Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
MACIEJA SZPUNARA
od 27. listopada 2022.[1]

Predmet C-470/21

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

(zahtjev za prethodnu odluku koji je uputio Conseil d'État (Državno vijeće, Francuska))

„Zahtjev za prethodnu odluku – Obrada osobnih podataka i zaštita privatnosti u području elektroničkih komunikacija – Direktiva 2002/58/EZ – Članak 15. stavak 1. – Mogućnost država članica da ograniče opseg određenih prava i obveza – Obveza prethodnog nadzora suda ili neovisnog upravnog tijela čije su odluke obvezujuće – Podaci o građanskom identitetu koji odgovaraju određenoj IP adresi"

I. Uvod

1. Pitanje zadržavanja određenih podataka i pristupa određenim podacima internetskih korisnika neprestano je aktualno i predmet je novije, ali već opsežne sudske prakse Suda.

2. Ovaj predmet Sudu pruža priliku da ponovno razmotri to pitanje u novom kontekstu borbe protiv povreda prava intelektualnog vlasništva počinjenih isključivo na internetu.

[1] Izvorni jezik: francuski

II. Pravni okvir

A. Pravo Unije

3. U uvodnim izjavama 2., 6., 7., 11., 22., 26. i 30. Direktive 2002/58/EZ[2] navodi se:

„(2) Ova Direktiva traži poštovanje temeljnih prava te poštuje načela priznata posebno Poveljom o temeljnim pravima Europske unije [u daljnjem tekstu: Povelja]. Ova Direktiva posebno traži osiguranje punoga poštovanja prava određenih u člancima 7. i 8. navedene Povelje.

[…]

(6) Internet mijenja tradicionalne tržišne strukture pružajući zajedničku globalnu infrastrukturu za dostavu širokog raspona elektroničkih komunikacijskih usluga. Javno dostupne elektroničke komunikacijske usluge preko interneta otvaraju korisnicima nove mogućnosti, ali također i nove opasnosti za njihove osobne podatke i privatnost.

(7) U slučaju javnih komunikacijskih mreža treba donijeti posebne zakone i druge propise s ciljem zaštite temeljnih prava i sloboda fizičkih osoba i legitimnih interesa pravnih osoba, posebno u vezi sa sve većom sposobnošću automatskog pohranjivanja i obrade podataka koji se odnose na pretplatnike i korisnike.

[…]

(11) Poput Direktive 95/46/EZ[3], ova Direktiva ne obuhvaća pitanja zaštite temeljnih prava i sloboda koje se odnose na aktivnosti koje nisu uređene pravom Zajednice. Stoga se njome ne mijenja postojeća ravnoteža između prava na privatnost pojedinca i mogućnosti država članica da poduzmu mjere iz članka 15. stavka 1. ove Direktive, koje su nužne za zaštitu javne sigurnosti, obrane, državne sigurnosti (uključujući gospodarsko blagostanje države kada se aktivnosti odnose na sigurnosna pitanja države) te za provođenje odredaba kaznenog prava. Kao posljedica toga, ova Direktiva ne utječe na sposobnost država članica da provode zakonito presretanje elektroničkih komunikacija, odnosno da poduzimaju druge mjere ako je to nužno u neku od gore navedenih svrha te u skladu s Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda [potpisanom u Rimu 4. studenoga 1950.], na način kako je tumači Europski sud za ljudska prava. Takve mjere moraju biti prikladne, strogo razmjerne svrsi za koju se poduzimaju i neophodne unutar demokratskog društva te trebaju biti podložne prikladnim zaštitnim mehanizmima u skladu s Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda.

[…]

(22) Zabrana pohranjivanja komunikacija i s njima povezanih podataka o prometu osobama koje nisu korisnici ili bez pristanka korisnika, nema namjeru zabraniti automatsko, posredničko i privremeno pohranjivanje ovih informacija u onoj mjeri u kojoj se ono odvija isključivo u svrhu provedbe prijenosa u elektroničkoj komunikacijskoj mreži te pod uvjetom da te

[2] Direktiva Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.)

[3] Direktiva Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.)

informacije nisu pohranjene na razdoblje koje je duže od razdoblja potrebnog za svrhe prijenosa i upravljanja prometom, kao i pod uvjetom da tijekom razdoblja pohrane povjerljivost ostane zajamčena. […]

[…]

(26) Podaci o pretplatnicima obrađeni unutar elektroničkih komunikacijskih mreža u svrhu uspostavljanja veze i prijenosa informacija sadrže informacije o privatnom životu fizičkih osoba te se tiču prava na poštovanje njihove korespondencije, odnosno legitimnih interesa pravnih osoba. Takvi se podaci mogu pohraniti isključivo u onoj mjeri koja je nužna za pružanje usluge u svrhu zaračunavanja i naplate međusobnog povezivanja te na ograničeno vrijeme. Bilo kakva daljnja obrada takvih podataka […] može se dopustiti samo ako se pretplatnik složio s time na temelju točne i potpune informacije koju je dobio od davatelja javno dostupnih elektroničkih komunikacijskih usluga o vrstama daljnje obrade koju davatelj usluga namjerava provesti te o pravu pretplatnika da ne pruži, odnosno opozove svoj pristanak na takvu obradu. […]

[…]

(30) Sustave pružanja elektroničkih komunikacijskih mreža i usluga treba koncipirati tako da ograniče količinu nužnih osobnih podataka na strogi minimum. […]”

4. U skladu s člankom 2. te direktive, naslovljenim „Definicije”:

„[…]

Sljedeće definicije se također primjenjuju:

(a) ‚korisnik’ znači svaka fizička osoba koja koristi javno dostupnu elektroničku komunikacijsku uslugu, u privatne ili poslovne svrhe, pri čemu nije nužno da se pretplatila na tu uslugu;

(b) ‚podaci o prometu’ znači svi podaci koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje;

(c) ‚podaci o lokaciji’ znači svi podaci koji se obrađuju u sklopu elektroničke komunikacijske mreže ili u sklopu usluga elektroničkih komunikacija, koji ukazuju na zemljopisnu lokaciju terminalne opreme korisnika javno dostupnih usluga elektroničkih komunikacija;

(d) ‚komunikacija’ znači svaka informacija koja se razmjenjuje ili prenosi između ograničenog broja stranaka putem javno dostupne elektroničke komunikacijske usluge. Ovo ne uključuje informaciju prenesenu kao dio usluge emitiranja za javnost putem elektroničke komunikacijske mreže, osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju koji se mogu identificirati;

[…]”

5. Člankom 3. navedene direktive, naslovljenim „Usluge”, određuje se:

„Ova se Direktiva primjenjuje na obradu osobnih podataka vezanih uz pružanje javno dostupnih usluga elektroničkih komunikacija na javno dostupnim komunikacijskim mrežama u Zajednici,

uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i naprava za identifikaciju.”

6. Člankom 5. te direktive, naslovljenim „Povjerljivost komunikacija”, predviđa se:

„1. Države članice putem svojih zakonodavstava osiguravaju povjerljivost komunikacija i s time povezanih podataka o prometu koji se šalju preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga. One posebno zabranjuju svim osobama koje nisu korisnici slušanje, prisluškivanje, pohranjivanje ili druge oblike presretanja odnosno nadzora nad komunikacijama i s time povezanim podacima o prometu, bez pristanka korisnika, osim u slučaju kada imaju zakonsko dopuštenje da to učine u skladu s člankom 15. stavkom 1. Ovaj stavak ne sprečava tehničko pohranjivanje koje je nužno za prijenos komunikacije, ne dovodeći u pitanje načelo povjerljivosti.

[…]

3. Države članice osiguravaju da je pohranjivanje podataka ili uspostavljanje pristupa već pohranjenim podacima na terminalnoj opremi pretplatnika ili korisnika, dozvoljeno samo pod uvjetom da je dotični pretplatnik ili korisnik dao svoj pristanak, nakon što je iscrpno i razumljivo, u skladu s Direktivom [95/46], između ostalog obaviješten o namjeni postupka obrade. Navedeno ne sprečava nikakav oblik tehničke pohrane ili pristupa samo u svrhu izvršavanja prijenosa komunikacije putem elektroničke komunikacijske mreže ili ako je to strogo potrebno, kako bi operator usluge informacijskog društva mogao pružiti uslugu koju je izričito zatražio pretplatnik ili korisnik.”

7. U skladu s člankom 6. Direktive 2002/58, naslovljenim „Podaci o prometu”:

„1. Podaci o prometu koji se odnose na pretplatnike i korisnike i koje je davatelj javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge obradio i pohranio moraju se obrisati ili učiniti anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije, ne dovodeći u pitanje stavke 2., 3. i 5. ovog članka te članak 15. stavak 1.

2. Podaci o prometu koji su nužni u svrhu naplaćivanja usluge od pretplatnika te u svrhu plaćanja međusobnog povezivanja mogu se obraditi. Takva je obrada dopustiva isključivo do kraja razdoblja tijekom kojega se račun može pravno pobijati ili tijekom kojega se može zahtijevati plaćanje.

[…]”

8. U članku 15. stavku 1. Direktive 2002/58, naslovljenom „Primjena određenih odredaba Direktive [95/46]”, navodi se:

Države članice mogu donijeti zakonske mjere kojima će ograničiti opseg prava i obveza koji pružaju članak 5., članak 6., članak 8. stavci 1., 2., 3. i 4., te članak 9. ove Direktive kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti (odnosno državne sigurnosti), obrane, javne sigurnosti te s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava iz članka 13. stavka 1. Direktive [95/46]. S tim u vezi, države članice mogu, između ostalog, donijeti zakonske mjere kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja opravdane razlozima određenim u ovom stavku. Sve

mjere iz ovog stavka moraju biti u skladu s općim načelima prava [Unije], uključujući ona iz članka 6. stavaka 1. i 2. [UEU-a].”

B. Francusko pravo

1. Code de la propriété intellectuelle (Zakonik o intelektualnom vlasništvu)

9. Člankom L. 331-12 Zakonika o intelektualnom vlasništvu, u verziji koja se primjenjuje na glavni postupak (u daljnjem tekstu: CPI), određuje se:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [(Visoko tijelo za emitiranje djela i zaštitu prava na internetu, Francuska, u daljnjem tekstu: Hadopi)] neovisno je javno tijelo.”

10. Člankom L. 331-13 CPI-ja predviđa se:

„[Hadopi] osigurava:

[…]

2° zaštitu [djela i predmeta kojima je pridruženo autorsko ili srodno pravo na elektroničkim komunikacijskim mrežama] od povreda tih prava na elektroničkim komunikacijskim mrežama koje se koriste za pružanje javnih internetskih komunikacijskih usluga; […]”

11. U skladu s člankom L. 331-15 tog zakonika:

„[Hadopi] je sastavljen od kolegija i odbora za zaštitu prava. […].

[…]

Pri izvršavanju svojih ovlasti članovi kolegija i odbora za zaštitu prava ne primaju upute ni od jednog tijela.”

12. Člankom L. 331-17 navedenog zakonika određuje se:

„Odbor za zaštitu prava zadužen je za poduzimanje mjera predviđenih u članku L. 331-25.”

13. U skladu s člankom L. 331-21 tog zakonika:

„Kako bi odbor za zaštitu prava mogao izvršavati svoje ovlasti, [Hadopi] ima na raspolaganju javne službenike koji su položili prisegu i koje je [njegov] predsjednik ovlastio u uvjetima utvrđenima uredbom donesenom uz prethodno pribavljeno mišljenje Državnog vijeća. […]

Članovi odbora za zaštitu prava i službenici iz prvog stavka zaprimaju zahtjeve upućene navedenom odboru u uvjetima predviđenima člankom L. 331-24. Oni provode ispitivanje činjenica.

Za potrebe postupka mogu zatražiti uvid u sve dokumente, bez obzira na medij na kojem su pohranjeni, uključujući i podatke koje su operateri elektroničkih komunikacija zadržali i obradili na temelju članka L. 34-1 Zakonika o poštanskim uslugama i elektroničkim komunikacijama i koje su zadržali i obradili pružatelji usluga navedeni u članku 6. stavku I. točkama 1. i 2. loia nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(Zakon br. 2004-575 od 21. lipnja 2004. za promicanje povjerenja u digitalnu ekonomiju)].

Također mogu dobiti preslike dokumenata navedenih u prethodnom stavku.

Među ostalim, od operatera elektroničkih komunikacija mogu zatražiti podatke o identitetu, poštanskoj adresi, adresi elektroničke pošte i telefonskom broju pretplatnika čiji je pristup javnim internetskim komunikacijskim uslugama upotrijebljen za reproduciranje, prikazivanje, stavljanje na raspolaganje ili priopćavanje javnosti zaštićenih djela ili predmeta bez odobrenja nositelja prava […] kad je ono potrebno."

14. Člankom L. 331-24 CPI-ja određuje se:

„Odbor za zaštitu prava postupa po zahtjevu ovlaštenih službenika koji su položili prisegu i […] koje imenuju:

– propisno osnovana strukovna tijela za zaštitu prava;

– tijela za kolektivno ostvarivanje prava;

– Nacionalni centar za filmsku i animiranu industriju.

Odbor za zaštitu prava može postupati i na temelju informacija koje mu dostavi državno odvjetništvo.

Ne može mu se podnijeti zahtjev koji se odnosi na djela počinjena prije više od šest mjeseci."

15. U skladu s člankom L. 331-25 tog zakonika, odredbom kojom se uređuje takozvani postupak „postupnog odgovora":

„Kada odlučuje o zahtjevu koji se odnosi na djela koja mogu činiti povredu obveze utvrđene u članku L. 336-3 [CPI-ja], odbor za zaštitu prava može poslati pretplatniku […] preporuku u kojoj ga podsjeća na odredbe članka L. 336-3 te mu nalaže da poštuje obvezu koja je njima utvrđena i upozorava ga na sankcije koje se mogu primijeniti u skladu s člancima L. 335-7 i L. 335-7-1. Ta preporuka sadržava i informaciju za pretplatnika o zakonitoj ponudi kulturnih sadržaja na internetu, postojanju mjera za zaštitu sigurnosti kojima se može spriječiti povreda obveze utvrđene u članku L. 336-3 te o opasnostima praksi kojima se povređuje autorsko pravo i srodna prava za ponavljanje umjetničkog ostvarenja i ekonomiju kulturnog sektora.

U slučaju ponavljanja djela koja mogu činiti povredu obveze utvrđene u članku L. 336-3 u roku od šest mjeseci od slanja preporuke iz prvog stavka, odbor može uputiti novu preporuku koja sadržava iste informacije kao i prethodna elektroničkim sredstvima […]. Toj preporuci treba priložiti dopis koji se dostavlja uz potpis ili bilo koje drugo sredstvo kojim se može dokazati datum uručenja te preporuke.

U preporukama koje se upućuju na temelju ovog članka navode se datum i vrijeme utvrđenja djela koja mogu činiti povredu obveze utvrđene u članku L.336-3. Suprotno tomu, u njima se ne otkriva sadržaj zaštićenih djela ili predmeta na koje se odnosi ta povreda. U njima se navode telefonski broj, poštanska adresa i adresa elektroničke pošte na koje njihov adresat, ako to želi, može uputiti primjedbe odboru za zaštitu prava te, ako podnese izričit zahtjev za to, dobiti pojašnjenja o sadržaju zaštićenih djela ili predmeta na koje se odnosi povreda koja mu se stavlja na teret."

16. Člankom L. 331-29 navedenog zakonika određuje se:

„[Hadopi] dopušta uspostavu sustava automatske obrade osobnih podataka u pogledu osoba na koje se odnosi postupak u okviru ovog pododjeljka.

Njegova je svrha omogućiti odboru za zaštitu prava provedbu mjera predviđenih ovim pododjeljkom, svih povezanih postupovnih radnji te pravila o obavješćivanju strukovnih tijela za zaštitu prava i tijela za kolektivno ostvarivanje prava o eventualnim postupcima pokrenutima pred sudskim tijelima, kao i o dostavi predviđenoj u članku L. 335-7 petom stavku.

Uredbom […] utvrđuju se pravila primjene ovog članka. U njoj se prije svega navode:

– kategorije zabilježenih podataka i trajanje njihova zadržavanja;

– adresati ovlašteni za primanje tih podataka, osobito osobe čija je djelatnost nuđenje pristupa javnim internetskim komunikacijskim uslugama;

– uvjeti u kojima zainteresirane osobe mogu pri [Hadopiju] ostvarivati svoje pravo na pristup podacima koji se na njih odnose […]."

17. Člankom R. 331-37 tog zakonika predviđa se:

„Operateri elektroničkih komunikacija […] i pružatelji usluga […] dužni su, povezivanjem u sustavu automatske obrade osobnih podataka navedenom u članku L. 331-29 ili upotrebom medija za snimanje kojima se osiguravaju njihov integritet i sigurnost, priopćiti osobne podatke i informacije navedene u točki 2. Priloga [décretu 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' (Uredba br. 2010-236 od 5. ožujka 2010. o sustavu automatske obrade osobnih podataka, koja je odobrena člankom L. 331-29 [CPI-ja], pod nazivom ‚Sustav upravljanja mjerama za zaštitu djela na internetu')[4]] […] u roku od osam dana nakon što odbor za zaštitu prava proslijedi tehničke podatke potrebne za identifikaciju pretplatnika čiji je pristup javnim internetskim komunikacijskim uslugama upotrijebljen za reproduciranje, prikazivanje, stavljanje na raspolaganje ili priopćavanje javnosti zaštićenih djela ili predmeta bez odobrenja nositelja prava […] kad je ono potrebno.

[…]"

[4] JORF od 7. ožujka 2010., tekst br. 19

18. Člankom R. 335-5 CPI-ja određuje se:

„I.- Smatra se krajnjom nepažnjom, koja se kažnjava novčanom kaznom predviđenom za laka kažnjiva djela 5. stupnja činjenica da, ako su ispunjeni uvjeti predviđeni u stavku II., nositelj pristupa javnim internetskim komunikacijskim uslugama bez opravdanog razloga

1° nije uveo mjeru za zaštitu sigurnosti tog pristupa; ili

2° nije primijenio dužnu pažnju u provedbi te mjere.

II.- Odredbe iz stavka I. primjenjuju se samo ako su ispunjena sljedeća dva uvjeta:

1° U skladu s člankom L. 331-25 te na načine predviđene tim člankom, odbor za zaštitu prava preporučio je nositelju pristupa da poduzme mjeru za zaštitu sigurnosti njegova pristupa kojom bi se spriječilo da se taj pristup ponovno upotrijebi za reproduciranje, prikazivanje, stavljanje na raspolaganje ili priopćavanje javnosti djela ili predmeta zaštićenih autorskim ili srodnim pravom bez odobrenja nositelja tih prava […] kad je ono potrebno;

2° U godini nakon uručenja te preporuke taj je pristup ponovno upotrijebljen u svrhe navedene u ovom stavku II. točki 1.”

19. U članku L. 336-3 tog zakonika navodi se:

„Nositelj pristupa javnim internetskim komunikacijskim uslugama obvezan je osigurati da se taj pristup ne upotrebljava za reproduciranje, prikazivanje, stavljanje na raspolaganje ili priopćavanje javnosti djela ili predmeta zaštićenih autorskim ili srodnim pravom bez odobrenja nositelja […] kad je ono potrebno.

Ako nositelj pristupa ne ispuni obvezu utvrđenu u prvom stavku, to ne dovodi do pokretanja postupka utvrđivanja kaznene odgovornosti zainteresirane osobe […].”

2. Uredba od 5. ožujka 2010.

20. U članku 1. Uredbe od 5. ožujka 2010., u verziji primjenjivoj na činjenice u glavnom postupku, predviđa se:

„Sustav obrade osobnih podataka pod nazivom ‚Sustav upravljanja mjerama za zaštitu djela na internetu’ namijenjen je tomu da [Hadopijev] odbor za zaštitu prava:

1° poduzima mjere predviđene knjigom III. zakonodavnog dijela [CPI-ja] (glava III., poglavlje I., odjeljak 3., pododjeljak 3.) i knjigom III. regulatornog dijela tog zakonika (glava III., poglavlje I., odjeljak 2., pododjeljak 2.);

2° podnosi zahtjeve državnom odvjetništvu zbog djela koja mogu činiti kažnjiva djela predviđena člancima L. 335-2, L. 335-3, L. 335-4 i R. 335-5 tog zakonika te obavješćuje strukovna tijela za zaštitu prava i tijela za kolektivno ostvarivanje prava o tim zahtjevima;

[…]”

21. Člankom 4. te uredbe određuje se:

„I.- Javni službenici koji su položili prisegu i koje je ovlastio [Hadopijev] predsjednik u skladu s člankom L. 331-21 [CPI-ja] i članovi odbora za zaštitu prava navedenog u članku 1. imaju izravan pristup osobnim podacima i informacijama navedenim u prilogu ovoj Uredbi.

II.- Operateri elektroničkih komunikacija i pružatelji usluga navedeni u točki 2. priloga ovoj Uredbi primaju:

– tehničke podatke potrebne za identifikaciju pretplatnika;

– preporuke predviđene u članku L. 331-25 [CPI-ja] kako bi ih elektroničkim sredstvima poslali svojim pretplatnicima;

– elemente potrebne za provođenje dodatnih kazni ukidanja pristupa javnoj internetskoj elektroničkoj usluzi o kojima državno odvjetništvo obavješćuje odbor za zaštitu prava.

III.- Strukovna tijela za zaštitu prava i tijela za kolektivno ostvarivanje prava primaju obavijest o podnošenju zahtjeva državnom odvjetništvu.

IV.- Sudska tijela primaju zapisnike o utvrđenju djela koja mogu činiti kažnjiva djela predviđena člancima L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 i R. 335-5 [CPI-ja].

O izvršenju kazne ukidanja šalje se obavijest u automatsku kaznenu evidenciju.”

22. U prilogu Uredbi od 5. ožujka 2010. predviđa se:

„Sljedeći osobni podaci i informacije bilježe se u sustavu obrade pod nazivom ‚Sustav upravljanja mjerama za zaštitu djela na internetu’:

1° Osobni podaci i informacije iz propisno osnovanih strukovnih tijela za zaštitu prava, tijela za kolektivno ostvarivanje prava, Nacionalnog centra za filmsku i animiranu industriju te oni iz državnog odvjetništva:

u pogledu djela koja mogu činiti povredu obveze utvrđene u članku L.336-3 [CPI-ja]:

datum i vrijeme počinjenja djela;

IP adresa dotičnih pretplatnika;

korišteni P2P protokol;

pseudonim kojim se koristi pretplatnik;

informacije o zaštićenim djelima ili predmetima na koje se odnose počinjena djela;

naziv datoteke kako se nalazi na pretplatnikovu računalu (ovisno o slučaju);

pružatelj internetskog pristupa koji pruža pretplatu za pristup ili koji je osigurao IP tehnički resurs. […]

2° Osobni podaci i informacije o pretplatniku koje prikupljaju operateri elektroničkih komunikacija […] i pružatelji usluga […]:

prezime, imena;

poštanska adresa i adrese elektroničke pošte;

telefonski broj;

adresa pretplatnikova telefonskog priključka;

pružatelj internetskog pristupa koji se koristi tehničkim resursima pružatelja pristupa navedenog u točki 1., s kojim je pretplatnik sklopio ugovor; broj spisa;

datum na koji je privremeno ukinut pristup javnoj internetskoj komunikacijskoj usluzi.

[…]"

3. Code des postes et des télécommunications (Zakonik o poštanskim uslugama i telekomunikacijama)

23. Člankom L. 34-1 codea des postes et des communications électroniques (Zakonik o poštanskim uslugama i elektroničkim komunikacijama), kako je izmijenjen člankom 17. loia n° 2021-998 du 30 juillet 2021 (Zakon br. 2021-998 od 30. srpnja 2021.[5], u daljnjem tekstu: CPCE), u njegovu stavku II.a, određuje se da su „operateri elektroničkih komunikacija dužni zadržavati:

1° za potrebe kaznenih postupaka, sprečavanja prijetnji javnoj sigurnosti i zaštite nacionalne sigurnosti, podatke o građanskom identitetu korisnika do isteka roka od pet godina od prestanka valjanosti njegova ugovora;

2° u iste svrhe kao što su one navedene u točki 1. ovog stavka II.a, druge podatke koje je korisnik dao prilikom sklapanja ugovora ili stvaranja računa i podatke o plaćanju do isteka roka od godinu dana od isteka valjanosti njegova ugovora ili zatvaranja njegova računa;

3° za potrebe borbe protiv kriminala i teških kaznenih djela, sprečavanja ozbiljnih prijetnji javnoj sigurnosti i zaštite nacionalne sigurnosti, tehničke podatke koji omogućuju identifikaciju izvora veze ili one koji se odnose na korištenu terminalnu opremu do isteka roka od godinu dana od spajanja ili korištenja terminalnom opremom."

[5] JORF od 31. srpnja 2021., tekst br. 1. Ta verzija članka L. 34-1 CPCE-a, koja je na snazi od 31. srpnja 2021., donesena je nakon odluke Conseila d'État (Državno vijeće) od 21. travnja 2021., br. 393099 (JORF od 25. travnja 2021.), kojom je odbačena prethodna verzija te odredbe koja je uključivala obvezu zadržavanja osobnih podataka „u svrhu istraživanja, utvrđivanja i progona kaznenih djela ili povrede obveze utvrđene u članku L. 336-3 [CPI-ja]" samo kako bi se omogućilo, po potrebi, stavljanje na raspolaganje, među ostalim, Hadopiju. Odlukom br. 2021-976-977 QPC od 25. veljače 2022. (Habib A. i dr.), Conseil constitutionnel (Ustavno vijeće, Francuska) proglasio je tu prethodnu verziju članka L. 34-1 CPCE-a protuustavnom prije svega jer se, „time što dopuštaju opće i neselektivno zadržavanje podataka o vezi, osporavanim odredbama nerazmjerno povređuje pravo na poštovanje privatnosti" (t. 13.). Naime, taj je sud smatrao da se podaci o vezi koje treba zadržavati na temelju tih odredbi ne odnose samo na identifikaciju korisnika elektroničkih komunikacijskih usluga, nego i na druge podatke koji, „s obzirom na svoju raznolikost i obrade koje se nad njima mogu izvršavati, pružaju brojne i precizne informacije o tim korisnicima te, ovisno o slučaju, trećim osobama koje osobito mogu ugroziti njihovu privatnost" (t. 11.).

III. Glavni postupak, prethodna pitanja i postupak pred Sudom

24. Tužbom od 12. kolovoza 2019. i dvama dodatnim podnescima od 12. studenoga 2019. i 6. svibnja 2021. La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net i French Data Network podnijeli su Conseilu d'État (Državno vijeće, Francuska) zahtjev za poništenje prešutne odluke kojom je Premier ministre (predsjednik vlade, Francuska) odbio njihov zahtjev za stavljanje izvan snage Uredbe od 5. ožujka 2010. jer ne samo da se tom uredbom i odredbama koje čine njezinu pravnu osnovu prekomjerno povređuju prava zajamčena francuskim Ustavom, nego su one usto protivne članku 15. Direktive 2002/58 te člancima 7., 8., 11. i 52. Povelje.

25. Konkretno, tužitelji iz glavnog postupka tvrde da se Uredbom od 5. ožujka 2010. i odredbama koje čine njezinu pravnu osnovu odobrava pristup podacima o vezi koji je neproporcionalan u odnosu na povrede autorskog prava počinjene na internetu i kažnjiva djela koja nisu teška, a da pritom ne postoji prethodni nadzor suda ili tijela koje pruža jamstva neovisnosti i nepristranosti.

26. U tom pogledu, sud koji je uputio zahtjev najprije naglašava da je Sud u svojoj posljednjoj presudi La Quadrature du Net i dr.[6] presudio da se članku 15. stavku 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje, ne protive zakonske mjere kojima se predviđa, u svrhu zaštite nacionalne sigurnosti, borbe protiv kriminala i zaštite javne sigurnosti, opće i neselektivno zadržavanje *podataka o građanskom identitetu* korisnika elektroničkih komunikacijskih sredstava. Stoga je takvo zadržavanje tih podataka moguće, bez određenog roka, u svrhu istrage, otkrivanja i progona kaznenih djela općenito.

27. Sud koji je uputio zahtjev iz toga zaključuje da se tužbeni razlog koji su istaknuli tužitelji iz glavnog postupka, koji se odnosi na nezakonitost Uredbe od 5. ožujka 2010. jer je donesena u okviru borbe protiv kažnjivih djela koja nisu teška, može samo odbiti.

28. Taj sud zatim podsjeća na to da je Sud u presudi Tele2 Sverige i Watson[7] presudio da članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje, treba tumačiti na način da mu se protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela.

29. Ističe da je Sud u presudi Tele2[8] pojasnio da je, u svrhu osiguranja punog poštovanja tih uvjeta u praksi, bitno da pristup nadležnih nacionalnih tijela zadržanim podacima u načelu, osim u valjano opravdanim hitnim slučajevima, bude podvrgnut zahtjevu prethodnog nadzora suda ili neovisnog upravnog tijela i da odluka tog suda ili tijela bude donesena nakon obrazloženog zahtjeva tih tijela podnesenog osobito u okviru postupaka sprečavanja, otkrivanja ili progona kaznenih djela.

6 Vidjeti presudu od 6. listopada 2020. (C-511/18, C-512/18 i C-520/18, u daljnjem tekstu: presuda La Quadrature du Net i dr., EU:C:2020:791, izreka).

7 Vidjeti presudu od 21. prosinca 2016. (C-203/15 i C-698/15, u daljnjem tekstu: presuda Tele2, EU:C:2016:970, izreka).

8 Točka 120. ove presude.

30. Sud koji je uputio zahtjev naglašava da je Sud podsjetio na taj zahtjev u presudi La Quadrature du Net i dr.[9] u pogledu prikupljanja podataka o vezi u stvarnom vremenu koje provode obavještajne službe, kao i u presudi Prokuratuur (Uvjeti pristupa podacima o elektroničkim komunikacijama)[10] u pogledu pristupa nacionalnih tijela podacima o vezi.

31. Taj sud naposljetku napominje da je Hadopi od svojeg osnivanja 2009. godine nositeljima pretplata uputio više od 12,7 milijuna preporuka na temelju postupka postupnog odgovora predviđenog u članku L. 331-25 CPI-ja, od čega 827 791 samo tijekom 2019. Radi toga službenici Hadopijeva odbora za zaštitu prava svake godine trebaju moći prikupiti znatan broj podataka o građanskom identitetu dotičnih korisnika. S obzirom na količinu tih preporuka, on smatra da bi se, kad bi se to prikupljanje podvrgnulo prethodnom nadzoru, time mogla onemogućiti provedba preporuka.

32. U tim je okolnostima Conseil d'État (Državno vijeće, Francuska) odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:

„1. Jesu li podaci o građanskom identitetu koji odgovaraju određenoj IP adresi dio podataka o prometu ili lokaciji koji u načelu podliježu obvezi prethodnog nadzora koju ima sud ili neovisno upravno tijelo kojima je dodijeljena obvezujuća ovlast?

2. Ako se na prvo pitanje odgovori potvrdno, te s obzirom na to da podaci o građanskom identitetu korisnika nisu posebno osjetljivi, uključujući njihove kontaktne podatke, treba li Direktivu [2002/58], u vezi s [Poveljom], tumačiti na način da joj se protivi nacionalni propis kojim se predviđa da upravno tijelo te podatke koji odgovaraju IP adresi korisnika prikuplja bez prethodnog nadzora suda ili neovisnog upravnog tijela kojima je dodijeljena obvezujuća ovlast?

3. Ako se na drugo pitanje odgovori potvrdno, te s obzirom na nisku razinu osjetljivosti podataka o građanskom identitetu, okolnost da se smiju prikupljati samo ti podaci, i to samo za potrebe sprečavanja povreda obveza koje su precizno, taksativno i usko utvrđene nacionalnim pravom, i okolnost da bi sustavan nadzor pristupa podacima svakog korisnika koji provodi sud ili treće upravno tijelo kojem je dodijeljena obvezujuća ovlast mogao ugroziti ispunjavanje zadaće javne usluge koja je povjerena upravnom tijelu koje je i samo neovisno i provodi to prikupljanje, sprečava li Direktiva [2002/58] to da se taj nadzor provodi u skladu s prilagođenim pravilima, kao što je automatski nadzor, po potrebi pod nadzorom unutarnje službe tog tijela koja pruža jamstva neovisnosti i nepristranosti u pogledu službenika zaduženih za to prikupljanje?"

33. Pisana očitovanja podnijeli su tužitelji iz glavnog postupka, francuska, estonska, švedska i norveška vlada te Europska komisija. Te stranke, osim estonske, danske i finske vlade, zastupane su na raspravi održanoj 5. srpnja 2022.

[9] Točka 189. ove presude.

[10] Presuda od 2. ožujka 2021., (C-746/18, u daljnjem tekstu: presuda Prokuratuur, EU:C:2021:152).

IV. Analiza

A. Prvo i drugo prethodno pitanje

34. Svojim prvim i drugim prethodnim pitanjem, koje prema mojem mišljenju valja ispitati zajedno, sud koji je uputio zahtjev u biti želi znati treba li članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje, tumačiti na način da mu se protivi nacionalni propis kojim se upravnom tijelu zaduženom za zaštitu autorskih i srodnih prava od povreda tih prava počinjenih na internetu dopušta pristup podacima o građanskom identitetu koji odgovaraju IP adresama kako bi to tijelo moglo identificirati nositelje tih adresa za koje se sumnjiči da su odgovorni za te povrede te da bi, po potrebi, moglo poduzeti mjere protiv njih a da taj pristup pritom ne podliježe prethodnom nadzoru suda ili neovisnog upravnog tijela.

1. Ograničenje prethodnih pitanja

a) Prethodno prikupljanje IP adresa koje provode organizacije nositeljâ prava

35. Iz odluke kojom se upućuje zahtjev za prethodnu odluku proizlazi da se mehanizam postupnog odgovora o kojem je riječ u glavnom postupku sastoji od dviju uzastopnih obrade podataka, od kojih prvu čini prethodno prikupljanje IP adresa koje provode organizacije nositeljâ prava na mrežama ravnopravnih članova (*peer-to-peer*) počiniteljâ povreda autorskog prava, a drugu postupak kojim Hadopi, nakon što mu se podnese određeni zahtjev, povezuje te IP adrese s građanskim identitetom osoba kako bi poslao preporuku osobama čiji je pristup javnim internetskim komunikacijskim uslugama korišten protivno pravilima o autorskom pravu.

36. Prvo i drugo prethodno pitanje odnose se samo na drugu obradu, koju izvršava Hadopi.

37. Međutim, tužitelji iz glavnog postupka tvrde da bi Sud trebao ispitati prvu obradu s obzirom na to da je, ako su te IP adrese dobivene na način da su povrijeđene odredbe Direktive 2002/58, njihova upotreba u okviru druge obrade nužno protivna tim odredbama.

38. Takvo rasuđivanje nije uvjerljivo. Člankom 3. stavkom 1. Direktive 2002/58 njezino se područje primjene ograničava na „obradu osobnih podataka u vezi s pružanjem […] elektroničkih komunikacijskih usluga”. Međutim, kao što je to na raspravi pojasnila francuska vlada, organizacije nositeljâ prava ne dobivaju predmetne IP adrese putem pružatelja elektroničkih komunikacijskih usluga, nego izravno na internetu pregledavanjem podataka dostupnih širokoj javnosti.

39. Stoga se samo može utvrditi da prethodno prikupljanje IP adresa koje provode organizacije nositeljâ prava nije obuhvaćeno odredbama Direktive 2002/58 te bi se stoga, kao što to ističe Komisija, moglo analizirati s obzirom na odredbe Uredbe (EU) 2016/679[11]. Zato mi se čini da takva analiza tako prekoračuje okvir prethodnih pitanja postavljenih Sudu, tim više što sud koji je uputio zahtjev ne iznosi pojašnjenja o prethodnom prikupljanju podataka na temelju kojih bi mu Sud mogao dati koristan odgovor.

[11] Uredba Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL 2016., L 119, str. 1. te ispravci SL 2018., L 127, str. 2. i SL 2021., L 74, str. 35.)

40. U tim okolnostima, u svojoj ću se analizi usredotočiti na pitanje Hadopijeva pristupa podacima o građanskom identitetu koji odgovaraju određenoj IP adresi.

b) Povezivanje IP adresa i podataka o građanskom identitetu

41. Prvo i drugo prethodno pitanje odnose se na „podatke o građanskom identitetu koji odgovaraju određenoj IP adresi”, koji prema mišljenju suda koji je uputio zahtjev nisu osobito osjetljivi. Taj sud u svojoj odluci upućuje isključivo na točke presude La Quadrature du Net i dr. koje se odnose na zadržavanje podataka o građanskom identitetu.

42. Točno je da sudska praksa Suda razlikuje sustav zadržavanja IP adresa i pristupa tim adresama od sustava zadržavanja podataka o građanskom identitetu korisnika elektroničkih komunikacijskih sredstava i pristupa tim podacima, pri čemu je taj drugi sustav manje strog od prvoga [12].

43. Međutim, čini mi se da u ovom slučaju, unatoč tekstu tih dvaju prethodnih pitanja, nije riječ samo o pitanju pristupa podacima o građanskom identitetu korisnika elektroničkih komunikacijskih sredstava, nego o povezivanju tih podataka s IP adresama kojima raspolaže Hadopi nakon što organizacije nositeljâ prava prikupe potonje adrese i dostave ih tom tijelu. Naime, kao što to ističe Komisija, pristup podacima o građanskom identitetu Hadopiju služi kako bi mogao pristupiti većem skupu podataka, osobito IP adresama i podacima preuzetim iz pretraženog sustava pohrane, i kako bi ih mogao iskoristiti, s obzirom na to da podaci o građanskom identitetu i IP adrese pojedinačno nisu relevantni nacionalnim tijelima jer ni građanski identitet ni IP adresa, ako nisu povezani, sami po sebi ne mogu pružiti informacije o aktivnostima fizičkih osoba na internetu.

44. Iz toga slijedi da prvo i drugo prethodno pitanje, prema mojem mišljenju, valja shvatiti na način da se ne odnose samo na podatke o građanskom identitetu korisnikâ elektroničkog komunikacijskog sredstva nego i na pristup IP adresama koji omogućuje da se utvrdi izvor veze.

c) Zadržavanje IP adresa kod pružatelja komunikacijskih usluga

45. Točno je, kao što to ističu francuska vlada i Komisija, da se prethodna pitanja upućena Sudu formalno ne odnose na zadržavanje podataka kod pružatelja elektroničkih komunikacijskih usluga, nego samo na Hadopijev pristup podacima o građanskom identitetu koji odgovaraju IP adresama.

46. Međutim, pitanje Hadopijeva pristupa tim podacima zapravo mi se čini neodvojivo od prethodno postavljenog pitanja o zadržavanju tih podataka kod pružateljâ komunikacijskih usluga. Kao što je to naglasio Sud, zadržavanje podataka izvršava se samo u svrhu da oni, po potrebi, budu dostupni nadležnim nacionalnim tijelima [13]. Drugim riječima, zadržavanje podataka i pristup podacima ne mogu se promatrati zasebno, iako drugonavedeno ovisi o prvonavedenom.

[12] Vidjeti presudu La Quadrature du Net i dr. (t. 155. i 159.).

[13] Vidjeti presudu Tele2 (t. 79.).

47. Točno je da je Sud već ispitao usklađenost nacionalnog propisa koji se odnosi samo na pristup nadležnih nacionalnih tijela određenim osobnim podacima s člankom 15. stavkom 1. Direktive 2002/58 neovisno o pitanju usklađenosti zadržavanja predmetnih podataka s tom odredbom [14]. Stoga bi se na prethodna pitanja u ovom predmetu moglo odgovoriti ne uzimajući u obzir pitanje jesu li se predmetni podaci zadržavali u skladu s odredbama prava Unije.

48. Međutim, najprije ističem da ispitivanje koje je Sud proveo u presudi Ministerio Fiscal [15] u pogledu usklađenosti pristupa nacionalnih tijela određenim osobnim podacima s pravom Unije strogo slijedi ista načela kao i ispitivanje koje Sud provodi u pogledu ocjenjivanja usklađenosti zadržavanja tih podataka s pravom Unije. Naime, Sud upućuje isključivo na sudsku praksu utvrđenu u potonjem pogledu kako bi je primijenio na pitanje pristupa osobnim podacima. Drugim riječima, budući da nije ispitana usklađenost zadržavanja određenih podataka s pravom Unije, to se ispitivanje prenosi na kasniju fazu koja se odnosi na pitanje pristupa tim podacima, tako da usklađenost tog pristupa *in fine* ovisi o usklađenosti njihova zadržavanja.

49. Nadalje, Sud je jasno naveo da se pristup osobnim podacima može odobriti samo ako su pružatelji elektroničkih komunikacijskih usluga te podatke zadržali na način koji je u skladu s člankom 15. stavkom 1. Direktive 2002/58 [16] i da je pristup fizičkih osoba osobnim podacima kako bi se omogućilo pokretanje postupka protiv povreda autorskog prava pred građanskim sudovima u skladu s pravom Unije samo pod uvjetom da se ti podaci zadržavaju na način koji je u skladu s tom odredbom [17].

50. Naposljetku, Sud dosljedno presuđuje da se pristup podacima o prometu i podacima o lokaciji koje su ti pružatelji zadržali primjenom mjere poduzete na temelju članka 15. stavka 1. Direktive 2002/58, koji se mora odvijati uz potpuno poštovanje uvjeta koji proizlaze iz sudske prakse kojom je protumačena Direktiva 2002/58, u načelu može opravdati samo ciljem od općeg interesa glede kojeg je to zadržavanje naloženo tim pružateljima [18]. Drugim riječima, usklađenost pristupa nacionalnih tijela određenim osobnim podacima s pravom Unije u potpunosti ovisi o usklađenosti zadržavanja tih podataka s pravom Unije.

51. Prema mojem mišljenju, iz toga proizlazi da analiza usklađenosti nacionalnog propisa kojim se predviđa pristup nacionalnog tijela određenim osobnim podacima s pravom Unije podrazumijeva da je prethodno utvrđena usklađenost zadržavanja tih podataka s pravom Unije.

52. U tim okolnostima, svoju ću analizu započeti podsjetnikom na sudsku praksu Suda o pitanju zadržavanja IP adresa dodijeljenih izvoru veze kako bih prikazao njezin doseg i predložio uređeni okvir za tumačenje predmetnog propisa.

[14] Vidjeti presudu od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788, t. 49.).

[15] Presuda od 2. listopada 2018. (C-207/16, EU:C:2018:788).

[16] Vidjeti presudu Prokuratuur (t. 29.).

[17] Vidjeti presudu od 17. lipnja 2021., M. I. C. M. (C-597/19, EU:C:2021:492, t. 127. do 130.).

[18] Vidjeti presudu La Quadrature du Net i dr., t. 166.; od 5. travnja 2022., Commissioner of An Garda Síochána i dr. (C-140/20, u daljnjem tekstu: presuda Commissioner of An Garda Síochána i dr., EU:C:2022:258, t. 98.) i od 20. rujna 2022., SpaceNet, (C-793/19 i C-794/19, u daljnjem tekstu: presuda SpaceNet, EU:C:2022:702, t. 131.).

2. Sudska praksa Suda koja se odnosi na tumačenje članka 15. stavka 1. Direktive 2002/58 u pogledu mjera za zadržavanje IP adresa dodijeljenih izvoru veze

53. Naime, u članku 5. stavku 1. Direktive 2002/58 utvrđeno je načelo povjerljivosti kako elektroničkih komunikacija tako i s time povezanih podataka o prometu te podrazumijeva, među ostalim, načelnu zabranu svim osobama koje nisu korisnici da bez pristanka potonjih pohranjuju te komunikacije i te podatke [19].

54. Što se tiče obrade i pohrane podataka o prometu koji se odnose na pretplatnike i korisnike koje provode pružatelji elektroničkih komunikacijskih usluga, Direktivom 2002/58 predviđa se, u njezinu članku 6. stavku 1., da se ti podaci moraju obrisati ili učiniti anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije te se, u njezinu članku 6. stavku 2., pojašnjava da se podaci o prometu koji su nužni u svrhu naplaćivanja usluge od pretplatnika te u svrhu plaćanja međusobnog povezivanja mogu obrađivati isključivo do kraja razdoblja tijekom kojega se račun može pravno pobijati ili tijekom kojega se može zahtijevati plaćanje. Kad je riječ o podacima o lokaciji koji nisu podaci o prometu, u članku 9. stavku 1. te direktive navodi se da se ti podaci mogu obraditi samo pod određenim uvjetima i nakon što su učinjeni anonimnima odnosno uz pristanak korisnika ili pretplatnika [20].

55. Stoga je zakonodavac Unije, donijevši Direktivu 2002/58, konkretizirao prava utvrđena u člancima 7. i 8. Povelje, tako da uslijed izostanka vlastitog pristanka korisnici elektroničkih komunikacijskih sredstava imaju u načelu pravo očekivati da njihove komunikacije i s time povezani podaci ostanu anonimni i da se ne mogu bilježiti [21]. Prema tome, tom se direktivom ne stvara samo okvir za pristup takvim podacima jamstvima kojima se nastoji spriječiti zlouporaba nego se njome osobito utvrđuje načelo zabrane njihove pohrane od strane trećih osoba.

56. U tim okolnostima, time što se člankom 15. stavkom 1. Direktive 2002/58 državama članicama dopušta da donesu zakonske mjere radi „ograničavanja opsega" prava i obveza predviđenih, među ostalim, u člancima 5., 6. i 9. te direktive, poput onih koji proizlaze iz načela povjerljivosti komunikacija i zabrane pohrane s time povezanih podataka, u toj odredbi navodi se iznimka od općeg pravila predviđenog osobito u njezinim člancima 5., 6. i 9. te se ona tako, u skladu s ustaljenom sudskom praksom, mora tumačiti usko. Stoga takva obveza ne može opravdati to da odstupanje od obveznosti tog načela da se zajamči povjerljivost elektroničkih komunikacija i s time povezanih podataka i osobito od zabrane pohrane tih podataka, predviđene u članku 5. navedene direktive, postane pravilo, kako potonja odredba ne bi izgubila na svojem dosegu [22].

57. Kad je riječ o ciljevima kojima se mogu opravdati ograničenja prava i obveza predviđenih, među ostalim, u člancima 5., 6. i 9. Direktive 2002/58, Sud je već presudio da su ciljevi u prvoj rečenici članka 15. stavka 1. te direktive navedeni taksativno, slijedom čega zakonska mjera donesena na temelju te odredbe treba strogo odgovarati jednom od tih ciljeva [23].

58. Usto, iz članka 15. stavka 1. treće rečenice Direktive 2002/58 proizlazi da se mjerama koje države članice donesu na temelju te odredbe moraju poštovati opća načela prava Unije, među kojima se nalazi načelo proporcionalnosti, i osigurati poštovanje temeljnih prava koja su zajamčena Poveljom. U tom je pogledu Sud već presudio da obveza koju je nacionalnim

[19] Vidjeti presude La Quadrature du Net i dr. (t. 107.); Commissioner of An Garda Síochána i dr. (t. 35.) i SpaceNet (t. 52.).

[20] Vidjeti presude Tele2 (t. 86.); La Quadrature du Net i dr. (t. 108.); Commissioner of An Garda Síochána i dr. (t. 38.) i SpaceNet (t. 55.).

[21] Vidjeti presude La Quadrature du Net i dr. (t. 109.); Commissioner of An Garda Síochána i dr. (t. 37.) i SpaceNet (t. 54.).

[22] Vidjeti presude La Quadrature du Net i dr. (t. 110. i 111.); Commissioner of An Garda Síochána i dr. (t. 40.) i SpaceNet (t. 57.).

[23] Vidjeti presude La Quadrature du Net i dr. (t. 112.); Commissioner of An Garda Síochána i dr. (t. 41.) i SpaceNet (t. 58.).

propisom država članica odredila pružateljima elektroničkih komunikacijskih usluga da zadržavaju podatke o prometu kako bi se, u slučaju potrebe, ti podaci učinili dostupnima nadležnim nacionalnim tijelima, postavlja pitanja ne samo u vezi s poštovanjem članaka 7. i 8. Povelje, koji se odnose na zaštitu privatnog života i zaštitu osobnih podataka, nego i u vezi s člankom 11. Povelje koji se odnosi na slobodu izražavanja, pri čemu je ta sloboda jedan od osnovnih temelja demokratskog i pluralističkog društva te je dio vrijednosti na kojima, u skladu s člankom 2. UEU-a, počiva Unija [24].

59. S obzirom na to, budući da se člankom 15. stavkom 1. Direktive 2002/58 državama članicama dopušta da ograniče prava i obveze predviđene člancima 5., 6. i 9. te direktive, ta odredba odražava okolnost da prava priznata člancima 7., 8. i 11. Povelje nisu apsolutna prava, nego da ih treba uzeti u obzir s obzirom na njihovu funkciju u društvu. Naime, kao što to proizlazi iz njezina članka 52. stavka 1., Povelja priznaje ograničenja pri ostvarivanju tih prava samo ako su ograničenja predviđena zakonom, ako poštuju bit tih prava te ako su, uz poštovanje načela proporcionalnosti, nužna i zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba. Stoga tumačenje članka 15. stavka 1. Direktive 2002/58 s obzirom na Povelju zahtijeva također da se vodi računa i o značaju ciljeva zaštite nacionalne sigurnosti i borbe protiv teških kaznenih djela, čime se doprinosi zaštiti prava i sloboda drugih osoba, te o značaju prava utvrđenih u člancima 3., 4., 6. i 7. Povelje [25], iz kojih mogu proizaći pozitivne obveze na teret tijela javne vlasti [26].

60. Stoga s obzirom na te različite pozitivne obveze treba pomiriti različite legitimne interese i prava o kojima je riječ. U tom kontekstu iz samog teksta članka 15. stavka 1. prve rečenice Direktive 2002/58 proizlazi da države članice mogu donijeti mjeru koja odstupa od načela povjerljivosti kada je takva mjera „nužn[a], prikladn[a] i razmjern[a] unutar demokratskog društva” s obzirom na to da se u uvodnoj izjavi 11. te direktive u tu svrhu navodi da takva mjera mora biti „strogo” razmjerna svrsi za koju se poduzima [27].

61. U tom pogledu, iz sudske prakse Suda proizlazi da mogućnost država članica da opravdaju ograničenje prava i obveza predviđenih, među ostalim, u člancima 5., 6. i 9. Direktive 2002/58 treba ocijeniti tako da se odmjeri ozbiljnost zadiranja takvog ograničenja i provjeri da je važnost cilja od općeg interesa koji se nastoji postići tim ograničenjem povezana s tom ozbiljnošću [28].

62. Usto, ističem da Sud u svojoj sudskoj praksi razlikuje, s jedne strane, zadiranja koja proizlaze iz pristupa podacima koji kao takvi pružaju precizne informacije o predmetnim komunikacijama i stoga o privatnom životu osobe i na koje se primjenjuje strog sustav zadržavanja te, s druge strane, zadiranja koja proizlaze iz pristupa podacima koji ne mogu pružiti takve informacije koje se kao takve povezuju s drugim podacima, kao što su IP adrese [29].

63. Što se konkretnije tiče IP adresa, Sud je tako istaknuo da se one stvaraju a da nisu povezane s određenom komunikacijom i uglavnom služe za to da se pomoću pružatelja elektroničkih komunikacijskih usluga identificira fizička osoba koja je vlasnik terminalne opreme s koje se

[24] Vidjeti presude La Quadrature du Net i dr. (t. 113. i 114.); Commissioner of An Garda Síochána i dr. (t. 42.) i SpaceNet (t. 60.).

[25] Vidjeti presude La Quadrature du Net i dr. (t. 120. i 122.); Commissioner of An Garda Síochána i dr. (t. 48.) i SpaceNet (t. 63.).

[26] Vidjeti presude La Quadrature du Net i dr. (t. 120. i 122.); Commissioner of An Garda Síochána i dr. (t. 49.) i SpaceNet (t. 64.).

[27] Vidjeti presude La Quadrature du Net i dr. (t. 127. do 129.); Commissioner of An Garda Síochána i dr. (t. 50. i 51.) i SpaceNet (t. 65. i 66.).

[28] Vidjeti presude La Quadrature du Net i dr. (t. 131.); Commissioner of An Garda Síochána i dr. (t. 53.) i SpaceNet (t. 68.).

[29] Vidjeti točku 41. i sljedeće ovog mišljenja.

obavlja komunikacija posredstvom interneta. Stoga, pod uvjetom da se zadržavaju samo IP adrese izvora komunikacije, a ne IP adrese njezina adresata, ta je kategorija podataka manje osjetljiva od drugih podataka o prometu [30].

64. Sud istodobno naglašava da, s obzirom na to da se IP adrese mogu upotrijebiti osobito za iscrpno praćenje tijeka kretanja korisnika interneta prilikom pregledavanja i, potom, njegove internetske aktivnosti, ti podaci omogućuju da se utvrdi detaljan profil potonjeg korisnika i da se donesu precizni zaključci o korisnikovu privatnom životu. Stoga su zadržavanje i analiza tih IP adresa *ozbiljna* zadiranja u temeljna prava utvrđena u člancima 7. i 8. Povelje te mogu imati odvraćajuće učinke na ostvarivanje slobode izražavanja zajamčene u njezinu članku 11. [31].

65. Međutim, prema ustaljenoj sudskoj praksi, radi potrebe za pomirenjem predmetnih legitimnih prava i interesa koje se zahtijeva tom sudskom praksom, valja uzeti u obzir činjenicu da, u slučaju kažnjivog djela počinjenog na internetu, IP adresa može biti jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja tog kažnjivog djela [32].

66. Stoga Sud smatra da se zakonska mjera koja predviđa opće i neselektivno zadržavanje samo IP adresa dodijeljenih izvoru veze u načelu ne protivi članku 15. stavku 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. kao i člankom 52. stavkom 1. Povelje, pri čemu ta mogućnost mora podlijegati strogom poštovanju materijalnih i postupovnih uvjeta kojima se mora urediti upotreba tih podataka, a s obzirom na ozbiljnost zadiranja koje podrazumijeva to zadržavanje, samo borba protiv *teških kaznenih djela* i sprečavanje ozbiljnih prijetnji javnoj sigurnosti mogu, kao i zaštita nacionalne sigurnosti, opravdati to zadiranje [33].

67. Usto, Sud pojašnjava da trajanje zadržavanja ne može prekoračiti ono što je strogo nužno s obzirom na cilj koji se želi postići te da se mjerom te naravi moraju predvidjeti strogi uvjeti i jamstva glede korištenja tih podataka [34]

3. Granice sudske prakse koja se odnosi na tumačenje članka 15. stavka 1. Direktive 2002/58 u pogledu mjera za zadržavanje IP adresa dodijeljenih izvoru veze

68. Čini mi se da rješenje do kojeg je Sud došao u pogledu nacionalnih mjera za zadržavanje IP adresa dodijeljenih izvoru veze, tumačenih s obzirom na članak 15. stavak 1. Direktive 2002/58, ipak ima dvije glavne poteškoće.

[30] Vidjeti presudu La Quadrature du Net i dr. (t. 152.).

[31] Vidjeti presude La Quadrature du Net i dr. (t. 153.); Commissioner of An Garda Síochána i dr. (t. 73.) i SpaceNet (t. 103.) (moje isticanje).

[32] Vidjeti presude La Quadrature du Net i dr. (t. 154.); Commissioner of An Garda Síochána i dr. (t. 73.) i SpaceNet (t. 103.).

[33] Vidjeti presude La Quadrature du Net i dr. (t. 155. i 156.); Commissioner of An Garda Síochána i dr. (t. 74.) i SpaceNet (t. 104. i 105.) (moje isticanje).

[34] Vidjeti presude La Quadrature du Net i dr. (t. 156.) i SpaceNet (t. 105.).

a) Usklađivanje sa sudskom praksom koja se odnosi na priopćavanje IP adresa dodijeljenih izvoru veze u okviru postupaka za zaštitu prava intelektualnog vlasništva

69. Kao prvo, kao što sam to već naveo u svojem mišljenju u predmetu M. I. C. M.[35], postoji određena nepodudarnost između tog smjera u sudskoj praksi i onog koji se odnosi na priopćavanje IP adresa u okviru postupaka za zaštitu prava intelektualnog vlasništva nositeljima tih prava, u kojoj se naglašava obveza država članica da osiguraju nositeljima prava intelektualnog vlasništva stvarne mogućnosti da dobiju naknadu štete koja je nastala zbog povreda tih prava[36].

70. Naime, što se tiče potonjeg smjera u sudskoj praksi, Sud dosljedno presuđuje da se pravu Unije ne protivi to da države članice propišu obvezu prijenosa osobnih podataka privatnim osobama kako bi se omogućilo pokretanje postupka protiv povreda autorskog prava pred građanskim sudovima[37].

71. Sud u tom pogledu ističe da mogućnost država članica da propišu obvezu otkrivanja osobnih podataka u okviru građanskih postupaka zapravo prije svega proizlazi iz mogućnosti predviđanja takvog otkrivanja u okviru progona kaznenih djela[38], koja je potom proširena na građanske postupke.

72. Istodobno, što se tiče IP adresa, Sud ipak nalaže da se ti podaci mogu zadržavati samo u okviru borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji javnoj sigurnosti[39].

73. Nastojanja da se ta dva smjera u sudskoj praksi usklade dovode, prema mojem mišljenju, do neprikladnih rezultata i nisu uvjerljiva.

74. S jedne strane, suprotno onomu što je na raspravi tvrdila francuska vlada, borba protiv povreda prava intelektualnog vlasništva ne može biti obuhvaćena borbom protiv teških kaznenih djela. Smatram da pojam „teška kaznena djela" treba tumačiti autonomno. On ne može ovisiti o shvaćanju svake države članice jer bi to omogućilo zaobilaženje zahtjeva iz članka 15. stavka 1. Direktive 2002/58 ovisno o tome shvaćaju li države članice borbu protiv teških kaznenih djela široko. Naime, kao što sam to već istaknuo, interesi povezani sa zaštitom prava intelektualnog vlasništva ne mogu se miješati s onima koji podrazumijevaju borbu protiv teških kaznenih djela[40].

75. S druge strane, dopuštanje prijenosa IP adresa nositeljima prava intelektualnog vlasništva u okviru postupaka za njihovu zaštitu, iako je zadržavanje tih adresa moguće samo u okviru borbe protiv teških kaznenih djela, bilo bi jasno protivno sudskoj praksi Suda koja se odnosi na zadržavanje podataka o vezi te bi zbog toga uvjeti koje je potrebno ispuniti za zadržavanje takvih podataka izgubili koristan učinak, s obzirom na to da bi im se u svakom slučaju moglo pristupiti zbog različitih razloga.

76. Iz toga proizlazi, prema mojem mišljenju, da bi zadržavanje IP adresa u svrhu zaštite prava intelektualnog vlasništva te priopćavanje tih adresa nositeljima tih prava u okviru postupaka koji se odnose na tu zaštitu moglo biti protivno članku 15. stavku 1. Direktive 2002/58, kako ga se

35 C-597/19, EU:C:2020:1063, t. 98.

36 Vidjeti moje mišljenje u predmetu M. I. C. M. (C-597/19, EU:C:2020:1063, t. 97.).

37 Vidjeti presude od 19. travnja 2012., Bonnier Audio i dr. (C-461/10, EU:C:2012:219, t. 55.); od 4. svibnja 2017., Rīgas satiksme (C-13/16, EU:C:2017:336, t. 34.) i od 17. lipnja 2021., M. I. C. M. (C-597/19, EU:C:2021:492, t. 47. do 54).

38 Vidjeti u tom smislu presudu od 29. siječnja 2008., Promusicae (C-275/06, EU:C:2008:54, t. 50. do 52.).

39 Vidjeti točku 65. ovog mišljenja.

40 Vidjeti moje mišljenje u predmetu M. I. C. M. (C-597/19, EU:C:2020:1063, t. 103.).

tumači u sudskoj praksi Suda. Obveza prijenosa osobnih podataka privatnim osobama kako bi se omogućilo pokretanje postupaka protiv povreda autorskog prava pred građanskim sudovima, iako ju je omogućio sam Sud, istodobno je tako u suprotnosti s njegovom vlastitom sudskom praksom koja se odnosi na zadržavanje IP adresa kod pružatelja elektroničkih komunikacijskih usluga.

77. Takvo rješenje ipak nije zadovoljavajuće jer bi dovelo u pitanje ravnotežu između različitih postojećih interesa koju je Sud nastojao uspostaviti kad je nositeljima prava intelektualnog vlasništva oduzeo glavnu, ako ne i jedinu mogućnost identifikacije počinitelja povreda tih prava na internetu. To me razmatranje dovodi do toga da iznesem drugu poteškoću koja, prema mojem mišljenju, može proizići iz sudske prakse Suda u pogledu nacionalnih mjera za zadržavanje IP adresa dodijeljenih izvoru veze, tumačenih s obzirom na članak 15. stavak 1. Direktive 2002/58.

b) Opasnost od sustavnog nekažnjavanja kažnjivih djela počinjenih isključivo na internetu

78. Stoga, kao drugo, smatram da to rješenje stvara poteškoće u praksi. Kao što to naglašava sam Sud, u slučaju kažnjivog djela počinjenog isključivo na internetu IP adresa može biti jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja tog kažnjivog djela.

79. Međutim, čini mi se da se taj element nije u potpunosti uzeo u obzir prilikom odvagivanja predmetnih interesa. Budući da Sud ipak ograničava mogućnost zadržavanja IP adresa u okviru borbe protiv teških kaznenih djela, istodobno ne dopušta da se ti podaci zadržavaju u svrhu borbe protiv kaznenih djela općenito, iako se neka od tih kaznenih djela mogu spriječiti, otkriti ili sankcionirati samo zahvaljujući navedenim podacima.

80. Drugim riječima, sudska praksa Suda mogla bi dovesti do toga da nacionalna tijela ostanu bez jedinog sredstva za identifikaciju počinitelja kažnjivih djela na internetu koja ipak ne spadaju u teška kaznena djela, kao što su povrede prava intelektualnog vlasništva. Posljedica toga zapravo bi bilo sustavno nekažnjavanje kažnjivih djela počinjenih isključivo na internetu, uostalom povrh samih povreda prava intelektualnog vlasništva. Osobito mislim na klevete počinjene na internetu. Iako pravo Unije doista predviđa naloge protiv posrednika čije se usluge koriste za počinjenje takvih kažnjivih djela [41], iz sudske prakse Suda moglo bi proizlaziti da sami počinitelji tih akata ne budu nikada kazneno gonjeni.

81. Osim ako se prizna da se cijeli niz kažnjivih djela ne može nikad kazneno goniti, smatram da bi trebalo ponovno analizirati ravnotežu između različitih postojećih interesa.

82. Slijedom tih različitih razmatranja, predložit ću Sudu određenu organizaciju sudske prakse koja se odnosi na nacionalne mjere za zadržavanje IP adresa, tumačene s obzirom na članak 15. stavak 1. Direktive 2002/58.

[41] Vidjeti članak 15. stavak 1. Direktive 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) (SL 2000., L 178, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 39., str. 58.)

4. Prijedlog organizacije sudske prakse Suda koja se odnosi na tumačenje članka 15. stavka 1. Direktive 2002/58 u pogledu mjera za zadržavanje IP adresa dodijeljenih izvoru veze

83. S obzirom na prethodna razmatranja, smatram da članak 15. stavak 1. Direktive 2002/58 treba tumačiti na način da mu se ne protive mjere kojima se predviđa opće i neselektivno zadržavanje IP adresa dodijeljenih izvoru veze tijekom razdoblja koje je vremenski ograničeno na ono što je strogo nužno kako bi se osiguralo sprečavanje, istraga, otkrivanje i progon kažnjivih djela na internetu za koja je IP adresa *jedino* istražno *sredstvo* kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kažnjivog djela.

84. U tom pogledu moram naglasiti da takav prijedlog, prema mojem mišljenju, ne dovodi u pitanje zahtjev razmjernosti propisan u pogledu zadržavanja podataka, s obzirom na ozbiljnost zadiranja u temeljna prava utvrđena u člancima 7. i 8. Povelje koju to zadiranje podrazumijeva [42]. Naprotiv, on je u potpunosti u skladu s tim zahtjevom.

85. S jedne strane, ograničenjem prava i obveza predviđenih člancima 5., 6. i 9. Direktive 2002/58 koje čini zadržavanje IP adresa nastoji se postići cilj u općem interesu povezan s tom ozbiljnosti, odnosno sprečavanje, istraga, otkrivanje i progon kaznenih djela na koje se upućuje u tekstovima koji bi u suprotnom ostali bez učinka.

86. S druge strane, to ograničenje ostaje u granicama onoga što je strogo nužno. Naime, takvo je zadržavanje ograničeno na točno određene slučajeve, odnosno na kaznena djela počinjena na internetu čiji se počinitelj može identificirati samo zahvaljujući IP adresi koja mu je dodijeljena. Drugim riječima, nije namjera da se dopusti opće i neselektivno zadržavanje podataka bez drugih uvjeta, nego samo da se omogući progon kaznenih djela, ne kaznenih djela općenito, nego onih točno određenih.

87. Međutim, iako se članku 15. stavku 1. Direktive 2002/58 ne protivi opće i neselektivno zadržavanje IP adresa dodijeljenih izvoru veze kako bi se osiguralo sprečavanje, istraga, otkrivanje i progon kaznenih djela na internetu za koja je IP adresa jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kaznenog djela, valja pojasniti i da ta mogućnost, prema sudskoj praksi, mora podlijegati „strogom poštovanju materijalnih i postupovnih uvjeta *kojima se mora urediti upotreba tih podataka*" [43]. Sud pojašnjava i da se takvom mjerom „moraju […] predvidjeti strogi uvjeti i jamstva glede *korištenja tih podataka*" [44].

88. Drugim riječima, kao što sam to već naglasio, zadržavanje podataka i pristup tim podacima ne mogu se razmatrati zasebno. U tim okolnostima, iako mogućnost Hadopija da pristupi IP adresama isprva nije protivna članku 15. stavku 1. Direktive 2002/58, ako se ti podaci zadržavaju u skladu sa zahtjevima predviđenim u toj odredbi, i dalje je, kako bi se odgovorilo na prethodna pitanja postavljena Sudu, potrebno ispitati jesu li uvjeti Hadopijeva pristupa IP adresama dodijeljenim izvoru veze sami po sebi u skladu s navedenom odredbom, osobito u pogledu pitanja nužnosti prethodnog nadzora suda ili neovisnog upravnog tijela kojem bi bio podvrgnut taj pristup.

89. Nakon što sam analizirao prethodno pitanje zadržavanja IP adresa dodijeljenih izvoru veze, ispitat ću Hadopijev pristup tim podacima s obzirom na članak 15. stavak 1. Direktive 2002/58.

[42] Vidjeti točke 60. i 61. ovog mišljenja.

[43] Vidjeti presudu La Quadrature du Net i dr. (t. 155.) (moje isticanje).

[44] Vidjeti presudu La Quadrature du Net i dr. (t. 156.) (moje isticanje).

5. Hadopijev pristup podacima o građanskom identitetu koji odgovaraju IP adresama

90. Što se tiče ciljeva koji mogu opravdati nacionalnu mjeru kojom se odstupa od načela povjerljivosti elektroničkih komunikacija, iz sudske prakse Suda proizlazi da pristup podacima treba strogo i objektivno slijediti jedan od tih ciljeva i da cilj koji se želi postići tom mjerom mora biti povezan s ozbiljnošću zadiranja u temeljna prava koje takav pristup podrazumijeva [45].

91. Usto, kao što sam to naveo [46], pristup podacima koje pružatelji zadržavaju primjenom mjere donesene na temelju članka 15. stavka 1. Direktive 2002/58 može se u načelu opravdati samo ciljem od općeg interesa glede kojeg je to zadržavanje naloženo tim pružateljima [47].

92. Sud je stoga presudio, u skladu s načelom proporcionalnosti, da se ozbiljno zadiranje u okviru sprečavanja, istrage, otkrivanja i progona kaznenih djela može opravdati samo ciljem borbe protiv kriminaliteta koji se također može okvalificirati teškim [48].

93. U tom pogledu ističem da, suprotno onomu što tvrde francuska vlada i Komisija, Hadopijev pristup podacima o građanskom identitetu koji odgovaraju određenoj IP adresi ozbiljno je zadiranje u temeljna prava. Naime, nije riječ samo o pristupu podacima o građanskom identitetu, koji sami po sebi nisu posebno osjetljivi, nego o povezivanju tih podataka s većim skupom podataka, odnosno IP adresama i, kao što to naglašavaju tužitelji iz glavnog postupka, s podacima preuzetim iz sustava pohrane protivno autorskom pravu. Stoga je riječ o povezivanju građanskog identiteta osobe sa sadržajem pretraženog sustava pohrane i IP adresom na kojoj je izvršena ta pretraga.

94. Međutim, jednako kao što smatram da treba dopustiti i zadržavanje podataka koje čini ozbiljno zadiranje u temeljna prava kako bi se osiguralo sprečavanje, istraga, otkrivanje i progon kaznenih djela na internetu za koja je IP adresa jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kaznenog djela [49], smatram da, osim ako se prizna sustavno nekažnjavanje kaznenih djela počinjenih isključivo na internetu, s istim ciljem treba omogućiti pristup tim podacima.

95. Stoga je Hadopijev pristup podacima o građanskom identitetu koji se povezuju s IP adresom opravdan ciljem u općem interesu s kojim je to zadržavanje naloženo pružateljima elektroničkih komunikacijskih usluga.

96. Sudskom praksom Suda ipak se pojašnjava da se nacionalno zakonodavstvo kojim se uređuje pristup nadležnih tijela zadržanim podacima o prometu i podacima o lokaciji ne može ograničiti na zahtjev da pristup odgovara cilju iz tog zakonodavstva, nego također mora predvidjeti materijalne i postupovne uvjete kojima se uređuje pristup nadležnih nacionalnih tijela predmetnim podacima [50].

97. Konkretno, Sud je presudio da, s obzirom na to da se opći pristup svim zadržanim podacima, neovisno o tome postoji li ikakva veza s ciljem koji se nastoji postići, ne može smatrati ograničenim na ono što je strogo nužno, nacionalni propis mora se temeljiti na objektivnim

45 Vidjeti presude od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788, t. 55.) i Prokuratuur (t. 32.).

46 Točka 47. ovog mišljenja

47 Vidjeti presude SpaceNet (t. 131.); La Quadrature du Net i dr. (t. 166.) i Commissioner of An Garda Síochána i dr. (t. 98.).

48 Vidjeti presudu Tele2 (t. 115.); od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788, t. 56.) i Prokuratuur (t. 33.).

49 Vidjeti točku 65. i sljedeće točke ovog mišljenja.

50 Vidjeti presude Tele2 (t. 118.); Prokuratuur (t. 49.) i Commissioner of An Garda Síochána i dr. (t. 104.).

kriterijima kako bi definirao okolnosti i uvjete u kojima nadležnim nacionalnim tijelima treba biti odobren pristup podacima korisnikâ, kako bi se provjerilo je li pristup odobren samo podacima osoba za koje postoji sumnja da namjeravaju počiniti, da čine ili su počinile teško kazneno djelo ili da su na kakav drugi način sudjelovale u tom djelu [51].

98. Stoga je, prema sudskoj praksi, u svrhu osiguranja punog poštovanja tih uvjeta u praksi, bitno da se prije pristupa nadležnih nacionalnih tijela zadržanim podacima u načelu provede nadzor suda ili neovisnog upravnog tijela [52].

99. Međutim, ističem da je Sud utvrdio tu potrebu za prethodnim nadzorom pristupa osobnim podacima u posebnim okolnostima koje su različite od okolnosti u ovom slučaju, koje podrazumijevaju *osobito ozbiljna* zadiranja u privatni život korisnikâ elektroničkih komunikacijskih usluga.

100. Naime, u svakoj od presuda u kojima je naglašen taj zahtjev bila je riječ o nacionalnim mjerama kojima se dopušta pristup svim podacima o prometu i lokaciji korisnikâ koji se odnose na sva sredstva elektroničke komunikacije [53] ili barem na fiksnu i mobilnu telefoniju [54]. Konkretnije, u pitanju je bio pristup „skupu podataka […] koji mogu pružiti informacije o komunikacijama koje izvršava korisnik sredstva elektroničke komunikacije ili o lokaciji terminalne opreme kojom se koristi i omogućiti izvođenje preciznih zaključaka o njegovu privatnom životu” [55], tako da zahtjev da sud ili neovisno upravno tijelo provodi prethodni nadzor pristupa tim podacima, prema mojem mišljenju, postoji samo u tim okolnostima.

101. Međutim, s jedne strane, Hadopijev pristup ostaje ograničen na to da se podaci o građanskom identitetu povezuju s korištenom IP adresom i pretraženim sustavom pohrane u točno određenom trenutku a da to nadležnim tijelima ne omogućuje da rekonstruiraju tijek kretanja dotičnog korisnika prilikom pregledavanja na internetu niti da, slijedom toga, izvedu precizne zaključke o njegovu privatnom životu osim saznanja o konkretnom pretraženom sustavu pohrane u trenutku počinjenja kaznenog djela. Stoga se time ne omogućuje praćenje cjelokupne internetske aktivnosti dotičnog korisnika.

102. S druge strane, ti podaci obuhvaćaju samo podatke osoba koje su, kao što je to utvrđeno u zapisnicima koje su sastavile organizacije nositeljâ prava, počinile djela koja mogu predstavljati povredu obveze predviđene člankom L. 336-3 CPI-ja. Hadopijev pristup podacima o građanskom identitetu koji se povezuju s IP adresama stoga je strogo ograničen na ono što je nužno da bi se ostvario željeni cilj, odnosno da bi se omogućilo sprečavanje, istraga, otkrivanje i progon kažnjivih djela na internetu za koja je IP adresa jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kažnjivog djela, u okviru kojeg je uspostavljen mehanizam postupnog odgovora.

103. U tim okolnostima, smatram da se člankom 15. stavkom 1. Direktive 2002/58 ne propisuje da sud ili neovisno upravno tijelo treba provoditi prethodni nadzor nad Hadopijevim pristupom podacima o građanskom identitetu koji se povezuju s IP adresama korisnikâ.

51 Vidjeti presude Tele2 (t. 119.); Prokuratuur (t. 50.) i Commissioner of An Garda Síochána i dr. (t. 105.).

52 Vidjeti presude Tele2 (t. 120.); Prokuratuur (t. 51.) i Commissioner of An Garda Síochána i dr. (t. 106.).

53 Vidjeti presude Tele2 i Commissioner of An Garda Síochána i dr.

54 Vidjeti presudu Prokuratuur.

55 Vidjeti presudu Prokuratuur (t. 45.).

104. Usto, ističem da, kao što to naglašava francuska vlada, Hadopijev pristup tim podacima, iako nije podvrgnut prethodnom nadzoru suda ili neovisnog tijela, ipak nije potpuno oslobođen svakog nadzora, s obzirom na to da datoteku koju Hadopi šalje operaterima elektroničkih komunikacija svaki dan izrađuje službenik koji je položio prisegu na temelju zahtjeva koji se zaprimaju i potvrđuju, na nasumičnoj osnovi, prije njihova dodavanja u datoteku [56]. Osobito valja napomenuti da postupak postupnog odgovora i dalje podliježe odredbama Direktive (EU) 2016/680 [57]. Na temelju toga fizičke osobe čije podatke Hadopi obrađuje imaju pravo na sve materijalne i postupovne zaštitne mjere predviđene tom direktivom. Te mjere obuhvaćaju pravo na pristup osobnim podacima koje Hadopi obrađuje, njihov ispravak i brisanje, kao i mogućnost podnošenja pritužbe neovisnom nadzornom tijelu i nakon toga, po potrebi, sudskog pravnog lijeka koji se podnosi u skladu s uvjetima općeg prava [58].

105. Slijedom toga, predlažem da se na prvo i drugo prethodno pitanje odgovori tako da članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje, treba tumačiti na način da mu se ne protivi nacionalni propis kojim se pružateljima elektroničkih komunikacijskih usluga omogućuje da zadrže, a upravnom tijelu zaduženom za zaštitu autorskih i srodnih prava od povreda tih prava počinjenih na internetu da pristupi samo podacima o građanskom identitetu, kako bi to tijelo moglo identificirati nositelje tih adresa za koje se sumnjiči da su odgovorni za te povrede te da bi, po potrebi, moglo poduzeti mjere protiv njih, a da taj pristup pritom ne podliježe prethodnom nadzoru suda ili neovisnog upravnog tijela, kada su ti podaci jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kažnjivog djela.

B. Treće prethodno pitanje

106. Svojim trećim prethodnim pitanjem sud koji je uputio zahtjev želi znati, ako se na prvo i drugo prethodno pitanje odgovori potvrdno te s obzirom na nisku osjetljivost podataka o građanskom identitetu, strogo ograničenje pristupa podacima i zahtjev da se ne ugrozi ispunjavanje zadaće javne usluge koja je povjerena predmetnom upravnom tijelu, treba li članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje, tumačiti na način da mu se protivi to da se prethodni nadzor pristupa provodi u skladu s prilagođenim pravilima, kao što je automatski nadzor, po potrebi pod nadzorom unutarnje službe tog tijela koja pruža jamstva neovisnosti i nepristranosti u pogledu službenika zaduženih za to prikupljanje.

107. Iz teksta trećeg prethodnog pitanja, kao i iz pisanog odgovora francuske vlade na pitanja Suda, proizlazi da se prilagođena pravila nadzora na koja se upućuje u tom pitanju ne odnose na postojeći sustav nadzora u nacionalnom pravu, nego na mogućnosti koje se mogu istražiti i kojima bi se francuski sustav po potrebi nastojao uskladiti s pravom Unije.

[56] Uzgredno ističem da ni argumenti izvedivosti ne idu u prilog postojanju obveze sustavnog prethodnog nadzora. Postojanje uređenog sustava za borbu protiv povreda autorskog prava počinjenih na internetu, poput onoga o kojem je riječ u glavnom postupku, pretpostavlja potrebu za obradom velikih količina osobnih podataka, u skladu s brojem kaznenih djela nad kojima se vodi progon, što je, na primjer za 2019., u skladu s očitovanjima francuske vlade, 33 465 zahtjeva za utvrđivanje IP adrese koje je Hadopi dnevno izvršavao. U tom kontekstu, obveza provođenja prethodnog nadzora pristupa tim podacima mogla bi u praksi ugroziti funkcioniranje mehanizama za organiziranu borbu protiv povreda na internetu, što bi dovelo u pitanje ravnotežu između pravâ korisnika i pravâ autora.

[57] Direktiva Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89. i ispravak SL 2018., L 127, str. 14.)

[58] Sve su te zaštitne mjere predviđene odredbama poglavlja III. glave III. loia nº 78-17 relative à l'informatique, aux fichiers et aux libertés, du 6 janvier 1978. (Zakon br. 78-17 od 6. siječnja 1978. o informatici, sustavima pohrane i slobodama) (JORF od 7. siječnja 1978.).

108. Međutim, prema ustaljenoj sudskoj praksi, cilj zahtjeva za prethodnu odluku nije u davanju savjetodavnih mišljenja o općim i hipotetskim pitanjima, nego u stvarnoj potrebi učinkovitog rješenja spora o pravu Unije [59].

109. Budući da je treće prethodno pitanje dakle, prema mojem mišljenju, hipotetsko, valja ga smatrati nedopuštenim.

110. U svakom slučaju, s obzirom na odgovor koji predlažem na prvo i drugo prethodno pitanje, nije potrebno dati odgovor na treće pitanje.

V. Zaključak

111. S obzirom na sva prethodna razmatranja, predlažem Sudu da na prethodna pitanja koja je uputio Conseil d'État (Državno vijeće, Francuska) odgovori na sljedeći način:

Članak 15. stavak 1. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima

treba tumačiti na način da mu se:

ne protivi nacionalni propis kojim se pružateljima elektroničkih komunikacijskih usluga omogućuje da zadrže, a upravnom tijelu zaduženom za zaštitu autorskih i srodnih prava od povreda tih prava počinjenih na internetu da pristupi samo podacima o građanskom identitetu koji odgovaraju IP adresama, kako bi to tijelo moglo identificirati nositelje tih adresa za koje se sumnjiči da su odgovorni za te povrede te da bi, po potrebi, moglo poduzeti mjere protiv njih, a da taj pristup pritom ne podliježe prethodnom nadzoru suda ili neovisnog upravnog tijela, kada su ti podaci jedino istražno sredstvo kojim se može identificirati osoba kojoj je ta adresa bila dodijeljena u trenutku počinjenja kažnjivog djela.

[59] Vidjeti presude od 26. listopada 2017., Balgarska energiyna borsa (C-347/16, EU:C:2017:816, t. 31.); od 31. svibnja 2018., Confetra i dr. (C-259/16 i C-260/16, EU:C:2018:370, t. 63.) i od 17. listopada 2019., Elektrorazpredelenie Yug (C-31/18, EU:C:2019:868, t. 32.).