Teismo praktikos rinkinys

GENERALINIO ADVOKATO
MACIEJ SZPUNAR IŠVADA,
pateikta 2023 m. rugsėjo 28 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* (Prancūzija) pateiktas prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas ir privataus gyvenimo apsauga elektroninių ryšių srityje – 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. Įvadas

1. Teisingumo Teismo didžiosios kolegijos prašymu, pateiktu pagal Procedūros reglamento 60 straipsnio 3 dalį, Teisingumo Teismas 2023 m. kovo 7 d. nusprendė perduoti šią bylą plenarinei sesijai.

2. 2023 m. kovo 23 d. nutartimi Teisingumo Teismas (plenarinė sesija) nusprendė atnaujinti žodinę proceso dalį ir pakvietė Europos Sąjungos Teisingumo Teismo statuto 23 straipsnyje nurodytus suinteresuotuosius asmenis, Europos duomenų apsaugos priežiūros pareigūną (EDAPP) ir Europos Sąjungos kibernetinio saugumo agentūrą (ENISA) dalyvauti naujame teismo posėdyje.

3. Pirmąją išvadą šioje byloje buvau pateikęs 2022 m. spalio 27 d., prieš pasibaigiant žodinei proceso daliai. Taigi šioje naujoje išvadoje turiu galimybę išsamiau panagrinėti tam tikrus savo argumentus šioje byloje, susijusius su esminiais asmens duomenų saugojimo ir prieigos prie jų aspektais.

[1] Originalo kalba: prancūzų.

II. Teisinis pagrindas

A. Sąjungos teisė

4. 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 išaiškinta Europos žmogaus teisių teismo nutarime [sprendimuose]. 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), iš dalies pakeista 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (OL L 337, 2009, p. 11, toliau Direktyva 2002/58).

[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. Jeigu vėliau viešai prieinamų elektroninių ryšių paslaugų teikėjas pageidauja tvarkyti šiuos duomenis [Bet koks kitas tokių duomenų tvarkymas] <…>, tai leidžiama [leidžiamas] 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. <…>“

5. 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“ – tai elektroninių ryšių tinkluose arba elektroninių ryšių paslaugų teikimo metu tvarkomi duomenys, nurodantys viešai prieinamų elektroninių ryšių paslaugų naudotojo 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;

<…>“

6. Minėtos direktyvos 3 straipsnyje „Paslaugos“ nustatyta:

„Ši direktyva taikoma asmens duomenims tvarkyti teikiant Bendrijoje viešai prieinamas elektroninių ryšių paslaugas viešaisiais ryšių tinklais, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius.“

7. Tos pačios direktyvos 5 straipsnyje „Pranešimų konfidencialumas“ numatoma:

„1. Valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai teikiamas [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 pateikiama aiški ir išsami informacija, kaip nurodyta Direktyvoje [95/46/EB], *inter alia*, apie tokio duomenų tvarkymo tikslus. Tai nedraudžia techninio saugojimo ar priėjimo prie informacijos, kurio vienintelis tikslas yra vykdyti informacijos perdavimą elektroninių ryšių tinklu, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.“

8. 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.

<…>“

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

„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 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 Bendrijos [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)

10. 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.“

11. 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; <…>“

12. 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.“

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

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

14. To paties kodekso L. 331-21 straipsnyje numatyta:

„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.“

15. 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.“

16. 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. Vis dėlto 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.“

17. 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, teikiantys prieigą visuomenei prie ryšių paslaugų internete,

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

18. 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 identifikuoti abonentui, 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 o 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] (toliau – 2010 m. kovo 5 d. dekretas)], <…> priedo 2°punkte nurodytą informaciją.

<…>“

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

19. CPI R. 335-5 straipsnyje nustatyta:

„I.– Akivaizdžiu aplaidumu, už kurį baudžiama bauda, numatyta už penktosios kategorijos pažeidimus, laikoma veika, kai asmuo turi 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.“

20. 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, nekyla suinteresuotojo asmens baudžiamosios atsakomybės. <…>“

2. 2010 m. kovo 5 d. dekretas

21. 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;

<…>“

22. 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.“

23. 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, gauti 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 elektroninių ryšių kodeksas

24. *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas), iš dalies pakeisto 2021 m. liepos 30 d. *Loi n° 2021-998* (Įstatymas Nr. 2021-998)[5] 17 straipsniu, L. 34-1 straipsnio II bis dalyje nustatyta:

„[E]lektroninių ryšių operatoriai privalo saugoti:

1° informaciją apie naudotojo civilinę tapatybę, kai to reikia baudžiamosiose bylose, taip pat siekiant užkirsti kelią grėsmei visuomenės saugumui ir užtikrinti nacionalinį saugumą – penkerius metus nuo naudotojo sutarties galiojimo pabaigos;

2° tais pačiais tikslais, kaip ir nurodytieji šio IIbis 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 šio kodekso 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. ir kt.*) *Conseil constitutionnel* (Konstitucinė Taryba, Prancūzija) pripažino, kad minėto kodekso ankstesnės redakcijos 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. Procesas Teisingumo Teisme

25. Atsiliepdami į Europos Sąjungos Teisingumo Teismo statuto 23 straipsnyje nurodytiems suinteresuotiesiems asmenims skirtą kvietimą, ieškovai pagrindinėje byloje, Prancūzijos, Danijos, Estijos, Airijos, Nyderlandų, Suomijos, Švedijos vyriausybės ir Europos Komisija atsakė į Teisingumo Teismo raštu pateiktus klausimus.

26. Tos pačios šalys, išskyrus Suomijos vyriausybę, Čekijos, Ispanijos, Kipro, Latvijos ir Norvegijos vyriausybės, taip pat EDAPP ir ENISA dalyvavo 2023 m. gegužės 15 d. posėdyje.

IV. Analizė

27. Išnagrinėjęs prejudicinius klausimus, savo pirmojoje išvadoje pasiūliau Teisingumo Teismui nuspręsti, kad Direktyvos 2002/58 15 straipsnio 1 dalis turi būti aiškinama taip, kad pagal ją nedraudžiami nacionalinės teisės aktai, pagal kuriuos elektroninių ryšių paslaugų teikėjams leidžiama saugoti, o tokiai administracinei institucijai, kaip *Hadopi*[6], gauti prieigą tik prie civilinės tapatybės duomenų, atitinkančių IP adresus, kad ši institucija galėtų nustatyti šių adresų turėtojus, įtariamus padarius autorių teisių ir gretutinių teisių 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.

28. Šioje išvadoje bandysiu išsamiau išnagrinėti tam tikrus mano ankstesnės analizės elementus ir per 2023 m. gegužės 15 d. įvykusį teismo posėdį aptartus klausimus, kad išdėstyčiau priežastis, dėl kurių toliau laikausi tiek savo pasiūlymo atsakyti į prejudicinius klausimus, tiek jį lėmusių argumentų[7].

29. Konkrečiau kalbant, įrodysiu, kad tai, jog be išankstinės kontrolės leidžiama saugoti ir gauti prieigą prie IP adresus atitinkančių civilinės tapatybės duomenų, siekiant nustatyti pažeidėjus, kai šie duomenys yra vienintelė priemonė juos identifikuoti, atitinka Teisingumo Teismo nustatytus reikalavimus, nagrinėjant priemones, kurių imamasi pagal
Direktyvos 2002/58 15 straipsnio 1 dalį (B dalis).

[6] 2022 m. sausio 1 d. *Conseil supérieur de l'audiovisuel* (Vyriausioji garso ir vaizdo transliacijų taryba) (CSA) ir *Hadopi* tapo *Autorité de régulation de la communication audiovisuelle et numérique* (Audiovizualinių ir skaitmeninių ryšių reguliavimo institucija) (*Arcom*). Vis dėlto atsižvelgdamas į laikotarpį, per kurį susiklostė pagrindinės bylos faktinės aplinkybės, šioje išvadoje naudosiu *Hadopi* pavadinimą.

[7] Šiuo klausimu taip pat laikausi savo pasiūlymo performuluoti prejudicinius klausimus ir savo supratimo apie jų dalyką. Iš tikrųjų, nors prejudicinių klausimų formuluotėse minima tik prieiga prie IP adresus atitinkančių civilinės tapatybės duomenų, vis dėlto prieigos prie šių duomenų klausimas neatsiejamas nuo klausimo, susijusio su elektroninių ryšių paslaugų teikėjų vykdomu jų saugojimu, todėl saugojimo suderinamumo su Sąjungos teise analizė yra būtina prieigos suderinamumo su Sąjungos teise sąlyga. Šiuo klausimu žr. mano pirmosios išvados 45 ir paskesnius punktus. Be to, nors prejudiciniuose klausimuose kalbama apie „IP adresą atitinkančius civilinės tapatybės duomenis“, juos reikia suprasti kaip susijusius ir su prieiga prie IP adresų, leidžiančių nustatyti prisijungimo šaltinį. Šiuo klausimu žr. mano pirmosios išvados 41 ir paskesnius punktus.

30. Tai darydamas pabrėžiu, kad toks sprendimas reiškia ne griežtos ir pagrindinių teisių apsaugą užtikrinančios Teisingumo Teismo jurisprudencijos, suformuotos sprendimuose *Tele2 Sverige ir Watson ir kt.*[8] bei *La Quadrature du Net ir kt.*[9], pakeitimą, o būtiną jos plėtrą, kuri, mano nuomone, atitinka Teisingumo Teismo nustatytus principus. Šis skirtumas nėra vien semantinis. Iš tikrųjų mano siūlomu sprendimu siekiama ne paneigti esamą jurisprudenciją, o siekiant tam tikro pragmatiškumo, – leisti ją pritaikyti ypatingoms ir labai griežtai apibrėžtoms aplinkybėms (C dalis).

31. Siekdamas aiškumo ir kadangi per teismo posėdį vykusios diskusijos parodė, kad reikia patikslinimų šiuo klausimu, savo analizę pradėsiu primindamas, kaip veikia *Hadopi* taikomas laipsniško reagavimo mechanizmas (A dalis).

A. Hadopi taikomas laipsniško reagavimo mechanizmas

32. *Hadopi* yra nepriklausoma administracinė institucija, atsakinga už autorių teisių ir gretutinių teisių apsaugą nuo šių teisių pažeidimų internete. Šiuo tikslu buvo sukurtas vadinamasis „laipsniško reagavimo“ mechanizmas, kurio įgyvendinimas patikėtas *Hadopi* Teisių apsaugos komitetui.

33. Į šį komitetą kreipiasi teisių turėtojų organizacijos, kuriose kai kurie prisiekusieji ir Kultūros ministro patvirtinti atstovai lygiarangių (*peer-to-peer*) tinkluose renka interneto naudotojų, kurie be teisių turėtojų leidimo padaro kūrinius viešai prieinamus, IP adresus. Tada surašomi protokolai. Juose, be kita ko, nurodomas interneto prieigos, naudotos šiems autorių teisių pažeidimams padaryti, IP adresas, nustatyto pažeidimo data ir laikas, taip pat nagrinėjamo kūrinio pavadinimas ir jie perduodami *Hadopi* teisių apsaugos komitetui. Šiuo klausimu reikia pabrėžti, kad, kaip pažymėjo EDAPP, leidimą asmens duomenų tvarkymui, kurį atlieka teisių turėtojų organizacijų atstovai, išduoda *Commission nationale de l'informatique et des libertés* (Nacionalinė informatikos ir laisvių komisija, CNIL) – Prancūzijos duomenų apsaugos priežiūros institucija[10].

34. Gavusi protokolus ir atlikusi automatizuotą patikrinimą, kuriuo siekiama užtikrinti, kad juose būtų visi reikalaujami duomenys, *Hadopi* teisių apsaugos komitetas gali iš elektroninių ryšių paslaugų teikėjų gauti abonento, kuriuo buvo pasinaudota autorių teisių pažeidimui, tapatybę, pašto adresą, el. pašto adresą ir telefono numerius.

35. Tuomet *Hadopi* gali pateikti šiam asmeniui „rekomendaciją“, kuria šis asmuo informuojamas, kad jo prieiga prie interneto buvo naudojama pažeidžiant autorių teises, ir kuria asmuo, kaip įtariama neįvykdęs jam tenkančios rūpestingumo pareigos, įpareigojamas užtikrinti, kad internete būtų paisoma autorių teisių ar gretutinių teisių saugomų kūrinių. Kitaip tariant, rekomendacija skiriama interneto prieigos turėtojui, o jis faktiškai gali būti kitas asmuo nei tas, kuris padarė kūrinį prieinamą, pažeisdamas autorių teises. Antra rekomendacija gali būti pateikta antrą kartą konstatavus autorių teisių pažeidimą naudojantis ta pačia interneto prieiga. Pakartotinių pažeidimų atveju *Hadopi* teisių apsaugos komitetas gali nuspręsti kreiptis į Respublikos prokurorą baudžiamojo persekiojimo tikslais. Šiuo klausimu, kaip Prancūzijos

8 2016 m. gruodžio 21 d. sprendimas (C-203/15 ir C-698/15, EU:C:2016:970, toliau – Sprendimas *Tele2*).

9 2020 m. spalio 6 d. sprendimas (C-511/18, C-512/18 ir C-520/18, EU:C:2020:791, toliau – Sprendimas *La Quadrature du Net ir kt.*).

10 Šiuo klausimu žr. 2010 m. birželio 10 d. CNIL nutarimą Nr. 2010-225, kuriuo iš dalies keičiamas *Société des auteurs, compositeurs et éditeurs de musique* (Kompozitorių ir muzikos leidėjų bendrija, SACEM) suteikiamas leidimas vykdyti asmens duomenų tvarkymą siekiant tirti ir registruoti autorių teisių pažeidimus, padarytus keitimosi failais tinkluose, vadinamuose „peer to peer“ (leidimas Nr. 1425421).

vyriausybė nurodė pirmose savo pastabose, *Hadopi* tarnautojai, atsakingi už laipsniško reagavimo mechanizmą, yra prisiekę ir *Hadopi* prezidento įgalioti tarnautojai, jie privalo saugoti profesinę paslaptį ir yra vieninteliai *Hadopi* darbuotojai, galintys susipažinti su pagal šį mechanizmą tvarkomais asmens duomenimis.

36. Šiuo klausimu reikia pažymėti, kad renkami ir *Hadopi* perduodami ne visų lygiarangių tinklų naudotojų duomenys, kai jie tik parsisiunčia tokį turinį[11], o tik asmenų, kurie, pažeisdami autorių teises, padarė šį turinį prieinamą, t. y. *įkėlė* tokį turinį, duomenys.

37. Pavyzdžiui, 2021 m. *Hadopi* gavo beveik keturi milijonai protokolų iš teisių turėtojų organizacijų, išsiuntė 210 595 pirmąsias rekomendacijas ir 53 564 antrąsias rekomendacijas, o 1 484 atvejais kreipėsi į Respublikos prokurorą.

38. Priminęs šią informaciją, parodysiu, kodėl manau, kad toks mechanizmas, kuriuo užtikrinamas IP adresus atitinkančių civilinės tapatybės duomenų saugojimas ir prieiga prie jų, atitinka jurisprudencijoje nustatytus reikalavimus, susijusius su nacionalinėmis priemonėmis, kurių imamasi pagal Direktyvos 2002/58 15 straipsnio 1 dalį.

B. Teisingumo Teismo jurisprudencijoje, susijusioje su Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimu, nustatytų reikalavimų laikymasis

39. Kadangi savo pirmoje išvadoje priminiau Teisingumo Teismo jurisprudenciją, susijusią su prisijungimo šaltiniui priskirtų IP adresų saugojimu ir prieiga prie jų[12], šioje išvadoje sutelksiu dėmesį į tai, kas, mano nuomone, sudaro šios jurisprudencijos esmę, t. y. pirma, proporcingumo reikalavimą ir, antra, kiek tai susiję su prieiga prie šių duomenų, galimai būtiną išankstinę kontrolę, kurią atliktų teismas ar nepriklausoma administracinė institucija.

1. Dėl nagrinėjamų priemonių proporcingumo

40. Siekiant nustatyti IP adresą atitinkančių civilinės tapatybės duomenų saugojimo ar prieigos prie jų priemonės suderinamumą su Sąjungos teise, reikia, kaip ne kartą pabrėžė Teisingumo Teismas, suderinti įvairius nagrinėjamus teisėtus interesus ir teises, t. y. pirma, Chartijos 7 ir 8 straipsniuose garantuojamas teises į privataus gyvenimo apsaugą ir asmens duomenų apsaugą[13] ir, antra, kitų asmenų teisių ir laisvių bei Chartijos 3, 4, 6 ir 7 straipsniuose įtvirtintų teisių apsaugą[14]. Pridursiu, kad nagrinėjamoje byloje teisės į privataus gyvenimo apsaugą ir asmens duomenų apsaugą taip pat turi būti suderinamos su Chartijos 17 straipsnyje įtvirtinta teise į nuosavybę, nes laipsniško reagavimo mechanizmu *in fine* siekiama apsaugoti autorių teises ir gretutines teises.

[11] Dėl lygiarangių tinklų veikimo ir įvairių interneto naudotojų profilių šiuose tinkluose žr. mano išvadą byloje *M.I.C.M.* (C-597/19, EU:C:2020:1063, 37 ir paskesni punktai).

[12] Mano pirmosios išvados 53 ir paskesni punktai.

[13] Direktyvos 2002/58 kontekste teisės į privataus gyvenimo apsaugą ir asmens duomenų apsaugą pasireiškia joje įtvirtintais pranešimų konfidencialumo ir draudimo saugoti su jais susijusius duomenis principais.

[14] Sprendimas *La Quadrature du Net ir kt.* (120–122, 127 ir 128 punktai), 2022 m. balandžio 5 d. Sprendimas *Commissioner of An Garda Síochána ir kt.* (C-140/20, EU:C:2022:258, 48 ir 50 punktai; toliau – Sprendimas *Commissioner of An Garda Síochána ir kt.*) ir 2022 m. rugsėjo 20 d. Sprendimas *SpaceNet ir Telekom Deutschland* (C-793/19 ir C-794/19, EU:C:2022:702, 63 ir 65 punktai; toliau – Sprendimas *SpaceNet ir Telekom Deutschland*).

41. Šiuo klausimu Teisingumo Teismas patikslino, kad dėl tokio suderinimo, atliekamo pagal Direktyvos 2002/58 15 straipsnio 1 dalį, valstybės narės gali imtis nuo konfidencialumo principo nukrypstančios priemonės, kai tokia priemonė yra „*būtina, tinkama ir adekvati* demokratinės visuomenės [proporcinga demokratinėje visuomenėje] priemonė“ (kursyvu išskirta mano). Šios direktyvos 11 konstatuojamojoje dalyje patikslinama, kad tokio pobūdžio priemonė turi „griežtai“ *atitikti* siekiamą tikslą [15].

42. Be to, Teisingumo Teismas remiasi proporcingumo principu visuose savo argumentuose, susijusiuose su Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimu, todėl jis yra pagal šią nuostatą priimtos nacionalinės asmens duomenų saugojimo ar prieigos prie jų priemonės nagrinėjimo raktas.

43. Išsamiau nagrinėjant šiuos argumentus matyti, kad proporcingumo principas, kiek tai susiję su Direktyvos 2002/58 15 straipsnio 1 dalimi, apima įvairius aspektus, siejamus, pirma, su pagrindinių teisių suvaržymo dėl srauto duomenų saugojimo ar prieigos prie jų dydžiu ir, antra, su nagrinėjamos priemonės būtinumu.

44. Dėl *Hadopi* atliekamo IP adresus atitinkančių civilinės tapatybės duomenų saugojimo ir prieigos prie jų laikausi nuomonės, kad tiek dėl suvaržymo dydžio, tiek dėl šių duomenų būtinumo Teisingumo Teismas turėtų pakoreguoti nacionalinės priemonės, priimtos pagal Direktyvos 2002/58 15 straipsnio 1 dalį, proporcingumo nagrinėjimą.

a) Santykinis pagrindinių teisių suvaržymo dydis

45. Iš Teisingumo Teismo suformuotos jurisprudencijos aiškiai matyti, kad, remiantis proporcingumo principu, pagal Direktyvos 2002/58 15 straipsnio 1 dalį priimta priemone siekiamo tikslo svarba turi būti vertinama atsižvelgiant į dėl to atsirandančio suvaržymo dydį [16].

46. Kalbant konkrečiau, kaip pabrėžiau savo pirmoje išvadoje, Teisingumo Teismas nusprendė, 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 kvalifikuojami kaip „sunkūs“ [17].

47. Dėl IP adresų Teisingumo Teismas pažymi, kad nors jie yra mažiau jautrūs nei kiti srauto duomenys, jų saugojimas ir analizė vis dėlto yra didelis pagrindinių teisių suvaržymas, nes jie gali būti naudojami išsamiam interneto naudotojo naršymo maršrutui atsekti, taigi, ir išsamiam šio interneto naudotojo profiliui nustatyti bei tikslioms išvadoms apie jo privatų gyvenimą padaryti [18].

[15] Sprendimas *La Quadrature du Net ir kt.* (129 punktas), Sprendimas *Commissioner of An Garda Síochána ir kt.* (51 punktas) ir Sprendimas *SpaceNet ir Telekom Deutschland* (66 punktas).

[16] Sprendimai *Commissioner of An Garda Síochána ir kt.* (56 punktas)ir *SpaceNet ir Telekom Deutschland* (71 punktas).

[17] Sprendimas *Tele2* (115 punktas); 2018 m. spalio 2 d. Sprendimas *Ministerio Fiscal* (C-207/16, EU:C:2018:788, 56 punktas) ir 2021 m. kovo 2 d. Sprendimas *Prokuratuur (Prieigos prie elektroninių ryšių duomenų sąlygos)* (C-746/18, EU:C:2021:152, 33 punktas; toliau – Sprendimas *Prokuratuur*). Taip pat žr. mano pirmosios išvados 92 punktą.

[18] Žr. sprendimus *La Quadrature du Net ir kt.* (152 ir 153 punktai); *Commissioner of An Garda Síochána ir kt.* (73 punktas) bei *SpaceNet ir Telekom Deutschland* (103 punktas). Taip pat žr. mano pirmosios išvados 63, 64 ir 93 punktus.

48. Pagrindinėje byloje civilinės tapatybės duomenų, atitinkančių IP adresus, saugojimas ir prieiga prie jų skirti kovai su autorių teisių ir gretutinių teisių pažeidimais. Vis dėlto, mano nuomone, aišku, kad net jei šie pažeidimai būtų vykdomi masiškai, ši kova negali būti laikoma kova su sunkiais nusikaltimais[19]. Taigi egzistuoja atotrūkis tarp pagrindinių teisių suvaržymo, kurį lemia nagrinėjama priemonė, ir ja siekiamo tikslo.

49. Pirmoje išvadoje, remdamasis Teisingumo Teismo jurisprudencija, laikiausi nuomonės, kad *Hadopi* prieiga prie IP adresą atitinkančių civilinės tapatybės duomenų yra didelis pagrindinių teisių suvaržymas. Nors taip pat laikiausi nuomonės, kad nagrinėjamoje byloje vis dėlto turi būti leidžiama saugoti šiuos duomenis ir turėti prieigą prie jų, po teismo posėdžio turiu kai ką patikslinti.

50. Taikant laipsniško reagavimo mechanizmą *Hadopi* gali susieti teisių turėtojų organizacijų nurodytą asmens, įtariamo tuo, kad pasinaudojo interneto prieiga, kad pažeistų autorių teises lygiarangių tinkle, IP adresą su šio asmens civilinės tapatybės duomenimis, ir rinkmenos, įkeltos pažeidžiant autorių teises, ištrauka. Kaip per posėdį pažymėjo Komisija ir EDAPP, nors remiantis tokia informacija tikrai galima gauti daugiau informacijos nei vien apie įtariamo pažeidėjo tapatybę, vis dėlto negalima daryti labai konkrečių išvadų apie šio asmens privatų gyvenimą. Iš tikrųjų, kaip nurodžiau savo pirmojoje išvadoje[20], taip tik atskleidžiamas faktas, kad konkrečiu momentu buvo peržiūrėtas tam tikras turinys, o toks atskleidimas, vertinamas atskirai, nėra pagrindas išsamiai apibrėžti tokią peržiūrą atlikusio asmens profilį.

51. Taip yra juo labiau dėl to, kad, pirma, didžioji dauguma *Hadopi* pateiktų IP adresų yra vadinamieji „dinamiški“ IP adresai, kurie dėl savo pobūdžio keičiasi ir konkrečią tapatybę atitinka tik tam tikru momentu, kuris sutampa su nagrinėjamo turinio pateikimu. Vadinasi, jais remiantis negali būti atliekama jokio išsamaus sekimo.

52. Be to, turiu pabrėžti, kad man neatrodo, jog remiantis pagrindinių teisių apsauga internete pateisinama tai, kad negalima susipažinti su IP adresu, kūrinio turiniu ir asmens, kuris šį kūrinį padarė prieinamą pažeisdamas autorių teises, tapatybės duomenimis, tokia apsauga tik reiškia, kad turi būti taikomos su šių duomenų saugojimu ir prieiga prie jų susijusios garantijos. Manau, kad šiuo klausimu iškalbinga analogija su realiuoju pasauliu: asmuo, įtariamas įvykdęs vagystę, negali remtis savo teise į privataus gyvenimo apsaugą, siekdamas, kad persekiojimą už šį nusikaltimą vykdantys asmenys negalėtų susipažinti su pavogtu turiniu. Vis dėlto šis asmuo gali pagrįstai remtis savo pagrindinėmis teisėmis, siekdamas, kad vykstant procesui būtų užkirstas kelias susipažinti su daugiau duomenų nei vien duomenimis, reikalingais tariamam pažeidimui nustatyti.

53. Galiausiai pažymėtina, kad, priešingai, nei teigia pareiškėjos, neatrodo, jog laipsniškas reagavimo mechanizmas reiškia visuotinę lygiarangių tinklų naudotojų stebėseną. Iš tikrųjų reikia ne patikrinti visą jų veiklą konkrečiame tinkle siekiant nustatyti, ar jie padarė kūrinį prieinamą pažeisdami autorių teises, o veikiau, pasinaudojant rinkmena, kuria buvo pažeistos autorių teisės, nustatyti interneto prieigos, iš kurios interneto naudotojas padarė kūrinį prieinamą, pažeisdamas autorių teises, turėtoją. Be to, kaip per posėdį pabrėžė EDAPP, turi būti stebima ne visų lygiarangių tinklų naudotojų, o tik asmenų, įkeliančių autorių teises pažeidžiančias rinkmenas,

[19] Pirmojoje išvadoje nurodžiau, kad sąvoka „sunkus nusikaltimas“ turėtų būti aiškinama savarankiškai, siekiant neleisti valstybėms narėms apeiti Direktyvos 2002/58 15 straipsnio 1 dalyje nustatytų reikalavimų. Aš ir toliau laikausi šios pozicijos. Vis dėlto reikia pabrėžti, kad net jei Teisingumo Teismas nuspręstų, jog sąvoka „sunkus nusikaltimas“ yra palikta valstybėms narėms, ji bet kuriuo atveju turėtų būti nustatyta neperžengiant Sąjungos teisės ribų ir negali būti išplėsta taip, kad ši nuostata netektų prasmės.

[20] Mano pirmosios išvados 101 punktas.

veikla, juo labiau kad tokių rinkmenų įkėlimas yra mažiau susijęs su asmens privačiu gyvenimu, nes rinkmenos gali būti įkeliamos tik tam, kad šie interneto naudotojai vėliau galėtų parsisiųsti kitas rinkmenas.

54. Šiomis aplinkybėmis nemanau, kad priežastys, dėl kurių Teisingumo Teismas IP adresų saugojimą ir prieigą prie jų laikė dideliu pagrindinių teisių suvaržymu, gali būti taikomos tokio laipsniško reagavimo mechanizmo, kokį taiko *Hadopi*, atveju. Darytina išvada, kad nagrinėjant proporcingumo principą reikėtų patikslinti suvaržymo, kurį lemia šis saugojimas ir ši prieiga, dydį.

55. Kitaip tariant, laikausi nuomonės, kad Teisingumo Teismo jurisprudenciją, susijusią su pagrindinių teisių suvaržymo dėl IP adresų saugojimo ir prieigos prie jų dydžiu, reikia aiškinti kaip reiškiančią, kad šis suvaržymas yra didelis suvaržymas ne visada, o tik tuo atveju, kai IP adresai gali lemti išsamų interneto naudotojo naršymo maršruto atsekimą ir leisti padaryti labai tikslias išvadas apie jo privatų gyvenimą.

56. Kadangi pagrindinėje byloje nagrinėjamoje situacijoje taip nėra, iš to matyti, kad suvaržymą, kurį lemia civilinės tapatybės duomenų, atitinkančių IP adresą, naudojamą siekiant padaryti prieinamą autorių teises pažeidžiantį turinį, saugojimas ir prieiga prie jų, turi būti galima pateisinti siekiant kovoti su platesnio masto, o ne vien su sunkiais, nusikaltimais.

57. Be to, pažymiu, kad pagrindinių teisių suvaržymo, kurį lemia IP adresą atitinkančių civilinės tapatybės duomenų saugojimas ir prieiga prie jų esant tokiai situacijai, kokia nagrinėjama pagrindinėje byloje, dydžio nekeičia tai, kad interneto prieigos, naudotos teises pažeidžiančiam turiniui padaryti prieinamą, turėtojas nebūtinai yra šio kūrinio padarymo prieinamo šaltinis, todėl, remiantis *Hadopi* pateikta rekomendacija, minėtas turinys, su kuriuo galėjo susipažinti trečioji šalis, galėtų būti atskleistas šiam teisių turėtojui. Pirma, primenu, kad *Hadopi* tiriamas pažeidimas yra pareigos užtikrinti, kad prieiga nebūtų naudojama siekiant padaryti turinį prieinamą pažeidžiant autorių teises, nevykdymas. Taigi būtina, kad informacija, kuria remiantis galima pažeidimą kvalifikuoti, būtų perduota tariamam pažeidėjui. Antra, kaip jau nurodžiau, manau, kad informacija apie nagrinėjamą kūrinį nėra pagrindas daryti tikslias išvadas apie asmens, kuris padarė kūrinį prieinamą, privatų gyvenimą. Taigi galimas šios informacijos perdavimas interneto prieigos turėtojui neviršija to, kas būtina, kad būtų galima patraukti atsakomybėn už nagrinėjamą autorių teisių pažeidimą.

b) Nagrinėjamų duomenų būtinumas, siekiant nustatyti nusikalstamą veiką ir patraukti atsakomybėn už ją

58. Siekiant užtikrinti pagal Direktyvos 2002/58 15 straipsnio 1 dalį nustatytos srauto duomenų, kaip antai IP adresą atitinkančių civilinės tapatybės duomenų, saugojimo ir prieigos prie jų priemonės proporcingumą, pagal Teisingumo Teismo jurisprudenciją reikia, kad suvaržymas, kurį ji suponuoja, neviršytų to, kas griežtai būtina siekiamam tikslui įgyvendinti[21]. Man atrodo, kad pagrindinėje byloje nagrinėjamos priemonės atveju yra būtent taip.

[21] Sprendimai *La Quadrature du Net ir kt.* (120–122 ir 132 punktai), *Commissioner of An Garda Síochána ir kt.* (48 ir 54 punktai) ir *SpaceNet ir Telekom Deutschland* (63 ir 69 punktai).

59. Kaip nurodžiau savo pirmojoje išvadoje [22], iš Teisingumo Teismo jurisprudencijos matyti, kad jei pažeidimas padaromas tik internetu, IP adresas gali būti vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam šis adresas buvo priskirtas šio pažeidimo padarymo metu [23]. Mano požiūriu, iš to matyti, kad IP adresus atitinkančių civilinės tapatybės duomenų saugojimas ir prieiga prie jų, siekiant nustatyti internete padarytus autorių teisių pažeidimus ir patraukti už juos atsakomybėn, pagal jurisprudenciją yra griežtai būtini siekiamam tikslui įgyvendinti.

60. Tiesa, kad bet koks asmens duomenų apsaugos reikalavimas reiškia tyrimo įgaliojimų apribojimą. Tai matyti iš paties priešingų interesų derinimo principo ir toks rezultatas negali būti ginčijamas. Vis dėlto situacija, kai IP adresas yra vienintelė priemonė nustatyti asmenį, kuris įtariamas padaręs intelektinės nuosavybės teisės pažeidimą internete, skiriasi nuo daugumos baudžiamojo persekiojimo atvejų, dėl kurių Teisingumo Teismas pažymi, kad „veiksmingumas paprastai priklauso ne nuo vienos, bet nuo visų tyrimo priemonių, kurias šiuo tikslu gali taikyti kompetentingos nacionalinės valdžios institucijos“ [24]. Pripažinus, kad tokiu atveju, kaip nagrinėjamas pagrindinėje byloje, IP adresus atitinkantys civilinės tapatybės duomenys neturėtų būti saugomi ir prieiga prie jų neturėtų būti suteikta, būtų ne tiesiog apriboti tyrimo įgaliojimai, kaip nutinka taikant bet kurią srauto duomenų apsaugos priemonę, o iš nacionalinių institucijų atimta vienintelė priemonė nustatyti tam tikras nusikalstamas veikas ir patraukti už jas atsakomybėn.

61. Kitaip tariant, remiantis mano siūlomu Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimu, nagrinėjant tokios priemonės būtinumą, nereikia leisti saugoti ir gauti prieigą prie duomenų, kurie tik *palengvina* pažeidimų atskleidimą ir persekiojimą už juos, kai šiuos pažeidimus taip pat galima nustatyti ir patraukti už juos atsakomybėn, pasitelkiant konkuruojančias, net ir mažiau veiksmingas, priemones. Vis dėlto kyla klausimas, ar galima šiuos duomenis saugoti ir suteikti prieigą prie jų, kai jie yra *būtini* asmeniui, įtariamam padarius nusikalstamą veiką, nustatyti, kai be šių priemonių jo nebūtų galima patraukti atsakomybėn, nes tuo atveju, kai pažeidimas daromas tik internete, aptariami duomenys yra vienintelė priemonė nustatyti interneto naudotojo tapatybę.

62. Mano nuomone, reikia vadovautis tokiu aiškinimu, nebent būtų pripažinta, kad už daugelį nusikalstamų veikų niekada nebus galima patraukti atsakomybėn [25].

63. Iš viso to, kas išdėstyta, mano nuomone, matyti, kad nacionalinės teisės aktai, pagal kuriuos elektroninių ryšių paslaugų teikėjams leidžiama saugoti tik IP adresus atitinkančius civilinės tapatybės duomenis, o administracinei institucijai – suteikti prieigą tik prie šių duomenų, yra visiškai proporcingi siekiamam tikslui, t. y. persekioti už autorių teisių ir gretutinių teisių pažeidimus internete, nes su jais susijęs pagrindinių teisių suvaržymas yra riboto dydžio, o šie duomenys yra vienintelė tyrimo priemonė, leidžianti nustatyti asmens, kuriam šis adresas buvo suteiktas pažeidimo padarymo momentu, tapatybę.

64. Taigi laikausi nuomonės, kad Direktyvos 2002/58 15 straipsnio 1 dalis turi būti aiškinama kaip nedraudžianti tokių teisės aktų.

[22] Mano pirmosios išvados 78 punktas.

[23] Sprendimai *La Quadrature du Net ir kt.* (154 punktas), *Commissioner of An Garda Síochána ir kt.* (73 punktas) ir *SpaceNet ir Telekom Deutschland* (100 punktas).

[24] Sprendimas *Commissioner of An Garda Síochána ir kt.* (69 punktas).

[25] Mano pirmosios išvados 81 punktas. Šiuo klausimu taip pat žr. šios išvados 79 ir paskesnius punktus.

2. Dėl tinkamų materialinių ir procesinių garantijų buvimo

65. Kalbant konkrečiai apie prieigą prie IP adresus atitinkančių civilinės tapatybės duomenų, iš Teisingumo Teismo jurisprudencijos matyti, kad vien griežto priemonės proporcingumo nepakanka, kad ji būtų suderinama su Direktyvos 2002/58 15 straipsnio 1 dalimi.

66. Iš tikrųjų siekiant užtikrinti, kad prieiga prie srauto ir vietos nustatymo duomenų būtų apribota tuo, kas griežtai būtina, Teisingumo Teismas yra nusprendęs, jog labai svarbu, kad šiai prieigai būtų taikoma išankstinė kontrolė, kurią atliktų teismas arba nepriklausoma administracinė institucija, turintys visus įgaliojimus ir suteikiantys visas būtinas garantijas, kad būtų suderinti įvairūs nagrinėjami teisėti interesai ir teisės [26].

67. Taigi siauras jurisprudencijos aiškinimas reikštų, kad *Hadopi* prieigai prie asmenų, įtariamų pažeidus autorių teises internete, IP adresus atitinkančių civilinės tapatybės duomenų turėtų būti taikoma tokia išankstinė kontrolė, kokios tokiame laipsniško reagavimo mechanizme nėra.

68. Vis dėlto, kaip per teismo posėdį nurodė Airijos vyriausybė ir kaip nurodžiau savo pirmojoje išvadoje, laikausi nuomonės, kad teismo arba nepriklausomos administracinės institucijos išankstinės kontrolės reikalavimas nėra sisteminis reikalavimas ir kad, atsižvelgiant tiek į suvaržymo, kurį lemtų nagrinėjama priemonė, dydį, tiek į joje numatytas garantijas, jis priklauso nuo išsamesnės šios priemonės analizės.

69. Pabrėžiu, kad kiekviename Teisingumo Teismo sprendime, kuriame buvo išdėstytas šis teismo arba nepriklausomos administracinės institucijos išankstinės kontrolės reikalavimas, buvo nagrinėjami nacionalinės teisės aktai, pagal kuriuos suteikiama prieiga prie visų naudotojų srauto ir vietos nustatymo duomenų, susijusių su visomis naudotojų elektroninio ryšio priemonėmis [27] arba bent su identifikuotų naudotojų fiksuotojo ir mobiliojo ryšio telefonais [28].

70. Iš to darau išvadą, kad tokios išankstinės kontrolės reikalavimas grindžiamas aptariamose bylose nagrinėto suvaržymo dydžiu. Kaip pabrėžė Teisingumo Teismas, iš šių duomenų galima „padaryti tikslias ar net labai tikslias išvadas apie asmenų, kurių duomenys saugomi, privatų gyvenimą, kaip antai šių asmenų kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir lankomą socialinę aplinką“ [29]. Be to, buvo nurodyti asmenų, kurie jau buvo nustatyti ir, remiantis kitais požymiais, įtariami padarę pažeidimą, duomenys, taigi, nagrinėjami duomenys leido sustiprinti atitinkamo naudotojo kaltę patvirtinančius įrodymus, išplečiant su juo susijusių duomenų apimtį.

71. Kiek tai susiję su pagrindinėje byloje nagrinėjamais teisės aktais, kaip jau pažymėjau, suvaržymas, kurį lemia civilinės tapatybės duomenų ir IP adreso susiejimas, yra daug mažesnis nei tas, kurį lemia prieiga prie visų asmens srauto ir vietos nustatymo duomenų, nes jų susiejimas nesuteikia informacijos, leidžiančios daryti tikslias išvadas apie atitinkamo asmens privatų gyvenimą.

[26] Sprendimai *Tele2* (120 punktas); *Prokuratuur* (51 ir 52 punktai) bei *Commissioner of An Garda Síochána ir kt.* (106 ir 107 punktai).

[27] Sprendimai *Tele2* ir *Commissioner of An Garda Síochána ir kt.*

[28] Sprendimas *Prokuratuur*.

[29] Sprendimas *Prokuratuur* (36 punktas).

72. Be to, kaip pažymėjau savo pirmoje išvadoje [30], šie duomenys susiję tik su asmenimis, kurie, teisių turėtojų organizacijoms objektyviai nustačius, kad IP adresas naudojamas pažeidžiant autorių teises, atliko veiksmus, galimus kvalifikuoti kaip CPI L. 336-3 straipsnyje numatytos rūpestingumo pareigos pažeidimą. Tokie asmenys iš anksto nenustatomi kitomis priemonėmis, nes IP adreso susiejimas su civilinės tapatybės duomenimis yra vienintelė atitinkamo asmens tapatybės nustatymo priemonė. Taigi prieiga prie šių duomenų leidžia ne gauti papildomos ir tikslios informacijos apie remiantis kitais duomenimis jau įtariamų asmenų veiklą, kaip tai buvo anksčiau Teisingumo Teismo nagrinėtose bylose, o tik padaryti IP adresą, kuris kitu atveju būtų nereikšmingas, prieinamą. Šiomis aplinkybėmis duomenys, prie kurių *Hadopi* turi prieigą, *de facto* yra riboti.

73. Mano nuomone, prieiga prie pažeidimo padarymu įtariamo asmens duomenų, siekiant įrodyti jo kaltę, iš esmės skiriasi nuo galimybės atskleisti jau konstatuotą pažeidimą padariusio asmens tapatybę.

74. Mano nuomone, taip juo labiau yra dėl to, kad IP adresų rinkimui iš lygiarangių tinklų taikomas išankstinis leidimas, galiojantis tik šiems duomenims, taigi *Hadopi* niekada neturi neribotos apimties duomenų apie interneto naudotojus, kurie įtariami padarę autorių teisių pažeidimą internete [31].

75. Taigi, logika, kuria grindžiamas teismo arba nepriklausomos administracinės institucijos vykdomos išankstinės kontrolės reikalavimas, netaikoma tokiam laipsniško reagavimo mechanizmui, koks nagrinėjamas pagrindinėje byloje; toks reikalavimas man neatrodo būtinas siekiant užtikrinti, kad šio mechanizmo lemiamas pagrindinių teisių suvaržymas neviršytų to, kas griežtai būtina.

76. Iš viso to, kas išdėstyta, matyti, kad nacionalinės teisės aktai, pagal kuriuos nepriklausomai administracinei institucijai, kaip antai *Hadopi*, leidžiama saugoti ir turėti prieigą prie IP adresus atitinkančių civilinės tapatybės duomenų, kad būtų galima nustatyti šių adresų savininkus, įtariamus autorių teisių pažeidimais, ir šiai prieigai netaikoma išankstinė teismo ar nepriklausomos administracinės institucijos kontrolė, *in fine*, atitinka Teisingumo Teismo jurisprudencijoje įtvirtintus principus, kai šie duomenys yra vienintelė priemonė nustatyti asmens, kuriam pažeidimo padarymo metu buvo suteiktas IP adresas, tapatybę, todėl Direktyvos 2002/58 15 straipsnio 1 dalis turi būti aiškinama kaip nedraudžianti tokių teisės aktų.

77. Be šių pagrindinėje byloje nagrinėjamų argumentų, dar reikia pateikti bendresnes pastabas dėl būtinybės plėtoti Teisingumo Teismo jurisprudenciją.

C. Būtina ir ribota jurisprudencijos raida

78. Teisingumo Teismo jurisprudencijos, susijusios su tokių duomenų, kaip su civilinės tapatybės duomenimis susieti IP adresai, saugojimu ir prieiga prie jų, tobulinimas grindžiamas keliais argumentais.

[30] Mano pirmosios išvados 102 punktas.

[31] Šios išvados 33 punktas.

79. Pirma, kaip jau pažymėjau [32], pagrindinėje byloje nagrinėjamoje situacijoje IP adresą atitinkančių civilinės tapatybės duomenų gavimas yra vienintelė tyrimo priemonė, leidžianti nustatyti asmens, kuriam šis adresas buvo priskirtas nagrinėjamos nusikalstamos veikos padarymo momentu, tapatybę.

80. Iš to neišvengiamai matyti, kad jei Teisingumo Teismas nuspręstų, jog pagal Direktyvos 2002/58 15 straipsnio 1 dalį vis dėlto draudžiama juos saugoti ir suteikti prieigą prie jų, nacionalinės valdžios institucijos *de facto* netektų šios vienintelės identifikavimo priemonės, todėl niekada nebūtų galima patraukti atsakomybėn nagrinėjamą pažeidimą padariusių asmenų [33]. Dėl to savo pirmojoje išvadoje nurodžiau sisteminio nebaudžiamumo už šį pažeidimą galimybę [34].

81. Sisteminio nebaudžiamumo rizika neapsiriboja autorių teisių pažeidimais, padarytais lygiarangių tinkluose, bet, kaip per teismo posėdį teigė Čekijos vyriausybė, apima visas nusikalstamas veikas, vykdomas tik internete.

82. Iš tikrųjų būtų neįmanoma persekioti už pažeidimus, kuriuos padaręs asmuo gali būti identifikuotas tik pagal jo IP adresą, o atsakomybę už juos numatantys teisės aktai niekada negalėtų būti taikomi, jeigu būtų nuspręsta, kad tiek tokių duomenų saugojimas, tiek prieiga prie jų prieštarauja Sąjungos teisei.

83. Šiuo klausimu pažymiu, kad, kaip nurodė ieškovės pagrindinėje byloje, žinoma, jog teoriškai tam tikrų pažeidimų, daromų tik internete, vykdytojus būtų galima nustatyti kitais būdais. Jos nurodo, be kita ko, socialiniuose tinkluose naudojamą identifikatorių ir duomenis, susijusius su naudotojo paskyra, jo el. pašto adresą, telefono numerį arba informaciją apie privatų gyvenimą, kuriuos asmuo yra atskleidęs. Vis dėlto tam, kad tokie duomenys būtų susieti su asmens tapatybe, reikia atlikti išsamius tyrimus, per kuriuos tikrinama interneto naudotojo veikla internete. Taigi, man atrodo, kad naudojant tokias tyrimo priemones, kitaip nei vien IP adreso atveju, galima padaryti labai tikslias išvadas apie asmenų privatų gyvenimą, todėl tokių duomenų saugojimas ir prieiga prie jų prieštarautų Direktyvos 2002/58 15 straipsnio 1 daliai.

84. Šiomis aplinkybėmis prieiga prie civilinės tapatybės duomenų, atitinkančių interneto naudotojo IP adresą, iš tiesų yra ne vienintelė teorinė tyrimo priemonė, leidžianti nustatyti šio adreso turėtojo tapatybę pažeidimo padarymo momentu, o priemonė patraukti jį atsakomybėn, kartu kuo mažiau suvaržant jo pagrindines teises, taigi, ir priemonė, leidžianti išvengti visuotinio nebaudžiamumo.

85. Antra, dar kartą pabrėžiu, kad pasirinkus tokį sprendimą, mano nuomone, būtų galima suderinti dvi Teisingumo Teismo jurisprudencijos kryptis, tarp kurių esama tam tikro nesuderinamumo, nurodyto mano pirmojoje išvadoje [35] ir išvadoje byloje *M.I.C.M.* [36], t. y. pirma, jurisprudenciją, susijusią su duomenų saugojimu ir prieiga prie jų, ir, antra, jurisprudenciją, susijusią su IP adresų, priskirtų ryšio šaltiniui, perdavimu nagrinėjant privačių asmenų pareikštus ieškinius dėl intelektinės nuosavybės teisių apsaugos.

[32] Šios išvados 59 punktas.

[33] Šios išvados 62 punktas.

[34] Mano pirmosios išvados 78 ir paskesni punktai.

[35] Mano pirmosios išvados 69 ir paskesni punktai.

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

86. Trečia, nors nuo tada, kai buvo priimti sprendimai *Tele2* ir *La Quadrature du Net ir kt.*, Teisingumo Teismo jurisprudencija turi būti vertinama teigiamai, nes ja remiantis pavyko sukurti elektroninių ryšių paslaugų naudotojų pagrindinių teisių apsaugos sistemą, jai vis dėlto būdinga tam tikra kazuistika. Iš tikrųjų nagrinėdamas jam pateiktas bylas Teisingumo Teismas laipsniškai tobulino savo jurisprudenciją, kurioje, atsižvelgdamas į Direktyvos 2002/58 15 straipsnio 1 dalį, turėjo progą išnagrinėti įvairius nacionalinės teisės aktus. Vis dėlto Teisingumo Teismas praktiškai negali iš anksto numatyti visų priemonių, kurios galėtų būti analizuojamos remiantis šia nuostata. Tai patvirtina ir prašymų priimti prejudicinį sprendimą [37], kurie dėl šios nuostatos buvo pateikti priėmus Sprendimą *Tele2*, skaičius, kuris, mano nuomone, rodo, kad nacionaliniams teismams sudėtinga pritaikyti Teisingumo Teismo jurisprudencijoje įtvirtintus principus situacijoms, kurios skiriasi nuo tų, dėl kurių buvo priimti atitinkami sprendimai [38].

87. Iš to matyti, kad, mano požiūriu, tais atvejais, kai Teisingumo Teismas nagrinėja priemones, kurių nebuvo galima numatyti ankstesniuose sprendimuose, kaip antai teisės aktus, susijusius su nusikalstamomis veikomis, už kurias gali būti persekiojama tik tuo atveju, jeigu IP adresus atitinkantys civilinės tapatybės duomenys yra saugomi ir prieinami, kurių Teisingumo Teismas iki šiol niekada nebuvo nagrinėjęs, būtinas tam tikras lankstumas.

88. Taigi, kaip teigė Danijos vyriausybė, reikia ne peržiūrėti Teisingumo Teismo jurisprudenciją, o pripažinti, kad, remiantis principais, kuriais ji grindžiama, labai ribotomis aplinkybėmis galima priimti labiau diferencijuotą sprendimą.

89. Iš tiesų pagal mano siūlomą Direktyvos 2002/58 15 straipsnio 1 dalies išaiškinimą IP adresus atitinkančių civilinės tapatybės duomenų saugojimas ir prieiga prie jų leidžiami tik tiek, kiek tai susiję su patraukimu atsakomybėn už pažeidimus, kurių vykdytojai, nesant šių duomenų, negalėtų būti identifikuoti. Taigi jis taikytinas tik pažeidimams, padaromiems išimtinai internete, ir juo nepaneigiami jurisprudencijoje nurodyti sprendimai, susiję su platesniu duomenų saugojimu ir platesne prieiga prie jų, kuriais siekiama kitų tikslų.

[37] 2018 m. spalio 2 d. sprendimai *Ministerio Fiscal* (C-207/16, EU:C:2018:788); *La Quadrature du Net ir kt.*; *Prokuratuur*; *Commissioner of An Garda Síochána ir kt.* bei *SpaceNet ir Telekom Deutschland*.

[38] Tai, kad daugėja prašymų priimti prejudicinį sprendimą dėl Direktyvos 2002/58 15 straipsnio 1 dalies išaiškinimo, taip pat gali reikšti tam tikrą nacionalinių teismų nenorą taikyti Teisingumo Teismo nustatytus principus situacijoms, kurios yra šiek tiek skirtingos dėl nacionalinės teisės sistemų ypatumų. Šiuo klausimu žr., be kita ko, I. Cameron „Metadata retention and national security: Privacy international and La Quadrature du Net“, *Common Market Law Review*, 2021, t. 58, Nr. 5, p. 1433–1471; arba B. Bertrand „L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?“ („Netaktiška drąsa: kiek per toli gali nueiti Teisingumo Teismas?“), *Dalloz IP/IT*, 2021, Nr. 9, p. 468–472. Todėl man atrodo dar svarbiau, kad, siekiant palaikyti sėkmingą Teisingumo Teismo ir valstybių narių teismų dialogą, Teisingumo Teismas galėtų prisitaikyti, kai to reikalauja aplinkybės. Kaip pažymėjo doktrinos autoriai, Teisingumo Teismo jurisprudencijoje nustatytas aukštas apsaugos standartas iš tikrųjų negali būti veiksmingai taikomas be nacionalinių teismų, kurie pirmiausia atsakingi už jo įgyvendinimą, indėlio. Šiuo klausimu žr., be kita ko, J. Teyssedre „Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*“, *Common Market Law Review*, t. 60, Nr. 2, 2023, p. 569–588; ir J. Sirinelli „La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite“ („Teisingumo Teismo vykdoma prisijungimo duomenų apsauga: naujos Europos jurisprudencijos kartografija“), *Revue trimestrielle de droit européen*, t. 57, Nr. 2, 2021, p. 313–329.

V. Išvada

90. 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), iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, 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 tokius 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 asmenis, kuriems pažeidimo padarymo metu buvo priskirtas toks adresas.