Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
MACIEJA SZPUNARJA,
predstavljeni 28. septembra 2023 [1]

Zadeva C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
proti
Premier ministre,
Ministère de la Culture

(Predlog za sprejetje predhodne odločbe, ki ga je vložil Conseil d'État (državni svet, Francija))

„Predhodno odločanje – Obdelava osebnih podatkov in varstvo zasebnosti na področju elektronskih komunikacij – Direktiva 2002/58/ES – Člen 15(1) – Možnost držav članic, da omejijo obseg nekaterih pravic in obveznosti – Obveznost predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločbe so zavezujoče – Podatki o civilni identiteti, ki ustrezajo IP-naslovu“

I. Uvod

1. Sodišče je na predlog velikega senata, vložen na podlagi člena 60(3) Poslovnika Sodišča, 7. marca 2023 odločilo, da se ta zadeva predodeli občni seji.

2. Sodišče (občna seja) je s sklepom z dne 23. marca 2023 odločilo, da ponovno odpre ustni del postopka, in zainteresirane subjekte iz člena 23 Statuta Sodišča Evropske unije ter Evropskega nadzornika za varstvo podatkov (ENVP) in Agencijo Evropske unije za kibernetsko varnost (ENISA) pozvalo, naj se udeležijo nove obravnave.

3. Prve sklepne predloge v tej zadevi sem predstavil 27. oktobra 2022 pred koncem ustnega dela postopka. Ti novi sklepni predlogi so torej priložnost za poglobitev nekaterih elementov mojega razlogovanja v tej zadevi, ki se nanaša na ključna vprašanja v zvezi s hrambo osebnih podatkov in dostopom do njih.

[1] Jezik izvirnika: francoščina.

II. Pravni okvir

A. Pravo Unije

4. V uvodnih izjavah 2, 6, 7, 11, 22, 26 in 30 Direktive 2002/58/ES[2] je navedeno:

„(2) Ta direktiva uveljavlja spoštovanje temeljnih pravic in upošteva načela, priznana zlasti z Listino o temeljnih pravicah Evropske unije [(v nadaljevanju: Listina)]. 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/ES[3]], 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.

[…]

[2] Direktiva Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), 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).

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

(22) Prepoved shranjevanja sporočil in s tem povezanih podatkov o prometu osebam, ki niso uporabniki ali ki nimajo privolitve uporabnikov, ni namenjena prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa v omrežju elektronskih komunikacij in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena v času njihovega hranjenja. […]

[…]

(26) Podatki o naročnikih, ki se obdelajo v elektronskih komunikacijskih omrežjih zaradi vzpostavitve povezav in prenosa podatkov, vsebujejo podatke o zasebnem življenju fizičnih oseb in zadevajo pravico do spoštovanja njihove korespondence ali legitimne interese pravnih oseb. Takšni podatki se lahko shranijo le v obsegu, potrebnem za izvedbo storitve, za namen zaračunavanja in plačila medsebojnih povezav ter za določen čas. Vsaka nadaljnja obdelava takih podatkov […] je dovoljena samo takrat, kadar naročnik v to privoli na podlagi točnih in popolnih podatkov, ki jih dobi od ponudnika javno razpoložljivih elektronskih komunikacijskih storitev o vrsti nadaljnje obdelave, ki jo ta namerava izvajati, in o naročnikovi pravici, da ne da privolitve za tako obdelavo ali da jo umakne. […]

[…]

(30) Sistemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev morajo biti zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum. […]“

5. Člen 2 te direktive, naslovljen „Opredelitve“, določa:

„[…]

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;

[…]“

6. Člen 3 navedene direktive, 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.“

7. Člen 5 iste 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/ES, 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.“

8. 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.

[…]“

9. 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 ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]. V ta namen lahko države članice med

drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje [Unije], vključno s tistimi iz člena 6(1) in (2) [PEU].“

B. Francosko pravo

1. Code de la propriété intellectuelle (zakonik o intelektualni lastnini)

10. Člen L. 331-12 code de la propriété intellectuelle (zakonik o intelektualni lastnini) v različici, ki se uporablja za spor o glavni stvari (v nadaljevanju: CPI), določa:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Visoka oblast za razširjanje del in varstvo pravic na spletu, v nadaljevanju: Hadopi) je neodvisen javni organ.“

11. Člen L. 331-13 CPI določa:

„[Hadopi] zagotavlja:

[…]

2. nalogo varstva [del in predmetov, varovanih z avtorsko ali sorodnimi pravicami v elektronskih komunikacijskih omrežjih,] pred kršitvami teh pravic, storjenimi v elektronskih komunikacijskih omrežjih, ki se uporabljajo za zagotavljanje javnih spletnih komunikacijskih storitev; […]“

12. Člen L. 331-15 tega zakonika določa:

„[Hadopi] je sestavljena iz kolegija in komisije za varstvo pravic. […]

[…]

Člani kolegija in komisije za varstvo pravic pri izvrševanju svojih pristojnosti ne prejemajo navodil nobenega organa.“

13. Člen L. 331-17 navedenega zakonika določa:

„Komisija za varstvo pravic je pristojna za sprejemanje ukrepov iz člena L. 331-25.“

14. Člen L. 331-21 istega zakonika določa:

„Za izvrševanje pristojnosti komisije za varstvo pravic ima [Hadopi] na voljo zaprisežene javne uslužbence, ki jih pooblasti [njen] predsednik pod pogoji, ki so določeni z odlokom na podlagi mnenja Conseil d’État (državni svet). […]

Članom komisije za varstvo pravic in uslužbencem iz prvega odstavka se predložijo zadeve, ki so na navedeno komisijo naslovljene pod pogoji iz člena L. 331–24. Njihova naloga je preučitev dejanskega stanja.

Za potrebe postopka lahko pridobijo vse dokumente, ne glede na njihov nosilec, vključno s podatki, ki jih hranijo in obdelujejo operaterji elektronskih komunikacij na podlagi člena L. 34-1

code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah) ter ponudniki storitev, navedeni v odstavkih 1 in 2 člena 6(I) loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo).

Pridobijo lahko tudi kopije dokumentov, navedenih v prejšnjem odstavku.

Zlasti lahko od operaterjev elektronskih komunikacij pridobijo informacije o identiteti, poštnem naslovu, elektronskem naslovu in telefonski številki naročnika, čigar dostop do javnih spletnih komunikacijskih storitev je bil uporabljen za reproduciranje, predstavitev, dajanje na voljo ali priobčitev varovanih del ali predmetov javnosti brez dovoljenja imetnikov pravic […], kadar se tako dovoljenje zahteva."

15. Člen L. 331-24 CPI določa:

„Komisiji za varstvo pravic zadeve v obravnavo predložijo pooblaščeni zapriseženi uslužbenci […], ki jih imenujejo:

– poklicna telesa, ustanovljena v skladu s predpisi;

– organizacije za kolektivno upravljanje pravic;

– državni center za kinematografijo in animirano podobo.

Komisija za varstvo pravic lahko ukrepa tudi na podlagi informacij, ki ji jih predloži Procureur de la République (državni tožilec, Francija).

Ni ji mogoče predložiti zadev v zvezi z dejanji, starejšimi od šestih mesecev."

16. Člen L. 331-25 tega zakonika, ki ureja tako imenovani postopek „postopnega odgovora", določa:

„Kadar je komisiji za varstvo pravic predložena zadeva v zvezi z dejanji, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3 [CPI], lahko naročniku pošlje […] priporočilo, v katerem ga opozori na določbe člena L. 336-3, mu odredi spoštovanje v njih opredeljene obveznosti in ga opozori na sankcije, zagrožene v skladu s členoma L. 335-7 in L. 335-7-1. To priporočilo vsebuje tudi informacijo naročniku o zakoniti ponudbi spletnih kulturnih vsebin, o obstoju sredstev za zavarovanje, s katerimi je mogoče preprečiti kršitve obveznosti, opredeljene v členu L. 336-3, ter o nevarnostih, ki jih za nadaljnje umetniško ustvarjanje in ekonomijo kulturnega sektorja pomenijo prakse, s katerimi se ne spoštujejo avtorska in sorodne pravice.

Če se v šestih mesecih od pošiljanja priporočila iz prvega odstavka dejanja, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3, ponovijo, lahko komisija po elektronski poti pošlje novo priporočilo, ki vsebuje enake informacije kot prejšnje […] To priporočilo mora poslati skupaj s priporočenim dopisom ali na kakršen koli drug način, s katerim se lahko dokaže datum vročitve tega priporočila.

V priporočilih, poslanih na podlagi tega člena, sta navedena datum in ura, ko so bila ugotovljena dejanja, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3. Nasprotno pa se v njih ne razkrije vsebina varovanih del ali predmetov, na katere se ta kršitev nanaša. V njih so

navedeni telefonska številka ter poštni in elektronski naslov, prek katerih lahko njihov naslovnik, če to želi, komisiji za varstvo pravic predloži pripombe in, če to izrecno zahteva, pridobi pojasnila o vsebini varovanih del ali predmetov, na katere se nanaša kršitev, ki se mu očita."

17. Člen L. 331-29 navedenega zakonika določa:

„[Hadopi] sme vzpostaviti avtomatsko obdelavo osebnih podatkov posameznikov, proti katerim je uveden postopek v okviru tega pododdelka.

Namen te obdelave je omogočiti, da komisija za varstvo pravic izvaja ukrepe, določene v tem pododdelku, vse z njimi povezane procesne akte in podrobna pravila o obveščanju poklicnih teles in organizacij za upravljanje avtorskih pravic o morebitnih sodnih postopkih ter vročitvah, določenih v petem odstavku člena L. 335-7.

[…] z odlokom [se] opredeli[jo] način[i] izvajanja tega člena. Z odlokom se zlasti določijo:

– kategorije hranjenih podatkov in obdobje njihove hrambe;

– naslovniki, ki so upravičeni do prejema teh podatkov, zlasti osebe, katerih dejavnost je zagotavljanje dostopa do storitev javnih spletnih komunikacijskih storitev;

– pogoji, pod katerimi lahko zainteresirane osebe pri [Hadopi] uveljavljajo svojo pravico do dostopa do podatkov, ki se nanašajo nanje […]"

18. Člen R. 331-37 istega zakonika določa:

„Operaterji elektronskih komunikacij […] in ponudniki storitev […] so zavezani, da prek povezave s sistemom za avtomatsko obdelavo osebnih podatkov iz člena L. 331-29 ali z uporabo nosilca za snemanje, ki zagotavlja njihovo integriteto in varnost, posredujejo osebne podatke in informacije, navedene v točki 2 priloge k [décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé ‚Système de gestion des mesures pour la protection des œuvres sur Internet' (odlok št. 2010-236 z dne 5. marca 2010 o avtomatizirani obdelavi osebnih podatkov, ki je dovoljena s členom L. 331-29 zakonika o intelektualni lastnini in ki je imenovana ‚Sistem upravljanja ukrepov za varstvo del na spletu'[4] (v nadaljevanju: odlok z dne 5. marca 2010))] […], v osmih dneh po tem, ko je komisija za varstvo pravic posredovala tehnične podatke, potrebne za identifikacijo naročnika, čigar dostop do podatkov o javnih spletnih komunikacijah je bil uporabljen za reproduciranje, predstavitev, dajanje na voljo ali priobčitev varovanih del ali predmetov javnosti brez dovoljenja imetnikov pravic […], kadar se to dovoljenje zahteva.

[…]"

[4] JORF z dne 7. marca 2010, besedilo št. 19.

19. Člen R. 335-5 CPI določa:

„I. Resno malomarnost, ki se kaznuje z globo, določeno za prekrške pete stopnje, pomeni dejstvo, da imetnik dostopa do javnih spletnih komunikacijskih storitev brez upravičenega razloga in če so izpolnjeni pogoji, določeni v odstavku II:

1. bodisi ni vzpostavil sredstva za zavarovanje tega dostopa

2. bodisi ni izkazal zadostne skrbnosti pri uporabi tega sredstva.

II. Določbe odstavka I se uporabljajo le, če sta izpolnjena oba spodaj navedena pogoja:

1. komisija za varstvo pravic je v skladu s členom L. 331-25 in na način, določen v tem členu, imetniku dostopa priporočila, naj uporabi sredstvo za zavarovanje svojega dostopa, s katerim bo mogoče preprečiti ponovno uporabo tega dostopa za reproduciranje, predstavitev, dajanje na voljo ali priobčitev javnosti del, varovanih z avtorsko ali sorodnimi pravicami, brez dovoljenja imetnikov teh pravic […], kadar se to dovoljenje zahteva;

2. v enem letu po predložitvi tega priporočila se ta dostop znova uporabi za namene, navedene v točki 1 tega odstavka II.“

20. Člen L. 336-3 tega zakonika določa:

„Imetnik dostopa do javnih spletnih komunikacijskih storitev mora zagotavljati, da se ta dostop ne uporablja za reproduciranje, predstavitev, dajanje na voljo ali priobčitev javnosti del, varovanih z avtorsko ali sorodnimi pravicami, brez dovoljenja imetnikov[…], kadar se to dovoljenje zahteva.

Če imetnik dostopa krši obveznost, opredeljeno v prvem odstavku, za zadevno osebo ne nastane kazenska odgovornost […]“

2. Décret du 5 mars 2010 (odlok z dne 5. marca 2010)

21. Odlok z dne 5. marca 2010 v različici, ki se uporablja za dejansko stanje v sporu o glavni stvari, v členu 1 določa:

„Namen obdelave osebnih podatkov, poimenovane ‚Sistem upravljanja ukrepov za varstvo del na spletu‘, je komisiji za varstvo pravic pri [Hadopi] omogočiti:

1. izvajanje ukrepov, določenih v knjigi III zakonodajnega dela [CPI] (naslov III, poglavje I, oddelek 3, pododdelek 3) in knjigi III uredbenega dela istega zakonika (naslov III, poglavje I, oddelek 2, pododdelek 2);

2. obravnavo zadev, ki jih predloži državni tožilec v zvezi z dejanji, ki bi lahko pomenila kršitev členov L. 335-2, L. 335-3, L. 335-4 in R. 335-5 istega zakonika, ter obveščanje poklicnih teles in organizacij za kolektivno upravljanje o tem, da so bile navedene zadeve predložene;

[…]“

22. Člen 4 tega odloka določa:

„I. Neposreden dostop do osebnih podatkov in informacij, navedenih v prilogi k temu odloku, imajo zapriseženi javni uslužbenci, ki jih pooblasti predsednik [Hadopi] v skladu s členom L. 331-21 [CPI], in člani komisije za varstvo pravic, navedene v členu 1.

II. Operaterjem elektronskih komunikacij in ponudnikom storitev, navedenim v točki 2 priloge k temu odloku, so predloženi:

– tehnični podatki, potrebni za identifikacijo naročnika;

– priporočila iz člena L. 331-25 [CPI], da zagotovijo njihovo pošiljanje svojim naročnikom po elektronski poti;

– elementi, potrebni za izvršitev dopolnilnih kazni začasne ukinitve dostopa do javne spletne komunikacijske storitve, s katerimi komisijo za varstvo pravic seznani državni tožilec.

III. Poklicna telesa in organizacije za kolektivno upravljanje so obveščeni o zadevah, ki jih je predložil državni tožilec.

IV. Pravosodnim organom so predloženi zapisniki o ugotovitvi dejanj, ki bi lahko pomenila kršitve, določene s členi L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 in R. 335-5 [CPI].

Informacija o izvršitvi kazni začasne ukinitve dostopa se vnese v avtomatizirano kazensko evidenco.“

23. Priloga k odloku z dne 5. marca 2010 določa:

„Osebni podatki in informacije, ki se hranijo v sistemu obdelave, poimenovanem ‚Sistem upravljanja ukrepov za varstvo del na spletu‘, so:

1. osebni podatki in informacije, katerih vir so poklicna telesa, ustanovljena v skladu s predpisi, organizacije za kolektivno upravljanje, državni center za kinematografijo in animirano podobo ter državni tožilec:

v zvezi z dejanji, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3 [CPI]:

datum in ura storitve dejanj;

IP-naslov zadevnih naročnikov;

uporabljeni protokol P2P;

psevdonim, ki ga uporablja naročnik;

informacije o varovanih delih ali predmetih, na katere se nanašajo storjena dejanja;

ime datoteke, kot je navedeno na naročnikovi terminalni opremi (če je to primerno);

ponudnik dostopa do spleta, pri katerem je bil sklenjen dostop ali ki je zagotovil tehnični vir IP. […]

[…]

2. osebni podatki in informacije o naročniku, zbrani pri operaterjih elektronskih komunikacij […] in ponudnikih […]:

priimek, imena;

poštni naslov in e-poštni naslovi;

telefonska številka;

naslov naročnikove telefonske naprave;

ponudnik dostopa do spleta, ki uporablja tehnične vire ponudnika dostopa, navedenega v točki 1, pri katerem je naročnik sklenil pogodbo; številka spisa;

datum začetka začasne ukinitve dostopa do javne spletne komunikacijske storitve.

[…]“

3. Code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah)

24. Člen L. 34-1 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah), kakor je bil spremenjen s členom 17 loi n° 2021-998 du 30 juillet 2021 (zakon št. 2021-998 z dne 30. julija 2021)[5], v odstavku IIa določa:

„[O]peraterji elektronskih komunikacij hranijo:

1. za potrebe kazenskih postopkov, preprečevanja groženj javni varnosti in zaščite nacionalne varnosti informacije o civilni identiteti uporabnika pet let po izteku veljavnosti njegove pogodbe;

2. za enake namene, kot so navedeni v točki 1 tega odstavka IIa, druge informacije, ki jih predloži uporabnik, ko sklene pogodbo ali ustvari račun, in informacije o plačilu eno leto po izteku veljavnosti njegove pogodbe ali zaprtju računa;

3. za potrebe boja proti kriminalu in hudim kaznivim dejanjem, preprečevanja resnih groženj javni varnosti in zaščite nacionalne varnosti tehnične podatke, na podlagi katerih je mogoče

[5] JORF z dne 31. julija 2021, besedilo št. 1. Ta različica člena L. 34-1 tega zakonika, ki velja od 31. julija 2021, je bila sprejeta po izdaji odločbe Conseil d'État (državni svet, Francija) z dne 21. aprila 2021, št. 393099 (JORF z dne 25. aprila 2021), s čimer je bila razveljavljena predhodna različica te določbe, ki je vsebovala obveznost hrambe osebnih podatkov „za potrebe preiskovanja, ugotavljanja in pregona kaznivih dejanj ali neizpolnitve obveznosti, opredeljene v členu L. 336-3 [CPI]“, in sicer zgolj zato, da se lahko po potrebi dajo na voljo zlasti Hadopi. Conseil constitutionnel (ustavni svet, Francija) je z odločbo št. 2021-976-977 QPC z dne 25. februarja 2022 (Habib A. in drugi) odločil, da je navedena prejšnja različica člena L. 34-1 navedenega zakonika v nasprotju s francosko ustavo, pri čemer je kot bistveni razlog navedel, da „je z izpodbijanimi določbami, ker se z njimi dovoljuje splošna in neselektivna hramba podatkov o povezavi, nesorazmerno poseženo v pravico do spoštovanja zasebnega življenja“ (točka 13). To sodišče je namreč menilo, da se podatki o povezavi, ki jih je treba hraniti v skladu s temi določbami, nanašajo ne samo na identifikacijo uporabnikov elektronskih komunikacijskih storitev, ampak tudi na druge podatke, ki „glede na njihovo raznolikost in to, kako se lahko obdelujejo, o teh uporabnikih in po potrebi tretjih osebah zagotavljajo številne natančne informacije, kar pomeni posebej hud poseg v njihovo zasebno življenje“ (točka 11).

identificirati vir povezave, ali podatke v zvezi z uporabljeno terminalsko opremo eno leto po povezavi ali uporabi terminalske opreme.“

III. Postopek pred Sodiščem

25. Tožeče stranke iz postopka v glavni stvari, francoska, danska, estonska, irska, nizozemska, finska in švedska vlada ter Komisija so v odgovor na poziv zainteresiranim subjektom iz člena 23 Statuta Sodišča Evropske unije odgovorile na pisna vprašanja Sodišča.

26. Iste stranke, razen finske vlade, ter češka, španska, ciprska, latvijska in norveška vlada ter ENVP in ENISA so se udeležili obravnave 15. maja 2023.

IV. Analiza

27. Na podlagi analize vprašanj za predhodno odločanje, ki sem jo opravil v okviru prvih sklepnih predlogov, sem Sodišču predlagal, naj razsodi, da je treba člen 15(1) Direktive 2002/58 razlagati tako, da ne nasprotuje nacionalni ureditvi, ki ponudnikom storitev elektronskih komunikacij omogoča hrambo, upravnemu organu, kot je Hadopi[6], pa dostop samo do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, zato da lahko ta organ identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za kršitve avtorske in sorodnih pravic, in lahko po potrebi v zvezi z njimi sprejme ukrepe brez predhodnega nadzora sodišča ali neodvisnega upravnega organa nad tem dostopom, če so ti podatki edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen.

28. V teh sklepnih predlogih bom poskušal podrobneje pojasniti nekatere elemente iz moje predhodne analize in vprašanja, o katerih se je razpravljalo na obravnavi, ki je potekala 15. maja 2023, da predstavim razloge, zaradi katerih vztrajam tako pri svojem predlogu odgovora na vprašanja za predhodno odločanje kot razlogovanju, ki me je pripeljalo do tega predloga.[7]

29. Natančneje, dokazal bom, da omogočanje hrambe in dostopa do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, brez predhodnega nadzora, da bi identificirali kršitelje, če so ti podatki edino sredstvo, s katerim je zadnjenavedene mogoče identificirati, izpolnjuje zahteve Sodišča, kar zadeva preučitev ukrepov, sprejetih v skladu s členom 15(1) Direktive 2002/58 (oddelek B).

30. Tako bom pokazal, da taka rešitev ne pomeni preobrata v sodni praksi, s katero se zahtevajo in varujejo temeljne pravice, ki jo je Sodišče razvijalo od sodb Tele2 Sverige in Watson in drugi[8] ter La Quadrature du Net in drugi[9], temveč njen nujen razvoj, ki po mojem mnenju dopolnjuje načela

6 Conseil supérieur de l’audiovisuel (višji svet za avdiovizualne medije, CSA) in Hadopi sta 1. januarja 2022 postala Autorité de régulation de la communication audiovisuelle et numérique (regulator avdiovizualne in digitalne komunikacije (Arcom)). Vendar se bom v teh sklepnih predlogih glede na obdobje, v katerem so se odvijala dejanja iz spora o glavni stvari, skliceval na Hadopi.

7 V zvezi s tem vztrajam tudi pri predlogu za preoblikovanje vprašanj za predhodno odločanje in svojem razumevanju njihovega predmeta. Čeprav je namreč v besedilu vprašanj za predhodno odločanje naveden samo dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, pa je vprašanje dostopa do teh podatkov neločljivo povezano z vprašanjem njihove hrambe pri ponudnikih elektronskih komunikacijskih storitev, tako da je analiza združljivosti hrambe s pravom Unije nujen predpogoj za analizo združljivosti dostopa. Glej v zvezi s tem točko 45 in naslednje mojih prvih sklepnih predlogov. Enako je treba vprašanja za predhodno odločanje, čeprav se nanašajo na „podatke o civilni identiteti, ki ustrezajo IP-naslovu“, razumeti tako, da se nanašajo tudi na dostop do IP-naslovov, ki omogoča identifikacijo vira povezave. Glej v zvezi s tem točko 41 in naslednje mojih prvih sklepnih predlogov.

8 Sodba z dne 21. decembra 2016 (C-203/15 in C-698/15, v nadaljevanju: sodba Tele2, EU:C:2016:970).

9 Sodba z dne 6. oktobra 2020 (C-511/18, C-512/18 in C-520/18, v nadaljevanju: sodba La Quadrature du Net in drugi, EU:C:2020:791).

Sodišča. To razlikovanje ni zgolj semantično. Namen rešitve, ki jo predlagam, namreč ni izpodbijati obstoječo sodno prakso, temveč zaradi določene pragmatičnosti omogočiti njeno prilagoditev v posebnih in zelo strogo opredeljenih okoliščinah (oddelek C).

31. Zaradi jasnosti in ker se je na razpravah med obravnavo izkazalo, da so v zvezi s tem potrebna pojasnila, bom analizo začel s predstavitvijo delovanja mehanizma postopnega odgovora, ki ga uporablja Hadopi (oddelek A).

A. Mehanizem postopnega odgovora, ki ga uporablja Hadopi

32. Hadopi je neodvisen upravni organ, ki je pristojen za varstvo avtorske in sorodnih pravic pred spletnimi kršitvami teh pravic. Za to je bil uveden tako imenovani mehanizem „postopnega odgovora“, ki ga izvaja komisija za varstvo pravic pri Hadopi.

33. Tej komisiji zadeve predložijo organizacije imetnikov pravic, v okviru katerih nekateri zapriseženi uslužbenci, ki jih pooblasti ministre de la culture (minister za kulturo), na omrežjih enakovrednih partnerjev *(peer to peer*) zbirajo IP-naslove spletnih uporabnikov, ki dajejo dela na voljo javnosti brez dovoljenja imetnikov pravic. Nato se pripravijo zapisniki. Ti med drugim vsebujejo IP-naslov dostopa do spleta, ki je bil uporabljen za storitev teh kršitev avtorske pravice, datum in uro ugotovljene kršitve ter naslov zadevnega dela, ter se posredujejo komisiji za varstvo pravic pri Hadopi. V zvezi s tem je treba poudariti, kot je navedel ENVP, da mora obdelavo osebnih podatkov s strani uslužbencev organizacij imetnikov pravic odobriti Commission nationale de l’informatique et des libertés (nacionalna komisija za informatiko in svoboščine, CNIL).[10]

34. Komisija za varstvo pravic pri Hadopi lahko po prejemu zapisnikov in po avtomatiziranem nadzoru, s katerim se zagotovi, da ti vsebujejo vse zahtevane podatke, od ponudnikov elektronske komunikacijske storitve pridobi identiteto, poštni naslov, elektronski naslov in telefonsko številko imetnika naročnine, ki je bila uporabljena za kršitev avtorske pravice.

35. Hadopi lahko nato tej osebi pošlje „priporočilo“, v katerem jo obvesti, da je bil njen dostop do spleta uporabljen v nasprotju z avtorskimi pravicami, in osebi, v zvezi s katero je podan sum, da ni izpolnila obveznosti skrbnega ravnanja, kar zadeva spoštovanje del, varovanih z avtorsko ali sorodnimi pravicami, na spletu, odredi, naj izpolni to obveznost. Povedano drugače, priporočilo je poslano imetniku dostopa do spleta, ki je dejansko lahko druga oseba, kot je tista, ki je dala delo na voljo in s tem kršila avtorsko pravico. V primeru ponovne ugotovitve kršitve prek istega dostopa do spleta je lahko poslano še eno priporočilo. V primeru vnovičnih ponovitev se komisija za varstvo pravic pri Hadopi lahko odloči, da zadevo predloži državnemu tožilcu za namene uvedbe kazenskega postopka. Kot je pojasnila francoska vlada v svojem prvem stališču, so uslužbenci Hadopi, ki so zadolženi za mehanizem postopnega odgovora, zapriseženi uslužbenci, pooblaščeni s strani predsednika Hadopi, ki so zavezani varovanju poklicne skrivnosti in so znotraj Hadopi edini, ki lahko dostopajo do osebnih podatkov, obdelovanih v okviru tega mehanizma.

[10] V zvezi s tem glej sklep št. 2010-225 CNIL z dne 10. junija 2010 o spremembi dovoljenja za izvajanje obdelave osebnih podatkov s strani Société des auteurs, compositeurs et éditeurs de musique (SACEM), katere namen je preiskovanje in ugotavljanje kaznivih dejanj ponarejanja, storjenih prek omrežij za izmenjavo datotek, imenovanih „peer to peer“ (dovoljenje št. 1425421).

36. V zvezi s tem moram pojasniti, da se ne zbirajo in Hadopi posredujejo podatki vseh uporabnikov omrežij enakovrednih partnerjev, če ti zgolj prenašajo take vsebine,[11] temveč samo podatki oseb, ki so vsebine, ki so predmet kršitve, dajali na voljo, namreč, ki so take vsebine *nalagali*.

37. Za ponazoritev naj navedem, da je Hadopi tako v letu 2021 od organizacij imetnikov pravic prejela skoraj štiri milijone zapisnikov, poslala je 210.595 prvih priporočil in 53.564 ponovnih priporočil ter državnem tožilcu predložila 1484 zadev.

38. Zdaj ko je ta predstavitev končana, bom pojasnil, zakaj menim, da tak mehanizem, ki predpostavlja hrambo in dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, izpolnjuje zahteve sodne prakse v zvezi z nacionalnimi ukrepi, sprejetimi v skladu s členom 15(1) Direktive 2002/58.

B. Spoštovanje zahtev, ki izhajajo iz sodne prakse Sodišča v zvezi z razlago člena 15(1) Direktive 2002/58

39. Ker sem sodno prakso Sodišča v zvezi s hrambo in dostopom do IP-naslovov, dodeljenih viru povezave, predstavil že v prvih sklepnih predlogih,[12] se bom v teh sklepnih predlogih osredotočil na to, kar je po mojem mnenju bistvo te sodne prakse, in sicer, prvič, na zahtevo po sorazmernosti in, drugič, kar zadeva dostop do teh podatkov, na morebitno potrebo po predhodnem nadzoru sodišča ali neodvisnega upravnega organa.

1. Sorazmernost zadevnega ukrepa

40. Za ugotovitev, ali je ukrep hrambe ali dostopa do podatkov o civilni identiteti, ki ustrezajo IP-naslovu, združljiv s pravom Unije, je treba, kot Sodišče redno poudarja, uskladiti različne zadevne zakonite interese in pravice, in sicer na eni strani pravici do varstva zasebnosti in do varstva osebnih podatkov[13], ki sta zagotovljeni s členoma 7 in 8 Listine, ter na drugi strani varstvo pravic in svoboščin drugih ter pravic, določenih v členih 3, 4, 6 in 7 Listine[14]. Naj dodam, da je treba v obravnavani zadevi pravici do varstva zasebnosti in do varstva osebnih podatkov uskladiti tudi z lastninsko pravico, ki je določena v členu 17 Listine, saj je mehanizem postopnega odgovora navsezadnje namenjen varstvu avtorske in sorodnih pravic.

41. Sodišče v zvezi s tem pojasnjuje, da ta uskladitev na podlagi člena 15(1) Direktive 2002/58 državam članicam omogoča, da sprejmejo ukrep, ki odstopa od načela zaupnosti, kadar je tak ukrep „*potreben, primeren in ustrezen [sorazmeren]* […] znotraj demokratične družbe“ (moj poudarek). V uvodni izjavi 11 te direktive je pojasnjeno, da mora biti tak ukrep „dosledno“ *sorazmeren* zastavljenemu cilju.[15]

[11] V zvezi z delovanjem omrežij enakovrednih partnerjev in različnimi profili uporabnikov spleta na teh omrežjih glej moje sklepne predloge v zadevi M.I.C.M. (C-597/19, EU:C:2020:1063, točka 37 in naslednje).

[12] Točka 53 in naslednje mojih prvih sklepnih predlogov.

[13] Pravici do varstva zasebnosti in do varstva osebnih podatkov sta v okviru Direktive 2002/58 izraženi z načeloma zaupnosti sporočil in prepovedi hrambe s tem povezanih podatkov, ki sta določeni v njej.

[14] Sodbe La Quadrature du Net in drugi (točke od 120 do 122, 127 in 128); z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, v nadaljevanju: sodba Commissioner of An Garda Síochána in drugi, EU:C:2022:258, točki 48 in 50), in z dne 20. septembra 2022, SpaceNet in Telekom Deutschland (C-793/19 in C-794/19, v nadaljevanju: sodba SpaceNet in Telekom Deutschland, EU:C:2022:702, točki 63 in 65).

[15] Sodbe La Quadrature du Net in drugi (točka 129); Commissioner of An Garda Síochána in drugi (točka 51) ter SpaceNet in Telekom Deutschland (točka 66).

42. Sodišče se poleg tega skozi celotno razlogovanje v zvezi z razlago člena 15(1) Direktive 2002/58 sklicuje na načelo sorazmernosti in ga torej obravnava kot ključni element preizkusa nacionalnega ukrepa hrambe ali dostopa do osebnih podatkov, ki je bil sprejet na podlagi te določbe.

43. Iz podrobnejše preučitve tega razlogovanja je razvidno, da načelo sorazmernosti v okviru člena 15(1) Direktive 2002/58 vsebuje več delov, ki se nanašajo na, prvič, resnost posega v temeljne pravice, ki ga pomeni hramba ali dostop do podatkov o prometu, in, drugič, nujnost zadevnega ukrepa.

44. Glede tega, da Hadopi hrani in dostopa do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, menim, da bi moralo Sodišče tako zaradi resnosti posega kot nujnosti teh podatkov prilagoditi preučitev sorazmernosti nacionalnega ukrepa, sprejetega na podlagi člena 15(1) Direktive 2002/58.

a) Relativna resnost posega v temeljne pravice

45. Iz ustaljene sodne prakse Sodišča jasno izhaja, da mora biti v skladu z načelom sorazmernosti pomembnost cilja, ki se uresničuje z ukrepom, sprejetim na podlagi člena 15(1) Direktive 2002/58, povezana z resnostjo posega, ki iz njega izhaja. [16]

46. Natančneje, Sodišče je razsodilo, kot sem poudaril v prvih sklepnih predlogih, da lahko resen poseg na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj upraviči le cilj boja proti kriminalu, ki mora biti prav tako opredeljen kot resen. [17]

47. Sodišče je v zvezi z IP-naslovi navedlo, da čeprav je stopnja občutljivosti teh podatkov nižja od stopnje občutljivosti drugih podatkov o prometu, njihova hramba in analiza vseeno pomenita resna posega v temeljne pravice, saj ju je mogoče uporabiti za izčrpno sledenje brskanju, ki ga je opravil uporabnik spleta, ter torej za ugotavljanje njegovega podrobnega profila in natančno sklepanje o njegovem zasebnem življenju. [18]

48. V postopku v glavni stvari je namen hrambe in dostopa do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, boj proti kršitvam avtorske in sorodnih pravic. Menim pa, da je jasno, da tega boja, kljub ogromnemu številu teh kršitev, ni mogoče uvrstiti v okvir boja proti hudemu kriminalu [19]. Resnost posega v temeljne pravice, ki ga pomeni zadevni ukrep, naj torej ne bi bila sorazmerna s ciljem, ki se z njim uresničuje.

49. V prvih sklepnih predlogih sem v skladu s sodno prakso Sodišča menil, da dostop Hadopi do podatkov o civilni identiteti, ki ustrezajo IP-naslovu, dejansko pomeni resen poseg v temeljne pravice. Čeprav sem menil tudi, da bi morala biti hramba in dostop do teh podatkov v obravnavani zadevi vseeno dovoljena, moram po obravnavi navesti še nekaj pojasnil.

[16] Sodbi Commissioner of An Garda Síochána in drugi (točka 56) ter SpaceNet in Telekom Deutschland (točka 71).

[17] Sodbe Tele2 (točka 115); z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 56), in z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov v zvezi z elektronskimi komunikacijami) (C-746/18, v nadaljevanju: sodba Prokuratuur, EU:C:2021:152, točka 33). Glej tudi točko 92 mojih prvih sklepnih predlogov.

[18] Glej sodbe La Quadrature du Net in drugi (točki 152 in 153); Commissioner of An Garda Síochána in drugi (točka 73) ter SpaceNet in Telekom Deutschland (točka 103). Glej tudi točke 63, 64 in 93 mojih prvih sklepnih predlogov.

[19] V prvih sklepnih predlogih sem trdil, da bi bilo treba pojem „hud kriminal“ razlagati samostojno, da bi preprečili, da bi se države članice kakor koli izogibale zahtevam iz člena 15(1) Direktive 2002/58. Vztrajam pri tem stališču. Poudariti pa moram, da čeprav bi Sodišče razsodilo, da je opredelitev pojma „hud kriminal“ prepuščena državam članicam, bi morala biti ta vsekakor določena v mejah prava Unije in ne bi smela biti razširjena tako, da bi ta določba izgubila svoj pomen.

50. Mehanizem postopnega odgovora Hadopi omogoča, da IP-naslov – ki ga posredujejo organizacije imetnikov pravic – oseb, za katere se sumi, da so svoj dostop do spleta uporabile za kršitev avtorske pravice na omrežju enakovrednih partnerjev, poveže s civilno identiteto teh oseb in z izvlečkom datoteke, z nalaganjem katere je bila kršena avtorska pravica. Kot sta na obravnavi navedla Komisija in ENVP, je s pomočjo takih elementov sicer gotovo mogoče pridobiti več informacij kot pa samo identiteto domnevnega kršitelja, vendar iz njih vseeno ni mogoče zelo natančno sklepati o zasebnem življenju te osebe. Kot sem navedel v prvih sklepnih predlogih,[20] gre zgolj za razkritje vsebine, ogledovane v točno določenem trenutku, ki samo po sebi ne more omogočiti ugotovitve podrobnega profila osebe, ki si je to vsebino ogledovala.

51. To velja še toliko bolj, ker je, prvič, velika večina IP-naslovov, posredovanih Hadopi, tako imenovanih „dinamičnih“ IP-naslovov, ki so po naravi spremenljivi in točno določeni identiteti ustrezajo le v enem samem trenutku, ki sovpada z dajanjem zadevne vsebine na voljo. Ti podatki torej izključujejo vsakršno izčrpno sledenje.

52. Drugič, poudariti moram, da z varstvom temeljnih pravic na spletu po mojem mnenju ni mogoče upravičiti tega, da ni mogoče dostopati zgolj do podatkov o IP-naslovu, vsebini dela in identiteti osebe, ki ga je dala na voljo v nasprotju z avtorsko pravico, temveč samo to, da morajo hrambo in dostop do teh podatkov spremljati jamstva. V zvezi s tem se mi zdi zgovorna analogija s stvarnim svetom: oseba, osumljena tatvine, se ne more sklicevati na pravico do varstva zasebnosti, zato da se osebe, pristojne za uvedbo postopka zoper to kaznivo dejanje, ne bi mogle seznaniti z ukradenimi predmeti. Ta oseba pa se nasprotno lahko upravičeno sklicuje na svoje temeljne pravice, zato da se med postopkom ne bi dostopalo do nabora podatkov, ki je širši od zgolj podatkov, potrebnih za opredelitev domnevnega kaznivega dejanja.

53. Naj nazadnje navedem, da v nasprotju s tem, kar so trdile tožeče stranke, ni videti, da bi mehanizem postopnega odgovora pomenil splošni nadzor nad uporabniki omrežij enakovrednih partnerjev. Ne gre namreč za preverjanje njihove celotne dejavnosti na danem omrežju, da bi ugotovili, ali so dali na voljo neko delo in s tem kršili avtorsko pravico, temveč bolj za to, da bi na podlagi datoteke, za katero je bilo ugotovljeno, da je ponaredek, ugotovili imetnika dostopa do spleta, s katerega je uporabnik spleta izvedel to dajanje na voljo. Prav tako, kot je na obravnavi poudaril ENVP, ne gre za nadzor dejavnosti vseh uporabnikov omrežij enakovrednih partnerjev, temveč samo dejavnosti oseb, ki nalagajo datoteke, ki so predmet kršitve, pri čemer so elementi, povezani z zasebnostjo posameznika, toliko manj razvidni iz nalaganja teh datotek, ker se to lahko izvaja izključno za to, da se tem uporabnikom spleta nato omogoči prenos drugih datotek.

54. V teh okoliščinah menim, da razlogov, zaradi katerih je Sodišče menilo, da sta hramba in dostop do IP-naslovov resen poseg v temeljne pravice, ni mogoče uporabiti v zvezi s mehanizmom postopnega odgovora, kot je ta, ki ga uporablja Hadopi. Iz tega sledi, da bi bilo treba resnost posega, ki ga pomenita ta hramba in dostop, pri preučitvi načela sorazmernosti prilagoditi.

55. Povedano drugače, menim, da se sodna praksa Sodišča v zvezi z resnostjo posega v temeljne pravice, povzročenega s hrambo in dostopom do IP-naslovov, ne sme razlagati tako, da pomeni, da je ta poseg vedno resen, temveč tako, da je resen samo, kadar je IP-naslove mogoče uporabiti za izčrpno sledenje brskanju uporabnika spleta in zelo natančno sklepanje o njegovem zasebnem življenju.

[20] Točka 101 mojih prvih sklepnih predlogov.

56. Ker v položaju, kot je ta iz postopka v glavni stvari, ni tako, iz tega izhaja, da bi moralo biti poseg, ki ga pomenita hramba in dostop do civilnih identitet, ki ustrezajo IP-naslovu, uporabljenemu za ponujanje vsebine, ki pomeni kršitev avtorske pravice, mogoče upravičiti s ciljem boja proti kriminalu, ki zajema širše področje kot samo hud kriminal.

57. Naj pojasnim še, da poseg v temeljne pravice, ki ga pomenita hramba in dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovu, v položaju, kot je ta iz postopka v glavni stvari, ni resnejši zaradi okoliščine, da imetnik dostopa do spleta, uporabljenega za dajanje vsebine, ki je predmet kršitve, na voljo, ni nujno izvajalec tega dajanja na voljo, tako da bi priporočilo Hadopi lahko pripeljalo do tega, da bi se temu imetniku razkrila navedena vsebina, do katere je lahko dostopala tretja oseba. Naj na eni strani spomnim, da Hadopi preiskuje kaznivo dejanje neizpolnitve obveznosti zagotavljanja, da se dostop ne uporabi za dajanje neke vsebine na voljo v nasprotju z avtorsko pravico. Zato je treba informacije, ki omogočajo njegovo opredelitev, posredovati domnevnemu storilcu. Na drugi strani menim, kot sem že navedel, da iz informacij v zvezi z zadevnim delom ni mogoče natančno sklepati o zasebnem življenju osebe, ki je to delo dala na voljo. Morebitno posredovanje teh informacij imetniku spletnega priključka torej ne presega tistega, kar je potrebno za to, da se omogoči uvedba kazenskega postopka zoper zadevno kršitev avtorske pravice.

b) Nujnost zadevnih podatkov za odkrivanje in pregon kršitve

58. Za zagotovitev sorazmernosti ukrepa hrambe in dostopa do podatkov o prometu – kot so podatki o civilni identiteti, ki ustrezajo IP-naslovu – sprejetega na podlagi člena 15(1) Direktive 2002/58, mora biti poseganje, ki ga ta ukrep predpostavlja, v skladu s sodno prakso Sodišča omejeno na to, kar je nujno potrebno, da je mogoče uresničiti zastavljeni cilj.[21] Menim, da prav to velja za ukrep iz postopka v glavni stvari.

59. Kot sem poudaril v prvih sklepnih predlogih,[22] iz same sodne prakse Sodišča izhaja, da je v primeru kršitve, storjene izključno na spletu, kot je kršitev avtorske pravice na omrežju enakovrednih partnerjev, IP-naslov lahko edino preiskovalno sredstvo, ki omogoča identifikacijo osebe, ki ji je bil ta naslov dodeljen ob storitvi te kršitve.[23] Menim, da iz tega izhaja, da sta hramba in dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, z namenom odkrivanja in pregona spletnih kršitev avtorske pravice v skladu s sodno prakso nujno potrebna za uresničitev zastavljenega cilja.

60. Res je, da vsaka zahteva po varstvu osebnih podatkov predpostavlja omejitev preiskovalnih pooblastil. To izhaja iz samega načela usklajevanja nasprotnih interesov, zato takega rezultata kot takega ni mogoče izpodbijati. Vendar se v primeru, da je IP-naslov edino sredstvo, ki omogoča identifikacijo osebe, osumljene storitve spletne kršitve pravice intelektualne lastnine, tak položaj razlikuje od večine kazenskih postopkov, v zvezi s katerimi je Sodišče navedlo, da „učinkovitost […] na splošno ni odvisna od enega samega preiskovalnega instrumenta, temveč od vseh preiskovalnih instrumentov, ki jih imajo pristojni nacionalni organi za te namene“.[24] Če bi priznali, da podatki o civilni identiteti, ki ustrezajo IP-naslovom, ne bi smeli biti predmet hrambe in dostopa v položaju, kot je ta iz postopka v glavni stvari, ne bi prišlo zgolj do omejitve

[21] Sodbe La Quadrature du Net in drugi (točke od 120 do 122 in 132); Commissioner of An Garda Síochána in drugi (točki 48 in 54) ter SpaceNet in Telekom Deutschland (točki 63 in 69).

[22] Točka 78 mojih prvih sklepnih predlogov.

[23] Sodbe La Quadrature du Net in drugi (točka 154); Commissioner of An Garda Síochána in drugi (točka 73) ter SpaceNet in Telekom Deutschland (točka 100).

[24] Sodba Commissioner of An Garda Síochána in drugi (točka 69).

preiskovalnih pooblastil, kot z vsakim ukrepom, s katerim se zagotavlja varstvo podatkov o prometu, temveč bi bilo nacionalnim organom dejansko odvzeto edino sredstvo za odkrivanje in pregon nekaterih kršitev.

61. Povedano drugače, v skladu z razlago člena 15(1) Direktive 2002/58, ki jo predlagam, ne gre za to, da se s preučitvijo nujnosti takega ukrepa omogočita hramba in dostop do podatkov, ki zgolj *olajšajo* odkrivanje in pregon kršitev, kadar je te kršitve mogoče odkriti in preganjati tudi s konkurenčnimi, vendar manj učinkovitimi sredstvi. Nasprotno, hramba in dostop do teh podatkov se omogočita, kadar so ti *nujni* za identifikacijo osebe, ki je osumljena storitve kršitve in ki je ne bi bilo mogoče preganjati brez teh sredstev, saj so zadevni podatki edini instrument za identifikacijo uporabnika spleta, če je kršitev storjena izključno na spletu.

62. Menim, da je treba upoštevati tako razlago, sicer bi dopustili, da cele vrste kaznivih dejanj ne bi bilo nikoli mogoče preganjati. [25]

63. Iz vsega navedenega izhaja, da je po mojem mnenju nacionalna ureditev, ki ponudnikom elektronskih komunikacijskih storitev omogoča hrambo, upravnemu organu pa dostop samo do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, popolnoma sorazmerna z zastavljenim ciljem, to je pregonom kršitev avtorske in sorodnih pravic na spletu, ker ima poseg v temeljne pravice, ki ga vključujeta, omejeno težo in ker so ti podatki edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen.

64. Zato menim, da bi bilo treba člen 15(1) Direktive 2002/58 razlagati tako, da ne nasprotuje taki ureditvi.

2. Obstoj ustreznih materialnih in postopkovnih jamstev

65. Kar posebej zadeva dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, je iz sodne prakse Sodišča razvidno, da zgolj stroga sorazmernost ukrepa ni dovolj za njegovo združljivost s členom 15(1) Direktive 2002/58.

66. Sodišče je namreč razsodilo, da je za zagotovitev, da je dostop do podatkov o prometu in lokaciji omejen na tisto, kar je nujno potrebno, bistveno, da je ta dostop odvisen od predhodnega nadzora, ki ga opravi bodisi sodišče bodisi neodvisen upravni organ, ki ima vsa pooblastila in zagotavlja vsa potrebna jamstva za uskladitev različnih zadevnih legitimnih interesov in pravic. [26]

67. Ozka razlaga sodne prakse bi torej pripeljala do tega, da bi se štelo, da bi moral biti dostop Hadopi do podatkov o civilni identiteti, ki ustrezajo IP-naslovom oseb, osumljenih storitve kršitve avtorske pravice na spletu, pogojen s takim predhodnim nadzorom, ki ga v obstoječem mehanizmu postopnega odgovora ni.

68. Vendar menim, kot je na obravnavi trdila irska vlada in kot sem navedel v prvih sklepnih predlogih, da zahteva po predhodnem nadzoru sodišča ali neodvisnega upravnega organa ni sistematična zahteva, ampak je odvisna od celovitejše analize zadevnega ukrepa, pri čemer se upoštevajo tako resnost posega, ki ga pomeni ta ukrep, kot jamstva, ki jih ta predvideva.

[25] Točka 81 mojih prvih sklepnih predlogov. V zvezi s tem glej tudi točko 79 in naslednje teh sklepnih predlogov.

[26] Sodbe Tele2 (točka 120); Prokuratuur (točki 51 in 52) ter Commissioner of An Garda Síochána in drugi (točki 106 in 107).

69. Poudarjam namreč, da so bile v vsaki od sodb, v katerih je bila navedena ta zahteva po predhodnem nadzoru sodišča ali neodvisnega upravnega organa, sporne nacionalne ureditve, ki so omogočale dostop do vseh podatkov o prometu in lokaciji uporabnikov v zvezi z vsemi sredstvi elektronske komunikacije uporabnikov [27] ali vsaj s fiksno in mobilno telefonijo [28] identificiranih uporabnikov.

70. Na podlagi tega sklepam, da je zahteva po takem predhodnem nadzoru odvisna od resnosti posega, ki se obravnava v zadevnih zadevah. Kot je poudarilo Sodišče, je šlo za podatke, ki „dejansko omogoča[jo] natančne, ali celo zelo natančne ugotovitve o zasebnem življenju oseb, […] kot so vsakodnevne navade, kraji stalnega ali začasnega bivanja, dnevne ali druge poti, dejavnosti, socialni odnosi teh oseb in družbena okolja, ki jih obiskujejo“. [29] Poleg tega je šlo za podatke oseb, ki so bile identificirane in osumljene storitve kršitve že na podlagi drugih indicev, tako da zadevni podatki omogočajo okrepitev obremenilnih dokazov zoper zadevnega uporabnika z razširitvijo področja uporabe podatkov, ki ga zadevajo.

71. Kar zadeva ureditev iz postopka v glavni stvari pa je, kot sem poudaril, poseg, ki ga pomeni povezava podatka o civilni identiteti in IP-naslova, občutno manj resen od posega, ki izhaja iz dostopa do vseh podatkov o prometu in lokaciji osebe, saj ta povezava ne prinaša nobenega elementa, s katerim bi bilo mogoče natančno sklepati o zasebnem življenju zadevne osebe.

72. Poleg tega, kot sem navedel v prvih sklepnih predlogih, [30] se ti podatki nanašajo le na osebe, ki so, glede na to, da so organizacije imetnikov pravic objektivno ugotovile uporabo IP-naslova, ki pomeni kršitev avtorske pravice, storile dejanja, ki bi lahko pomenila kršitev obveznosti skrbnega ravnanja, določene s členom L.336-3 CPI. Te osebe niso predhodno identificirane z drugimi sredstvi, tako da je povezava IP-naslova s podatki o civilni identiteti edino sredstvo za identificiranje zadevne osebe. Dostop do teh podatkov torej ne omogoča pridobitve dodatnih in točnih informacij o dejavnosti oseb, ki so osumljene že na podlagi drugih elementov, tako kot je bilo v zadevah, v katerih je Sodišče že razsodilo, ampak samo uporabo IP-naslova, ki bi bil sicer neuporaben. V teh okoliščinah so podatki, do katerih dostopa Hadopi, dejansko omejeni.

73. Menim, da se dejanje dostopa do osebnih podatkov, ki se nanašajo na posameznika, osumljenega storitve kršitve, da se dokaže njegova krivda, bistveno razlikuje od dejanja omogočanja razkritja identitete storilca že ugotovljene kršitve.

74. To po mojem velja še toliko bolj, ker je za zbiranje IP-naslovov na omrežjih enakovrednih partnerjev potrebno predhodno dovoljenje, ki je omejeno na izključno te podatke, tako da Hadopi nikoli nima na voljo neomejenega nabora podatkov v zvezi z uporabniki spleta, ki so osumljeni storitve kršitve avtorskih pravic na spletu. [31]

75. Logike, na kateri temelji zahteva po predhodnem nadzoru sodišča ali neodvisnega upravnega organa, zato ni mogoče uporabiti v zvezi z mehanizmom postopnega odgovora, kot je ta iz postopka v glavni stvari, tako da se mi ta zahteva ne zdi potrebna za to, da se zagotovi, da je poseg v temeljne pravice, ki ga pomeni ta mehanizem, omejen na to, kar je nujno potrebno.

27 Sodbi Tele2 ter Commissioner of An Garda Síochána in drugi.

28 Sodba Prokuratuur.

29 Sodba Prokuratuur (točka 36).

30 Točka 102 mojih prvih sklepnih predlogov.

31 Točka 33 teh sklepnih predlogov.

76. Iz vsega navedenega izhaja, da je nacionalna ureditev, ki neodvisnemu upravnemu organu, kot je Hadopi, omogoča hrambo in dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, da lahko identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za kršitve avtorske pravice, brez predhodnega nadzora sodišča ali neodvisnega upravnega organa nad tem dostopom, navsezadnje v skladu z načeli, določenimi v sodni praksi Sodišča, če so ti podatki edino sredstvo, ki omogoča identifikacijo osebe, kateri je bil v času storitve kršitve dodeljen IP-naslov, tako da bi bilo treba člen 15(1) Direktive 2002/58 razlagati tako, da ne nasprotuje taki ureditvi.

77. Poleg teh preudarkov, ki se nanašajo na zadevo iz postopka v glavni stvari, moram navesti še splošnejše pripombe o potrebi po takem razvoju sodne prakse Sodišča.

C. Nujen in omejen razvoj sodne prakse

78. Več argumentov govori v prid izpopolnitvi sodne prakse Sodišča v zvezi s hrambo in dostopom do podatkov, kot so IP-naslovi, povezani s podatki o civilni identiteti.

79. Na prvem mestu in kot sem že poudaril,[32] je v položaju iz postopka v glavni stvari pridobitev podatkov o civilni identiteti, ki ustrezajo IP-naslovu, edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve zadevne kršitve dodeljen.

80. Iz tega nujno izhaja, da če bi Sodišče menilo, da člen 15(1) Direktive 2002/58 vseeno nasprotuje njihovi hrambi in dostopu do njih, bi nacionalni organi dejansko ostali brez tega edinega identifikacijskega sredstva, zaradi česar zoper storilce zadevne kršitve ne bi bilo mogoče nikoli uvesti kazenskega postopka.[33] Zato sem v prvih sklepnih predlogih spomnil na možnost sistemske nekaznovanosti te kršitve.[34]

81. Tveganje sistemske nekaznovanosti ni omejeno na kršitve avtorske pravice, storjene na omrežjih enakovrednih partnerjev, ampak zajema, kot je na obravnavi trdila češka vlada, vse kršitve, storjene izključno na spletu.

82. Kršitev, katerih storilca je mogoče identificirati samo prek njegovega IP-naslova, namreč ne bi bilo mogoče nikoli preganjati, besedil, s katerimi se sankcionirajo, pa ne bi bilo mogoče nikoli uporabiti, če bi bilo treba šteti, da sta hramba podatkov in dostop do njih v nasprotju s pravom Unije.

83. V zvezi s tem ugotavljam, da drži, kot so navedle tožeče stranke v postopku v glavni stvari, da bi bilo storilce nekaterih kršitev, storjenih izključno na spletu, teoretično mogoče identificirati z drugimi sredstvi. Med drugim se tako sklicujejo na uporabniško ime, ki se uporablja v družbenih omrežjih, in na podatke, povezane z računom uporabnika, njegovim elektronskim naslovom, telefonsko številko, ali element o zasebnem življenju, ki ga je ta oseba razkrila. Vendar so za take podatke, da jih je mogoče povezati z identiteto posameznika, potrebne podrobne preiskave, med katerimi se preučuje spletna dejavnost uporabnika spleta. Menim torej, da je z uporabo takih preiskovalnih sredstev mogoče priti do zelo natančnih ugotovitev o zasebnem življenju posameznikov, za razliko od samo IP-naslova, tako da bi bila hramba in dostop do teh podatkov v tem smislu v nasprotju s členom 15(1) Direktive 2002/58.

[32] Točka 59 teh sklepnih predlogov.

[33] Točka 62 teh sklepnih predlogov.

[34] Točka 78 in naslednje mojih prvih sklepnih predlogov.

84. V teh okoliščinah dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovu uporabnika spleta, sicer ni edino teoretično preiskovalno sredstvo, s katerim je mogoče identificirati imetnika tega naslova v času storitve kršitve, je pa sredstvo, ki omogoča uvedbo postopka zoper to osebo in pri tem pomeni najmanjši poseg v njegove temeljne pravice ter tako preprečuje splošno nekaznovanost.

85. Na drugem mestu naj znova poudarim, da bi taka rešitev po mojem mnenju omogočila uskladitev dveh usmeritev sodne prakse Sodišča, ki sta razlog za trenja, opredeljena v prvih sklepnih predlogih [35] in v sklepnih predlogih v zadevi M.I.C.M. [36], in sicer sodne prakse v zvezi s hrambo in dostopom do podatkov na eni strani ter sodne prakse v zvezi s sporočanjem IP-naslovov, dodeljenih viru povezave, v okviru tožb zaradi varstva pravic intelektualne lastnine, ki so jih vložile osebe zasebnega prava, na drugi strani.

86. Na tretjem mestu, sodna praksa Sodišča od sodb Tele2 in La Quadrature du Net in drugi je sicer dobrodošla, ker je omogočila vzpostavitev okvira za varovanje temeljnih pravic uporabnikov elektronskih komunikacijskih storitev, vendar je nekoliko kazuistična. Sodišče je namreč z zadevami, ki so mu bile predložene v obravnavo, postopno izpopolnjevalo svojo sodno prakso, kar mu je omogočilo preučevanje različnih nacionalnih ureditev z vidika člena 15(1) Direktive 2002/58. Vendar Sodišče ne more predvideti praktično vseh ukrepov, ki bi lahko bili predmet analize z vidika te določbe. To je med drugim razvidno iz številnih predlogov za sprejetje predhodne odločbe, [37] katerih predmet je zadnjenavedena določba, od sodbe Tele2, ki po mojem mnenju potrjujejo težave, ki jih imajo lahko nacionalna sodišča pri uporabi načel, določenih v sodni praksi Sodišča, za položaje, ki se razlikujejo od položajev v zadevah, v katerih sta bili izdani zadevni sodbi. [38]

87. Iz tega torej izhaja, da je potrebna določena prožnost, kadar so Sodišču v obravnavo predloženi ukrepi, ki jih ni bilo mogoče predvideti pri predhodnih sodbah, kot so ureditve, ki se nanašajo na kršitve, zoper katere je mogoče uvesti kazenski postopek samo, če se podatki o civilni identiteti, ki ustrezajo IP-naslovom, hranijo in so dostopni, o katerih Sodišče doslej še ni odločalo.

88. Ne gre torej za spremembo sodne prakse Sodišča, kot je trdila danska vlada, temveč za priznanje, na podlagi načel, na katerih temelji, da je v zelo omejenih okoliščinah mogoče sprejeti bolj prilagodljivo rešitev.

35 Točka 69 in naslednje mojih prvih sklepnih predlogov.

36 C-597/19, EU:C:2020:1063.

37 Sodbe z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net in drugi; Prokuratuur; Commissioner of An Garda Síochána in drugi ter SpaceNet in Telekom Deutschland.

38 V zvezi s tem lahko povečanje števila predlogov za sprejetje predhodne odločbe, ki se nanašajo na razlago člena 15(1) Direktive 2002/58, kaže tudi na določeno zadržanost nacionalnih sodišč pri uporabi načel, ki jih je določilo Sodišče, za nekoliko drugačne položaje zaradi posebnosti nacionalnih pravnih redov. V zvezi s tem glej med drugim Cameron, I., „Metadata retention and national security: *Privacy international* and *La Quadrature du Net*“, *Common Market Law Review*, 2021, zvezek 58, št. 5, str. od 1433 do 1471, ali Bertrand, B., „L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?“, *Dalloz IP/IT*, 2021, št. 9, str. od 468 do 472. Zato se mi zdi še toliko bolj bistveno, da je Sodišče lahko prilagodljivo, kadar okoliščine to zahtevajo, da se ohrani ploden dialog med Sodiščem in sodišči držav članic. Kot so navedli avtorji pravne teorije, visoka raven varstva, ki je določena s sodno prakso Sodišča, ne more biti resnično učinkovita brez sodelovanja nacionalnih sodišč, ki so v prvi vrsti pristojna za njeno izvajanje. V zvezi s tem glej med drugim Teyssedre, J., „Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*“, *Common Market Law Review*, zvezek 60, št. 2, 2023, str. od 569 do 588, in Sirinelli, J., „La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite“, *Revue trimestrielle de droit européen*, zvezek 57, št. 2, 2021, str. od 313 do 329.

89. Razlaga člena 15(1) Direktive 2002/58, ki jo predlagam, namreč omogoča hrambo in dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, samo v zvezi z uvedbo postopkov zoper kršitve, katerih storilcev brez teh podatkov ne bi bilo mogoče identificirati. Nanaša se torej samo na kršitve, storjene izključno na spletu, in ne postavlja pod vprašaj rešitev iz sodne prakse v zvezi s hrambo in dostopom do večjega nabora podatkov, s katerimi se uresničujejo drugi cilji.

V. Predlog

90. Ob upoštevanju vseh navedenih ugotovitev Sodišču predlagam, naj na vprašanja za predhodno odločanje, ki jih je predložil Conseil d'État (državni svet, Francija), odgovori:

Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, v povezavi s členi 7, 8, 11 in 52(1) Listine Evropske unije o temeljnih pravicah

je treba razlagati tako, da

ne nasprotuje nacionalni ureditvi, ki ponudnikom storitev elektronskih komunikacij omogoča hrambo, upravnemu organu, pristojnemu za varstvo avtorske in sorodnih pravic pred kršitvami teh pravic, storjenimi na spletu, pa dostop samo do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, zato da lahko ta organ identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za te kršitve, in lahko po potrebi v zvezi z njimi sprejme ukrepe brez predhodnega nadzora sodišča ali neodvisnega upravnega organa nad tem dostopom, če so ti podatki edino preiskovalno sredstvo, s katerim je mogoče identificirati osebe, ki so jim bili navedeni naslovi v času storitve kršitve dodeljeni.