GENERALINIO ADVOKATO
M. SZPUNAR IŠVADA,
pateikta 2022 m. spalio 27 d.[1]

Byla C-470/21

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

(*Conseil d'État* (Valstybės Taryba, Prancūzija) pateiktas prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas ir privataus gyvenimo apsauga elektroninių ryšių sektoriuje – Direktyva 2002/58/EB – 15 straipsnio 1 dalis – Valstybių narių teisė riboti tam tikrų teisių ir pareigų apimtį – Įpareigojimas, kad teismas ar nepriklausoma administracinė institucija, kurios sprendimas turi privalomąją galią, atliktų išankstinę kontrolę – Civilinės tapatybės duomenys, atitinkantys IP adresą"

I. Įžanga

1. Klausimas dėl interneto naudotojų tam tikrų duomenų saugojimo ir prieigos prie šių duomenų yra aktualus nuolat ir gvildenamas naujausioje, tačiau jau gausiai suformuotoje Teisingumo Teismo jurisprudencijoje.

2. Šioje byloje Teisingumo Teismas turi galimybę iš naujo išnagrinėti šį klausimą, atsižvelgdamas į naujas kovos su intelektinės nuosavybės teisių pažeidimais, padarytais išimtinai internetu, aplinkybes.

[1] Originalo kalba – prancūzų.

II. Teisinis pagrindas

A. Sąjungos teisė

3. Direktyvos 2002/58/EB [2] 2, 6, 7, 11, 22, 26 ir 30 konstatuojamosiose dalyse nurodyta:

„(2) Šia direktyva siekiama gerbti pagrindines žmogaus teises ir laikomasi Europos Sąjungos pagrindinių teisių chartijos [toliau – Chartija] principų. visų pirma šia direktyva siekiama užtikrinti visapusišką pagarbą minėtos Chartijos 7 ir 8 straipsniuose išdėstytoms teisėms.

<…>

(6) Internetas keičia tradicines rinkos struktūras sukurdamas bendrą, pasaulinę infrastruktūrą įvairioms elektroninių ryšių paslaugoms teikti. Viešai prieinamos elektroninių ryšių interneto paslaugos atveria naujas galimybes naudotojams, bet dėl jų taip pat iškyla [nauja] rizika asmens duomenims ir privatumui.

(7) Viešiesiems ryšių tinklams reikėtų nustatyti specifines teisines, normines ir technines nuostatas, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės bei juridinių asmenų teisėti interesai, visų [pirma] dėl didėjančių automatinio duomenų, susijusių su abonentais ir naudotojais, kaupimo ir tvarkymo pajėgumų.

<…>

(11) Ši direktyva, kaip ir Direktyva [95/46/EB [3]], nenagrinėja pagrindinių teisių ir laisvių apsaugos klausimų, susijusių su veiklos rūšimis, kurių nereglamentuoja Bendrijos teisės aktai. Todėl ji nekeičia esamos pusiausvyros tarp fizinio asmens teisės į privatumą ir valstybių narių galimybės imtis šios direktyvos 15 straipsnio 1 dalyje nurodytų priemonių, kurių reikia užtikrinti visuomenės saugumą, gynybą, valstybės saugumą (įskaitant valstybės ekonominę gerovę, kai veiklos rūšys yra susijusios su valstybės saugumo klausimais) ir baudžiamosios teisės vykdymu. Tokiu būdu ši direktyva neturi jokio poveikio valstybių narių galimybėms teisėtu būdu perimti elektroninių ryšių pranešimus arba imtis kitų priemonių, kurių reikia minėtiems tikslams pasiekti laikantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos [, pasirašytos Romoje 1950 m. lapkričio 4 d.], [kaip ją savo sprendimuose yra išaiškinęs Europos Žmogaus Teisių Teismas]. Tokios priemonės turi būti tinkamos, griežtai atitinkančios siekiamą tikslą ir būtinos demokratinėje visuomenėje, taip pat joms turi būti taikoma tinkama apsaugos garantija pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją.

<…>

[2] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 514).

[3] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355).

(22) Draudimas saugoti pranešimus ir srauto duomenis kitiems nei naudotojai asmenims, taip pat saugoti juos be naudotojų sutikimo nėra skirtas uždrausti šios informacijos automatinį, tarpinį ir tranzitinį saugojimą, jeigu tai daroma tik siekiant perduoti pranešimą elektroninių ryšių tinklu, ir ne ilgiau, nei reikia perdavimui ir srautams valdyti, garantuojant konfidencialumą saugojimo metu. <…>

<…>

(26) Su abonentais susiję duomenys, kurie yra tvarkomi elektroninių ryšių tinkluose sujungimų ir informacijos perdavimo tikslais, apima duomenis apie fizinių asmenų privatų gyvenimą ir susiję su jų teise į susirašinėjimo slaptumą arba susiję su teisėtais juridinių asmenų interesais. Tokie duomenys saugotini tiek, kiek jie reikalingi sąskaitoms pateikti ir sumokėti už tinklų sujungimus, ir tik ribotą laiko tarpą. [Bet koks kitas tokių duomenų tvarkymas] <…> leidžiama[s] tik abonentui sutikus, kuris apsisprendžia, remdamasis tikslia ir išsamia informacija iš šio teikėjo apie numatomus duomenų tolimesnio tvarkymo būdus, apie abonento teisę nesutikti arba panaikinti duotą sutikimą tvarkyti tokius duomenis. <…>

<…>

(30) Elektroninių ryšių tinklų ir paslaugų teikimo sistemos turi būti suprojektuotos taip, kad reikalingas asmens duomenų kiekis būtų griežtai apribotas iki minimumo. <…>“

4. Šios direktyvos 2 straipsnyje „Sąvokų apibrėžimai“ nurodyta:

„<…>

Šioje direktyvoje:

a) „naudotojas“ – tai bet kuris fizinis asmuo, vartojantis viešai prieinamą elektroninių ryšių paslaugą privačiais ar verslo tikslais, ir nebūtinai tai darantis išankstinio paslaugos užsakymo būdu;

b) „srauto duomenys“ – tai duomenys, tvarkomi pranešimui perduoti elektroninių ryšių tinklu, taip pat sąskaitoms už tokį perdavimą pateikti;

c) „vietos nustatymo duomenys“ – elektroninių ryšių tinkluose arba elektroninių ryšių paslaugų teikimo metu tvarkomi duomenys, nurodantys viešosios elektroninių ryšių paslaugos gavėjo galinių įrenginių geografinę padėtį;

d) „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Jam nepriskiriama informacija, perduodama kaip dalis viešojo transliavimo paslaugos, naudojant elektroninių ryšių tinklus, išskyrus tuos atvejus, kai tokia informacija gali būti susijusi su informaciją gaunančiu abonentu arba naudotoju, kurio tapatybę galima nustatyti;

<…>“

5. Minėtos direktyvos 3 straipsnyje „Paslaugos“ nustatyta:

„Ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Bendrijoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius.“

6. Tos pačios direktyvos 5 straipsnyje „Pranešimų konfidencialumas“ numatyta:

„1. Valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai [prieinamas] elektroninių ryšių paslaugas, konfidencialumą, taikydamos nacionalinės teisės aktus. Visų pirma jos draudžia be atitinkamų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis, išskyrus atvejus, kai tai galima teisėtai daryti pagal 15 straipsnio 1 dalį. Šios dalies nuostatos nedraudžia techninio saugojimo, būtino perduoti pranešimą nepažeidžiant konfidencialumo principo.

<…>

3. Valstybės narės užtikrina, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar naudotojo galiniame įrenginyje būtų leidžiama tik su sąlyga, jei atitinkamam abonentui ar naudotojui sutikus pagal Direktyvą [95/46] pateikiama aiški ir išsami informacija, *inter alia*, apie tokio duomenų tvarkymo tikslus. Ši nuostata nedraudžia vykdyti techninį saugojimą ar naudotis duomenimis, jei siekiama tik atlikti pranešimo perdavimą elektroninių ryšių tinklu, taip pat būtinais atvejais, kad informacinės visuomenės paslaugų teikėjas galėtų teikti paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.“

7. Direktyvos 2002/58 6 straipsnyje „Srauto duomenys“ nustatyta:

„1. Su abonentais ir naudotojais susiję srauto duomenys, kuriuos tvarko ir saugo viešųjų ryšių tinklo ar viešai prieinamų elektroninių ryšių paslaugų teikėjas, turi būti sunaikinti arba pakeisti taip, kad taptų anoniminiais, kai šie duomenys nebėra reikalingi pranešimui perduoti, jeigu nepažeidžiamos šio straipsnio 2, 3 ir 5 dalių ir 15 straipsnio 1 dalies nuostatos.

2. Srauto duomenys gali būti tvarkomi, kai reikia abonentams pateikti sąskaitas ir atsiskaityti už tinklų sujungimą. Toks tvarkymas leistinas tol, kol nepasibaigęs terminas, per kurį sąskaita gali būti teisėtai užginčyta ar išieškotas apmokėjimas.

<…>“

8. Šios Direktyvos 2002/58 15 straipsnio „Kai kurių Direktyvos [95/46] nuostatų taikymas“ 1 dalyje nurodyta:

„1. Valstybės narės gali patvirtinti teisines [teisėkūros] priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą, jeigu toks ribojimas yra būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės [demokratinėje visuomenėje] priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą [taip pat užtikrinti baudžiamųjų veikų ar neteisėto elektroninių ryšių sistemos naudojimo prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas], kaip nurodyta Direktyvos [95/46] 13 straipsnio 1 dalyje. Valstybės narės gali,

inter alia, patvirtinti teisines [teisėkūros] priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis šioje dalyje nustatytais motyvais. Visos šioje dalyje nurodytos priemonės turi atitikti bendruosius [Sąjungos] teisės principus, tarp jų ir nurodytus [ESS] 6 straipsnio 1 ir 2 dalyse.“

B. Prancūzijos teisė

1. Code de la propriété intellectuelle (Intelektinės nuosavybės kodeksas)

9. Pagrindinės bylos faktinėms aplinkybėms taikytinos redakcijos *Code de la propriété intellectuelle* (toliau – CPI) L.331-12 straipsnyje nustatyta:

„*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* [Vyriausioji kūrinių platinimo ir teisių apsaugos internete valdyba] (toliau – *Hadopi*) yra nepriklausoma viešoji institucija.“

10. CPI L.331-13 straipsnyje numatyta:

„[*Hadopi*] užtikrina:

<…>

2° [kūrinių ir objektų, kurie elektroninių ryšių tinkluose saugomi autorių ar gretutinių teisių,] apsaugą nuo šių teisių pažeidimų, padarytų elektroninių ryšių tinkluose, naudojamuose teikiant visuomenei ryšių paslaugas internetu; <…>“

11. Šio Kodekso L.331-15 straipsnyje nurodyta:

„[*Hadopi*] sudaro valdyba ir Teisių apsaugos komitetas. <…>.

<…>

Įgyvendindami savo įgaliojimus, valdybos ir Teisių apsaugos komiteto nariai negauna jokios institucijos nurodymų.“

12. Minėto kodekso L.331-17 straipsnyje nustatyta:

„Teisių apsaugos komitetas yra atsakingas už L.331-25 straipsnyje numatytų priemonių taikymą.“

13. To paties kodekso L.331-21 straipsnyje nurodyta:

„Teisių apsaugos komiteto funkcijoms vykdyti [*Hadopi*] pasitelkia prisaikdintus valstybės tarnautojus, kuriems [*Hadopi*] pirmininkas suteikia įgaliojimus, laikydamasis sąlygų, nustatytų dekrete, priimtame gavus *Conseil d'État* (Valstybės Taryba) nuomonę. <…>

Pirmoje pastraipoje nurodyti Teisių apsaugos komiteto nariai ir tarnautojai gauna šiam komitetui teikiamus prašymus L.331-24 straipsnyje numatytomis sąlygomis. Jie nagrinėja faktines aplinkybes.

Jei to reikia vykstant procedūrai, jie gali gauti visus dokumentus, neatsižvelgiant į naudojamas laikmenas, įskaitant elektroninių ryšių operatorių pagal *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas) L.34-1 straipsnį saugomus ir tvarkomus duomenis ir *Loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (2004 m. birželio 21 d. Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika) 6 straipsnio I dalies 1 ir 2 punktuose nurodytų paslaugų teikėjų saugomus ir tvarkomus duomenis.

Jie taip pat gali gauti pirmesnėje pastraipoje nurodytų dokumentų kopijas.

Jie gali, be kita ko, iš elektroninių ryšių operatorių gauti abonento, kurio prieiga prie viešųjų elektroninių ryšių paslaugų buvo naudojama kūriniams ar saugomiems objektams atgaminti, atvaizduoti, padaryti prieinamus ar viešai paskelbti be <…> teisių turėtojų leidimo, kai toks leidimas reikalingas, tapatybę, pašto adresą, elektroninio pašto adresą ir telefono numerį.“

14. CPI L.331-24 straipsnyje nustatyta:

„Teisių apsaugos komitetas imasi veiksmų, kai į jį kreipiasi prisiekusieji ir įgaliotieji atstovai <…>, kuriuos skiria:

– teisėtai įsteigtos profesinės gynybos institucijos,

– kolektyvinio administravimo organizacijos,

– *Centre national du cinéma et de l'image animée* (Nacionalinis kino ir animacijos centras).

Teisių apsaugos komitetas taip pat gali veikti remdamasis Respublikos prokuroro jam perduota informacija.

Jis negali nagrinėti daugiau nei prieš šešis mėnesius susiklosčiusių aplinkybių.“

15. Šio kodekso L.331-25 straipsnyje, kuriame reglamentuojama vadinamoji „laipsniško reagavimo“ procedūra, nustatyta:

„Teisių apsaugos komitetas, sužinojęs apie faktines aplinkybes, galinčias reikšti [CPI] L.336-3 straipsnyje nustatytos pareigos pažeidimą, gali nusiųsti abonentui <…> rekomendaciją, kuria jam primenamos L.336-3 straipsnio nuostatos, nurodoma laikytis jose nustatytos pareigos ir įspėjama apie nuobaudas, gresiančias pagal L.335-7 ir L. 335-7-1 straipsnius. Šioje rekomendacijoje abonentui taip pat pateikiama informacija apie teisėtą kultūrinio turinio internete pasiūlą, saugumo užtikrinimo priemones, kuriomis siekiama užkirsti kelią L.336-3 straipsnyje nustatytos pareigos pažeidimams, taip pat apie veiksmų, kuriais nesilaikoma autorių ir gretutinių teisių, keliamą pavojų kūrybinės veiklos atnaujinimui ir kultūros sektoriaus ekonomikai.

Jei per šešis mėnesius nuo pirmoje pastraipoje nurodytos rekomendacijos pateikimo ir vėl pasikartoja faktinės aplinkybės, kurios gali reikšti L.336-3 straipsnyje apibrėžtos pareigos pažeidimą, komitetas gali elektroninėmis priemonėmis <…> išsiųsti naują rekomendaciją, kurioje pateikiama ta pati informacija kaip ir ankstesnėje rekomendacijoje. Prie šios rekomendacijos jis turi pridėti raštą, įteikiamą pasirašytinai arba bet kokiu kitu būdu, tinkamu nustatyti šios rekomendacijos pateikimo datą.

Pagal šį straipsnį parengtose rekomendacijose nurodoma data ir laikas, kada buvo užfiksuotos faktinės aplinkybės, galinčios reikšti L.336-3 straipsnyje nustatytos pareigos pažeidimą. Tačiau jose neatskleidžiamas saugomų kūrinių ar objektų, su kuriais šis pažeidimas susijęs, turinys. Jose nurodomas telefono numeris, adresas ir elektroniniai kontaktiniai duomenys, kuriais adresatas, jei pageidauja, gali pateikti pastabas Teisių apsaugos komitetui ir gauti, šiuo tikslu aiškiai suformulavęs prašymą, išsamią informaciją apie saugomų kūrinių ar objektų, susijusių su pažeidimu, kuriuo jis kaltinamas, turinį.“

16. Minėto kodekso L.331-29 straipsnyje nustatyta:

„[*Hadopi*] gali automatizuotai tvarkyti asmenų, dėl kurių pradėta procedūra pagal šį poskirsnį, asmens duomenis.

Šiuo duomenų tvarkymu siekiama, kad Teisių apsaugos komitetas įgyvendintų šiame poskirsnyje numatytas priemones, visus susijusius procedūrinius veiksmus ir informuotų profesines gynybos institucijas bei kolektyvinio administravimo asociacijas apie galimą kreipimąsi į teisminę instituciją, taip pat siųstų L.335-7 straipsnio penktoje pastraipoje numatytus pranešimus.

<…> dekrete nustatoma šio straipsnio taikymo tvarka. Jame konkrečiai nurodoma:

– išsaugotų duomenų kategorijos ir jų saugojimo trukmė,

– adresatai, turintys teisę gauti šiuos duomenis, visų pirma asmenys, kurių veikla yra teikti prieigą visuomenei prie elektroninių ryšių paslaugų internetu,

– sąlygos, kuriomis suinteresuotieji asmenys gali pasinaudoti teise susipažinti su [*Hadopi*] turimais su jais susijusiais duomenimis. <…>“

17. To paties kodekso R.331-37 straipsnyje numatyta:

„<…> elektroninių ryšių operatoriai ir <…> paslaugų teikėjai, prisijungdami prie L.331-29 straipsnyje nurodytos automatizuoto asmens duomenų tvarkymo sistemos arba naudodamiesi įrašymo laikmena, užtikrinančia šių duomenų vientisumą ir saugumą, per aštuonias dienas nuo tada, kai Teisių apsaugos komitetas perdavė techninius duomenis, būtinus abonento, kurio prieiga prie viešųjų ryšių paslaugų internetu buvo naudojama kūriniams ar saugomiems objektams atgaminti, atvaizduoti, padaryti prieinamus ar viešai paskelbti be <…> teisių turėtojų leidimo, privalo perduoti asmens duomenis ir [*Décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel* (2010 m. kovo 5 d. Dekretas Nr. 2010-236 dėl automatizuoto asmens duomenų tvarkymo), leidžiamo pagal [CPI] L.331-29 straipsnį „Kūrinių apsaugos internete priemonių valdymo sistema“[4]] <…> priedo 2° punkte nurodytą informaciją.

<…>“

[4] JORF, tekstas Nr. 19, 2010 m. kovo 7 d.

18. CPI R.335-5 straipsnyje nustatyta:

„I.- Akivaizdžiu aplaidumu, už kurį baudžiama bauda, numatyta už penktosios kategorijos pažeidimus, laikoma veika, kai asmuo, turintis prieigą prie interneto viešųjų ryšių paslaugų, be teisėto pagrindo, jei įvykdomos II skyriuje numatytos sąlygos:

1° neįdiegė šios prieigos saugumo užtikrinimo priemonės; arba

2° įdiegė šią priemonę nerūpestingai.

II.- I skyriaus nuostatos taikomos tik tada, kai įvykdomos šios dvi sąlygos:

1° pagal L.331-25 straipsnį ir šiame straipsnyje numatytu būdu prieigos turėtojui Teisių apsaugos komitetas rekomendavo įdiegti jo prieigos saugumo užtikrinimo priemonę, kuri neleistų iš naujo naudoti prieigos autorių ar gretutinių teisių saugomiems kūriniams ar objektams atgaminti, atvaizduoti, padaryti viešai prieinamus ar viešai paskelbti be teisių turėtojų leidimo <…>, kai toks leidimas reikalingas;

2° per vienus metus nuo šios rekomendacijos pateikimo tokia prieiga vėl naudojama šios II dalies 1 °punkte nurodytais tikslais.“

19. Šio kodekso L.336-3 straipsnyje nustatyta:

„Prieigos prie visuomenei prieinamų elektroninių ryšių paslaugų internetu turėtojas privalo užtikrinti, kad ši prieiga nebūtų naudojama autorių teisių ar gretutinių teisių saugomiems kūriniams ar objektams atgaminti, atvaizduoti, padaryti viešai prieinamus ar viešai skelbti be autorių teisių ar gretutinių teisių turėtojų leidimo <…>, kai jis reikalingas.

Jei prieigą turintis asmuo nesilaiko pirmoje pastraipoje nustatytos pareigos, suinteresuotojo asmens baudžiamoji atsakomybė nekyla <…>“

2. 2010 m. kovo 5 d. dekretas

20. Pagrindinės bylos faktinėms aplinkybėms taikytinos redakcijos 2010 m. kovo 5 d. dekreto 1 straipsnyje numatyta:

„Asmens duomenų tvarkymu, vadinamu „Kūrinių apsaugos internete priemonių valdymo sistema“, siekiama, kad [*Hadopi*] Teisių apsaugos komitetas:

1° įgyvendintų priemones, numatytas [CPI] norminės dalies III knygoje (III antraštinės dalies I skyriaus 3 skirsnio 3 poskirsnis) ir to paties kodekso norminės dalies III knygoje (III antraštinės dalies I skyriaus 2 skirsnio 2 poskirsnis);

2° kreiptųsi į Respublikos prokurorą dėl faktinių aplinkybių, kurios gali būti kvalifikuojamos kaip nusikalstamos veikos, numatytos to paties kodekso L.335-2, L.335-3, L.335-4 ir R.335-5 straipsniuose, taip pat informuotų profesinės gynybos ir kolektyvinio administravimo organizacijas apie tokius kreipimusis;

<…>“

21. Šio dekreto 4 straipsnyje nurodyta:

„I.- Prisiekusieji valstybės tarnautojai, kuriuos pagal [CPI] L.331-21 straipsnį įgaliojo [*Hadopi*] prezidentas, ir 1 straipsnyje minėto Teisių apsaugos komiteto nariai turi tiesioginę prieigą prie šio dekreto priede nurodytų asmens duomenų ir informacijos.

II.- Elektroninių ryšių operatoriai ir paslaugų teikėjai, nurodyti šio dekreto priedo 2°punkte, gauna:

– techninius duomenis, reikalingus abonentui identifikuoti,

– [CPI] L.331-25 straipsnyje numatytas rekomendacijas, skirtas abonentams elektroninėmis priemonėmis siųsti,

– informaciją, reikalingą papildomoms nuobaudoms dėl prieigos prie viešųjų elektroninių ryšių paslaugų sustabdymo, kurią Teisių apsaugos komitetas gavo iš Respublikos prokuroro, įgyvendinti.

III.- Profesinės gynybos organizacijos ir kolektyvinio administravimo organizacijos yra informacijos, susijusios su kreipimusi į Respublikos prokurorą, gavėjos.

IV.- Teisminėms institucijoms pateikiami faktinių aplinkybių, kurios gali būti kvalifikuojamos kaip [CPI] L.335-2, L.335-3, L.335-4, L.335-7, R.331-37, R.331-38 ir R.335-5 straipsniuose numatyti pažeidimai, nustatymo protokolai.

Apie sustabdymo bausmės įvykdymą pranešama automatizuotam nuosprendžių registrui.“

22. 2010 m. kovo 5 d. dekreto priede numatyta:

„Asmens duomenys ir informacija, išsaugomi tvarkant duomenis pagal „Kūrinių apsaugos internete priemonių valdymo sistemą“, yra šie:

1° asmens duomenys ir informacija, gauta iš teisėtai sudarytų profesinės gynybos organizacijų, kolektyvinio administravimo organizacijų, *Centre national du cinéma et de l'image animée* ir Respublikos prokuroro:

dėl faktinių aplinkybių, kurios gali būti kvalifikuojamos kaip [CPI] L.336-3 straipsnyje nustatytos pareigos pažeidimas:

faktinių aplinkybių data ir laikas;

atitinkamų abonentų IP adresas;

naudotas lygiarangių protokolas;

abonento naudotas pseudonimas;

informacija apie saugomus kūrinius ar objektus, su kuriais susijusios faktinės aplinkybės;

abonento įrenginyje esančios rinkmenos pavadinimas (jei taikoma);

interneto prieigos paslaugų teikėjas, iš kurio buvo įsigyta prieiga arba kuris suteikė IP techninius išteklius.

<…>

2° iš elektroninių ryšių operatorių <…> ir paslaugų teikėjų <…> surinkti asmens duomenys ir informacija apie abonentą:

pavardė, vardai;

pašto adresas ir el. pašto adresai;

telefono numeris;

abonento telefono įrenginio adresas;

interneto prieigos paslaugų teikėjas, naudojantis 1°punkte nurodyto prieigos teikėjo, su kuriuo abonentas sudarė sutartį, techninius išteklius; bylos numeris;

prieigos prie viešųjų elektroninių ryšių paslaugos sustabdymo data.

<…>“

3. Pašto ir telekomunikacijų kodeksas

23. *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas), iš dalies pakeisto 2021 m. liepos 30 d. Įstatymo Nr. 2021-998[5] (toliau – CPCE) 17 straipsniu, L.34-1 straipsnio II bis dalyje nustatyta, kad „elektroninių ryšių operatoriai privalo saugoti:

1° baudžiamojo proceso, grėsmių visuomenės saugumui prevencijos ir nacionalinio saugumo užtikrinimo tikslais informaciją, susijusią su naudotojo civiline tapatybe, kol pasibaigs penkerių metų terminas, skaičiuojamas nuo jo sutarties galiojimo pabaigos;

2° tais pačiais tikslais, kaip ir nurodytieji šio II bis dalies 1°punkte, kitą informaciją, kurią naudotojas pateikė pasirašydamas sutartį arba susikurdamas paskyrą, taip pat informaciją, susijusią su mokėjimais, kol pasibaigs vienų metų terminas, skaičiuojamas nuo sutarties galiojimo pabaigos arba jo paskyros uždarymo;

[5] JORF, tekstas Nr. 1, 2021 m. liepos 31 d. Ši CPCE L.34-1 straipsnio redakcija, galiojanti nuo 2021 m. liepos 31 d., buvo priimta po *Conseil d'État* (Prancūzija) 2021 m. balandžio 21 d. Sprendimo Nr. 393099 (JORF, 2021 m. balandžio 25 d.), kuriuo buvo panaikinta ankstesnės redakcijos nuostata, numatanti pareigą saugoti asmens duomenis „nusikalstamų veikų tyrimo, nustatymo ir patraukimo baudžiamojon atsakomybėn tikslais arba dėl [CPI] L.336-3 straipsnyje nustatytos pareigos neįvykdymo“ tik tam, kad prireikus galimybė ja naudotis būtų suteikta būtent *Hadopi*. 2022 m. vasario 25 d. Sprendime Nr. 2021-976-977 *QPC (M. Habib A. et autre) Conseil constitutionnel* (Konstitucinė Taryba, Prancūzija) pripažino, kad šios ankstesnės redakcijos CPCE L.34-1 straipsnis prieštaravo Konstitucijai iš esmės dėl to, kad „ginčijamomis nuostatomis leidžiant bendrą ir nediferencijuotą ryšio duomenų saugojimą, neproporcingai pažeidžiama teisė į privataus gyvenimo gerbimą“ (13 punktas). Minėtas teismas nusprendė, kad prisijungimo duomenys, kurie turi būti saugomi pagal šias nuostatas, susiję ne tik su elektroninių ryšių paslaugų naudotojų nustatymu, bet ir su kitais duomenimis, kurie, „atsižvelgiant į jų pobūdį, įvairovę ir galimą tvarkymą, <…> suteikia daug tikslios informacijos apie šiuos naudotojus ir tam tikrais atvejais trečiuosius asmenis, taip ypač suvaržant jų privatų gyvenimą (11 punktas)“.

3° siekiant kovoti su nusikalstamumu ir sunkiais nusikaltimais, vykdyti didelių grėsmių visuomenės saugumui ir nacionalinio saugumo užtikrinimui prevenciją, techninius duomenis, leidžiančius nustatyti prisijungimo šaltinį arba susijusius su naudojamais galiniais įrenginiais, kol pasibaigs vienų metų terminas, skaičiuojamas nuo galinių įrenginių prijungimo ar naudojimo dienos.“

III. Ginčas pagrindinėje byloje, prejudiciniai klausimai ir procesas Teisingumo Teisme

24. 2019 m. rugpjūčio 12 d. skundu ir dviem papildomais 2019 m. lapkričio 12 d. ir 2021 m. gegužės 6 d. procesiniais dokumentais *La Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *Franciliens.net* ir *French Data Network* kreipėsi į *Conseil d'Etat* (Valstybės Taryba, Prancūzija), prašydami panaikinti implicitinį sprendimą, kuriuo Ministras Pirmininkas atmetė jų prašymą panaikinti 2010 m. kovo 5 d. dekretą, motyvuodami tuo, kad šis dekretas ir jo teisinį pagrindą sudarančios nuostatos ne tik per daug pažeidžia Prancūzijos Konstitucijoje garantuojamas teises, bet ir prieštarauja Direktyvos 2002/58 15 straipsniui bei Chartijos 7, 8, 11 ir 52 straipsniams.

25. Visų pirma pareiškėjos pagrindinėje byloje tvirtina, kad 2010 m. kovo 5 d. dekretu ir jo teisinį pagrindą sudarančiomis nuostatomis neproporcingai leidžiama susipažinti su prisijungimo duomenimis dėl internete padarytų nesunkių autorių teisių pažeidimų, nei teismui, nei nepriklausomumo ir nešališkumo garantijas užtikrinančiai institucijai neatliekant jokios išankstinės kontrolės.

26. Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas pirmiausia pažymi, jog Teisingumo Teismas neseniai priimtame Sprendime *La Quadrature du Net ir kt.*[6] konstatavo, kad pagal Direktyvos 2002/58 15 straipsnio 1 dalį, aiškinamą atsižvelgiant į Chartijos 7, 8, 11 straipsnius ir 52 straipsnio 1 dalį, nėra draudžiamos teisėkūros priemonės, kuriose nacionalinio saugumo, kovos su nusikalstamumu ir visuomenės saugumo užtikrinimo tikslais numatomas bendras ir nediferencijuotas *duomenų, susijusių su* elektroninių ryšių priemonių naudotojų *civiline tapatybe*, saugojimas. Vadinasi, toks duomenų saugojimas būtų galimas be jokio konkretaus termino, apskritai nusikalstamų veikų tyrimo, atskleidimo ir patraukimo baudžiamojon atsakomybėn už jas tikslais.

27. Prašymą priimti prejudicinį sprendimą pateikęs teismas iš to sprendžia, kad pareiškėjų pagrindinėje byloje nurodytas pagrindas, grindžiamas 2010 m. kovo 5 d. dekreto neteisėtumu, tiek, kiek jis buvo priimtas kovai su nesunkiais pažeidimais, gali būti tik atmestas.

28. Toliau minėtas teismas pažymi, jog Teisingumo Teismas Sprendime *Tele2 Sverige ir Watson*[7] konstatavo, kad Direktyvos 2002/58 15 straipsnio 1 dalis atsižvelgiant į Chartijos 7, 8, 11 straipsnius ir 52 straipsnio 1 dalį turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriais reglamentuojama srauto ir vietos nustatymo duomenų apsauga ir saugumas, ypač kompetentingų nacionalinių institucijų prieiga prie saugomų duomenų, jeigu tokiai prieigai netaikoma išankstinė teismo ar nepriklausomos administracinės institucijos kontrolė.

6 Žr. 2020 m. spalio 6 d. sprendimą (C-511/18, C-512/18 ir C-520/18, toliau – Sprendimas *La Quadrature du Net ir kt.*, EU:C:2020:791, rezoliucinė dalis).

7 Žr. 2016 m. gruodžio 21 d. sprendimą (C-203/15 ir C-698/15, toliau – Sprendimas *Tele2*, EU:C:2016:970, rezoliucinė dalis).

29. Prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad Sprendime *Tele2*[8] Teisingumo Teismas patikslino, jog siekiant praktiškai užtikrinti visišką tokių sąlygų laikymąsi iš esmės būtina, kad prieš suteikiant kompetentingoms nacionalinėms institucijoms prieigą prie saugomų duomenų, išskyrus tinkamai pagrįstus skubos atvejus, teismas arba nepriklausoma administracinė institucija atliktų išankstinę kontrolę ir toks teismas ar tokia institucija savo sprendimą priimtų gavę motyvuotą kompetentingų nacionalinių institucijų prašymą, kurį jos pateiktų, be kita ko, vykdydamos nusikalstamų veikų prevencijos, atskleidimo ar baudžiamojo persekiojimo procedūras.

30. Prašymą priimti prejudicinį sprendimą pateikęs teismas primena, kad Teisingumo Teismas šį reikalavimą priminė Sprendime *La Quadrature du Net ir kt.*[9], kiek tai susiję su žvalgybos tarnybų realiuoju laiku renkamais prisijungimo duomenimis, ir Sprendime *Prokuratuur (Prieigos prie elektroninių pranešimų duomenų sąlygos)*[10], kalbant apie nacionalinių institucijų prieigą prie prisijungimo duomenų.

31. Galiausiai minėtas teismas pažymi, kad nuo tos dienos, kai buvo įsteigta 2009 m., *Hadopi* pagal CPI L.331-25 straipsnyje numatytą laipsniško reagavimo procedūrą išsiuntė daugiau kaip 12,7 mln. rekomendacijų abonementų turėtojams, ir vien 2019 m. tokių rekomendacijų išsiųsta 827 791. Šiuo tikslu *Hadopi* Teisių apsaugos komiteto darbuotojai kasmet turi galėti surinkti nemažai duomenų, susijusių su atitinkamų naudotojų civiline tapatybe. Prašymą priimti prejudicinį sprendimą pateikusio teismo nuomone, atsižvelgiant į šių rekomendacijų kiekį, jei šiam duomenų rinkimui būtų taikoma išankstinė kontrolė, rekomendacijų gali būti neįmanoma įgyvendinti.

32. Šiomis aplinkybėmis *Conseil d'État* nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar IP adresą atitinkantys civilinės tapatybės duomenys yra vieni iš srauto ar vietos nustatymo duomenų ir jiems iš esmės taikoma teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, išankstinė kontrolė?

2. Jei į pirmąjį klausimą būtų atsakyta teigiamai, ar, atsižvelgiant į tai, kad su naudotojų civiline tapatybe susiję duomenys yra mažiau jautrūs, [Direktyva 2002/58], siejama su [Chartija], turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriuose numatyta, kad administracinė institucija renka šiuos naudotojų IP adresą atitinkančius duomenis ir tokiu atveju netaikoma išankstinė teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė?

3. Jei į antrąjį klausimą būtų atsakyta teigiamai, ar, atsižvelgiant į tai, kad su civiline tapatybe susiję duomenys yra mažiau jautrūs, ir į aplinkybę, kad gali būti renkami tik šie duomenys ir tik siekiant užkirsti kelią nacionalinės teisės aktuose tiksliai, išsamiai ir griežtai apibrėžtų pareigų nesilaikymui, taip pat į aplinkybę, kad teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, atliekama sisteminga prieigos prie kiekvieno naudotojo duomenų kontrolė gali trukdyti šiuos duomenis renkančiai administracinei institucijai teikti jai patikėtas viešąsias paslaugas, pagal [Direktyvą 2002/58]

8 Šio sprendimo 120 punktas.

9 Šio sprendimo 189 punktas.

10 2021 m. kovo 2 d. sprendimas (C-746/18, toliau – Sprendimas *Prokuratuur*, EU:C:2021:152).

draudžiama šią kontrolę atlikti pritaikyta tvarka, pavyzdžiui, ją automatizuoti, o prireikus priežiūrą vykdytų tokius duomenis renkančių pareigūnų atžvilgiu nepriklausomos ir nešališkos institucijos vidaus padalinys?“

33. Pareiškėjos pagrindinėje byloje, Prancūzijos, Estijos, Švedijos ir Norvegijos vyriausybės, taip pat Europos Komisija pateikė rašytines pastabas. 2022 m. liepos 5 d. vykusiame teismo posėdyje dalyvavo tos pačios šalys, išskyrus Estijos, Danijos ir Suomijos vyriausybes.

IV. Analizė

A. Dėl pirmojo ir antrojo prejudicinių klausimų

34. Savo pirmuoju ir antruoju prejudiciniais klausimais, kuriuos, manau, reikėtų nagrinėti kartu, prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, pagal kuriuos administracinei institucijai, kuriai pavesta ginti autorių ir gretutines teises nuo pažeidimų internete, leidžiama prieiga prie civilinės tapatybės duomenų, atitinkančių IP adresus, kad ši institucija galėtų nustatyti šių adresų turėtojus, įtariamus padarius tokius pažeidimus, ir prireikus imtis priemonių prieš juos, šiai prieigai netaikant išankstinės teismo ar nepriklausomos administracinės institucijos kontrolės.

1. Prejudicinių klausimų atribojimas

a) Teisių turėtojų organizacijų išankstinis IP adresų rinkimas

35. Iš sprendimo dėl prašymo priimti prejudicinį sprendimą matyti, kad pagrindinėje byloje nagrinėjamas laipsniško reagavimo mechanizmas apima dvi iš eilės einančias duomenų tvarkymo operacijas: pirma, teisių turėtojų organizacijų atliekamą išankstinį autorių teisių pažeidėjų IP adresų rinkimą lygiarangių tinkluose ir, antra, *Hadopi* po to, kai į ją kreipiamasi, atliekamą šių pažeidėjų IP adresų susiejimą su asmenų civiline tapatybe, kad asmenims, kurių prieiga prie viešųjų elektroninių ryšių paslaugų internetu buvo naudojama pažeidžiant autorių teisių taisykles, būtų išsiųstos rekomendacijos.

36. Pirmasis ir antrasis prejudiciniai klausimai susiję tik su antrąja *Hadopi* atliekama duomenų tvarkymo operacija.

37. Vis dėlto pareiškėjos pagrindinėje byloje tvirtina, kad Teisingumo Teismas turėtų išnagrinėti pirmąją duomenų tvarkymo operaciją, nes jei šie IP adresai buvo gauti pažeidžiant Direktyvos 2002/58 nuostatas, jų panaudojimas per antrąją duomenų tvarkymo operaciją neabejotinai prieštarautų šioms nuostatoms.

38. Tokie argumentai neįtikina. Direktyvos 2002/58 3 straipsnio 1 dalyje jos taikymo sritis apribojama, nurodant, kad ši direktyva taikoma „asmens duomenų tvarkymui, susijusiam su elektroninių ryšių paslaugų teikimu“. Tačiau, kaip Prancūzijos vyriausybė patikslino per teismo posėdį, teisių turėtojų organizacijos atitinkamus IP adresus gauna ne iš elektroninių ryšių paslaugų teikėjų, o tiesiogiai internete, susipažindamos su plačiajai visuomenei prieinamais duomenimis.

39. Taigi, galima konstatuoti tik tai, kad Direktyvos 2002/58 nuostatos netaikomos teisių turėtojų organizacijų atliekamam išankstiniam IP adresų rinkimui, todėl, kaip teigia Komisija, šis duomenų rinkimas galėtų būti analizuojamas atsižvelgiant į Reglamento (ES) 2016/679[11] nuostatas. Taigi man atrodo, kad tokia analizė išeina už Teisingumo Teismui pateiktų prejudicinių klausimų ribų, juo labiau kad prašymą priimti prejudicinį sprendimą pateikęs teismas nepateikia jokios papildomos informacijos apie išankstinį duomenų rinkimą, kuri leistų Teisingumo Teismui pateikti naudingą atsakymą.

40. Tokiomis aplinkybėmis savo analizę sutelksiu į klausimą dėl *Hadopi* prieigos prie IP adresą atitinkančių civilinės tapatybės duomenų.

b) IP adresų ir civilinės tapatybės duomenų susiejimas

41. Pirmasis ir antrasis prejudiciniai klausimai susiję su „IP adresą atitinkančiais civilinės tapatybės duomenimis“, kurie, prašymą priimti prejudicinį sprendimą pateikusio teismo nuomone, yra mažiau jautrūs. Šis teismas savo sprendime nurodo tik tuos Sprendimo *Quadrature du Net ir kt.* punktus, kurie susiję su civilinės tapatybės duomenų saugojimu.

42. Teisingumo Teismo jurisprudencijoje iš tikrųjų daromas skirtumas tarp IP adresų saugojimo ir prieigos prie jų tvarkos ir duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimo ir prieigos prie jų tvarkos; antroji tvarka yra ne tokia griežta kaip pirmoji[12].

43. Vis dėlto man atrodo, kad nagrinėjamu atveju, nepaisant šių dviejų prejudicinių klausimų formuluotės, kalbama ne tik apie prieigą prie elektroninių ryšių priemonių naudotojų civilinės tapatybės duomenų, bet ir apie šių duomenų susiejimą su *Hadopi* turimais IP adresais po to, kai juos surenka ir perduoda teisių turėtojų organizacijos. Kaip nurodo Komisija, suteikiant *Hadopi* prieigą prie civilinės tapatybės duomenų, siekiama atskleisti daugiau duomenų, visų pirma IP adresus ir peržiūrėtų rinkmenų ištraukas, ir leisti jais naudotis, nes vien civilinės tapatybės duomenys ir IP adresai atskirai, nesusiejus jų tarpusavyje, nedomina nacionalinės valdžios institucijų, kadangi nei iš civilinės tapatybės duomenų, nei iš IP adresų, jeigu jie nėra susieti tarpusavyje, negalima gauti informacijos apie fizinių asmenų veiklą internete.

44. Mano nuomone, darytina išvada, kad pirmasis ir antrasis prejudiciniai klausimai turėtų būti suprantami kaip susiję ne tik su elektroninių ryšių priemonės naudotojų civilinės tapatybės duomenimis, bet ir su prieiga prie IP adresų, pagal kuriuos galima nustatyti prisijungimo šaltinį.

c) Ryšių paslaugų teikėjų vykdomas IP adresų saugojimas

45. Kaip nurodo Prancūzijos vyriausybė ir Komisija, Teisingumo Teismui pateikti prejudiciniai klausimai iš tikrųjų formaliai susiję ne su elektroninių ryšių paslaugų teikėjų vykdomu duomenų saugojimu, o tik su *Hadopi* turima prieiga prie civilinės tapatybės duomenų, atitinkančių IP adresus.

[11] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016, p. 119, p. 1).

[12] Žr. Sprendimą *Quadrature du Net ir kt.* (155 ir 159 punktai).

46. Vis dėlto man atrodo, kad klausimas dėl *Hadopi* prieigos prie šių duomenų neatsiejamas nuo pirma kilusio klausimo dėl ryšių paslaugų teikėjų vykdomo šių duomenų saugojimo. Kaip yra pažymėjęs Teisingumo Teismas, duomenys saugomi tik tam, kad prireikus su jais galėtų susipažinti kompetentingos nacionalinės institucijos [13]. Kitaip tariant, duomenų saugojimo ir prieigos prie duomenų negalima analizuoti atskirai, nors prieiga prie duomenų ir priklauso nuo jų saugojimo.

47. Tiesa, Teisingumo Teismas jau yra nagrinėjęs nacionalinės teisės aktų, susijusių tik su kompetentingų nacionalinių institucijų prieiga prie tam tikrų asmens duomenų, suderinamumą su Direktyvos 2002/58 15 straipsnio 1 dalimi, neatsižvelgiant į atitinkamų duomenų saugojimo suderinamumo su šia nuostata klausimą [14]. Taigi į šioje byloje pateiktus prejudicinius klausimus būtų galima atsakyti atsiribojant nuo to, ar aptariami duomenys buvo saugomi laikantis Sąjungos teisės nuostatų.

48. Vis dėlto pirmiausia noriu pažymėti, kad Sprendime *Ministerio Fiscal* [15] Teisingumo Teismas, nagrinėdamas nacionalinių institucijų prieigos prie tam tikrų asmens duomenų suderinamumą su Sąjungos teise, rėmėsi lygiai tais pačiais principais, kaip ir vertindamas šių duomenų saugojimo suderinamumą su Sąjungos teise. Teisingumo Teismas rėmėsi tik pastaruoju klausimu suformuota jurisprudencija ir pritaikė ją prie prieigos prie asmens duomenų klausimo. Kitaip tariant, nenagrinėjant tam tikrų duomenų saugojimo atitikties Sąjungos teisei, šis nagrinėjimas perkeliamas į prieigos prie šių duomenų etapą, todėl prieigos prie duomenų suderinamumas galiausiai priklauso nuo jų saugojimo suderinamumo su Sąjungos teise.

49. Vėliau Teisingumo Teismas aiškiai nurodė, kad prieiga prie asmens duomenų gali būti suteikta tik tuo atveju, jei elektroninių ryšių paslaugų teikėjai šiuos duomenis saugojo laikydamiesi Direktyvos 2002/58 [16] 15 straipsnio 1 dalies reikalavimų, ir kad privačių asmenų prieiga prie asmens duomenų, siekiant iškelti civilinę bylą dėl autorių teisių pažeidimo, yra suderinama su Sąjungos teise tik tuo atveju, jei šie duomenys saugomi minėtą nuostatą atitinkančiu būdu [17].

50. Galiausiai Teisingumo Teismas nuosekliai konstatuoja, kad prieiga prie srauto ir vietos nustatymo duomenų, kuriuos paslaugų teikėjai saugo taikydami
Direktyvos 2002/58 15 straipsnio 1 dalyje numatytą priemonę – tokia prieiga turi būti suteikta laikantis sąlygų, nustatytų jurisprudencijoje, kurioje aiškinama Direktyva 2002/58, – iš esmės gali būti pateisinama tik bendrojo intereso tikslu, dėl kurio šiems teikėjams nustatytas toks įpareigojimas saugoti duomenis [18]. Kitaip tariant, nacionalinių institucijų teisės susipažinti su tam tikrais asmens duomenimis suderinamumas su Sąjungos teise visiškai priklauso nuo šių duomenų saugojimo suderinamumo su Sąjungos teise.

51. Taigi, mano nuomone, analizuojant, ar nacionalinės teisės aktai, kuriuose numatyta nacionalinės institucijos prieiga prie asmens duomenų, yra suderinami su Sąjungos teise, pirmiausia reikia nustatyti, ar šių duomenų saugojimas yra suderinamas su Sąjungos teise.

[13] Žr. Sprendimą *Tele2* (79 punktas).

[14] Žr. 2018 m. spalio 2 d. Sprendimą *Ministerio Fiscal* (C-207/16, EU:C:2018:788, 49 punktas).

[15] 2018 m. spalio 2 d. sprendimas (C-207/16, EU:C:2018:788).

[16] Žr. Sprendimą *Prokuratuur* (29 punktas).

[17] Žr. 2021 m. birželio 17 d. Sprendimą M.I.C.M. (C-597/19, EU:C:2021:492, 127–130 punktai).

[18] Žr. Sprendimo *La Quadrature du Net ir kt.* 166 punktą; 2022 m. balandžio 5 d. Sprendimą *Commissioner of An Garda Síochána ir kt.* (C-140/20, toliau – Sprendimas *Commissioner of An Garda Síochána ir kt.*, EU:C:2022:258, 98 punktas) ir 2022 m. rugsėjo 20 d. Sprendimą *SpaceNet* (C-793/19 ir C-794/19, toliau – Sprendimas *SpaceNet*, EU:C:2022:702, 131 punktas).

52. Šiomis aplinkybėmis savo analizę pradėsiu primindamas Teisingumo Teismo jurisprudenciją, susijusią su IP adresų, priskiriamų prie prisijungimo šaltinio, saugojimo klausimu, kad parodyčiau jos ribas ir pasiūlyčiau patikslintą aptariamo reglamentavimo aiškinimą.

2. Teisingumo Teismo jurisprudencija dėl Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo, kiek tai susiję su IP adresų, priskiriamų prie prisijungimo šaltinio, saugojimo priemonėmis

53. Direktyvos 2002/58 5 straipsnio 1 dalyje įtvirtintas elektroninių pranešimų ir su jais susijusių srauto duomenų konfidencialumo principas, kuris, be kita ko, reiškia, kad iš esmės bet kuriam asmeniui, išskyrus naudotoją, draudžiama saugoti šiuos pranešimus ir duomenis be jo sutikimo [19].

54. Kalbant apie elektroninių ryšių paslaugų teikėjų atliekamą su abonentais ir naudotojais susijusių srauto duomenų tvarkymą ir saugojimą, pažymėtina, jog Direktyvos 2002/58 6 straipsnio 1 dalyje numatyta, kad tokie duomenys turi būti sunaikinami arba anoniminami, kai jie nebereikalingi pranešimui perduoti, o 6 straipsnio 2 dalyje nurodyta, kad srauto duomenys gali būti tvarkomi, kai reikia abonentams pateikti sąskaitas ir mokėjimams už tinklų sujungimą, tačiau šie duomenys gali būti tvarkomi tik kol nepasibaigęs terminas, per kurį sąskaita gali būti teisėtai užginčyta arba išieškotas mokėjimas. Kalbant apie vietos nustatymo duomenis, kurie nėra srauto duomenys, pažymėtina, jog tos pačios direktyvos 9 straipsnio 1 dalyje nustatyta, kad tokie duomenys gali būti tvarkomi, tik kai įvykdomos tam tikros sąlygos ir kai jie buvo anoniminti, arba kai tam gautas naudotojų ar abonentų sutikimas [20].

55. Taigi priimdamas Direktyvą 2002/58 Sąjungos teisės aktų leidėjas sukonkretino Chartijos 7 ir 8 straipsniuose įtvirtintas teises taip, kad elektroninių ryšių priemonių naudotojai iš esmės turi teisę tikėtis, jog be jų sutikimo jų pranešimai ir su jais susiję duomenys išliks anonimiški ir negalės būti įrašomi [21]. Taigi šioje direktyvoje ne tik reglamentuojama prieiga prie tokių duomenų numatant garantijas, kuriomis siekiama užkirsti kelią piktnaudžiavimui, bet visų pirma įtvirtinamas principas, pagal kurį tretiesiems asmenims draudžiama saugoti šiuos duomenis.

56. Tokiomis aplinkybėmis, kadangi Direktyvos 2002/58 15 straipsnio 1 dalyje valstybėms narėms leidžiama imtis teisėkūros priemonių, kuriomis „ribojama“ teisių ir pareigų, numatytų, be kita ko, šios direktyvos 5, 6 ir 9 straipsniuose, kaip antai kylančių iš pranešimų konfidencialumo ir draudimo saugoti su jais susijusius duomenis principų, taikymo sritis, ši nuostata yra, be kita ko, minėtuose 5, 6 ir 9 straipsniuose nustatytos bendrosios taisyklės išimtis, todėl pagal suformuotą jurisprudenciją ji turi būti aiškinama siaurai. Vadinasi, tokia nuostata negali pateisinti to, kad pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą ir ypač šios direktyvos 5 straipsnyje aiškiai numatyto draudimo saugoti šiuos duomenis išimtis taptų taisykle, antraip ši nuostata netektų prasmės [22].

[19] Žr. sprendimus *La Quadrature du Net ir kt.* (107 punktas); *Commissioner of An Garda Síochána ir kt.* (35 punktas) ir *SpaceNet* (52 punktas).

[20] Žr. sprendimus *Tele2* (86 punktas); *La Quadrature du Net ir kt.* (108 punktas); *Commissioner of An Garda Síochána ir kt.* (38 punktas) ir *SpaceNet* (55 punktas).

[21] Žr. sprendimus *La Quadrature du Net ir kt.* (109 punktas); *Commissioner of An Garda Síochána ir kt.* (37 punktas) ir *SpaceNet* (54 punktas).

[22] Žr. sprendimus *La Quadrature du Net ir kt.* (110 ir 111 punktai); *Commissioner of An Garda Síochána ir kt.* (40 punktas) ir *SpaceNet* (57 punktas).

57. Dėl tikslų, kuriais gali būti pateisinamas, be kita ko, Direktyvos 2002/58 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų ribojimas, Teisingumo Teismas jau yra nusprendęs, kad šios direktyvos 15 straipsnio 1 dalies pirmame sakinyje pateiktas tikslų sąrašas yra baigtinis, todėl pagal šią nuostatą priimtas teisės aktas turi iš tikrųjų griežtai atitikti vieną iš šių tikslų [23].

58. Be to, iš Direktyvos 2002/58 15 straipsnio 1 dalies trečio sakinio matyti, kad priemonės, kurių valstybės narės imasi pagal šią nuostatą, turi atitikti bendruosius Sąjungos teisės principus, įskaitant proporcingumo principą, ir užtikrinti pagarbą Chartijos garantuojamoms pagrindinėms teisėms. Šiuo klausimu Teisingumo Teismas jau yra nusprendęs, kad elektroninių ryšių paslaugų teikėjams valstybės narės nacionalinės teisės aktuose nustatyta pareiga saugoti srauto duomenis, kad prireikus jie būtų prieinami kompetentingoms nacionalinėms institucijoms, kelia klausimų ne tik dėl Chartijos 7 ir 8 straipsnių, susijusių atitinkamai su privataus gyvenimo ir asmens duomenų apsaugos užtikrinimu, bet ir dėl Chartijos 11 straipsnyje garantuojamos saviraiškos laisvės, kuri yra vienas iš esminių demokratinės ir pliuralistinės visuomenės pagrindų ir viena iš vertybių, kuriomis pagal ESS 2 straipsnį grindžiama Sąjunga, paisymo [24].

59. Vis dėlto, kadangi pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama riboti jos 5, 6 ir 9 straipsniuose numatytas teises ir pareigas, ši nuostata atspindi aplinkybę, kad Chartijos 7, 8 ir 11 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų funkciją visuomenėje. Kaip matyti iš Chartijos 2 straipsnio 1 dalies, Chartija leidžiama riboti naudojimąsi šiomis teisėmis, jeigu tokie apribojimai yra numatyti įstatymo, jeigu jais nekeičiama šių teisių esmė ir jeigu, laikantis proporcingumo principo, jie reikalingi ir veiksmingai padeda siekti Sąjungos pripažintų bendrojo intereso tikslų arba apsaugoti kitų asmenų teises ir laisves. Taigi aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį atsižvelgiant į Chartiją, taip pat reikia atsižvelgti į nacionalinio saugumo bei kovos su sunkiais nusikaltimais tikslų svarbą, prisidedant prie kitų asmenų teisių ir laisvių apsaugos, taip pat į Chartijos 3, 4, 6 ir 7 straipsniuose įtvirtintų teisių [25], iš kurių gali kilti pozityvios valdžios institucijų pareigos, apsaugą [26].

60. Taigi, atsižvelgiant į šias skirtingas pozityvias prievoles, reikia suderinti įvairius aptariamus teisėtus interesus ir teises. Šiomis aplinkybėmis iš Direktyvos 2002/58 15 straipsnio 1 dalies pirmo sakinio matyti, kad valstybės narės gali nustatyti priemonę, kuria nukrypstama nuo konfidencialumo principo, jei tokia priemonė yra „būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės [demokratinėje visuomenėje] priemonė“, o šios direktyvos 11 konstatuojamojoje dalyje nurodyta, kad tokia priemonė turi būti „griežtai“ proporcinga siekiamam tikslui [27].

[23] Žr. sprendimus *La Quadrature du Net ir kt.* (112 punktas); *Commissioner of An Garda Síochána ir kt.* (41 punktas) ir *SpaceNet* (58 punktas).

[24] Žr. sprendimus *La Quadrature du Net ir kt.* (113 ir 114 punktai); *Commissioner of An Garda Síochána ir kt.* (42 punktas) ir *SpaceNet* (60 punktas).

[25] Žr. sprendimus *La Quadrature du Net ir kt.* (120–122 punktai); *Commissioner of An Garda Síochána ir kt.* (48 punktas) ir *SpaceNet* (63 punktas).

[26] Žr. sprendimus *La Quadrature du Net ir kt.* (120–122 punktai); *Commissioner of An Garda Síochána ir kt.* (49 punktas) ir *SpaceNet* (64 punktas).

[27] Žr. sprendimus *La Quadrature du Net ir kt.* (127–129 punktai); *Commissioner of An Garda Síochána ir kt.* (50 ir 51 punktai) ir *SpaceNet* (65 ir 66 punktai).

61. Šiuo klausimu iš Teisingumo Teismo jurisprudencijos matyti, kad valstybių narių galimybė pateisinti, be kita ko, Direktyvos 2002/58 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų ribojimą turi būti vertinama atsižvelgiant į suvaržymo, kurį lemia toks ribojimas, dydį ir tikrinant, ar šiuo ribojimu siekiamo bendrojo intereso tikslo svarba atitinka šį dydį [28].

62. Be to, reikėtų atkreipti dėmesį, kad Teisingumo Teismas savo jurisprudencijoje atskiria, pirma, suvaržymus, atsirandančius dėl prieigos prie duomenų, kurie patys suteikia tikslią informaciją apie atitinkamus pranešimus, taigi, ir apie privatų asmens gyvenimą, ir kuriems taikoma griežta saugojimo tvarka, ir, antra, suvaržymus, atsirandančius dėl prieigos prie duomenų, kurie tokią informaciją gali suteikti tik tada, kai yra susieti su kitais duomenimis, pavyzdžiui, IP adresais [29].

63. Konkrečiai dėl IP adresų Teisingumo Teismas pažymėjo, kad jie sugeneruojami nesiejant jų su konkrečiu pranešimu ir iš esmės, tarpininkaujant elektroninių ryšių paslaugų teikėjams, yra skirti fiziniam asmeniui, kuriam priklauso galinis įrenginys, iš kurio internetu siunčiamas pranešimas, identifikuoti. Taigi, jei išsaugomi tik pranešimo šaltinio, o ne jo adresato, IP adresai, šios kategorijos duomenys yra mažiau jautrūs nei kiti srauto duomenys [30].

64. Kartu Teisingumo Teismas pažymėjo, kad IP adresai gali būti naudojami, be kita ko, išsamiai atsekti interneto naudotojo naršymo keliams, taigi, ir jo veiklai internete, taip pat šie duomenys leidžia nustatyti išsamų šio naudotojo profilį ir padaryti tikslias išvadas apie privatų naudotojo gyvenimą. Taigi šių IP adresų saugojimas ir analizė yra *didelis* Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymas, galintis turėti atgrasomąjį poveikį Chartijos 11 straipsnyje užtikrinamos saviraiškos laisvės įgyvendinimui [31].

65. Vis dėlto pagal suformuotą jurisprudenciją, siekiant suderinti atitinkamas teises ir teisėtus interesus, kaip to reikalaujama pagal jurisprudenciją, reikia atsižvelgti į tai, kad tuo atveju, kai pažeidimas padaromas internetu, IP adresas gali būti vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam toks adresas buvo suteiktas šio pažeidimo padarymo metu [32].

66. Taigi Teisingumo Teismas konstatuoja, kad teisės aktas, kuriuo numatomas bendras ir nediferencijuotas tik IP adresų, priskirtų prie prisijungimo šaltinio, saugojimas iš esmės neprieštarauja Direktyvos 2002/58 15 straipsnio 1 daliai, siejamai su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, tačiau ši galimybė turi būti suteikta griežtai laikantis materialinių ir procedūrinių sąlygų, kuriomis reglamentuojamas tokių duomenų naudojimas, ir turint omenyje tai, kad, atsižvelgiant į šio saugojimo sukeliamą didelį suvaržymą, jį galima pateisinti tik kova su *sunkiais nusikaltimais* ir didelių grėsmių visuomenės saugumui, kaip ir nacionaliniam saugumui, prevencija [33].

[28] Žr. sprendimus *La Quadrature du Net ir kt.* (131 punktas); *Commissioner of An Garda Síochána ir kt.* (53 punktas) ir *SpaceNet* (68 punktas).

[29] Žr. šios išvados 41 ir paskesnius punktus.

[30] Žr. Sprendimą *La Quadrature du Net ir kt.* (152 punktas).

[31] Žr. sprendimus *La Quadrature du Net ir kt.* (153 punktas); *Commissioner of An Garda Síochána ir kt.* (73 punktas) ir *SpaceNet* (103 punktas) (kursyvu išskirta mano).

[32] Žr. sprendimus *La Quadrature du Net ir kt.* (154 punktas); *Commissioner of An Garda Síochána ir kt.* (73 punktas) ir *SpaceNet* (103 punktas).

[33] Žr. sprendimus *La Quadrature du Net ir kt.* (155 ir 156 punktai); *Commissioner of An Garda Síochána ir kt.* (74 punktas) ir *SpaceNet* (104 ir 105 punktai) (kursyvu išskirta mano).

67. Teisingumo Teismas taip pat patikslina, kad duomenų saugojimo trukmė negali viršyti to, kas griežtai būtina atsižvelgiant į siekiamą tikslą ir kad nustatant tokio pobūdžio priemonę turi būti numatytos griežtos duomenų naudojimo sąlygos ir garantijos [34].

3. Jurisprudencijos ribos aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį, kiek tai susiję su priemonėmis, kuriomis siekiama saugoti prie prisijungimo šaltinio priskirtus IP adresus

68. Vis dėlto man atrodo, kad dėl pozicijos, kurios Teisingumo Teismas laikėsi dėl nacionalinių priemonių, kuriose numatytas prie prisijungimo šaltinio priskiriamų IP adresų saugojimas, aiškinant jas atsižvelgiant į Direktyvos 2002/58 15 straipsnio 1 dalį, kyla du pagrindiniai sunkumai.

a) Suderinamumas su jurisprudencija dėl prie prisijungimo šaltinio priskiriamų IP adresų perdavimo, kai yra pareiškiami ieškiniai dėl intelektinės nuosavybės teisių apsaugos

69. Pirma, kaip jau nurodžiau savo išvadoje byloje M.I.C.M. [35], tarp šios jurisprudencijos ir jurisprudencijos, susijusios su IP adresų perdavimu, kai yra pareiškiami ieškiniai dėl intelektinės nuosavybės teisių apsaugos šių teisių turėtojams, pabrėžiant valstybių narių pareigą užtikrinti intelektinės nuosavybės teisių turėtojams realias galimybes gauti žalos, atsiradusios dėl šių teisių pažeidimo, atlyginimą, esama tam tikro nesuderinamumo [36].

70. Kalbant apie šios antrosios krypties jurisprudenciją, pažymėtina, jog Teisingumo Teismas nuosekliai konstatuoja, kad pagal Sąjungos teisę valstybėms narėms nedraudžiama nustatyti pareigos perduoti asmens duomenis privatiems asmenims, kad šie galėtų kreiptis į civilinių bylų teismus dėl autorių teisių pažeidimų [37].

71. Šiuo klausimu Teisingumo Teismas pažymi, kad valstybių narių galimybė numatyti pareigą atskleisti asmens duomenis nagrinėjant civilinę bylą iš tiesų pirmiausia kyla iš galimybės numatyti tokį atskleidimą vykdant baudžiamąjį persekiojimą už nusikalstamas veikas [38], o vėliau ji buvo išplėsta, įtraukiant ir civilines bylas.

72. Kiek tai susiję su IP adresais, Teisingumo Teismas vis dėlto yra konstatavęs, kad tokie duomenys gali būti saugomi tik siekiant kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui [39].

73. Mano nuomone, mėginimai suderinti šių dviejų krypčių jurisprudenciją veda prie netinkamų rezultatų ir negali būti įtikinami.

74. Pirma, priešingai, nei Prancūzijos vyriausybė teigė per teismo posėdį, kova su intelektinės nuosavybės teisių pažeidimais negali būti priskiriama kovos su sunkiais nusikaltimais sričiai. Mano nuomone, sąvoka „sunkus nusikaltimas“ turi būti aiškinama savarankiškai. Ji negali priklausyti nuo kiekvienos valstybės narės supratimo, antraip būtų sudarytos galimybės apeiti

[34] Žr. sprendimus *La Quadrature du Net ir kt.* (156 punktas) ir *SpaceNet* (105 punktas).

[35] C-597/19, EU:C:2020:1063, 98 punktas.

[36] Žr. mano išvadą byloje M.I.C.M. (C-597/19, EU:C:2020:1063, 97 punktas).

[37] Žr. 2012 m. balandžio 19 d. Sprendimą *Bonnier Audio ir kt.* (C-461/10, EU:C:2012:219, 55 punktas); 2017 m. gegužės 4 d. Sprendimą *Rīgas satiksme* (C-13/16, EU:C:2017:336, 34 punktas) ir 2021 m. birželio 17 d. Sprendimą *M.I.C.M.* (C-597/19, EU:C:2021:492, 47–54 punktai).

[38] Šiuo klausimu žr. 2008 m. sausio 29 d. Sprendimą *Promusicae* (C-275/06, EU:C:2008:54, 50–52 punktai).

[39] Žr. šios išvados 65 punktą.

Direktyvos 2002/58 15 straipsnio 1 dalies reikalavimus, priklausomai nuo to, ar valstybės narės taiko plačią, ar siaurą kovos su sunkiais nusikaltimais sampratą. Tačiau, kaip jau minėjau, su intelektinės nuosavybės teisių apsauga susijusių interesų negalima painioti su interesais, kuriais grindžiama kova su sunkiais nusikaltimais [40].

75. Antra, jeigu būtų leista perduoti IP adresus intelektinės nuosavybės teisių turėtojams vykstant jų apsaugos procedūroms, nors tokius duomenis leidžiama saugoti tik kovojant su sunkiais nusikaltimais, tai aiškiai prieštarautų Teisingumo Teismo jurisprudencijai dėl prisijungimo duomenų saugojimo ir dėl to tokiems duomenims saugoti būtinos sąlygos taptų visiškai neveiksmingos, nes bet kuriuo atveju juos būtų galima gauti dėl įvairių priežasčių.

76. Mano nuomone, iš to darytina išvada, kad IP adresų saugojimas intelektinės nuosavybės teisių apsaugos tikslais ir jų perdavimas šių teisių turėtojams vykstant šių teisių apsaugos procedūroms, prieštarautų Direktyvos 2002/58 15 straipsnio 1 daliai, kaip ji yra išaiškinta Teisingumo Teismo jurisprudencijoje. Todėl įpareigojimą perduoti asmens duomenis privatiems asmenims, kad būtų galima civiliniuose teismuose kelti bylas už autorių teisių pažeidimus, nors jis ir leidžiamas paties Teisingumo Teismo, tuo pat metu neutralizuoja jo paties jurisprudencija dėl elektroninių ryšių paslaugų teikėjų vykdomo IP adresų saugojimo.

77. Vis dėlto tokia išeitis netenkina, nes būtų pažeista įvairių interesų pusiausvyra, kurią Teisingumo Teismas siekė nustatyti, atimant iš intelektinės nuosavybės teisių turėtojų pagrindinę, jei ne vienintelę, priemonę nustatyti šių teisių pažeidėjus internete. Dėl šios aplinkybės norėčiau paminėti antrąją problemą, mano nuomone, galinčią kilti dėl Teisingumo Teismo jurisprudencijos, kalbant apie nacionalines priemones, taikomas prie prisijungimo šaltinio priskirtų IP adresų saugojimui, aiškinamas atsižvelgiant į
Direktyvos 2002/58 15 straipsnio 1 dalį.

b) Sisteminio nebaudžiamumo už nusikalstamas veikas, padarytas tik internetu, pavojus

78. Taigi, antra, manau, kad tokia išeitis kelia praktinių sunkumų. Kaip yra nurodęs pats Teisingumo Teismas, jei pažeidimas padaromas tik internetu, IP adresas gali būti vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam šis adresas buvo priskirtas šio pažeidimo padarymo metu.

79. Vis dėlto man atrodo, kad į šį aspektą nevisiškai atsižvelgiama derinant esamus interesus. Kadangi Teisingumo Teismas riboja galimybę saugoti IP adresus, numatydamas ją tik kovos su sunkiais nusikaltimais tikslais, jis kartu atmeta galimybę, kad šie duomenys gali būti saugomi siekiant kovoti su nusikalstamomis veikomis apskritai, nors kai kurioms iš šių veikų galima užkirsti kelią, jas atskleisti ar už jas nubausti tik turint tokius duomenis.

80. Kitaip tariant, dėl Teisingumo Teismo jurisprudencijos nacionalinės valdžios institucijos galėtų netekti vienintelės priemonės, leidžiančios nustatyti pažeidimus internete padariusius asmenis, kai šie pažeidimai vis dėlto nėra sunkūs nusikaltimai, pavyzdžiui, intelektinės nuosavybės teisių pažeidimai. Tai iš tikrųjų lemtų sisteminį nebaudžiamumą už pažeidimus, padarytus tik internete, ir tai apimtų ne vien intelektinės nuosavybės teisių pažeidimus. Visų pirma turiu omenyje šmeižto veiksmus internete. Sąjungos teisėje neabejotinai numatyti

[40] Žr. mano išvadą byloje *M.I.C.M.* (C-597/19, EU:C:2020:1063, 103 punktas).

draudimai tarpininkams, kurių paslaugomis naudojamasi darant tokius pažeidimus [41], tačiau pagal Teisingumo Teismo jurisprudenciją galėtų nutikti ir taip, kad patys šiuos veiksmus atlikę asmenys gali ir niekada nebūti patraukti atsakomybėn.

81. Manau, reikėtų iš naujo analizuoti skirtingų esamų interesų pusiausvyrą, nebent būtų pripažinta, kad už daugelį nusikalstamų veikų niekada nebus galima patraukti atsakomybėn.

82. Atsižvelgiant į šiuos įvairius argumentus, siūlyčiau Teisingumo Teismui šiek tiek patikslinti jurisprudenciją dėl nacionalinių priemonių, susijusių su IP adresų saugojimu, aiškinamų atsižvelgiant į Direktyvos 2002/58 15 straipsnio 1 dalį.

4. Siūlymas patikslinti Teisingumo Teismo jurisprudenciją dėl Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo, susijusio su IP adresų, priskiriamų prie prisijungimo šaltinio, saugojimo priemonėmis

83. Atsižvelgdamas į tai, kas išdėstyta, manau, kad Direktyvos 2002/58 15 straipsnio 1 dalis turėtų būti aiškinama taip, kad pagal ją nedraudžiama imtis priemonių, kuriomis numatomas bendras ir nediferencijuotas prie prisijungimo šaltinio priskirtų IP adresų saugojimas tik tiek laiko, kiek tai griežtai būtina siekiant užtikrinti internete daromų nusikalstamų veikų, kurių atveju IP adresas yra *vienintelė* tyrimo *priemonė*, leidžianti nustatyti asmenį, kuriam tas adresas buvo priskirtas nusikalstamos veikos padarymo metu, prevenciją, tyrimą, atskleidimą ir patraukimą baudžiamojon atsakomybėn už jas.

84. Šiuo klausimu reikėtų pažymėti, kad toks siūlymas, mano nuomone, neleidžia suabejoti duomenų saugojimui taikomu proporcingumo reikalavimu, atsižvelgiant į didelį Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo pobūdį, kurį lemia toks ribojimas [42]. Atvirkščiai, jis visiškai atitinka šį reikalavimą.

85. Pirma, Direktyvos 2002/58 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų ribojimu, pasireiškiančiu IP adresų išsaugojimu, siekiama su šiuo suvaržymo dydžiu susijusio bendrojo intereso tikslo, t. y. užkirsti kelią teisės aktuose nurodytoms nusikalstamoms veikoms, jas tirti, atskleisti ir vykdyti baudžiamąjį persekiojimą už jas, antraip šios nuostatos liktų neveiksmingos.

86. Antra, šis ribojimas neviršija to, kas yra griežtai būtina. Toks saugojimas galimas tik tam tikrais atvejais, t. y. kai internetu padaromi pažeidimai ir kai pažeidimą padariusį asmenį įmanoma nustatyti tik pagal jam priskirtą IP adresą. Kitaip tariant, kalbama ne apie leidimą bendrai ir nediferencijuotai saugoti duomenis, netaikant papildomų sąlygų, o tik apie tai, kad būtų galima vykdyti baudžiamąjį persekiojimą už nusikalstamas veikas ne apskritai, o konkrečiai apibrėžtais atvejais.

87. Vis dėlto, nors pagal Direktyvos 2002/58 15 straipsnio 1 dalį nedraudžiamas bendras ir nediferencijuotas prie prisijungimo šaltinio priskirtų IP adresų saugojimas, siekiant užtikrinti internete daromų nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, kai IP adresas yra vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam tas adresas buvo priskirtas nusikalstamos veikos padarymo metu, taip pat reikia patikslinti, kad pagal

[41] Žr. 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyvos 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) (OL L 178, 2000, p. 1; 2004 m. specialusis leidimas lietuvių k., 13 sk., 25 t., p. 399) 15 straipsnio 1 dalį.

[42] Žr. šios išvados 60 ir 61 punktus.

jurisprudenciją ši galimybė turi būti suteikiama „griežtai laikantis materialinių ir procedūrinių sąlygų, *reglamentuojančių šių duomenų naudojimą*“ [43]. Teisingumo Teismas taip pat yra pažymėjęs, kad tokia priemone „turi būti numatytos griežtos *šių duomenų naudojimo* sąlygos ir garantijos“ [44].

88. Kitaip tariant, kaip jau nurodžiau, duomenų saugojimo ir prieigos prie šių duomenų negalima analizuoti atskirai. Tokiomis aplinkybėmis, nors *Hadopi* galimybė gauti IP adresus iš pirmo žvilgsnio neprieštarauja Direktyvos 2002/58 15 straipsnio 1 daliai, nes šie duomenys buvo saugomi laikantis šioje nuostatoje nustatytų reikalavimų, vis dėlto siekiant atsakyti į Teisingumo Teismui pateiktus prejudicinius klausimus dar reikia išnagrinėti, ar minėtą nuostatą atitinka pačios *Hadopi* prieigos prie IP adresų, priskiriamų prie prisijungimo šaltinio, sąlygos, visų pirma kiek tai susiję su klausimu, ar būtina, kad teismas arba nepriklausoma administracinė institucija atliktų išankstinę tokios prieigos kontrolę.

89. Išnagrinėjęs preliminarų klausimą dėl prie prisijungimo šaltinio priskiriamų IP adresų saugojimo toliau nagrinėsiu *Hadopi* prieigą prie šių duomenų, atsižvelgiant į Direktyvos 2002/58 15 straipsnio 1 dalį.

5. „Hadopi“ prieiga prie IP adresus atitinkančių civilinės tapatybės duomenų

90. Iš Teisingumo Teismo jurisprudencijos, susijusios su tikslais, kuriais gali būti pateisinama nacionalinė priemonė, kuria nukrypstama nuo elektroninių ryšių konfidencialumo principo, matyti, kad prieiga prie duomenų turi griežtai ir objektyviai atitikti vieną iš šių tikslų ir kad tikslas, kurio siekiama šia priemone, turi būti proporcingas dėl tokios prieigos atsiradusio pagrindinių teisių suvaržymo dydžiui [45].

91. Be to, kaip jau paaiškinau [46], prieiga prie duomenų, kuriuos paslaugų teikėjai saugo taikydami priemonę, kurios imtasi pagal Direktyvos 2002/58 15 straipsnio 1 dalį, iš esmės gali būti pateisinama tik viešojo intereso tikslu, kurio siekiant šie paslaugų teikėjai buvo įpareigoti saugoti šiuos duomenis [47].

92. Taigi Teisingumo Teismas, remdamasis proporcingumo principu, konstatavo, kad, siekiant nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir patraukimo baudžiamojon atsakomybėn už jas tikslo, didelis suvaržymas gali būti pateisinamas tik kai kovojama su nusikaltimais, kurie taip pat kvalifikuojami kaip sunkūs [48].

93. Šiuo klausimu, priešingai, nei teigia Prancūzijos vyriausybė ir Komisija, pažymėtina, kad *Hadopi* prieiga prie civilinės tapatybės duomenų, atitinkančių IP adresą, yra didelis pagrindinių teisių suvaržymas. Tai yra ne tik galimybė gauti civilinės tapatybės duomenis, kurie patys yra ne tokie jautrūs, bet ir galimybė susieti šiuos duomenis su kitais duomenimis, t. y. IP adresu, ir dar,

[43] Žr. Sprendimą *La Quadrature du Net ir kt.* (155 punktas) (kursyvu išskirta mano).

[44] Žr. Sprendimą *La Quadrature du Net ir kt.* (156 punktas) (kursyvu išskirta mano).

[45] Žr. 2018 m. spalio 2 d. Sprendimą *Ministerio Fiscal* (C-207/16, EU:C:2018:788, 55 punktas) ir Sprendimą *Prokuratuur* (32 punktas).

[46] Šios išvados 47 punktas.

[47] Žr. sprendimus *SpaceNet* (131 punktas); *La Quadrature du Net ir kt.* (166 punktas) ir *Commissioner of An Garda Síochána ir kt.* (98 punktas).

[48] Žr. Sprendimą *Tele2* (115 punktas); 2018 m. spalio 2 d. Sprendimą *Ministerio Fiscal* (C-207/16, EU:C:2018:788, 56 punktas) ir Sprendimą *Prokuratuur* (33 punktas).

kaip nurodo pareiškėjos pagrindinėje byloje, ištrauka iš rinkmenos, atsisiųstos pažeidžiant autorių teises. Taigi kalbama apie asmens civilinės tapatybės susiejimą su peržiūrėtos rinkmenos turiniu ir IP adresu, kurį naudojant su ja buvo susipažinta.

94. Vis dėlto, nors manau, kad turi būti leidžiamas duomenų saugojimas, kuris reiškia didelį pagrindinių teisių suvaržymą nusikalstamų veikų internete prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas tikslais, kai tokių veikų atveju IP adresas yra vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam tas adresas buvo priskirtas nusikalstamos veikos padarymo metu [49], taip pat laikausi nuomonės, kad siekiant to paties tikslo turėtų būti sudaryta galimybė susipažinti su tokiais duomenimis, nebent būtų pripažįstamas bendras nebaudžiamumas už nusikalstamas veikas, padarytas tik internetu.

95. Taigi man atrodo, kad *Hadopi* turima prieiga prie civilinės tapatybės duomenų, susietų su IP adresu, yra pateisinama bendrojo intereso tikslu, dėl kurio elektroninių ryšių paslaugų teikėjams buvo nustatyta tokių duomenų saugojimo pareiga.

96. Vis dėlto Teisingumo Teismo jurisprudencijoje patikslinta, kad nacionalinės teisės aktuose, kuriais reglamentuojama kompetentingų institucijų prieiga prie srauto ir vietos nustatymo duomenų, negali būti apsiribojama reikalavimu, kad institucijų prieiga prie duomenų atitiktų tais teisės aktais siekiamą tikslą; juose taip pat turi būti numatytos tokią kompetentingų nacionalinių institucijų prieigą prie atitinkamų duomenų reglamentuojančios materialinės ir procedūrinės sąlygos [50].

97. Visų pirma Teisingumo Teismas yra konstatavęs: kadangi bendra prieiga prie visų saugomų duomenų, nepaisant to, ar yra koks nors ryšys su siekiamu tikslu, negali būti laikoma neviršijančia to, kas griežtai būtina, nacionalinės teisės aktai turi būti grindžiami objektyviais kriterijais, pagal kuriuos būtų galima nustatyti aplinkybes ir sąlygas, kuriomis kompetentingoms nacionalinėms institucijoms turi būti suteikta prieiga prie naudotojų duomenų, siekiant užtikrinti, kad prieiga būtų suteikta tik prie asmenų, kurie įtariami planuojantys sunkų nusikaltimą, jį darantys arba padarę, arba vienaip ar kitaip dalyvavę jį darant, duomenų [51].

98. Taigi, remiantis jurisprudencija, siekiant praktiškai užtikrinti visišką šių sąlygų laikymąsi, labai svarbu, kad kompetentingų nacionalinės valdžios institucijų prieigai prie saugomų duomenų iš esmės būtų taikoma išankstinė teismo arba nepriklausomos administracinės institucijos kontrolė [52].

99. Vis dėlto reikėtų atkreipti dėmesį, jog Teisingumo Teismas yra nustatęs šią prieigos prie asmens duomenų išankstinės kontrolės būtinybę ypatingomis aplinkybėmis (jos skiriasi nuo šios bylos aplinkybių), kai kalbama apie *labai didelius* elektroninių ryšių paslaugų naudotojų privataus gyvenimo suvaržymus.

100. Kiekviename iš sprendimų, kuriuose buvo pabrėžiamas šis reikalavimas, buvo kalbama apie nacionalines priemones, pagal kurias leidžiama prieiga prie naudotojų visų srauto ir vietos nustatymo duomenų, susijusių su visomis elektroninių ryšių priemonėmis [53] arba bent fiksuotojo

[49] Žr. šios išvados 65 ir paskesnius punktus.

[50] Žr. sprendimus *Tele2* (118 punktas); *Prokuratuur* (49 punktas) ir *Commissioner of An Garda Síochána ir kt.* (104 punktas).

[51] Žr. sprendimus *Tele*2 (119 punktas); *Prokuratuur* (50 punktas) ir *Commissioner of An Garda Síochána ir kt.* (105 punktas).

[52] Žr. sprendimus *Tele2* (120 punktas); *Prokuratuur* (51 punktas) ir *Commissioner of An Garda Síochána ir kt.* (106 punktas).

[53] Žr. sprendimus *Tele2* ir *Commissioner of An Garda Síochána ir kt.*

ir mobiliojo ryšio priemonėmis [54]. Konkrečiai buvo kalbama apie prieigą prie „visų <…> duomenų, kurie gali suteikti informaciją apie elektroninių ryšių priemonės naudotojo pranešimus arba jo naudojamų galinių įrenginių buvimo vietą ir leisti padaryti tikslias išvadas apie jo privatų gyvenimą“ [55], todėl manau, jog reikalavimas, kad teismas arba nepriklausoma administracinė institucija atliktų išankstinę prieigos prie tokių duomenų kontrolę, egzistuoja tik tokiomis sąlygomis.

101. Pirma, *Hadopi* prieiga apribota civilinės tapatybės duomenų susiejimu su naudojamu IP adresu ir konkrečiu metu peržiūrėta rinkmena, tačiau kompetentingoms institucijoms neleidžiama atkurti atitinkamo naudotojo naršymo internete kelio ar atitinkamai daryti tikslių išvadų apie jo asmeninį gyvenimą, išskyrus tai, kad joms tampa žinoma pažeidimo padarymo metu jo peržiūrėta konkreti laikmena. Vadinasi, tai nereiškia, kad leidžiama sekti visą atitinkamo naudotojo veiklą internete.

102. Antra, šie duomenys yra susiję tik su duomenimis apie asmenis, kurie, kaip pažymima teisių turėtojų organizacijų parengtuose protokoluose, atliko veiksmus, galimus kvalifikuoti kaip CPI L.336-3 straipsnyje nustatytos pareigos pažeidimą. Todėl *Hadopi* prieiga prie civilinės tapatybės duomenų, susietų su IP adresais, yra griežtai apribota tuo, kas yra būtina užsibrėžtam tikslui pasiekti, t. y. sudaryti sąlygas užkirsti kelią nusikalstamoms veikoms internete, kurių atveju IP adresas yra vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam šis adresas buvo suteiktas nusikalstamos veikos padarymo metu, jas tirti, atskleisti ir vykdyti baudžiamąjį persekiojimą už jas, o šio tikslo dalis yra laipsniško reagavimo mechanizmas.

103. Šiomis aplinkybėmis manau, jog pagal Direktyvos 2002/58 15 straipsnio 1 dalį nereikalaujama, kad teismas ar nepriklausoma administracinė institucija taikytų *Hadopi* prieigos prie civilinės tapatybės duomenų, susietų su naudotojų IP adresais, išankstinę kontrolę.

104. Be to, pažymiu, kaip nurodo Prancūzijos vyriausybė, kad nors *Hadopi* prieigai prie šių duomenų netaikoma išankstinė teismo ar nepriklausomos institucijos kontrolė, vis dėlto tai nereiškia, kad nėra visiškai jokios kontrolės, nes *Hadopi* elektroninių ryšių operatoriams siunčiamą rinkmeną kasdien parengia prisiekęs darbuotojas, remdamasis gautais prašymais, kurie, prieš juos įtraukiant į rinkmeną, patvirtinami atsitiktinės atrankos būdu [56]. Visų pirma reikėtų pažymėti, kad laipsniškam reagavimui ir toliau taikomos Direktyvos (ES) 2016/680 [57] nuostatos. Šiuo tikslu fiziniams asmenims, į kuriuos nukreipta *Hadopi* veikla, taikomos visos šioje direktyvoje numatytos materialinės ir procedūrinės garantijos. Jos apima teisę susipažinti su *Hadopi* tvarkomais asmens duomenimis, teisę į jų ištaisymą ir ištrynimą, taip pat galimybę pateikti skundą nepriklausomai priežiūros institucijai, paskui, jei reikia, pasinaudoti teismine teisių gynimo priemone bendrosiose teisės normose nustatytomis sąlygomis [58].

[54] Žr. Sprendimą *Prokuratuur*.

[55] Žr. Sprendimą *Prokuratuur* (45 punktas).

[56] Papildomai norėčiau pažymėti, kad taip pat esama argumentų dėl pagrįstumo, kurie irgi neleidžia pritarti sistemingos išankstinės kontrolės įpareigojimui. Organizuotos kovos su autorių teisių pažeidimais internete sistemos, kaip antai nagrinėjamos pagrindinėje byloje, buvimas suponuoja poreikį tvarkyti didelį asmens duomenų kiekį, atitinkantį pažeidimų, už kuriuos persekiojama, skaičių, t. y. pavyzdžiui, kaip savo pastabose nurodė Prancūzijos vyriausybė, 2019 m. *Hadopi* per dieną gavo 33 465 prašymus nustatyti IP adresą. Šiomis aplinkybėmis įpareigojimas vykdyti išankstinę prieigos prie tokių duomenų kontrolę galėtų praktiškai pakenkti organizuotų kovos su pažeidimais internete mechanizmų veikimui ir keltų abejonių dėl naudotojų ir autorių teisių pusiausvyros.

[57] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir [kuria] panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89).

[58] Visos šios garantijos numatytos *Loi nº 78-17 relative à l'informatique, aux fichiers et aux libertés, du 6 janvier 1978* (1978 m. sausio 6 d. Įstatymas Nr. 78-17 dėl informacinių technologijų, rinkmenų ir laisvių; JORF, 1978 m. sausio 7 d.) III antraštinės dalies III skyriaus nuostatose.

105. Taigi į pirmąjį ir antrąjį prejudicinius klausimus siūlau atsakyti, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais bei 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją nedraudžiami nacionalinės teisės aktai, pagal kuriuos elektroninių ryšių paslaugų teikėjams leidžiama saugoti, o administracinei institucijai, atsakingai už autorių teisių ir gretutinių teisių apsaugą nuo šių teisių pažeidimų, padarytų internete, gauti prieigą prie civilinės tapatybės duomenų, atitinkančių IP adresus, kad ši institucija galėtų nustatyti šių adresų turėtojus, įtariamus padarius šiuos pažeidimus, ir prireikus imtis priemonių prieš juos, nereikalaujant, kad prieš tai teismas ar nepriklausoma administracinė institucija atliktų tokios prieigos kontrolę, kai tokie duomenys yra vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam pažeidimo padarymo metu buvo priskirtas toks adresas.

B. Dėl trečiojo prejudicinio klausimo

106. Trečiuoju prejudiciniu klausimu prašymą priimti prejudicinį sprendimą pateikęs nacionalinis teismas siekia išsiaiškinti, ar, teigiamai atsakius į pirmąjį ir antrąjį klausimus ir atsižvelgiant į tai, kad civilinės tapatybės duomenys yra ne tokie jautrūs, į griežtą prieigos prie šių duomenų tvarką ir reikalavimą nepakenkti nagrinėjamai administracinei institucijai pavestai užduočiai teikti viešąsias paslaugas, Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiama, kad išankstinė prieigos kontrolė būtų atliekama pritaikyta tvarka, pavyzdžiui, ją automatizuojant, o prireikus priežiūrą vykdytų tokius duomenis renkančių pareigūnų atžvilgiu nepriklausomos ir nešališkos institucijos vidaus padalinys.

107. Iš trečiojo prejudicinio klausimo formuluotės ir iš Prancūzijos vyriausybės rašytinio atsakymo į Teisingumo Teismo klausimus matyti, kad šiame klausime minima pritaikyta kontrolės tvarka reiškia ne nacionalinėje teisėje numatytą esamą kontrolės mechanizmą, o tam tikras galimybes, kurios gali būti išnagrinėtos ir kuriomis siekiama prireikus suderinti Prancūzijos mechanizmą su Sąjungos teise.

108. Pagal suformuotą jurisprudenciją prašymas priimti prejudicinį sprendimą skirtas ne konsultacinėms nuomonėms bendrais ar hipotetiniais klausimais gauti, bet poreikiui veiksmingai išspręsti su Sąjungos teise susijusį ginčą patenkinti [59].

109. Taigi, mano nuomone, trečiasis prejudicinis klausimas yra hipotetinis ir turėtų būti pripažintas nepriimtinu.

110. Bet kuriuo atveju, atsižvelgiant į mano siūlomą atsakymą į pirmąjį ir antrąjį prejudicinius klausimus, į trečiąjį klausimą atsakyti nereikia.

[59] Žr. 2017 m. spalio 26 d. Sprendimą *Balgarska energiyna borsa* (C-347/16, EU:C:2017:816, 31 punktas); 2018 m. gegužės 31 d. Sprendimą *Confetra ir kt.* (C-259/16 ir C-260/16, EU:C:2018:370, 63 punktas) ir 2019 m. spalio 17 d. Sprendimą *Elektrorazpredelenie Yug* (C-31/18, EU:C:2019:868, 32 punktas).

V. Išvada

111. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui taip atsakyti į *Conseil d'État* (Valstybės Taryba, Prancūzija) pateiktus prejudicinius klausimus:

2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) 15 straipsnio 1 dalis, siejama su Europos Sąjungos pagrindinių teisių chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi,

turi būti aiškinama taip:

pagal ją nedraudžiami nacionalinės teisės aktai, pagal kuriuos elektroninių ryšių paslaugų teikėjams leidžiama saugoti, o administracinei institucijai, atsakingai už autorių teisių ir gretutinių teisių apsaugą nuo šių teisių pažeidimų, padarytų internete, gauti prieigą prie civilinės tapatybės duomenų, atitinkančių IP adresus, kad ši institucija galėtų nustatyti šių adresų turėtojus, įtariamus padarius šiuos pažeidimus, ir prireikus imtis priemonių prieš juos, nereikalaujant, kad prieš tai teismas ar nepriklausoma administracinė institucija atliktų tokios prieigos kontrolę, kai tokie duomenys yra vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam pažeidimo padarymo metu buvo priskirtas toks adresas.