podobno je Sodišče v točki 145 sodbe 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), pojasnilo, da niti pozitivne obveznosti držav članic, ki bi lahko glede na primer izhajale iz členov 3, 4 oziroma 7 Listine in se nanašajo – kot je bilo navedeno v točki 64 te sodbe – na določitev pravil, ki omogočajo učinkovit boj proti kaznivim dejanjem, ne morejo učinkovati tako, da bi utemeljevale tako resne posege v temeljne pravice, določene v členih 7 in 8 Listine, kot jih vsebuje nacionalna ureditev, ki določa hrambo podatkov o prometu in podatkov o lokaciji za praktično celotno prebivalstvo, ne da bi lahko bila iz podatkov zadevnih oseb razvidna vsaj posredna povezava z zastavljenim ciljem (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 95).
- 125 Poleg tega s sodbama ESČP z dne 25. maja 2021, Big Brother Watch in drugi proti Združenemu kraljestvu (CE:ECHR:2021:0525JUD 005817013), in z dne 25. maja 2021, Centrum för Rättvisa proti Švedski (CE:ECHR:2021:0525JUD 003525208), na kateri so se na obravnavi sklicevale nekatere vlade, da bi dokazale, da EKČP ne nasprotuje nacionalnim ureditvam, ki v bistvu določajo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, ni mogoče omajati razlage člena 15(1) Direktive 2002/58, ki izhaja iz zgoraj navedenih preudarkov. V teh sodbah je namreč šlo za množično prestrezanje podatkov v zvezi z mednarodnimi komunikacijami. Kot je Komisija poudarila na obravnavi, Evropsko sodišče za človekove pravice v teh sodbah ni odločalo o skladnosti splošne in nediferencirane hrambe podatkov o prometu in lokaciji na nacionalnem ozemlju ali celo obsežnega prestrezanja takih podatkov za namene preprečevanja, odkrivanja in preiskovanja hudih kaznivih dejanj z EKČP. Vsekakor je treba spomniti, da je namen člena 52(3) Listine zagotoviti potrebno usklajenost med pravicami iz te listine in ustreznimi pravicami, zagotovljenimi z EKČP, ne da bi se posegalo v avtonomijo prava Unije in Sodišča Evropske unije, tako da je treba pri razlagi Listine ustrezne pravice iz EKČP upoštevati le kot minimalno raven varstva (sodba z dne 17. decembra 2020, Centraal Israëlitisch Consistorie van België in drugi, C-336/19, EU:C:2020:1031, točka 56).

Dostop do podatkov, ki so bili hranjeni na splošno in neselektivno

- 126 Na obravnavi je danska vlada trdila, da morajo imeti pristojni nacionalni organi za boj proti hudemu kriminalu dostop do podatkov o prometu in podatkov o lokaciji, ki so bili splošno in neselektivno shranjeni, v skladu s sodno prakso iz sodbe 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 135 do 139), da bi se spopadli z resno grožnjo za nacionalno varnost, ki se izkaže za resnično, sedanjo ali predvidljivo.
- 127 Najprej je treba poudariti, da bi bil v primeru dovolitve dostopa do podatkov o prometu in do podatkov o lokaciji, ki so bili shranjeni splošno in neselektivno – zaradi boja proti hudemu kriminalu – ta dostop odvisen od okoliščin, ki niso povezane s tem ciljem, glede na to, ali v zadevni državi članici obstaja resna grožnja za nacionalno varnost, kot je navedena v prejšnji točki, medtem ko naj zgolj z vidika cilja boja proti hudemu kriminalu, s katerim morata biti utemeljena hramba in dostop do takih podatkov, nikakor ne bi bilo mogoče upravičiti različnega obravnavanja, zlasti med državami članicami (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 97).

- 128 Kot je Sodišče že razsodilo, je dostop do podatkov o prometu in podatkov o lokaciji, ki jih hranijo ponudniki elektronskih telekomunikacijskih storitev, na podlagi ukrepa, sprejetega na podlagi člena 15(1) Direktive 2002/58, ki ga je treba izvesti ob polnem spoštovanju pogojev, ki izhajajo iz sodne prakse, s katero je bila podana razlaga te direktive, načeloma mogoče upravičiti le s ciljem v splošnem interesu, za katerega je bila ta hramba naložena tem ponudnikom. Drugače je le, če pomembnost cilja, ki se uresničuje z dostopom, presega pomembnost cilja, s katerim je bila utemeljena hramba (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 98).
- 129 Trditve danske vlade pa se nanašajo na položaj, v katerem je cilj nameravane prošnje za dostop, in sicer boj proti hudemu kriminalu, v hierarhiji ciljev v splošnem interesu manj pomemben kot cilj, ki je upravičil hrambo, in sicer varovanje nacionalne varnosti. Če bi se v takem položaju dovolil dostop do shranjenih podatkov, bi bilo to v nasprotju s to hierarhijo ciljev v splošnem interesu, navedeno v prejšnji točki ter v točkah 68, 71, 72 in 73 te sodbe (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 99).
- 130 Poleg tega in predvsem v skladu s sodno prakso, navedeno v točki 74 te sodbe, podatki o prometu in podatki o lokaciji ne morejo biti predmet splošne in neselektivne hrambe zaradi boja proti hudemu kriminalu in zato dostopa do teh podatkov ni mogoče upravičiti s tem istim namenom. Če pa so bili ti podatki izjemoma splošno in neselektivno shranjeni zaradi zaščite nacionalne varnosti pred grožnjo, ki se v okoliščinah iz točke 71 te sodbe izkaže za resnično, sedanjo ali predvidljivo, nacionalni organi, pristojni za kazenske preiskave, ne morejo dostopati do navedenih podatkov v okviru kazenskega pregona, sicer bi se prepovedi take hrambe za boj proti hudemu kriminalu, na katero je opozorjeno v navedeni točki 74, odvzel vsakršen polni učinek (sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi, C-140/20, EU:C:2022:258, točka 100).
- 131 Glede na vse zgornje preudarke je treba na vprašanje za predhodno odločanje odgovoriti, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine razlagati tako, da nasprotuje nacionalnim zakonskim ukrepom, ki preventivno zaradi boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti določajo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji. Navedeni člen 15(1) v povezavi s členi 7, 8 in 11 ter 52(1) Listine pa je treba razlagati tako, da ne nasprotuje nacionalnim zakonskim ukrepom, s katerimi je:
- v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero se ponudnikom elektronskih komunikacijskih storitev naloži splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, pri čemer je sklep o tej odredbi lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni, in je navedeni sklep mogoče izdati le za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je v primeru nadaljnega obstoja te grožnje mogoče podaljšati;
 - za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je mogoče podaljšati, določena ciljna hramba podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije zadevnih oseb ali z geografskim merilom;

- za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, določena splošna in neselektivna hramba naslovov IP, dodeljenih viru povezave;
- za zaščito nacionalne varnosti, boj proti kriminalu in zaščito javne varnosti določena splošna in neselektivna hramba podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev ter
- za boj proti hudemu kriminalu in *a fortiori* za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero je ponudnikom elektronskih komunikacijskih storitev prek sklepa pristojnega organa, ki je predmet učinkovitega sodnega nadzora, za določeno obdobje naložena takojšnja hramba podatkov o prometu in podatkov o lokaciji, ki jih imajo ti ponudniki storitev na voljo,

če je s temi ukrepi z jasnimi in natančnimi pravili zagotovljeno, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe.

Stroški

- 132 Ker je ta postopek za stranke v postopkih v glavni stvari ena od stopenj v postopkih 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, v povezavi s členi 7, 8 in 11 ter 52(1) Listine Evropske unije o temeljnih pravicah

je treba razlagati tako, da

nasprotuje nacionalnim zakonskim ukrepom, ki preventivno zaradi boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti določajo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji;

ne nasprotuje nacionalnim zakonskim ukrepom, s katerimi je:

- **v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero se ponudnikom elektronskih komunikacijskih storitev naloži splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, pri čemer je sklep o tej odredbi lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni, in je navedeni sklep mogoče izdati le za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je v primeru nadaljnega obstoja te grožnje mogoče podaljšati;**

- za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je mogoče podaljšati, določena ciljna hramba podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije zadevnih oseb ali z geografskim merilom;
- za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, določena splošna in neselektivna hramba naslovov IP, dodeljenih viru povezave;
- za zaščito nacionalne varnosti, boj proti kriminalu in zaščito javne varnosti določena splošna in neselektivna hramba podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev ter
- za boj proti hudemu kriminalu in *a fortiori* za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero je ponudnikom elektronskih komunikacijskih storitev prek sklepa pristojnega organa, ki je predmet učinkovitega sodnega nadzora, za določeno obdobje naložena takojšnja hramba podatkov o prometu in podatkov o lokaciji, ki jih imajo ti ponudniki storitev na voljo,

če je s temi ukrepi z jasnimi in natančnimi pravili zagotovljeno, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe.

Podpisi