Teismo praktikos rinkinys

GENERALINIO ADVOKATO
MANUEL CAMPOS SÁNCHEZ-BORDONA IŠVADA,
pateikta 2020 m. sausio 15 d.[1]

Byla C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
prieš
Conseil des ministres,
dalyvaujant
Child Focus

(*Cour constitutionnelle* (Konstitucinis Teismas, Belgija) prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas ir privataus gyvenimo apsauga elektroninių ryšių sektoriuje – Direktyva 2002/58 EB – Taikymo sritis – 1 straipsnio 3 dalis – 15 straipsnio 1 dalis – ESS 4 straipsnio 2 dalis – Europos Sąjungos pagrindinių teisių chartija – 4, 6, 7, 8, 11 straipsniai ir 52 straipsnio 1 dalis – Pareiga bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis – Nusikalstamų veikų tyrimų veiksmingumas ir kiti viešojo intereso tikslai“

1. Pastaruosius kelerius metus Teisingumo Teismas laikėsi nuoseklaus požiūrio formuodamas jurisprudenciją dėl asmens duomenų saugojimo ir prieigos prie jų; ją sudaro šie svarbiausi sprendimai:

– 2014 m. balandžio 8 d. Sprendimas *Digital Rights Ireland ir kt.*[2], kuriame Teisingumo Teismas pripažino, kad Direktyva 2006/24/EB[3] negalioja, nes dėl jos galėjo būti neproporcingai ribojamos Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniais pripažįstamos teisės,

1 Originalo kalba: ispanų.

2 Bylos C-293/12 ir C-594/12, EU:C:2014:238 (toliau – Sprendimas *Digital Rights*).

3 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (OL L 105, 2006, p. 54).

– 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.*[4], kuriame Teisingumo Teismas išaiškino Direktyvos 2002/58/EB[5] 15 straipsnio 1 dalį,

– 2018 m. spalio 2 d. Sprendimas *Ministerio Fiscal*[6], kuriame Teisingumo Teismas patvirtino tos pačios Direktyvos 2002/58 nuostatos išaiškinimą.

2. Šie sprendimai (visų pirma antrasis) kelia tam tikrų valstybių narių institucijų susirūpinimą, nes jos mano, kad taikydamos tuos sprendimus netenka priemonės, kurią laiko būtina siekiant apsaugoti nacionalinį saugumą ir kovoti su nusikalstamumu ir terorizmu. Taigi kai kurios valstybės narės prašo pakeisti arba patikslinti tą jurisprudenciją.

3. Tam tikri valstybių narių teismai tokį patį susirūpinimą išreiškė keturiuose prašymuose priimti prejudicinį sprendimą[7]; dėl šių prašymų savo išvadą teikiu tą pačią dieną.

4. Visų pirma keturiose bylose keliama problema dėl Direktyvos 2002/58 taikymo veiklai, susijusiai su nacionaliniu saugumu ir kova su terorizmu. Jeigu šiomis aplinkybėmis minėta direktyva būtų taikoma, reikia išsiaiškinti, kokiu mastu valstybės narės gali riboti direktyvos saugomas teises į privatumą. Galiausiai reikia išnagrinėti, kiek su šia sritimi susijusiuose įvairiuose nacionalinės teisės aktuose (Jungtinės Karalystės[8], Belgijos[9] ir Prancūzijos[10]) atsižvelgiama į Sąjungos teisę, kaip ją aiškino Teisingumo Teismas.

5. Paskelbus Sprendimą *Digital Rights*, *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) panaikino nacionalinės teisės aktą, kuriuo į nacionalinę teisę iš dalies perkelta Direktyva 2006/24, tame sprendime pripažinta negaliojančia. Tada Belgijos įstatymų leidėjas priėmė naują teisės aktą, dėl kurio atitikties Sąjungos teisei vėl suabejota priėmus Sprendimą *Tele2 Sverige ir Watson*.

6. Šis prašymas priimti prejudicinį sprendimas ypatingas tuo, kad jame keliamas klausimas, ar galima laikinai pratęsti nacionalinės teisės akto galiojimą, kai nacionaliniai teismai šį teisės aktą turi panaikinti dėl to, kad jis neatitinka Sąjungos teisės.

I. Teisinis pagrindas

A. Sąjungos teisė

7. Darau nuorodą į atitinkamą savo išvados bylose C-511/18 ir C-512/18 punktą.

4 Bylos C-203/15 ir C-698/15, EU:C:2016:970 (toliau – Sprendimas *Tele2 Sverige ir Watson*).

5 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).

6 Byla C-207/16, EU:C:2018:788 (toliau – Sprendimas *Ministerio Fiscal*).

7 Be šios Bylos (*Ordre des barreaux francophones et germanophone ir kt.*, C-520/18), Bylos *La Quadrature du Net ir kt.*, C-511/18 ir C-512/18 ir *Privacy International*, C-623/17.

8 Byla *Privacy International*, C-623/17.

9 Byla *Ordre des barreaux francophones et germanophone ir kt.*, C-520/18.

10 Bylos *La Quadrature du Net ir kt.*, C-511/18 ir C-512/18.

B. Nacionalinė teisė. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. 4 straipsnyje nustatyta, kad *Loi du 13 juin 2005 relative aux communications électroniques* [12] 126 straipsnis formuluojamas taip:

„1. Nepažeidžiant *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (1992 m. gruodžio 8 d. Įstatymas dėl privataus gyvenimo apsaugos tvarkant asmens duomenis), telefonijos (įskaitant internetinę telefoniją), interneto prieigos ir interneto elektroninio pašto viešųjų paslaugų teikėjai, operatoriai, teikiantys viešai prieinamų elektroninių ryšių tinklų paslaugas, ir operatoriai, teikiantys vieną iš šių paslaugų, saugo 3 dalyje nurodytus duomenis, kuriuos jie generuoja ar tvarko, teikdami atitinkamas ryšių paslaugas.

Šis straipsnis netaikomas ryšių turiniui.

<…>

2. Tik toliau išvardytos valdžios institucijos, pateikusios prašymą, gali iš 1 dalies pirmoje pastraipoje nurodytų paslaugų teikėjų ir operatorių gauti pagal šį straipsnį saugomus duomenis toliau išvardytais tikslais ir sąlygomis:

1) teisminės institucijos tam, kad būtų nustatytos nusikalstamos veikos, atliktas jų ikiteisminis tyrimas ir vykdomas persekiojimas dėl jų, siekiant įgyvendinti *Code d'instruction criminelle* (Baudžiamojo proceso kodeksas) 46bis ir 88bis numatytas priemones, šiuose straipsniuose numatytomis sąlygomis;

2) žvalgybos ir saugumo tarnybos tam, kad būtų įvykdytos žvalgybos užduotys, naudojant duomenų rinkimo metodus, numatytus *Loi du 30 novembre 1998 organique des services de renseignement et de Sécurité* [13] 16/2, 18/7 ir 18/8 straipsniuose, ir laikantis šiame įstatyme numatytų sąlygų <…>;

3) bet kuris [*Institut belge des services postaux et des télécommunications* (Belgijos pašto ir telekomunikacijų paslaugų institutas] kriminalinės policijos pareigūnas, siekdamas nustatyti su [tinklų saugumo taisyklėmis] ir šio straipsnio pažeidimais susijusias nusikalstamas veikas, atlikti jų ikiteisminį tyrimą ir vykdyti persekiojimą dėl jų;

4) skubios pagalbos tarnybos, teikiančios pagalbą įvykio vietoje, kai po pagalbos skambučio jos iš tam tikro paslaugų teikėjo ar operatoriaus negauna skambintoją identifikuojančių duomenų <…> arba gauna neišsamius arba neteisingus duomenis. Galima prašyti tik skambintoją identifikuojančių duomenų ir ne vėliau kaip per 24 valandas po skambučio;

11 2016 m. gegužės 29 d. Įstatymas dėl duomenų rinkimo ir saugojimo elektroninių ryšių sektoriuje; toliau – 2016 m. gegužės 29 d. įstatymas (Moniteur belge, 2016 m. liepos 18 d., p. 44717).

12 2005 m. birželio 13 d. Įstatymas dėl elektroninių ryšių; toliau – 2005 m. įstatymas (*Moniteur belge*, 2005 m. birželio 20 d., p. 28070).

13 1998 m. lapkričio 30 d. Pagrindinis įstatymas dėl žvalgybos ir saugumo tarnybų; toliau – 1998 m. įstatymas (*Moniteur belge*, 1998 m. gruodžio 18 d., p. 40312).

5) *Cellule des personnes disparues de la Police Fédérale* (Federalinės policijos dingusių asmenų padalinys) kriminalinės policijos pareigūnas, vykdydamas pagalbos pavojuje atsidūrusiam asmeniui užduotį, ieškantis neaiškiomis aplinkybėmis dingusių asmenų, ir jeigu yra rimtų prielaidų ar požymių, kad dingusio asmens fizinei neliečiamybei gresia tiesioginis pavojus. Karaliaus paskirtas policijos tarnybos tarpininkas gali atitinkamo operatoriaus ar paslaugų teikėjo prašyti tik 3 dalies pirmoje ir antroje pastraipose nurodytų duomenų, susijusių su dingusiu asmeniu ir saugomų 48 valandas iki prašymo pateikti duomenų gavimo;

6) *Service de médiation pour les télécommunications* (Tarpininkavimo sprendžiant telekomunikacijų ginčus tarnyba), siekdama identifikuoti asmenį, kuris pasinaudojo elektroninių ryšių tinklu ar paslauga kenkėjiškais tikslais <…>. Gali būti prašoma tik identifikavimo duomenų.

1 dalies pirmoje pastraipoje nurodyti paslaugų teikėjai ir operatoriai užtikrina, kad 3 dalyje nurodyti duomenys būtų neribotai pasiekiami iš Belgijos ir kad šiuos duomenis ir bet kurią kitą su jais susijusią būtiną informaciją būtų galima nedelsiant perduoti tik šioje dalyje nurodytoms institucijoms.

Nepažeidžiant kitų teisės nuostatų, 1 dalies pirmoje pastraipoje nurodyti paslaugų teikėjai ir operatoriai negali pagal 3 dalį saugomų duomenų naudoti kitais tikslais.

3. Duomenys, leidžiantys identifikuoti naudotoją ar abonentą ir ryšio priemones, išskyrus antroje ir trečioje pastraipose konkrečiai numatytus duomenis, saugomi dvylika mėnesių nuo tos dienos, kurią ryšys paskutinį kartą buvo įmanomas naudojantis atitinkama paslauga.

Duomenys, susiję su galinio įrenginio prieiga ir prijungimu prie tinklo ir paslaugų bei šios įrangos buvimo vieta, įskaitant tinklo galinį tašką, saugomi dvylika mėnesių nuo ryšio datos.

Ryšio duomenys, įkaitant jų siuntėją ir adresatą, išskyrus turinį, saugomi dvylika mėnesių nuo ryšio datos.

Conseil des ministres (Ministrų Taryba) apsvarstytame nutarime Karalius, remdamasis teisingumo ministro ir ministro pasiūlymu, *Commission de la protection de la vie privée* (Privatumo apsaugos komisija) ir Institutui pateikus nuomonę, nustato saugotinus duomenis, suskirstytus į pirmoje–trečioje pastraipose nurodytas kategorijas, ir reikalavimus, kuriuos šie duomenys turi atitikti.

4. Siekiant saugoti 3 dalyje nurodytus duomenis, 1 dalies pirmoje pastraipoje nurodyti paslaugų teikėjai ir operatoriai:

1) garantuoja, kad saugomi duomenys būtų tokios pačios kokybės ir jiems būtų taikomi tokie patys saugumo ir apsaugos reikalavimai kaip ir tinkle esantiems duomenims;

2) užtikrina, kad saugomiems duomenims būtų taikomos tinkamos techninės ir organizacinės priemonės, siekiant apsaugoti juos nuo atsitiktinio ar neteisėto sunaikinimo, atsitiktinio praradimo ar pakeitimo, neleistino ar neteisėto saugojimo, tvarkymo, prieigos ar atskleidimo;

3) garantuoja, kad prieigą prie saugomų duomenų siekiant atsakyti į 2 dalyje nurodytų institucijų prašymus turėtų tik vienas ar keli 126/1 straipsnio 1 dalyje nurodyto koordinavimo padalinio nariai;

4) saugo duomenis Europos Sąjungos teritorijoje;

5) įgyvendina technologinės apsaugos priemones, dėl kurių saugomi duomenys nuo jų įrašymo tampa nenuskaitomi ir jų negali panaudoti joks asmuo, neturintis prieigos leidimo;

6) sunaikina visus saugomus duomenis pasibaigus šiems duomenims taikomam saugojimo laikotarpiui, nustatytam 3 dalyje, nepažeidžiant 122 ir 123 straipsnių;

7) užtikrina saugomų duomenų naudojimo atsekamumą pagal kiekvieną 2 dalyje nurodytos institucijos prašymą suteikti šiuos duomenis.

Pirmos pastraipos 7 punkte nurodytas atsekamumas užtikrinamas pildant žurnalą. Institutas ir Privatumo apsaugos komisija gali susipažinti su šiuo žurnalu arba pareikalauti viso šio žurnalo ar jo dalies kopijos. Institutas ir Privatumo apsaugos komisija sudaro bendradarbiavimo protokolą dėl susipažinimo su žurnalo turiniu ir jo kontrolės.

5. Ministras ir Teisingumo ministras kasmet *Chambre des représentants* (Atstovų Rūmai) perduoda statistiką apie duomenų, generuojamų ar tvarkomų teikiant visuomenei prieinamas ryšių ar ryšių tinklų paslaugas, saugojimą.

Ši statistika visų pirma apima:

1) atvejus, kai pagal taikytinas teisės nuostatas duomenys buvo perduoti kompetentingoms institucijoms;

2) laikotarpį nuo duomenų saugojimo pradžios dienos iki dienos, kurią kompetentingos institucijos paprašė perduoti šiuos duomenis;

3) atvejus, kai prašymų pateikti duomenų nebuvo galima patenkinti.

Ši statistika negali apimti asmens duomenų.

<…>“

9. 5 straipsnyje nustatyta, kad 2005 m. įstatymas papildomas 126/1 straipsniu, kuris suformuluotas taip:

„1. Kiekvieno operatoriaus ir kiekvieno 126 straipsnio 1 dalies pirmoje pastraipoje nurodyto paslaugų teikėjo įmonėje įsteigiamas koordinavimo padalinys, kuris pagal teisės aktus įgaliotoms Belgijos institucijoms jų prašymu pateikia duomenis, saugomus pagal 122, 123 ir 126 straipsnius, skambintojo identifikavimo duomenis pagal 107 straipsnio 2 dalies pirmą pastraipą arba duomenis, kurių galima reikalauti pagal Baudžiamojo proceso kodekso 46bis, 88bis ir 90ter straipsnius ir [1998 m. įstatymo] 18/7, 18/8, 18/16 ir 18/17 straipsnius.

<…>

2. Kiekvienas 126 straipsnio 1 dalies pirmoje pastraipoje nurodytas operatorius ir paslaugų teikėjas nustato vidaus procedūrą, pagal kurią teikiami atsakymai į institucijų prašymus suteikti prieigą prie naudotojų asmens duomenų. Gavęs prašymą, jis teikia Institutui informaciją apie šias procedūras, gautų prašymų skaičių, nurodytą teisinį pagrindą ir savo atsakymą.

<…>

3. Kiekvienas 126 straipsnio 1 dalies pirmoje pastraipoje nurodytas operatorius ir paslaugų teikėjas paskiria vieną ar kelis už asmens duomenų apsaugą atsakingus darbuotojus, kurie turi atitikti visas 1 dalies trečioje pastraipoje išvardytas sąlygas.

<…>

Vykdydamas savo funkcijas, už asmens duomenų apsaugą atsakingas darbuotojas veikia visiškai nepriklausomai ir turi prieigą prie visų institucijoms perduodamų asmens duomenų ir visų paslaugų teikėjo ar operatoriaus atitinkamų patalpų.

<…>

4. Ministrų Tarybos apsvarstytu nutarimu Karalius, gavęs Privatumo apsaugos komisijos ir Instituto nuomonę, nustato:

<…>

2) reikalavimus, kuriuos turi atitikti koordinavimo padalinys, atsižvelgiant į tuos operatorius ir paslaugų teikėjus, kurie gauna mažai teisminių institucijų prašymų, nėra įsisteigę Belgijoje ar veiklą daugiausia vykdo užsienyje;

3) informaciją, kuri turi būti teikiama Institutui ir Privatumo apsaugos komisijai pagal 1 ir 3 dalis, ir institucijas, kurios turi prieigą prie šios informacijos;

4) kitas taisykles, reglamentuojančias 126 straipsnio 1 dalies pirmoje pastraipoje nurodytų operatorių ir paslaugų teikėjų bendradarbiavimą su Belgijos institucijomis ar kai kuriomis iš jų, siekiant teikti 1 dalyje nurodytus duomenis, įskaitant, jei reikia, konkrečiai institucijai taikomą prašymo formą ir turinį.

<…>“

10. 8 straipsnyje nustatyta, kad Baudžiamojo proceso kodekso 46bis straipsnio 1 dalis išdėstoma taip:

„1. Tirdamas nusikalstamas veikas *procureur du Roi* (prokuroras) gali motyvuotu rašytiniu sprendimu, kuriame jis prireikus gali prašyti elektroninių ryšių tinklo operatoriaus, elektroninių ryšių paslaugos teikėjo arba policijos tarnybos, paskirtos Karaliaus, pagalbos, remdamasis visais turimais duomenimis ar naudodamasis prieiga prie operatorių ir paslaugų teikėjų klientų duomenų, atlikti arba įpareigoti atlikti šiuos veiksmus:

1) identifikuoti elektroninių ryšių paslaugos abonentą ar įprastą naudotoją arba naudotą elektroninio ryšio priemonę;

2) identifikuoti elektroninių ryšių paslaugas, kurių abonentas yra konkretus asmuo arba kuriomis įprastai naudojasi konkretus asmuo.

Turi būti įrodytas priimtos priemonės proporcingumas atsižvelgiant į privatumą ir subsidiarumas atsižvelgiant į visas kitas su tyrimu susijusias pareigas.

Ypatingos skubos atveju kiekvienas kriminalinės policijos pareigūnas gali, turėdamas išankstinį žodinį prokuroro leidimą, motyvuotu rašytiniu sprendimu reikalauti pateikti šiuos duomenis. Kriminalinės policijos pareigūnas šį motyvuotą rašytinį sprendimą ir per 24 valandas surinktą informaciją įteikia karališkajam prokurorui ir, be kita ko, motyvuoja ypatingą skubą.

Dėl nusikalstamų veikų, kurios neužtraukia vienų metų laisvės atėmimo ar sunkesnės bausmės, prokuroras arba, ypatingos skubos atvejais, kriminalinės policijos pareigūnas gali prašyti tik pirmoje pastraipoje nurodytų duomenų už šešių mėnesių laikotarpį iki jo sprendimo priėmimo.

2. Kiekvienas elektroninių ryšių tinklo operatorius ir kiekvienas elektroninių ryšių paslaugos teikėjas, iš kurio reikalaujama pateikti pirmoje pastraipoje nurodytus duomenis, prašytus duomenis prokurorui arba kriminalinės policijos pareigūnui pateikia per Karaliaus nustatytą terminą <…>.

<…>

Bet kuris asmuo, kuris dėl savo atliekamų funkcijų žino apie priemonę arba padeda ją įgyvendinti, yra saistomas konfidencialumo pareigos. Už bet kokį konfidencialumo pareigos pažeidimą baudžiama pagal Baudžiamojo kodekso 458 straipsnį.

Už atsisakymą pateikti duomenis skiriama 26–10 000 EUR bauda.“

11. 9 straipsnyje Baudžiamojo proceso kodekso 88bis straipsnis suformuluotas taip:

„1. Jeigu yra rimtų požymių, kad nusikalstamos veikos gali užtraukti vienų metų laisvės atėmimo ar sunkesnę bausmę, ir ikiteisminio tyrimo teisėjas mano, kad yra aplinkybių, dėl kurių elektroninių ryšių sekimas, jų siuntėjo ar adresato vietos nustatymas yra būtinas siekiant nustatyti tiesą, jis, jei reikia, paprašęs techninės elektroninių ryšių tinklo operatoriaus arba elektroninių ryšių paslaugos teikėjo pagalbos, tiesiogiai ar tarpininkaujant Karaliaus paskirtai policijos tarnybai gali atlikti arba nurodyti atlikti šiuos veiksmus:

1) sekti elektroninių ryšių priemonių, iš kurių ar į kurias siunčiami ar buvo siunčiami elektroniniai pranešimai, srauto duomenis;

2) nustatyti elektroninių ryšių siuntėjo ar adresato vietą.

Pirmoje pastraipoje nurodytais atvejais dėl kiekvienos elektroninių ryšių priemonės, kurios skambučio duomenys sekami ar pagal kurią nustatoma elektroninių ryšių siuntėjo ar adresato vieta, protokole fiksuojama elektroninio ryšio diena, laikas, trukmė ir prireikus – vieta.

Ikiteisminio tyrimo teisėjas motyvuotoje nutartyje nurodo faktines Bylos aplinkybes, kurios pateisina priemonę ir dėl kurių ji proporcinga atsižvelgiant į privatumo apsaugą ir subsidiari atsižvelgiant į visas kitas su tyrimu susijusias pareigas.

Jis taip pat nurodo laikotarpį, kiek priemonė gali būti taikoma ateityje (šis laikotarpis negali viršyti dviejų mėnesių nuo nutarties priėmimo, išskyrus atvejus, kai yra pratęsiamas), ir prireikus laikotarpį praeityje, kuriam nutartis taikoma pagal 2 dalį.

<…>

2. Kiek tai susiję su 1 dalies pirmoje pastraipoje nurodytos priemonės taikymu srauto ar vietos nustatymo duomenims, saugomiems pagal 2005 m. <…> įstatymo <…> 126 straipsnį, taikomos šios nuostatos:

– dėl *Code pénal* (Baudžiamasis kodeksas) II knygos Iter antraštinėje dalyje numatytos nusikalstamos veikos ikiteisminio tyrimo teisėjas gali savo nutartyje reikalauti duomenų už dvylikos mėnesių laikotarpį iki nutarties priėmimo,

– dėl kitos nusikalstamos veikos, numatytos 90ter straipsnio 2–4 dalyse ir nenurodytos pirmoje įtraukoje, arba dėl nusikalstamos veikos, kurią padarė Baudžiamojo kodekso 324bis straipsnyje numatytas nusikalstamas susivienijimas, arba dėl nusikalstamos veikos, kuri užtraukia penkerių metų laisvės atėmimo ar sunkesnę bausmę, ikiteisminio tyrimo teisėjas gali savo nutartyje reikalauti duomenų už devynių mėnesių laikotarpį iki nutarties priėmimo,

– dėl kitų nusikalstamų veikų ikiteisminio tyrimo teisėjas duomenų gali reikalauti tik už šešių mėnesių laikotarpį iki nutarties priėmimo.

3. Ši priemonė advokato ar gydytojo elektroninių ryšių priemonėms gali būti taikoma tik tada, kai jis pats įtariamas padaręs 1 dalyje nurodytą nusikalstamą veiką ar dalyvavęs ją darant arba kai remiantis konkrečiomis faktinėmis aplinkybėmis galima daryti prielaidą, kad šias elektroninių ryšių priemones naudoja tretieji asmenys, įtariami 1 dalyje numatytos nusikalstamos veikos padarymu.

Priemonė gali būti įgyvendinama tik tada, jeigu, atsižvelgiant į atvejį, apie tai pranešama advokatų tarybos pirmininkui ar provincijos gydytojų institucijai. Tuos pačius asmenis ikiteisminio tyrimo teisėjas informuoja apie aplinkybes, kurioms, jo manymu, taikoma profesinė paslaptis. Šie duomenys nefiksuojami protokole.

4. <…>

Bet kuris asmuo, kuris dėl savo atliekamų funkcijų žino apie priemonę arba padeda ją įgyvendinti, yra saistomas konfidencialumo pareigos. Už bet kokį konfidencialumo pareigos pažeidimą baudžiama pagal Baudžiamojo kodekso 458 straipsnį.

<…>“

12. 12 straipsnyje nustatyta, kad 1998 m. įstatymo 13 straipsnis išdėstomas taip:

„Žvalgybos ir saugumo tarnybos gali tirti, rinkti, gauti ir tvarkyti informaciją ir asmens duomenis, kurie gali būti naudingi vykdant savo užduotis, ir atnaujinti dokumentus, visų pirma susijusius su įvykiais, grupėmis ir asmenimis, kurie jas domina siekiant atlikti savo užduotis.

Dokumentuose esanti žvalgybos informacija turi sietis su galutiniu Bylos tikslu ir neviršyti to, kas reikalinga siekiant šio tikslo.

Žvalgybos ir saugumo tarnybos užtikrina savo šaltinių duomenų bei šių šaltinių suteiktos informacijos ir asmens duomenų saugumą.

Žvalgybos ir saugumo tarnybų agentai gali susipažinti su atitinkamos tarnybos surinkta ir tvarkoma informacija, žvalgybos informacija ir asmens duomenimis, jeigu jie naudingi vykdant jų funkciją ar užduotį.“

13. 14 straipsnyje 18/3 straipsnis išdėstytas nauja redakcija. Dabar 18/3 straipsnyje nustatyta:

„1. 18/2 straipsnio 1 dalyje numatytus specialius duomenų rinkimo metodus galima naudoti, jei yra 18/1 straipsnyje nurodyta potenciali grėsmė, kai įprasti duomenų rinkimo metodai laikomi nepakankamais, kad būtų galima surinkti informaciją, reikalingą žvalgybos užduočiai įvykdyti. Specialus metodas turi būti pasirinktas pagal potencialios grėsmės, dėl kurios jis naudojamas, sunkumo laipsnį.

Specialus metodas gali būti naudojamas tik po to, kai tarnybos vadovas priima rašytinį motyvuotą sprendimą ir šis sprendimas pateikiamas Komisijai.

2. Tarnybos vadovo sprendime nurodoma:

1) specialaus metodo pobūdis;

2. atsižvelgiant į aplinkybes – fiziniai ar juridiniai asmenys, asociacijos ar susivienijimai, objektai, vietos, renginiai ar informacija, kuriems taikomas specialus metodas;

3) potenciali grėsmė, pateisinanti specialų metodą;

4) faktinės aplinkybės, pateisinančios specialų metodą, su subsidiarumu ir proporcingumu susiję motyvai, įskaitant 2 ir 3 punktų ryšį;

5) laikotarpis, kuriuo specialus metodas gali būti taikomas, skaičiuojant nuo Komisijos sprendimo pateikimo;

<…>

9) kai taikoma, rimti požymiai, kad advokatas, gydytojas ar žurnalistas asmeniškai ir aktyviai prisideda ar prisidėjo prie potencialios grėsmės atsiradimo ar didėjimo;

10) jeigu taikomas 18/8 straipsnis, motyvai dėl laikotarpio, su kuriuo susiję renkami duomenys, trukmės;

<…>

8. Tarnybos vadovas nustoja taikyti specialų metodą, jeigu jį pateisinusi potenciali grėsmė išnyko, jeigu metodas nebėra naudingas siekiant tikslo, dėl kurio jis pradėtas naudoti, arba jeigu vadovas nustato neteisėtus veiksmus. Jis kuo skubiau informuoja Komisiją apie savo sprendimą.“

14. 1988 m. įstatymo 18/8 straipsnis suformuluotas taip:

„1. Žvalgybos ir saugumo tarnybos, siekdamos atlikti savo užduotis, prireikus šiuo tikslu naudodamosi elektroninių ryšių tinklo operatoriaus ar elektroninių ryšių paslaugos teikėjo techninе pagalba, gali atlikti ar nurodyti atlikti šiuos veiksmus:

1) sekti elektroninių ryšių priemonių, iš kurių ar į kurias siunčiami ar buvo siunčiami elektroniniai pranešimai, srauto duomenis;

2) nustatyti elektroninių ryšių siuntėjo ar adresato vietą.

<…>

2. Kiek tai susiję su 1 dalyje nurodyto metodo taikymu pagal 2005 m. <…> įstatymo <…> 126 straipsnį saugomiems duomenims, taikomos šio nuostatos:

1) dėl potencialios grėsmės, kylančios dėl veiklos, kuri gali būti susijusi su nusikalstamais susivienijimais ar kenkėjiškomis sektinėmis organizacijomis, tarnybos vadovas savo sprendime gali reikalauti tik duomenų už šešių mėnesių laikotarpį iki sprendimo priėmimo;

2) dėl kitos nei 1 ir 3 punktuose nurodytos potencialios grėsmės tarnybos vadovas gali savo sprendime reikalauti duomenų už devynių mėnesių laikotarpį iki sprendimo priėmimo;

3) dėl potencialios grėsmės, kylančios dėl veiklos, kuri gali būti susijusi su terorizmu ar ekstremizmu, tarnybos vadovas savo sprendime gali reikalauti tik duomenų už dvylikos mėnesių laikotarpį iki sprendimo priėmimo. <…>“

II. Faktinės aplinkybės ir pateikti prejudiciniai klausimai

15. Savo 2015 m. birželio 11 d. sprendime[14] *Cour constitutionnelle* (Konstitucinis Teismas) panaikino 2005 m. įstatymo 126 straipsnį (naujos redakcijos), remdamasis tais pačiais motyvais, dėl kurių Teisingumo Teismas Sprendime *Digital Rights* Direktyvą 2006/24 pripažino negaliojančia.

16. Nacionalinės teisės aktų leidėjas, atsižvelgdamas į šį panaikinimą, priėmė 2016 m. gegužės 29 d. įstatymą (prieš priimant Sprendimą *Tele2 Sverige ir Watson*).

17. VZ ir kiti asmenys, *Ordre des barreaux francophones et germanophone* (toliau – *Ordre des barreaux*), *Liga voor Mensenrechten ASBL* (toliau – LMR), *Ligue des Droits de l'Homme ASBL* (toliau – LDH) ir *Académie Fiscale ASBL* (toliau – *Académie Fiscale*) prašymą priimti prejudicinį sprendimą pateikusiame teisme dėl nurodyto įstatymo pateikė kelis konstitucinius skundus; iš esmės jie tvirtino, kad šis įstatymas viršija tai, kas griežtai būtina, ir jame nenustatyta pakankamai apsaugos garantijų.

[14] Sprendimas Nr. 84/2015, *Moniteur belge*, 2015 m. rugpjūčio 11 d.

18. Šiomis aplinkybėmis *Cour constitutionnelle* (Konstitucinis Teismas) Teisingumo Teismui pateikė šiuos klausimus:

„1. Ar Direktyvos 2002/58/EB 15 straipsnio 1 dalį, siejamą su teise į saugumą, garantuojama Europos Sąjungos pagrindinių teisių chartijos [toliau – Chartija] 6 straipsnyje, ir teise į asmens duomenų apsaugą, garantuojama [Chartijos] 7, 8 straipsniuose ir 52 straipsnio 1 dalyje, reikia aiškinti taip, kad pagal ją draudžiamas toks nacionalinės teisės aktas, koks yra nagrinėjamas, kuriame numatyta bendra operatorių ir elektroninių ryšių paslaugų teikėjų pareiga saugoti srauto ir vietos nustatymo duomenis, kaip jie suprantami pagal Direktyvą 2002/58/EB, jų generuojamus ar tvarkomus teikiant šias paslaugas, t. y. nacionalinės teisės aktas, kurio tikslas yra ne vien sunkių nusikaltimų tyrimas, nustatymas ar persekiojimas dėl jų, bet ir nacionalinio saugumo, teritorijos gynybos ir viešojo saugumo užtikrinimas, kitų nei sunkūs nusikaltimai veikų tyrimas, nustatymas ir persekiojimas dėl jų ar draudžiamo elektroninių ryšių sistemų naudojimo prevencija ar kito tikslo, nurodyto [2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 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. 1)] 23 straipsnio 1 dalyje, siekimas, ir šiame teisės akte taip pat numatytos garantijos, susijusios su duomenų saugojimu ir prieiga prie jų?

2. Ar Direktyvos 2002/58/EB 15 straipsnio 1 dalį, siejamą su [Chartijos] 4, 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, reikia aiškinti taip, kad pagal ją draudžiamas toks nacionalinės teisės aktas, koks yra nagrinėjamas, kuriame numatyta bendra operatorių ir elektroninių ryšių paslaugų teikėjų pareiga saugoti srauto ir vietos nustatymo duomenis, kaip jie suprantami pagal Direktyvą 2002/58/EB, jų generuojamus ar tvarkomus teikiant šias paslaugas, jeigu šio nacionalinės teisės akto tikslas, be kita ko, yra padėti valdžios institucijoms vykdyti pagal Chartijos 4 ir 8 straipsnius joms tenkančias pozityvias pareigas, pagal kurias turi būti nustatytas teisinis pagrindas, kuris sudarytų sąlygas efektyviam nusikalstamos veikos tyrimui ir efektyviam nubaudimui už nepilnamečių seksualinį išnaudojimą ir kuris faktiškai leistų identifikuoti nusikalstamą veiką padariusį asmenį ir tuomet, kai naudotasi elektroninių ryšių priemonėmis?

3. Ar tuo atveju, jeigu remdamasis atsakymais į pirmąjį ir antrąjį prejudicinius klausimus *Cour constitutionnelle* (Konstitucinis Teismas) padarytų išvadą, kad ginčijamu įstatymu pažeidžiamas vienas ar keli įsipareigojimai pagal šiuose klausimuose nurodytas nuostatas, jis galėtų laikinai palikti galioti [ginčijamą įstatymą], kad būtų išvengta teisinio nesaugumo ir anksčiau surinkti bei saugomi duomenys dar galėtų būti panaudoti įstatyme numatytais tikslais?“

III. Procesas Teisingumo Teisme

19. Prašymas priimti prejudicinį sprendimą Teisingumo Teismo kanceliarijoje užregistruotas 2018 m. rugpjūčio 2 d.

20. Rašytines pastabas pateikė VZ ir kiti asmenys, *Académie Fiscale*, LMR, LDH, *Ordre des barreaux*, *Fondation pour Enfants Disparus et Sexuellement Exploités* (*Child Focus*), Vokietijos, Belgijos, Jungtinės Karalystės, Čekijos, Kipro, Danijos, Ispanijos, Estijos, Prancūzijos, Vengrijos, Airijos, Nyderlandų, Lenkijos ir Švedijos vyriausybės, taip pat Komisija.

21. 2019 m. rugsėjo 9 d. buvo surengtas viešas teismo posėdis (kartu su teismo posėdžiais bylose C-511/18, C-512/18 ir C-623/17); jame dalyvavo bylų, susijusių su keturiais prašymais priimti prejudicinį sprendimą, šalys, pirma minėtų vyriausybių ir Norvegijos vyriausybės, taip pat Komisijos atstovai ir Europos asmens duomenų apsaugos priežiūros pareigūnas.

IV. Analizė

22. Pirmasis šiame prašyme priimti prejudicinį sprendimą pateiktas klausimas iš esmės sutampa su klausimais, nagrinėjamais bylose C-511/18 ir C-512/28. Vis dėlto nuo šių bylų jis skiriasi tikslais, kurių siekiama nacionalinės teisės aktu: tokie tikslai yra ne tik kova su terorizmu ir sunkiausių formų nusikalstamumu ar nacionalinio saugumo apsauga, bet ir „teritorijos gynyba, viešasis saugumas, kitų nei sunkūs nusikaltimai veikų tyrimas, nustatymas ir persekiojimas dėl jų“ ir apskritai bet kuris tikslas, numatytas Reglamento 2016/679 23 straipsnio 1 dalyje.

23. Antrasis klausimas susijęs su pirmuoju, tačiau jį papildo tuo požiūriu, kad klausiama, ar pozityvios pareigos ištirti nepilnamečių seksualinį išnaudojimą ir nubausti už jį, tenkančios valdžios institucijoms, pateisina nagrinėjamas priemones.

24. Trečiasis klausimas suformuluotas darant prielaidą, kad nacionalinės teisės aktas gali neatitikti Sąjungos teisės. Prašymą priimti prejudicinį sprendimą pateikęs teismas nori išsiaiškinti, ar tokiu atveju būtų galima laikinai palikti galioti 2016 m. gegužės 29 d. įstatymą.

25. Pirma, šiuos klausimus nagrinėsiu analizuodamas Direktyvos 2002/58 taikytinumą; šiuo tikslu remsiuosi savo išvada bylose, kuriose pateikti minėti kiti prašymai priimti prejudicinį sprendimą. Antra, apibrėšiu pagrindines Teisingumo Teismo jurisprudencijos gaires šioje srityje ir galimybes ją išplėtoti. Galiausiai nagrinėsiu, kaip atsakyti į kiekvieną prejudicinį klausimą.

A. Direktyvos 2002/58 taikytinumas

26. Kaip ir kituose trijuose prašymuose priimti prejudicinį sprendimą, šiame prašyme taip pat abejojama, ar Direktyva 2002/58 taikytina. Kadangi valstybių narių požiūriai šiuo klausimu sutampa, darau nuorodą į savo išvadą bylose C-511/18 ir C-512/18 [15].

B. Teisingumo Teismo jurisprudencija, susijusi su asmens duomenų saugojimu ir valdžios institucijų prieiga prie jų pagal Direktyvą 2002/58

1. Pranešimų ir su jais susijusių duomenų konfidencialumo principas

27. Direktyvos 2002/58 nuostatos „smulkiau išaiškina ir papildo“ Direktyvą 95/46/EB [16], kad būtų užtikrinta aukšto lygio asmens duomenų apsauga teikiant elektroninių ryšių paslaugas [17].

15 40 ir paskesni punktai.

16 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). Žr. Direktyvos 2002/58 1 straipsnio 2 dalį. 2018 m. gegužės 25 d. Direktyva 95/46 panaikinta Reglamentu 2016/679. Taigi, kadangi Direktyvoje 2002/58 daroma nuoroda į Direktyvą 95/46 arba nenustatyta jos pačios teisės normų, būtina atsižvelgti į šio reglamento nuostatas (žr. Reglamento 2016/679 94 straipsnio 1 ir 2 dalis).

17 Sprendimo *Tele2 Sverige ir Watson* 82 ir 83 punktai.

28. Direktyvos 2002/58 5 straipsnio 1 dalyje nurodyta, kad valstybės narės savo nacionalinės teisės aktuose turi užtikrinti pranešimų, perduodamų per viešąjį ryšių tinklą ir teikiant viešai teikiamas elektroninių ryšių paslaugas, konfidencialumą, taip pat atitinkamų srauto duomenų konfidencialumą.

29. Užtikrinant ryšių konfidencialumą, be kita ko, draudžiama be atitinkamų naudotojų sutikimo kaupti su elektroniniais ryšiais susijusius srauto duomenis
(Direktyvos 2002/58 5 straipsnio 1 dalies antras sakinys). Išimtys taikomos „asmenims, kuriems teisėtai suteiktas leidimas <…>, ir dėl techninio saugojimo, būtino pranešimui perduoti“ [18].

30. Direktyvos 2002/58 5 ir 6 straipsnių bei 9 straipsnio 1 dalies tikslas yra užtikrinti pranešimų ir su jais susijusių duomenų konfidencialumą ir kuo labiau sumažinti piktnaudžiavimo riziką. Direktyvos taikymo sritį reikia vertinti atsižvelgiant į jos 30 konstatuojamąją dalį, kurioje nustatyta, kad „[e]lektroninių ryšių tinklų ir paslaugų teikimo sistemos turi būti suprojektuotos taip, kad reikalingas asmens duomenų kiekis būtų griežtai apribotas iki *minimumo*“ [19].

31. Kalbant apie šiuos duomenis, galima išskirti:

– *srauto* duomenis, kuriuos leidžiama tvarkyti ir saugoti tik kiek to reikia ir kol to reikia sąskaitoms už paslaugas pateikti, šių paslaugų rinkodarai ir teikiant pridėtinės vertės paslaugas (Direktyvos 2002/58 6 straipsnis). Pasibaigus šiam terminui, tvarkomi ir saugomi duomenys turi būti sunaikinti arba pakeisti taip, kad taptų anoniminiai [20],

– *vietos nustatymo* duomenis, kurie nėra srauto duomenys ir kurie gali būti tvarkomi tik tuo atveju, kai tenkinamos tam tikros sąlygos ir kai jie pakeisti taip, kad tapo anoniminiai, arba kai tam gautas naudotojų arba abonentų sutikimas (Direktyvos 2002/58 9 straipsnio 1 dalis) [21].

2. Direktyvos 2002/58 15 straipsnio 1 dalyje numatyta apribojimo sąlyga

32. Pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybės narės gali „patvirtinti teisines priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą“.

33. Toks apribojimas turi būti „būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės priemonė, skirta nacionalin[iam] saugum[ui] (t. y. valstybės saugum[ui]), gynyb[ai], visuomenės saugum[ui] [apsaugoti], taip užkardant, tiriant ir nustatant baudžiamąsias [nusikalstamas] veikas ar neteisėtą elektroninių ryšių sistemos naudojimą, kaip nurodyta [Direktyvos 95/46] 13 straipsnio 1 dalyje“.

34. Toks tikslų sąrašas yra baigtinis [22]: pavyzdžiui, (*inter alia*) galima „patvirtinti teisines priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis šioje dalyje nustatytais motyvais“.

18 Ten pat, 85 punktas ir jame nurodyta jurisprudencija.

19 Ten pat, 87 punktas. Pasviruoju šriftu originale neišskirta.

20 Ten pat, 86 punktas ir jame nurodyta jurisprudencija.

21 Ten pat, 86 punktas *in fine*.

22 Ten pat, 90 punktas.

35. Bet kuriuo atveju „[v]isos šioje dalyje nurodytos priemonės turi atitikti bendruosius Bendrijos teisės principus, tarp jų ir [įskaitant] nurodytus Europos Sąjungos [s]utarties 6 straipsnio 1 ir 2 dalyse“. Taigi Direktyvos 2002/58 15 straipsnio 1 dalis turi būti aiškinama atsižvelgiant į Chartijos užtikrinamas pagrindines teises [23].

36. Kiek tai svarbu nagrinėjamu atveju, iš šių Chartijoje pripažįstamų teisių Teisingumo Teismas paminėjo teisę į privatumą (7 straipsnis), teisę į asmens duomenų apsaugą (8 straipsnis) ir teisę į saviraiškos laisvę (11 straipsnis) [24].

37. Teisingumo Teismas taip pat pabrėžė, kad yra taikoma
Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo taisyklė, pagal kurią pareigos užtikrinti pranešimų ir su jais susijusių srauto duomenų konfidencialumą apribojimai turi būti aiškinami siaurai.

38. Konkrečiai kalbant, jis paneigė, kad „nukrypimas nuo šios pagrindinės pareigos ir ypač nuo šios direktyvos 5 straipsnyje nustatyto draudimo saugoti tokius duomenis ta[mpa] taisykle, nes taip būtų labai susiaurinta šio straipsnio apimtis“ [25].

39. Manau, kad šios dvi pastabos yra lemiamos siekiant suprasti, kodėl Teisingumo Teismas bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų, susijusių su elektroniniais ryšiais, saugojimą laikė neatitinkančiu Direktyvos 2002/58.

40. Tai pripažinęs Teisingumo Teismas tik „griežtai“ [26] taikė proporcingumo kriterijų, kurį jau buvo naudojęs anksčiau [27]: „pagrindinės teisės į privatų gyvenimą apsauga Sąjungos lygiu reikalauja, kad nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir jos apribojimai neviršytų to, kas griežtai būtina“ [28].

3. Duomenų saugojimo proporcingumas

a) Bendro ir nediferencijuoto saugojimo neproporcingumas

41. Teisingumo Teismas pripažino, kad kova su sunkiais nusikaltimais, visų pirma organizuotu nusikalstamumu ir terorizmu, neabejotinai yra pirmaeilės svarbos užtikrinant visuomenės saugumą, o jos veiksmingumas gali labai priklausyti nuo galimybės panaudoti pažangius tyrimo metodus. Jis pridūrė: „Tačiau kad ir koks fundamentalus būtų, vien toks bendrojo intereso tikslas negali pateisinti to, kad saugojimo priemonė, kaip antai įtvirtintina Direktyva 2006/24, būtų laikoma būtina šios kovos tikslais.“ [29]

23 Ten pat, 91 punktas ir jame nurodyta jurisprudencija.

24 Ten pat, 93 punktas ir jame nurodyta jurisprudencija.

25 Ten pat, 89 punktas.

26 Sprendimo *Tele2 Sverige ir Watson* 95 punkte šis prieveiksmis vartojamas remiantis Direktyvos 2002/58 11 konstatuojamąja dalimi.

27 Sprendimo *Digital Rights* 48 punkte nustatyta: „[A]tsižvelgiant, viena vertus, į asmens duomenų apsaugos svarbą pagrindinei teisei į privataus gyvenimo gerbimą ir, kita vertus, į šios teisės apribojimo, kurį lemia Direktyva 2006/24, dydį ir rimtumą, Sąjungos teisės aktų leidėjo vertinimo diskrecija yra nedidelė, todėl reikia taikyti griežtą šios diskrecijos kontrolę“.

28 Sprendimo *Tele2 Sverige ir Watson* 96 punktas ir jame nurodyta jurisprudencija.

29 Sprendimo *Digital Rights* 51 punktas. Taip pat žr. Sprendimo *Tele2 Sverige ir Watson* 103 punktą.

42. Siekdamas nustatyti, ar šios rūšies priemonė neviršija to, kas griežtai būtina, Teisingumo Teismas visų pirma pabrėžė, kad taikant tokią priemonę Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių ribojimas yra labai rimtas [30]. Taip yra būtent dėl to, kad nacionalinės teisės aktuose numatytas „bendras ir nediferencijuotas *visų su visais abonentais ir registruotais naudotojais susijusių srauto ir vietos nustatymo duomenų, perduodamų bet kokia elektroninio ryšio priemone*, saugojimas ir jais elektroninių ryšių paslaugų teikėjai įpareigojami saugoti šiuos duomenis *sistemingai, nuolat ir be jokios išimties galimybės*“ [31].

43. Tai, kad šia priemone ribojamas piliečių gyvenimas, matyti iš Teisingumo Teismo atlikto duomenų saugojimo pasekmių vertinimo.

Šie duomenys [32]:

– „leidžia surasti ir identifikuoti pranešimo šaltinį ir adresatą, identifikuoti ryšio datą, laiką, trukmę ir rūšį, naudotojų ryšio įrangą ir nustatyti judriojo ryšio įrangos buvimo vietą“ [33],

– „visų pirma leidžia išsiaiškinti asmenį, su kuriuo vyko abonento ar registruoto naudotojo komunikacija, ir komunikacijos būdą, laiką ir vietą, iš kurios ji vykdyta. Be to, jie leidžia sužinoti, kaip dažnai vyko abonento arba registruoto naudotojo ir tam tikrų asmenų komunikacija tam tikru laikotarpiu“ [34],

– „[leidžia padaryti] labai tiksli[as] išvad[as] apie asmenų, kurių duomenys saugomi, privatų gyvenimą, pavyzdžiui, kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir lankomą socialinę aplinką“ [35],

– „suteikia priemonių atitinkamų asmenų profiliui, jautriai informacijai, kiek tai susiję su teise į privataus gyvenimo užtikrinimą, ir net pranešimų turiniui nustatyti“ [36].

44. Be to, ribojimas gali „sudaryti atitinkamiems asmenims įspūdį, kad jų privatus gyvenimas yra nuolat stebimas“, nes „duomenys saugomi apie tai neinformuojant elektroninių ryšių paslaugų naudotojų“ [37].

45. Atsižvelgiant į ribojimo dydį pažymėtina, kad priemonę, pagal kurią saugomi tokio pobūdžio duomenys, gali pateisinti tik kovos su sunkiais nusikaltimais tikslas [38]. Vis dėlto ši priemonė negali tapti bendra taisykle, nes pagal „Direktyva 2002/58 nustatytą sistemą reikalaujama, kad toks duomenų saugojimas būtų išimtis“ [39].

30 Sprendimo *Digital Rights* 65 punktas ir Sprendimo *Tele2 Sverige ir Watson* 100 punktas.

31 Sprendimo *Tele2 Sverige ir Watson* 97 punktas. Kursyvu išskirta mano.

32 Jie, be kita ko, apima abonento ar registruoto naudotojo vardą, pavardę ir adresą, telefono numerius, į kuriuos ir iš kurių skambinta, ir IP adresą interneto paslaugų atveju.

33 Sprendimo *Tele2 Sverige ir Watson* 98 punktas.

34 Ten pat, 98 punktas.

35 Ten pat, 99 punktas.

36 Ten pat, 99 punktas *in fine*.

37 Ten pat, 100 punktas.

38 Ten pat, 102 punktas.

39 Ten pat, 104 punktas.

46. Be to, buvo susiklosčiusios dvi aplinkybės, susijusios su tuo, kad pagal nagrinėjamą priemonę nenumatyta „jokio skirtumo, apribojimo arba išimties atsižvelgiant į siekiamą tikslą“ [40] ir „nereikalaujama jokios sąsajos tarp numatytų saugoti duomenų ir grėsmės visuomenės saugumui“ [41]:

– pirma, priemonė buvo „taikom[a] visuotinai, visiems elektroninių ryšių paslaugas naudojantiems asmenims, nepaisant to, kad tokių asmenų padėtis net netiesiogiai nėra pagrindas inicijuoti baudžiamąjį persekiojimą. <…> Be to, [priemonėje] nenumatyta jokių išimčių, taigi [ji] taikom[a] net tiems asmenims, kurių komunikacija pagal nacionalinę teisę pripažįstama profesine paslaptimi“ [42],

– antra, pagal priemonę „<…> nenustatyta, kad saugomi tik tie duomenys, kurie susiję su tam tikru laikotarpiu ir (arba) geografine zona, ir (arba) asmenų, kurie, vienaip ar kitaip, galėtų būti siejami su vienu iš sunkių nusikaltimų arba asmenimis, kurių duomenų saugojimas dėl kitų priežasčių galėtų prisidėti prie kovos su nusikalstamumu“ [43].

47. Šiomis aplinkybėmis nagrinėjami nacionalinės teisės aktai viršijo tai, kas griežtai būtina. Taigi jie negalėjo būti laikomi pateisinamais demokratinėje visuomenėje, kaip to reikalaujama pagal Direktyvos 2002/58 15 straipsnio 1 dalį, atsižvelgiant į Chartijos 7, 8, 11 straipsnius ir 52 straipsnio 1 dalį [44].

b) Galimybė tikslingai saugoti duomenis

48. Teisingumo Teismas pripažino, kad Sąjungos teisę atitinka nacionalinės teisės aktai, pagal kuriuos „siekiant prevencijos leidžiamas *tikslinis* srauto ir vietos nustatymo duomenų *saugojimas* kovos su sunkiais nusikaltimais tikslais“ [45].

49. Šis tikslinis duomenų saugojimas yra teisėtas su sąlyga, kad, „kiek tai susiję su saugotinų duomenų kategorijomis, konkrečiomis ryšio priemonėmis, atitinkamais asmenimis ir numatyta saugojimo trukme, [jis] būtų apribotas tuo, kas griežtai būtina“.

50. Sprendime *Tele2 Sverige ir Watson* pateikiamos taisyklės, taikomos norint nustatyti, kada šios sąlygos įvykdytos, nėra (ir galbūt negalėtų būti) išsamios, jos suformuluotos gana abstrakčiai. Siekdamos jų laikytis valstybės narės turi:

– įtvirtinti aiškias ir tikslias taisykles, kuriomis būtų reglamentuojama tokios duomenų saugojimo priemonės apimtis ir taikymas [46],

– nustatyti „objektyvius kriterijus, kuriais saugotini duomenys būtų susieti su siekiamu tikslu“ [47], ir

40 Ten pat, 105 punktas.

41 Ten pat, 106 punktas.

42 Ten pat, 105 punktas.

43 Ten pat, 106 punktas.

44 Ten pat, 107 punktas.

45 Ten pat, 108 punktas. Kursyvu išskirta mano.

46 Ten pat, 109 punktas. Jose konkrečiai turi būti nurodyta, „kokiomis aplinkybėmis ir sąlygomis galima siekiant prevencijos numatyti duomenų saugojimo priemonę, ir taip užtikrinta, kad tokia priemonė neviršytų to, kas griežtai būtina“.

47 Ten pat, 110 punktas.

– remtis „objektyviais kriterijais, leidžiančiais nustatyti asmenis, kurių duomenys gali bent netiesiogiai atskleisti ryšį su sunkia nusikalstama veika, vienaip ar kitaip prisidėti prie kovos su sunkiais nusikaltimais arba užkirsti didelį pavojų visuomenės saugumui“ [48].

51. Dėl šių objektyvių kriterijų pažymėtina, kad Teisingumo Teismas kaip pavyzdį nurodo galimybę taikyti geografinį kriterijų, siekiant apibrėžti atitinkamus asmenis ir situacijas. Manau, kad šis kriterijus (kai kurios valstybės narės jį kritikavo) nurodytas neturint tikslo nustatyti, kad leidžiamų tikslingumo veiksnių sąrašui taikytinas vien šis kriterijus.

4. Prieigos prie duomenų proporcingumas

a) Sprendimas „Tele2 Sverige ir Watson“

52. Teisingumo Teismas nacionalinių institucijų *prieigą* prie duomenų nagrinėja neatsižvelgdamas į pareigos *saugoti* duomenis, nustatytos elektroninių ryšių paslaugų teikėjams, apimtį ir visų pirma į tai, ar šių duomenų saugojimas yra visuotinio, ar konkretaus pobūdžio [49].

53. Iš tikrųjų, nors saugojimas pagrįstas logika, kad prieiga prie duomenų suteikiama vėliau, ir dėl saugojimo, ir dėl prieigos gali būti padaryta įvairių Chartijos saugomų pagrindinių teisių pažeidimų. Vis dėlto toks diferencijavimas nereiškia, kad kai kurie argumentai dėl saugojimo nėra taikytini taip pat ir prieigai prie saugomų duomenų.

54. Atsižvelgiant į tai, prieiga:

– „iš tikrųjų griežtai turi atitikti vieną iš šių tikslų“, įtvirtintų Direktyvos 2002/58 15 straipsnio 1 dalies pirmame sakinyje. Siekiamas tikslas taip pat turi būti susietas su teisių apribojimo rimtumu. Jeigu apribojimas laikomas rimtu, jis gali būti pateisinamas tik kova su sunkiais nusikaltimais [50],

– gali būti leidžiama tik tiek, kiek tai griežtai būtina [51]. Be to, teisinės priemonės turi numatyti „aiškias ir tikslias taisykles, nustatančias, kokiomis aplinkybėmis ir sąlygomis elektroninių ryšių paslaugų teikėjai turi suteikti kompetentingoms nacionalinėms institucijoms prieigą prie duomenų. Be to, tokio pobūdžio priemonė pagal vidaus teisę turi būti teisiškai privaloma“ [52],

– konkrečiai kalbant, nacionalinės teisės aktuose turi būti numatytos „materialinės ir procedūrinės sąlygos, reglamentuojančios kompetentingų nacionalinių institucijų prieigą prie saugomų duomenų“ [53].

55. Atsižvelgiant į tai, kas išdėstyta, galima daryti išvadą, kad „bendra prieiga prie visų saugomų duomenų, nepaisant to, ar egzistuoja koks nors bent jau netiesioginis ryšys su siekiamu tikslu, negali būti laikoma neviršijančia to, kas griežtai būtina“ [54].

48 Ten pat, 111 punktas.

49 Ten pat, 113 punktas.

50 Ten pat, 115 punktas.

51 Ten pat, 116 punktas.

52 Ten pat, 117 punktas.

53 Ten pat, 118 punktas.

54 Ten pat, 119 punktas.

56. Teisingumo Teismas teigia, kad „atitinkami nacionalinės teisės aktai turi būti grindžiami objektyviais kriterijais, kai nustatomos aplinkybės ir sąlygos, kuriomis kompetentingoms nacionalinėms institucijoms turi būti suteikta prieiga prie abonentų ar registruotų naudotojų duomenų“ [55]. Šiuo klausimu pažymėtina, kad, „kalbant apie kovą su nusikalstamumu, iš principo prieiga gali būti suteikta tik prie *asmenų, kurie įtariami planuojantys sunkų nusikaltimą, jį darantys arba padarę, arba vienaip ar kitaip dalyvavę jį darant, duomenų*“ [56].

57. Kitaip tariant, nacionalinės teisės normų, pagal kurias kompetentingoms nacionalinėms institucijoms suteikiama prieiga prie saugomų duomenų, taikymo sritis turi būti gana ribota. Atitinkami asmenys turi būti susiję su siekiamu tikslu, kad prieiga nebūtų suteikta prie daug ar net visų asmenų duomenų, visų elektroninių ryšių priemonių ir visų saugomų duomenų.

58. Vis dėlto šios taisyklės gali būti sušvelnintos tam tikromis aplinkybėmis. Teisingumo Teismas nurodo „ypating[us] atvej[us], pvz., kai terorizmo veikla kėsinamasi į gyvybinius nacionalinio saugumo, gynybos arba visuomenės saugumo interesus“. Tokiais atvejais „gali būti leidžiama prieiga ir prie kitų asmenų duomenų, jeigu turima objektyvios informacijos, leidžiančios manyti, kad konkrečiu atveju šie duomenys iš tiesų prisidės kovojant [su] toki[a] veikl[a]“ [57].

59. Pagal šį Teisingumo Teismo išaiškinimą valstybės narės gali nustatyti konkrečią platesnės prieigos prie duomenų tvarką, jeigu išimtiniais atvejais to reikia siekiant kovoti su valstybės svarbiausiems interesams (nacionaliniam saugumui, gynybai ir visuomenės saugumui) kylančiomis grėsmėmis [58], taigi tokia prieiga taip pat gali apimti asmenis, kurie tik netiesiogiai susiję su minėtais pavojais.

60. Prieiga prie saugomų duomenų, neatsižvelgiant į jos rūšį, nacionalinėms institucijoms turi būti suteikiama laikantis trijų sąlygų:

– „iš esmės būtina, kad <…>, išskyrus tinkamai pagrįstus skubos atvejus, teismas arba nepriklausoma administracinė institucija atliktų išankstinę kontrolę“. Šio teismo ar institucijos sprendimas turi būti priimtas „gav[us] motyvuotą kompetentingų nacionalinių institucijų prašymą, kurį jos pateik[ė] vykdydamos prevencijos, atskleidimo arba baudžiamojo persekiojimo procedūras“ [59],

– „kompetentingos nacionalinės institucijos, kurioms suteikta prieiga prie saugomų duomenų, vykstant taikytinoms nacionalinėms procedūroms apie tai informuo[ja] atitinkamus asmenis, kai pasiekiamas momentas, nuo kurio toks informavimas negali neigiamai paveikti šių institucijų atliekamų tyrimų“ [60],

– valstybės narės turi priimti teisės normas dėl elektroninių ryšių paslaugų teikėjų turimų duomenų saugumo ir apsaugos, kad būtų išvengta netinkamo duomenų naudojimo ir neteisėtos prieigos prie jų [61].

55 Ten pat.

56 Ten pat. Kursyvu išskirta mano.

57 Ten pat.

58 Be terorizmo veiklos, tokią išimties tvarka suteikiamą prieigą galėtų pateisinti ir kiti galimi atvejai, kaip antai didelio masto kibernetinis išpuolis prieš labai svarbius valstybės infrastruktūros objektus arba grėsmė, susijusi su branduolinio ginklo platinimu.

59 Sprendimo *Tele2 Sverige ir Watson* 120 punktas.

60 Ten pat, 121 punktas.

61 Ten pat, 122 punktas.

b) Sprendimas „Ministerio Fiscal“

61. Šioje byloje buvo keliamas klausimas, ar nacionalinės teisės norma, kurioje numatyta kompetentingų institucijų prieiga prie duomenų, susijusių su tam tikras SIM korteles turinčių asmenų civiline tapatybe, atitinka Direktyvos 2002/58 15 straipsnio 1 dalį, aiškinamą atsižvelgiant į Chartijos 7 ir 8 straipsnius.

62. Teisingumo Teismas pripažino, kad Direktyvos 2002/58 15 straipsnio 1 dalies pirmame sakinyje, kalbant apie tikslą užkardyti, tirti ir nustatyti nusikalstamas veikas, taip pat vykdyti persekiojimą dėl jų, neapsiribojama tik kova su sunkiomis nusikalstamomis veikomis, bet nurodomos apskritai „nusikalstamos veikos“ [62].

63. Jis pridūrė, kad siekiant pateisinti kompetentingų nacionalinių institucijų prieigą prie duomenų turi būti ryšys tarp apribojimo rimtumo ir atitinkamų nusikalstamų veikų sunkumo. Taigi:

– „rimtas ribojimas <…> gali būti pateisinamas tik siekiu kovoti su nusikaltimais, kurie taip pat turi būti kvalifikuojami kaip „sunkūs“ [63],

– vis dėlto „jeigu ribojimas, kurį lemia tokia prieiga, nėra rimtas, minėta prieiga gali būti pateisinama tikslu užkardyti, tirti ir nustatyti „baudžiamąsias [nusikalstamas] veikas“ apskritai [taip pat vykdyti persekiojimą dėl jų]“ [64].

64. Remdamasis šia prielaida Teisingumo Teismas, kitaip nei Sprendime *Tele2 Sverige ir Watson*, Chartijos 7 ir 8 straipsniais saugomų teisių ribojimo nelaikė „rimtu“, nes prašymu suteikti prieigą buvo „siekiama tik nustatyti SIM kortelių, aktyvuotų per dvylikos dien[ų] laikotarpį naudojantis pavogto mobiliojo telefono IMEI kodu, savininkus“ [65].

65. Norėdamas pabrėžti, kad apribojimas ne toks rimtas, jis paaiškino, kad „pagrindinėje byloje nagrinėjamu prašymu siekiama prieigos tik prie duomenų, kurie apibrėžtu laikotarpiu leidžia susieti pavogtu mobiliuoju telefonu aktyvuotą SIM kortelę arba aktyvuotas SIM korteles su šių SIM kortelių savininkais. Šie duomenys, jei nesutikrinti su duomenimis, susijusiais su minėtomis SIM kortelėmis atliktais pranešimais ir vietos nustatymu, neleidžia nustatyti nei minėta SIM kortele arba minėtomis SIM kortelėmis atliktų pranešimų datos, valandos, trukmės ir jų gavėjų, nei vietų, kuriose buvo atlikti pranešimai, arba pranešimų dažnumo su tam tikrais asmenimis nurodytu laikotarpiu. Vadinasi, minėti duomenys neleidžia daryti tikslių išvadų dėl asmenų, su kuriais susiję šie duomenys, privataus gyvenimo“ [66].

62 Sprendimo *Ministerio Fiscal* 53 punktas.

63 Ten pat, 56 punktas.

64 Ten pat, 57 punktas.

65 Ten pat, 59 punktas. Buvo nagrinėjama prieiga „prie šių SIM kortelių telefonų numerių ir duomenų, susijusių su minėtų kortelių savininkų tapatybe, t. y. pavardėmis, vardais ir prireikus adresais. Tačiau šie duomenys nesusiję nei su pavogtu mobiliuoju telefonu atliktais pranešimais, nei su jo vietos nustatymu, kaip per teismo posėdį tai patvirtino Ispanijos vyriausybė ir prokuratūra“.

66 Ten pat, 60 punktas.

66. Byloje, kurioje priimtas Sprendimas *Ministerio Fiscal*, nebuvo klausiama, ar elektroninių ryšių paslaugų teikėjai asmens duomenis, prie kurių suteikta prieiga, saugojo laikydamiesi Direktyvos 2002/58 15 straipsnio 1 dalyje, aiškinamoje atsižvelgiant į Chartijos 7 ir 8 straipsnius, numatytų sąlygų [67]. Taip pat nebuvo nagrinėjamas klausimas, ar įvykdytos kitos iš to straipsnio kylančios prieigos sąlygos.

67. Taigi aiškinant Sprendimą *Ministerio Fiscal* negalima daryti išvados, kad pakeista Teisingumo Teismo jurisprudencija dėl nacionalinės sistemos, leidžiančios bendrai ir nediferencijuotai saugoti duomenis, kaip tai suprantama pagal Sprendimą *Tele2 Sverige ir Watson*, atitikties Sąjungos teisei.

68. Vis dėlto manau, kad Teisingumo Teismas, pripažinęs, jog sistema, pagal kurią suteikiama prieiga tik prie tam tikrų asmens duomenų (susijusių su SIM kortelių turėtojų civiline tapatybe), yra teisėta, netiesiogiai pritaria tam, kad paslaugų teikėjai gali saugoti tuos duomenis.

C. Esminė Teisingumo Teismo jurisprudencijos kritika

69. Ir prašymą priimti prejudicinį sprendimą pateikęs teismas, ir dauguma pastabas pateikusių valstybių narių prašo Teisingumo Teismo išaiškinti, patikslinti ar net persvarstyti įvairius šios srities jurisprudencijos, kurią jie kritikuoja, aspektus.

70. Dauguma šių kritiškų pastabų tiesiogiai ar netiesiogiai jau buvo išdėstytos Sprendime *Digital Rights* ir atmestos Sprendime *Tele2 Sverige ir Watson*. Dabar jos vėl pateikiamos, siekiant iš esmės atkreipti dėmesį į tai, kad užtenka griežtų teisės normų dėl prieigos prie elektroninių ryšių paslaugų teikėjų turimų duomenų – jas taikant galima tam tikru būdu kompensuoti apribojimo, kurį lemia bendras ir nediferencijuotas tų duomenų saugojimas, rimtumą.

71. Keliose kritiškose pastabose taip pat pabrėžiama, kad reikia nustatyti iš tikrųjų veiksmingas priemones kovojant su didele grėsme saugumui ir apskritai su nusikalstamumu, ir prašoma Teisingumo Teismo atsižvelgti į teisę į saugumą (Chartijos 6 straipsnis) bei valstybių narių diskreciją siekiant užtikrinti nacionalinį saugumą. Vienu atveju priduriama, kad Teisingumo Teismas neįvertino prevencinio saugumo ir žvalgybos tarnybų veiksmų pobūdžio.

D. Dėl šios kritikos ir galimybės patikslinti Teisingumo Teismo jurisprudenciją pateiktas mano vertinimas

72. Manau, kad Teisingumo Teismas turėtų toliau laikytis principinės pozicijos, įtvirtintos ankstesniuose jo sprendimuose: pareiga bendrai ir nediferencijuotai saugoti visus su visais abonentais ir registruotais naudotojais susijusius srauto ir vietos nustatymo duomenis neproporcingai riboja Chartijos 7, 8 ir 11 straipsniais saugomas pagrindines teises.

73. *A sensu contrario*, nacionalinės teisės aktai, kuriuose nustatyti tinkami kai kurių iš šių duomenų, generuojamų teikiant elektroninių ryšių paslaugas, saugojimo apribojimai, galėtų atitikti Sąjungos teisę. Taigi esminis dalykas yra šių duomenų saugojimas *ribotas saugojimas*.

[67] Sprendimo *Ministerio Fiscal* 49 punktas.

74. Dėl toliau nurodytų priežasčių šis ribotas saugojimas neturėtų būti taikomas vien konkrečiai geografinei vietovei ar konkrečiai asmenų kategorijai: iš diskusijų dėl šių saugojimo kriterijų matyti, kad jie galėtų būti arba neįgyvendinami, arba neveiksmingi, norint įvykdyti jais siekiamus tikslus, arba net tapti diskriminacijos šaltiniu.

75. Visų pirma nepritariu kritiškam argumentui, kad taikytinas toks binomas: „platesnio masto saugojimas, mainais suteikiant labiau ribojamą prieigą“. Teisingumo Teismas teigia (ir aš jam pritariu), kad duomenų saugojimas ir prieiga prie jų yra dviejų skirtingų rūšių ribojimas. Net jeigu duomenų saugojimas įgyja prasmę atsižvelgiant į tai, kad kompetentingos institucijos vėliau gali gauti prieigą prie jų, kiekvienas teisių ribojimas turi būti pateisinamas atskirai, atlikus konkretų tyrimą pagal siekiamą tikslą.

76. Taigi nacionalinės sistemos, pagal kurią numatyta bendrai ir nediferencijuotai saugoti duomenis, negalima pateisinti remiantis tuo, kad atitinkamose teisės normose kartu nustatytos griežtos materialinės ir procesinės prieigos prie šių duomenų sąlygos.

77. Vadinasi, turi būti įtvirtintos konkrečiai su duomenų saugojimu susijusios teisės normos, pagal kurias tokiam saugojimui taikomos tam tikros sąlygos, siekiant neleisti duomenų saugoti bendrai ir nediferencijuotai. Tik taip bus užtikrinta, kad šios teisės normos atitiktų Direktyvos 2002/58 15 straipsnio 1 dalį, atsižvelgiant į Chartijos 7, 8, 11 straipsnius ir 52 straipsnio 1 dalį.

78. Be to, tokio požiūrio laikėsi Taryboje posėdžiavusios darbo grupės, siekdamos apibrėžti duomenų saugojimą ir prieigą prie jų reglamentuojančias teisės normas, atitinkančias Teisingumo Teismo jurisprudenciją; jos lygiagrečiai nagrinėjo abiejų rūšių teisių apribojimus [68].

79. Ribojant abiejų rūšių teisių apribojimus galima įvertinti, ar bendras galimas šio veiksmo poveikis, kartu taikant patikimas apsaugos priemones, yra toks, kad sumažėja duomenų saugojimo įtaka Chartijos 7, 8 ir 11 straipsnių saugomoms pagrindinėms teisėms ir kartu užtikrinamas tyrimų veiksmingumas.

80. Norint apsaugoti šias teises, sistemoje turi būti:

– numatyta, kad duomenys saugomi taikant tam tikrus apribojimus ir diferencijavimą pagal siekiamą tikslą,

– prieiga prie šių duomenų reglamentuojama tik tiek, kiek griežtai būtina norint įgyvendinti siekiamą tikslą, teismui ar nepriklausomai administracinei institucijai atliekant kontrolę.

81. Elektroninių ryšių paslaugų teikėjų atliekamas tam tikrų duomenų saugojimo (ne vien tam, kad būtų valdomi jų sutartiniai įsipareigojimai naudotojams) pateisinimas įgyja platesnį mastą, lygiagrečiai vykstant technologinei raidai. Pripažinus, kad toks saugojimas naudingas siekiant užkirsti kelią nusikaltimams ir kovoti su jais (tai sunkiai paneigiama [69]), atrodytų nelogiška riboti jo apimtį – leisti naudoti tik duomenis, kuriuos operatoriai saugo, siekdami vykdyti savo komercinę veiklą, ir tik tol, kol griežtai būtina šiai veiklai vykdyti.

[68] Valstybės narės nuo 2017 m. dalyvauja darbo grupėje, kurios tikslas yra suderinti jų teisės aktus su Teisingumo Teismo jurisprudencijoje nustatytais šios srities kriterijais (Keitimosi informacija ir duomenų apsaugos darbo grupė (DAPIX)).

[69] Bet kuriuo atveju valstybės narės turi diskreciją nustatyti šiuos tyrimo metodus ir įvertinti jų veiksmingumą.

82. Pripažinus, kad pareiga saugoti duomenis, t. y. platesnės apimties pareiga nei ta, kurią operatoriai gali vykdyti, siekdami patenkinti savo techninius ir komercinius poreikius, yra naudinga siekiant užtikrinti nacionalinį saugumą ir kovoti su nusikalstamumu, būtina apibrėžti šios pareigos ribas.

83. Kiekviena saugojimo sistema turi būti griežtai suderinta su siekiamu tikslu, kad negalėtų tapti sistema, pagal kurią duomenys saugomi nediferencijuotai[70]. Taip pat reikia užtikrinti, kad atsižvelgiant į visus šiuos duomenis nebūtų galima *susidaryti vaizdo* apie atitinkamą asmenį (t. y. apie jo įprastą veiklą ir socialinius ryšius), panašaus į tą, kurį būtų galima susidaryti žinant pranešimų turinį.

84. Siekiant paaiškinti kai kurias dviprasmybes ir neaiškumus, svarbu atsižvelgti į aspektus, dėl kurių Teisingumo Teismas *nenusprendė* savo sprendimuose *Digital Rigths* ir *Tele2 Sverige ir Watson*. Juose pats duomenų saugojimo sistemos, kaip naudingos priemonės kovojant su nusikalstamumu, buvimas nebuvo pripažintas netinkamu. Priešingai, pripažinta, kad tikslas užkirsti kelią nusikalstamai veikai ir už ją bausti yra teisėtas ir kad duomenų saugojimo sistema naudinga šiam tikslui pasiekti.

85. Kartoju, tada buvo tvirtai paneigta, kad Sąjunga ar jos valstybės narės, remdamosi šiuo tikslu, gali įpareigoti nediferencijuotai saugoti *visus* duomenis, generuojamus teikiant elektroninių ryšių paslaugas, ir leisti bendrą prieigą prie šių duomenų.

86. Taigi reikia rasti būdų, kaip saugoti duomenis, kad toks saugojimas nebūtų laikomas „bendru ir nediferencijuotu“, t. y. neatitinkančiu Chartijos 7, 8 ir 11 straipsniuose įtvirtinto apsaugos reikalavimo.

87. Vienas iš tokių būdų yra *tikslingai* saugoti duomenis, susijusius su konkrečiais asmenimis (teoriškai tai yra asmenys, kurie tam tikrais daugiau ar mažiau tiesioginiais ryšiais susiję su didžiausiomis grėsmėmis) arba su tam tikra geografine vietove.

88. Vis dėlto šis metodas kelia tam tikrų sunkumų:

– tikriausiai neužtektų nustatyti galimų agresorių grupę, jeigu šie agresoriai naudoja nuasmeninimo priemones arba klastoja savo tapatybę. Be to, atrinkus šias grupes galėtų būti sukurta bendra įtarimų sistema, taikoma tam tikriems gyventojų segmentams, ir tokia atranka galėtų būti laikoma diskriminacine, atsižvelgiant į naudojamą algoritmą,

– dėl atrankos pagal geografinius kriterijus (ją reikėtų taikyti nelabai mažoms teritorijoms, kad atranka būtų veiksminga) kyla tokių pačių ir papildomai kitų problemų, kaip per teismo posėdį nurodė Europos asmens duomenų apsaugos priežiūros pareigūnas, nes tam tikros vietovės gali būti stigmatizuojamos.

89. Be to, galėtų atsirasti tam tikras prieštaravimas tarp prevencinio konkretiems asmenims ar geografinei vietovei skirto duomenų saugojimo pobūdžio ir to, kad nusikalstamų veikų vykdytojai iš anksto nežinomi, taip pat nežinoma tų veikų padarymo vieta ir laikas.

70 Sprendimo *Digital Rights* 57 punktas ir Sprendimo *Tele2 Sverige ir Watson* 105 punktas.

90. Bet kuriuo atveju nereikia drausti šiais kriterijais pagrįstų teisės normų, reglamentuojančių tikslinį saugojimą – jos yra naudingos norint pasiekti nurodytus tikslus. Įstatymų leidžiamoji valdžia šias teisės normas, pagal kurias būtų užtikrinama Teisingumo Teismo saugomų pagrindinių teisių apsauga, turi parengti kiekvienoje valstybėje narėje ar visoje Sąjungoje.

91. Būtų klaidinga manyti, kad tikslinį duomenų, susijusių su konkrečiais asmenimis ar tam tikra geografine vietove, saugojimą reglamentuojančios teisės normos yra vienintelės, kurias Teisingumo Teismas laiko atitinkančiomis Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7 ir 8 straipsniais.

92. Kartoju, gali būti ir kitų tikslinį duomenų saugojimą reglamentuojančių taisyklių, ne tik pagrįstų konkrečiomis asmenų grupėmis ar geografinėmis vietovėmis. Iš tikrųjų taip nusprendė pirma nurodytos Tarybos darbo grupės: jos kaip tyrimo kryptis pirmiausia nagrinėjo saugomų duomenų kategorijų ribojimą[71], pseudonimų suteikimą duomenims[72], ribotų saugojimo laikotarpių įtvirtinimą[73], išimties taikymą tam tikrų kategorijų elektroninių ryšių paslaugų teikėjams[74], saugojimo leidimus, kuriuos galima pratęsti[75], pareigą saugoti Sąjungoje saugomus duomenis ir nepriklausomos administracinės institucijos atliekamą sisteminę ir nuolatinę garantijų, kurias elektroninių ryšių paslaugų teikėjai suteikia tam, kad duomenys nebūtų naudojami netinkamai, kontrolę.

93. Manau, kad, siekiant užtikrinti saugojimo atitiktį Teisingumo Teismo jurisprudencijai, pirmenybę reikėtų teikti tam, kad srauto ir vietos nustatymo duomenys, kurie priskiriami prie tam tikrų *kategorijų* (t. y. atsižvelgiant į griežtus saugumo poreikius ribojamų kategorijų) ir kurie, vertinami kaip visuma, neleidžia susidaryti tikslaus ir išsamaus vaizdo apie atitinkamų asmenų gyvenimą, būtų saugomi laikinai.

94. Praktiškai tai reiškia, kad taikant tinkamus filtrus turi būti saugomi tik *būtiniausi* dviejų pagrindinių kategorijų duomenys (srauto ir vietos nustatymo duomenys), laikomi būtinai reikalingais siekiant veiksmingai užkirsti kelią nusikalstamumui ir jį kontroliuoti, taip pat apsaugoti nacionalinį saugumą.

95. Sąjungos institucijos ar valstybės narės, naudodamosi teisėkūros priemonėmis (padedant jų pačių ekspertams), turi atrinkti šiuos duomenis ir atsisakyti bet kokio bandymo įpareigoti bendrai ir nediferencijuotai saugoti visus srauto ir vietos nustatymo duomenis.

71 Duomenys, kurie nėra griežtai būtini ir objektyviai reikalingi siekiant užkirsti kelią nusikalstamoms veikoms ir dėl jų persekioti, taip pat apsaugoti visuomenės saugumą, neturi būti saugomi. Visų pirma atsižvelgiant į siekiamą tikslą reikėtų atkreipti dėmesį į tai, kokių rūšių srauto, vietos nustatymo ir abonentų duomenys būtinai turi būti saugomi, kad šis tikslas būtų pasiektas. Konkrečiai kalbant, nėra saugomi duomenys, kurie nelaikomi būtinais siekiant ištirti nusikalstamas veikas ir persekioti dėl jų.

72 Metodas, kurį taikant vardai ir pavardės pakeičiamos pseudonimais, taigi duomenys nebėra susiję su tais vardais ir pavardėmis. Kitaip nei nuasmeninimas, pseudonimų suteikimas leidžia vėl susieti duomenis su atitinkamo asmens vardu ir pavarde.

73 Būtų galima nagrinėti galimybę saugojimo laikotarpius derinti pagal įvairias duomenų kategorijas, atsižvelgiant į tai, ar privatus asmenų gyvenimas dėl saugojimo ribojamas daugiau, ar mažiau. Be to, reikėtų nustatyti, kad pasibaigus saugojimo laikotarpiui duomenys sunaikinami visam laikui.

74 Būtų galima apsvarstyti galimybę pareigą saugoti duomenis nustatyti ne visiems elektroninių ryšių paslaugų teikėjams, o atsižvelgiant į paslaugų teikėjų įmonės dydį ir teikiamų paslaugų rūšį, pavyzdžiui, neįpareigojant duomenų saugoti labai specializuotas paslaugas teikiančių subjektų.

75 Leidimo suteikimo sistemos galėtų būti grindžiamos periodiniais grėsmių vertinimais kiekvienoje valstybėje narėje. Turi būti užtikrinta, kad saugomų duomenų ir siekiamo tikslo ryšys būtų nustatytas ir pritaikytas, atsižvelgiant į konkrečią kiekvienos valstybės narės situaciją. Taigi pagal paslaugų teikėjams suteiktus saugojimo leidimus tam tikrų rūšių duomenis būtų galima saugoti nustatytos trukmės laikotarpį, atsižvelgiant į grėsmės vertinimą. Šiuos leidimus galėtų suteikti teismas ar nepriklausoma administracinė institucija ir pagal juos būtų periodiškai peržiūrima, ar toks saugojimas būtinas.

96. Be šio apribojimo pagal kategorijas, taikomas apribojimas, pagal kurį duomenys gali būti saugomi tik tam tikrą saugojimo laikotarpį, kad jais remiantis nebūtų galima susidaryti išsamaus vaizdo apie atitinkamų asmenų gyvenimą. Šis saugojimo laikotarpis taip pat turi būti suderintas, atsižvelgiant į duomenų pobūdį, kad duomenys, suteikiantys tikslesnės informacijos apie šių asmenų gyvenimo būdą ir įpročius, būtų saugomi trumpiau [76].

97. Kitaip tariant, priemonė, kurią reikia nagrinėti, – tai kiekvienos kategorijos duomenų saugojimo laikotarpio diferencijavimas pagal tai, kiek šie duomenys naudingi saugumo tikslams pasiekti. Apribojus laikotarpį, kurį kartu saugomi abiejų kategorijų duomenys (taigi jie gali būti naudojami siekiant nustatyti ryšius, atskleidžiančius atitinkamų asmenų gyvenimo būdą), išplečiama pagal Chartijos 8 straipsnį saugomos teisės apsauga.

98. Per teismo posėdį šiuo klausimu išreiškė nuomonę Europos duomenų apsaugos priežiūros pareigūnas: kuo daugiau kategorijų metaduomenų saugoma ir kuo ilgesnis saugojimo laikotarpis, tuo lengviau nustatyti išsamų asmens profilį (ir atvirkščiai) [77].

99. Be to, kaip buvo akcentuota per teismo posėdį, sunku atriboti tam tikrus elektroninių ryšių metaduomenis ir šių ryšių turinį. Kai kurie metaduomenys gali atskleisti tiek pat ar daugiau informacijos negu pats šių ryšių turinys: tokie metaduomenys galėtų būti tinklalapių, kuriuose lankytasi, adresai (URL) [78]. Taigi šios rūšies duomenims ir kitiems panašiems duomenims reikėtų skirti ypatingą dėmesį, siekiant kuo labiau apriboti būtinybę juos saugoti ir tokio saugojimo laikotarpį.

100. Nelengva rasti subalansuotą sprendimą, nes tyrimą atliekančios ir priežiūrą vykdančios tarnybos, taikydamos saugomų duomenų kryžminės patikros ir susiejimo metodą, atitinkamai gali identifikuoti įtariamąjį arba grėsmę. Vis dėlto duomenų, skirtų šiam įtariamajam ar grėsmei nustatyti, ir duomenų, kuriais remiantis susidaromas išsamus vaizdas apie asmens gyvenimą, saugojimo lygis skiriasi.

101. Nemanau, kad laukiant, kol visoje Sąjungoje bus pradėtas taikyti bendras šio konkretaus klausimo reguliavimas, galima prašyti Teisingumo Teismo, kad jis vykdytų reguliavimo funkcijas ir išsamiai patikslintų, kokių kategorijų duomenis galima saugoti ir kiek laiko. Nustačius apribojimus, kurie, kaip teigia Teisingumo Teismas, kyla iš Chartijos, Sąjungos institucijos ir valstybės narės turi priimti teisingas nuostatas, kad būtų pasiekta pusiausvyra tarp saugumo užtikrinimo ir Chartija saugomų pagrindinių teisių.

102. Žinoma, atsisakius informacijos, gaunamos turint daugiau saugomų duomenų, tam tikrais atvejais galėtų būti sunkiau kovoti su galimomis grėsmėmis. Vis dėlto tai yra kaina, kurią (be kita ko) valdžios institucijos turi mokėti, kai joms yra nustatyta pareiga užtikrinti pagrindinių teisių apsaugą.

[76] Atrodo, kad tokia sistema taikoma Vokietijos Federacinėje Respublikoje; jos vyriausybė per teismo posėdį nurodė, kad pagal šios šalies teisės aktus srauto duomenų saugojimo terminas yra dešimt savaičių, o vietos nustatymo duomenų – tik keturios savaitės. Priešingai, Prancūzijos Respublikoje srauto ir vietos nustatymo duomenis būtina saugoti vienus metus. Ši valstybė narė teigia, kad nustačius trumpesnį nei vienų metų laikotarpį sumažėtų kriminalinės policijos tarnybų efektyvumas.

[77] Žinoma, reikia užtikrinti, kad pasibaigus saugojimo laikotarpiui elektroninių ryšių paslaugų teikėjai duomenis sunaikintų visam laikui (išskyrus tuos duomenis, kuriuos pagal Direktyvą 2002/58 galima toliau saugoti komerciniais tikslais).

[78] Per teismo posėdį Prancūzijos vyriausybė teigė, kad URL adresai nėra priskiriami prie prisijungimo duomenų, dėl kurių Prancūzijos įstatymų leidėjas numatė bendrą saugojimo pareigą.

103. Niekas neskatina nustatyti *ex ante* pareigos bendrai ir nediferencijuotai saugoti su privačiais elektroniniais ryšiais susijusių pranešimų *turinio* (net kai įstatymuose užtikrinama vėlesnė ribota prieiga prie šio turinio), lygiai taip pat negalima nediferencijuotai ir bendrai saugoti šių pranešimų metaduomenų, iš kurių galima sužinoti labai jautrios informacijos, kaip antai patį jų turinį.

104. Aplinkybė, kad teisės aktuose sunku tiksliai apibrėžti atvejus ir sąlygas, kuriomis galima vykdyti tikslinį saugojimą (tai pripažįstu), nepateisina to, kad valstybės narės, įtvirtinusios išimtį teisės normoje, bendrą asmens duomenų saugojimą padarytų kaip esminį savo teisės aktų principą. Jeigu taip būtų, tai reikštų, kad leidžiama neribotą laiką labai apriboti teisę į asmens duomenų apsaugą.

105. Turiu pridurti, kad susidarius visiškai *išimtinėms* situacijoms, kai kyla tiesioginė grėsmė arba labai didelė rizika ir dėl to valstybėje narėje pagrįstai oficialiai paskelbiama nepaprastoji padėtis, nacionalinės teisės aktuose yra numatyta galimybė ribotą laikotarpį nustatyti tokią plačią ir bendrą pareigą saugoti duomenis, kokia laikoma būtina.

106. Šiomis aplinkybėmis būtų galima priimti teisės aktus, kuriuose konkrečiai leidžiama saugoti daugiau duomenų (ir suteikti prieigą prie jų), laikantis sąlygų ir tvarkos, užtikrinančių, kad šios priemonės būtų išimtinės, kiek tai susiję su jų materialine taikymo sritimi ir trukme, taip pat, kad būtų suteikiamos atitinkamos teisminės garantijos.

107. Atlikus lyginamąjį reguliavimo sistemų, reglamentuojančių Konstitucijoje įtvirtintą nepaprastąją padėtį, tyrimą akivaizdu, kad nėra neįmanoma apibrėžti faktinius atvejus, kai gali būti pradėta taikyti speciali reguliavimo sistema, ir nustatyti, kokia institucija gali priimti šį sprendimą ir kokiomis sąlygomis, taip pat, kokia priežiūra turi būti vykdoma [79].

E. Konkretūs atsakymai į tris prejudicinius klausimus

1. Pirminės pastabos

108. Prašymą priimti prejudicinį sprendimą pateikęs teismas prašo išaiškinti Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su keliomis pagal Chartiją užtikrinamomis teisėmis: teise į privatų ir šeimos gyvenimą (7 straipsnis), teise į asmens duomenų apsaugą (8 straipsnis) ir teise į saviraiškos ir informacijos laisvę (11 straipsnis).

109. Kaip nurodžiau bylose C-511/18 ir C-512/18 pateiktoje išvadoje, Teisingumo Teismas teigia, kad tokiais atvejais šios teisės iš tikrųjų galėtų būti pažeistos.

110. Vis dėlto *Cour constitutionnelle* (Konstitucinis Teismas) taip pat nurodo Chartijos 4 ir 6 straipsnius, su kuriais susiję atitinkamai antrasis ir pirmasis prejudiciniai klausimai.

111. Kalbant apie Chartijos 6 straipsnį, kuriuo užtikrinama teisė į laisvę ir saugumą, pažymėtina, kad bylose C-511/18 ir C-512/18 juo taip pat remiamasi; savo poziciją dėl šio straipsnio reikšmės pateikiau atitinkamoje išvadoje, į kurią darau nuorodą [80].

[79] Ackerman, B., „The Emergency Constitution“, *Yale Law Journal*, t. 113, 2004, p. 1029–1092; Ferejohn, J. ir Pasquino, P., „The Law of the Exception: A typology of Emergency Powers“, *International Journal of Constitutional Law*, t. 2, 2004, p. 210–239.

[80] Bylose C-511/18 ir C-512/18 pateiktos išvados 95 ir paskesni punktai.

112. Dėl Chartijos 4 straipsnio pažymėtina, kad atsakymas priklauso ne tiek nuo nacionalinės teisės aktų analizės, atliktos lyginant šiuos teisės aktus su Sąjungos teise, kiek nuo tos nuostatos išaiškinimo, todėl manau, kad pirmiausia reikėtų atsakyti į klausimą, susijusį su šiuo straipsniu.

2. Antrasis prejudicinis klausimas

113. Šiame prašyme priimti prejudicinį sprendimą iš tikrųjų nurodytas tik kankinimo ir nežmoniško ar žeminančio elgesio arba baudimo uždraudimas, užtikrinamas pagal Chartijos 4 straipsnį, todėl turiu į tai atkreipti dėmesį.

114. Darydamas nuorodą į Chartijos 4 straipsnį prašymą priimti prejudicinį sprendimą pateikęs teismas nori pabrėžti, kad nacionalinės teisės normos tikslas taip pat yra įvykdyti valdžios institucijai tenkančią *pozityvią pareigą* nustatyti „teisin[į] pagrind[ą], kuris sudarytų sąlygas efektyviam nusikalstamos veikos tyrimui ir efektyviam nubaudimui už nepilnamečių seksualinį išnaudojimą ir kuris faktiškai leistų identifikuoti nusikalstamą veiką padariusį asmenį ir tuomet, kai naudotasi elektroninių ryšių priemonėmis“ [81].

115. Manau, kad ši konkreti *pozityvi pareiga* labai nesiskiria nuo kiekvienos konkrečios pareigos, kurią valstybė turi vykdyti, laikydamasi paskelbto pagrindinių teisių sąrašo. Žmogaus teisė į gyvybę (Chartijos 2 straipsnis), teisė į fizinę neliečiamybę (Chartijos 3 straipsnis) ar teisė į duomenų apsaugą (Chartijos 8 straipsnis), taip pat saviraiškos laisvė (Chartijos 11 straipsnis) ar minties, sąžinės ir religijos laisvė (Chartijos 10 straipsnis) reiškia, kad valstybė privalo nustatyti teisinį pagrindą, pagal kurį užtikrinama, kad šiomis teisėmis ir laisvėmis būtų veiksmingai naudojamasi, prireikus panaudojant valdžios institucijų monopolizuotas jėgos priemones prieš bet kurį subjektą, ketinantį uždrausti arba sudaryti kliūčių naudotis jomis [82].

116. Dėl nepilnamečių seksualinio išnaudojimo EŽTT mano, kad vaikai ir kiti pažeidžiami asmenys turi specialią teisę į valstybės teikiamą apsaugą, užtikrinamą priimant baudžiamojo pobūdžio teisės normas, pagal kurias veiksmingai baudžiama už šių nusikalstamų veikų padarymą ir toks baudimas turi atgrasomąjį poveikį [83].

117. Ši speciali teisė į apsaugą įtvirtinta ne tik Chartijos 4 straipsnyje, taigi natūraliai galima remtis 1 straipsniu (žmogaus orumas) arba 3 straipsniu (teisė į asmens fizinę ir psichinę neliečiamybę).

[81] Antrojo klausimo formuluotė (*in fine*). Ši nuoroda į elektroninių ryšių priemones reiškia, kad klausime minima antroji valstybėms tenkanti *pozityvi pareiga*, nustatyta Chartijos 8 straipsnyje dėl asmens duomenų apsaugos. Tai, kad Chartijos 8 straipsnis nurodytas du kartus, rodo, jog prašymą priimti prejudicinį sprendimą pateikęs teismas Chartijoje įtvirtintoms teisėms priskiria dvejopą funkciją, atsižvelgdamas į jų pobūdį: funkciją *riboti* ginčijamą pareigą ir ją *pateisinti*.

[82] Šią pareigą užtikrinti veiksmingumą lemia socialinėje ar paslaugas teikiančioje valstybėje valdžios institucijoms suteiktas įgaliojimas siekti rezultatų; tokioje valstybėje ne tik oficialiai pripažįstamos teisės, bet ir svarbu praktiškai įgyvendinti materialinį šių teisių turinį.

[83] 2008 m. gruodžio 2 d. EŽTT sprendimas *K.U. prieš Suomiją* (ECHR:2008:1202JUD000287202, 46 punktas).

118. Nors vertinant teisines vertybes, kurioms turi poveikį nacionalinės teisės aktai, negalima neatsižvelgti į valdžios institucijų pozityvią pareigą užtikrinti vaikų ir kitų pažeidžiamų asmenų apsaugą [84], ši pareiga taip pat negali tapti „pernelyg didele našta“ valdžios institucijoms [85] ir būti įgyvendinama, nepaisant teisėtumo ar pagarbos likusioms pagrindinėms teisėms [86].

3. Pirmasis prejudicinis klausimas

119. Prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės nori išsiaiškinti, ar pagal Sąjungos teisę yra draudžiamas nacionalinis įstatymas, dėl kurio jis turi nuspręsti, nagrinėdamas konstitucinį skundą.

120. Kadangi Teisingumo Teismas jau pateikė Direktyvos 2002/58 išaiškinimą, atitinkantį susijusias Chartijos nuostatas, atsakant į prejudicinį klausimą reikės atsižvelgti į Sprendime *Tele2 Sverige ir Watson* įtvirtintą jurisprudenciją ir prireikus pateikti papildomų patikslinimų.

121. Remiantis šia prielaida, aiškinimo gairėse, kurias galima pateikti *Cour constitutionnelle* (Konstitucinis Teismas), kad jis pats patikrintų, ar nacionalinės teisės aktas atitinka Sąjungos teisę, turi būti atskirai nagrinėjamas tame nacionalinės teisės akte reglamentuojamas duomenų saugojimas ir prieiga prie šių duomenų.

a) Duomenų saugojimo sąlygos

122. Belgijos vyriausybė pabrėžia, kad ji norėjo nustatyti aiškų teisinį pagrindą, apimantį garantijas, kurių reikia privačiam gyvenimui apsaugoti, o ne remtis elektroninių ryšių paslaugas teikiančių operatorių praktika, susijusia su duomenų saugojimu siekiant pateikti sąskaitas ir tvarkyti klientų prašymus dėl informacijos.

123. Ši vyriausybė mano, kad bendros prevencinės pareigos saugoti duomenis tikslas yra ne tik nustatyti sunkias nusikalstamas veikas, atlikti jų ikiteisminį tyrimą ir vykdyti persekiojimą dėl jų, bet ir užtikrinti nacionalinio saugumo apsaugą, ginti teritoriją, užtikrinti visuomenės saugumą, nustatyti ir ištirti veikas, kurios nėra sunkios nusikalstamos veikos, ir vykdyti persekiojimą dėl jų arba užkirsti kelią draudžiamam elektroninių ryšių sistemų naudojimui [87], taip pat bet kuris kitas tikslas, nurodytas Reglamento 2016/679 23 straipsnio 1 dalyje.

84 Šiuo klausimu manau, kad prašymą priimti prejudicinį sprendimą pateikusio teismo nurodytas teises (kaip *ribojančias*, o ne *pateisinančias* nagrinėjamą pareigą) būtų galima papildyti teise į veiksmingą teisinę gynybą (Chartijos 47 straipsnis) arba teise į gynybą (Chartijos 48 straipsnis), kurių galimas pažeidimas taip pat buvo nagrinėjamas pagrindinėje byloje. Vis dėlto nutarties dėl prašymo priimti prejudicinį sprendimą rezoliucinėje dalyje minimi tik Chartijos 7, 8 ir 11 straipsniai ir 52 straipsnio 1 dalis.

85 1998 m. spalio 28 d. EŽTT sprendimas *Osman prieš Jungtinę Karalystę* (CE:ECHR:1998:1028JUD002345294, 116 punktas).

86 Ten pat, 116 punktas *in fine*: „[reikia užtikrinti], kad policija vykdytų savo įgaliojimus kovoti su nusikalstamomis veikomis ir užkirsti joms kelią, visiškai laikydamasi teisės aktuose numatytų priemonių ir kitų garantijų, kuriomis teisėtai apribojama jos veiksmų, atliekamų tiriant nusikalstamas veikas, apimtis“. Taip pat žr. 2008 m. gruodžio 2 d. EŽTT sprendimą *K.U. prieš Suomiją* (CE:ECHR:2008:1202JUD000287202, 48 punktas). Teisingumo Teismas 2019 m. liepos 29 d. Sprendimo *Gambino ir Hyka* (C-38/18, EU:C:2019:628) 49 punkte taip pat yra nurodęs, kad nukentėjusiam asmeniui pripažįstamos teisės negali daryti poveikio veiksmingam naudojimuisi kaltinamajam pripažįstamomis teisėmis.

87 Ši pareiga taip pat pateisinama siekiu reaguoti į skambutį skubios pagalbos tarnybai ar rasti dingusį asmenį, kurio fizinei neliečiamybei gresia tiesioginis pavojus.

124. Belgijos vyriausybė teigia, kad:

– vien dėl paties duomenų saugojimo negalima daryti labai tikslių išvadų, susijusių su atitinkamų asmenų privačiu gyvenimu: tokias išvadas būtų galima daryti tik jeigu taip pat būtų teikiama prieiga prie saugomų duomenų,

– įstatyme numatyta apsaugos priemonių, skirtų privatumui apsaugoti, kaip antai, be kita ko, duomenų saugojimas nėra susijęs su pranešimų turiniu; visapusiškai taikomos garantijos, kiek tai susiję su saugojimo pateisinimu, teise į prieigą, teise taisyti duomenis ir kitomis teisėmis; paslaugų teikėjai ir operatoriai saugomiems duomenims turi taikyti tas pačias saugumo ir apsaugos pareigas bei priemones kaip ir tos, kurios taikomos tinkle pateikiamiems duomenims, ir neleisti netyčia arba neteisėtai juos sunaikinti arba netyčia prarasti ar pakeisti,

– duomenys gali būti saugomi dvylika mėnesių (pasibaigus šiam laikotarpiui jie turi būti sunaikinti) ir tik Sąjungos teritorijoje,

– paslaugų teikėjai ir operatoriai turi taikyti technologinės apsaugos priemones, dėl kurių vos tik užregistruoti saugomi duomenys taptų nenuskaitomi ir joks asmuo, neturintis leidimo susipažinti su jais, negalėtų jų naudoti,

– bet kuriuo atveju šie veiksmai vykdomi prižiūrint Belgijos pašto ir telekomunikacijų sektorių reguliavimo institucijai ir Duomenų apsaugos institucijai.

125. Nepaisant šių garantijų, Belgijos teisės aktuose iš tikrųjų nustatyta elektroninių ryšių paslaugų teikėjams ir operatoriams taikoma bendra ir nediferencijuota pareiga saugoti srauto ir vietos nustatymo duomenis, kaip tai suprantama pagal Direktyvą 2002/58, tvarkomus teikiant šias paslaugas. Jau minėta, kad apskritai saugojimo laikotarpis yra dvylika mėnesių: nenumatyta jokio laiko apribojimo atsižvelgiant į saugomų duomenų kategorijas.

126. Ši bendra ir nediferencijuota pareiga saugoti duomenis taikoma nuolat ir visą laiką. Net jeigu jos tikslas yra užkirsti kelią visų rūšių nusikalstamai veikai (pradedant su nacionaliniu saugumu ir gynyba susijusia ar labai sunkia nusikalstama veika ir baigiant veika, už kurią skiriama trumpesnė nei vienų metų laisvės atėmimo bausmė), ištirti šią veiką ir vykdyti persekiojimą dėl jos, tokio pobūdžio pareiga neatitinka Teisingumo Teismo jurisprudencijos, taigi negali būti laikoma atitinkančia Chartiją.

127. Belgijos įstatymų leidėjas, siekdamas suderinti nacionalinę teisę su šia jurisprudencija, turės išnagrinėti kitas priemones (kaip antai nurodytas pirma), kuriose būtų nustatytos riboto saugojimo taisyklės. Šios kiekvienai duomenų kategorijai skirtingos taisyklės turi atitikti principą, pagal kurį saugotini tik *būtinai* reikalingi duomenys, atsižvelgiant į riziką ar grėsmę, ir tik ribotą laikotarpį, priklausantį nuo saugomos informacijos pobūdžio. Bet kuriuo atveju negali būti suteikiama galimybė remiantis saugomais duomenimis susidaryti tikslų *vaizdą* apie atitinkamų asmenų privatų gyvenimą, įpročius, elgesį ar socialinius ryšius.

b) Sąlygos, kuriomis valdžios institucijoms suteikiama prieiga prie saugomų duomenų

128. Manau, kad Sprendime *Tele2 Sverige ir Watson* [88] nurodytos sąlygos yra svarbios, taip pat ir kalbant apie prieigą: nacionalinės teisės aktuose turi būti numatytos materialinės ir procedūrinės sąlygos, reglamentuojančios kompetentingų institucijų prieigą prie saugomų duomenų [89].

129. Belgijos vyriausybė nurodo, kad 2005 m. įstatymo (dėl elektroninių ryšių) 126 straipsnio 2 dalyje [90] nacionalinės institucijos, galinčios gauti saugomus duomenis pagal to paties straipsnio 1 dalį, yra apibrėžiamos siaurai.

130. Prie šių institucijų priskiriamos visiškai teisminės institucijos ir prokuratūra; valstybės saugumo pajėgos; Generalinė žvalgybos ir saugumo tarnyba, kontroliuojama atitinkamų nepriklausomų komisijų; Belgijos pašto ir telekomunikacijų instituto kriminalinės policijos pareigūnai; skubios pagalbos tarnybos; Federalinės policijos dingusių asmenų padalinio kriminalinės policijos pareigūnai; Tarpininkavimo sprendžiant telekomunikacijų ginčus tarnyba ir finansų sektoriaus priežiūros įstaiga.

131. Apskritai Belgijos vyriausybė teigia, kad nacionalinės teisės aktuose neleidžiama įvairioms tarnyboms suteikti prieigą prie duomenų tam, kad būtų aktyviai siekiama išsiaiškinti nenustatytas grėsmes arba grėsmes, apie kurias nėra konkrečios informacijos. Taigi nacionalinės institucijos paprasčiausiai negali susipažinti su neapdorotais pranešimų duomenimis ir automatiškai juos tvarkyti, siekdamos gauti informacijos ir aktyviai užkirsti kelią saugumui kylantiems pavojams.

132. Belgijos vyriausybė tvirtina, kad prieigai prie duomenų taikomos griežtos sąlygos, atsižvelgiant į kiekvienos kompetentingos nacionalinės institucijos statusą.

133. Manau, kad norėdamas atsakyti į pirmąjį prejudicinį klausimą Teisingumo Teismas neturi išsamiai nagrinėti sąlygų, taikomų siekiant kiekvienai iš šių institucijų suteikti saugomus duomenis. Šią užduotį veikiau turi atlikti prašymą priimti prejudicinį sprendimą pateikęs teismas – jis ją turės įvykdyti, atsižvelgdamas į sprendimuose *Tele2 Sverige ir Watson* ir *Ministerio Fiscal* pateiktas gaires.

134. Be to, iš Belgijos vyriausybės pateiktos informacijos matyti, kad prieigos sąlygos, taikomos teisminėms institucijoms ar prokuratūrai [91], siekiant nustatyti nusikalstamas veikas, atlikti jų ikiteisminį tyrimą ir vykdyti persekiojimą dėl jų pagal Baudžiamojo proceso kodekso 46bis [92] ir 88bis [93] straipsnius, labai skiriasi nuo sąlygų, taikomų kitoms institucijoms.

88 Žr. šios išvados 60 punktą.

89 Sprendimo *Tele2 Sverige ir Watson* 118 punktas.

90 126 straipsnis suformuluotas 2016 m. gegužės 29 d. įstatyme.

91 Tai, ar prokuratūra gali nustatyti šios rūšies priemones, nagrinėjama gavus prašymą priimti prejudicinį sprendimą byloje *HK / Prokuratur*, C-746/18 (Byla dar nagrinėjama).

92 Prokuratūra turi kompetenciją reikalauti iš operatorių identifikacinių duomenų motyvuotu sprendimu, kuris pateikiamas raštu (skubiais atvejais žodžiu) ir kuriame patvirtinama, kad priemonė proporcinga atsižvelgiant į privatumą ir subsidiari atsižvelgiant į visas kitas su tyrimu susijusias pareigas. Dėl nusikalstamų veikų, kurios neužtraukia pagrindinės vienų metų laisvės atėmimo ar sunkesnės bausmės, prokuratūra gali prašyti tik duomenų už šešių mėnesių laikotarpį iki savo sprendimo priėmimo.

93 Ikiteisminio tyrimo teisėjas turi kompetenciją reikalauti, kad operatoriai atliktų elektroninių pranešimų ar saugomų srauto ir vietos nustatymo duomenų paiešką; šią priemonę jis gali taikyti priėmęs motyvuotą rašytinę (skubiais atvejais žodinę) nutartį, kuriai taikomi tie patys proporcingumo ir subsidiarumo reikalavimai kaip ir prokuratūros atveju, jei yra rimtų požymių, kad padaryta nusikalstama veika, už kurią baudžiama konkrečia bausme. Tam tikros išimtys taikomos tuo atveju, kai priemonė nukreipta prieš tam tikrų kategorijų specialistus, kuriems taikoma apsauga (pavyzdžiui, advokatus ar gydytojus).

135. Dėl žvalgybos ir saugumo tarnybų pažymėtina, kad pagal 1998 m. įstatymą prašymas suteikti prieigą prie operatorių turimų srauto ir vietos nustatymo duomenų turi būti pagrįstas objektyviais kriterijais, siekiant užtikrinti, kad prieiga būtų apribota tuo, kas griežtai būtina, remiantis anksčiau nustatyta grėsme [94]. Atsižvelgiant į galimą grėsmę, numatyti įvairūs prieigos terminai (šeši, devyni ar dvylika mėnesių), o prašymas turi atitikti proporcingumo ir subsidiarumo principus. Taip pat buvo sukurtas kontrolės mechanizmas, už kurį atsakinga nepriklausoma institucija [95].

136. Dėl Belgijos pašto ir telekomunikacijų instituto (BIPT) kriminalinės policijos pareigūnų pažymėtina, kad prieiga prie telekomunikacijų operatorių turimų duomenų jiems suteikiama labai ribotais konkrečiais atvejais [96], prižiūrint prokuratūrai; Belgijos vyriausybė teigia, kad šių pareigūnų veikla neapima asmenų, kurių duomenys saugomi.

137. Dėl skubios pagalbos tarnybų, teikiančių pagalbą įvykio vietoje, pažymėtina, kad jos gali reikalauti skubios pagalbos prašiusio skambintojo duomenų, jeigu po pagalbos skambučio tos tarnybos iš paslaugų teikėjo ar operatoriaus negauna skambintoją identifikuojančių duomenų arba gauna neišsamius ar neteisingus duomenis.

138. Kalbant apie Federalinės policijos dingusių asmenų padalinio kriminalinės policijos pareigūnus, pažymėtina, kad jie gali operatoriaus prašyti duomenų, reikalingų siekiant rasti dingusį asmenį, kurio fizinei neliečiamybei gresia tiesioginis pavojus. Suteikus prieigą, kuriai taikomos griežtos sąlygos, galima susipažinti tik su duomenimis, leidžiančiais identifikuoti naudotoją, ir duomenimis, susijusiais su galinio įrenginio prieiga bei prijungimu prie tinklo ir paslaugų, taip pat šios įrangos buvimo vieta; tokia prieiga suteikiama tik prie duomenų, saugomų 48 valandas iki prašymo gavimo.

139. Dėl Tarpininkavimo sprendžiant telekomunikacijų ginčus tarnybos pažymėtina, kad ji gali prašyti tik duomenų, identifikuojančių asmenį, kuris elektroninių ryšių tinklu ar paslauga pasinaudojo kenkėjiškais tikslais. Šiuo atveju teisminė institucija ar nepriklausoma administracinė institucija (kuri nėra Tarpininkavimo tarnyba) nevykdo išankstinės kontrolės.

140. Galiausiai finansų sektoriaus priežiūros įstaiga, siekdama kovoti su finansiniais nusikaltimais, gali prašyti suteikti prieigą prie srauto ir vietos nustatymo duomenų; dėl šios prieigos turi būti gautas išankstinis ikiteisminio tyrimo teisėjo leidimas.

141. Išdėsčius šias prieigos prie saugomų duomenų taisykles ir sąlygas, taikomas kiekvienai tuos duomenis galinčiai gauti institucijai, akivaizdu, kad atvejai ir apsaugos priemonės yra įvairūs ir prašymą priimti prejudicinį sprendimą pateikęs teismas turi išnagrinėti, ar jie tiksliai atitinka Teisingumo Teismo jurisprudencijoje taikomus kriterijus [97].

94 Prireikus sprendime nurodomi fiziniai ar juridiniai asmenys, faktinės asociacijos ar grupės, objektai, vietos, įvykiai ar informacija, kuriems taikomas konkretus metodas. Taip pat turi būti nurodytas prašomų duomenų tikslo ir galimos grėsmės, pateisinančios šį konkretų metodą, ryšys.

95 Administracinė komisija, kuriai pavesta žvalgybos ir saugumo tarnybų naudojamų specialių ir išimtinių duomenų rinkimo metodų priežiūra (Komisija BIM) ir Nuolatinis žvalgybos tarnybų kontrolės komitetas (Komitetas R). Belgijos vyriausybė pažymi, kad Komisija BIM atsakinga už žvalgybos ir saugumo tarnybų naudojamų paieškos metodų stebėjimą – ji atlieka šių metodų pirmos linijos patikrinimą. Komisija, kurią sudaro teisėjai, savo užduotis vykdo visiškai nepriklausomai. Taip pat organizuojamas nepriklausomas antros linijos patikrinimas, už kurį atsakingas Komitetas R.

96 Prieigą leidžiama suteikti siekiant nustatyti nusikalstamas veikas, numatytas 2005 m. birželio 13 d. Įstatymo dėl elektroninių ryšių 114 straipsnyje (tinklų saugumas), 124 straipsnyje (elektroninių ryšių konfidencialumas) ir 126 straipsnyje (duomenų saugojimas ir prieiga), atlikti šių veikų ikiteisminį tyrimą ir vykdyti persekiojimą dėl jų.

97 Darau nuorodą į šios išvados 60 punktą.

142. Pavyzdžiui, atkreipiu dėmesį į tai, kad nagrinėjamuose teisės aktuose nenustatyta, jog kompetentingos nacionalinės institucijos privalo sistemingai informuoti duomenų subjektus apie tai, kad su jų duomenimis buvo susipažinta (išskyrus atvejus, kai toks informavimas kenkia atliekamiems tyrimams). Taip pat atrodo, kad bent tam tikrais atvejais, kaip antai susijusiais su finansiniais nusikaltimais, nėra nustatyta iš anksto apibrėžtų taisyklių dėl šių nusikaltimų sunkumo, siekiant pateisinti prieigą prie atitinkamų duomenų. Ne visada yra akivaizdus ryšys tarp apribojimo dydžio ir tiriamos nusikalstamos veikos sunkumo, kaip tai suprantama pagal Sprendimą *Ministerio Fiscal*.

143. Bet kuriuo atveju manau, kad, kai dėl jau išdėstytų priežasčių pats bendras ir nediferencijuotas šių duomenų saugojimas yra pagrindinė priežastis, kodėl nacionalinės teisės aktai, dėl kurių pateiktas šis prašymas priimti prejudicinį sprendimą, neatitinka Sąjungos teisės, pagrindai, susiję su institucijų prieiga prie duomenų, tampa antraeiliai.

4. Trečiasis prejudicinis klausimas

144. *Cour constitutionnelle* (Konstitucinis Teismas) nori išsiaiškinti, ar tuo atveju, jeigu atsižvelgiant į Teisingumo Teismo atsakymą būtų pripažinta, kad nacionalinės teisės aktai neatitinka Sąjungos teisės, būtų galima laikinai palikti galioti tuos teisės aktus. Taip būtų išvengta teisinio nesaugumo ir sudarytos sąlygos surinktus ir saugomus duomenis toliau naudoti siekiamiems tikslams įgyvendinti.

145. Egzistuoja suformuota jurisprudencija, pagal kurią „tik Teisingumo Teismas gali išimties tvarka ir dėl privalomų teisinio saugumo pagrindų laikinai sustabdyti tiesiogiai taikytinos Sąjungos teisės normos naikinamąjį poveikį jai prieštaraujančios nacionalinės teisės atžvilgiu“. Jeigu „nacionaliniai teismai turėtų įgaliojimus, nors ir laikinai, suteikti nacionalinėms nuostatoms viršenybę prieš Sąjungos teisę, kurios jos neatitinka, būtų padaryta žala vienodam Sąjungos teisės taikymui“ [98].

146. Komisija mano, kad į šį prašymą priimti prejudicinį sprendimą pateikusio teismo klausimą reikėtų atsakyti neigiamai, nes Teisingumo Teismas Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo galiojimo neapribojo laiko atžvilgiu [99].

147. Vis dėlto Teisingumo Teismas 2012 m. vasario 28 d. Sprendime *Inter-Environnement Wallonie ir Terre wallonne* [100] pažymėjo, kad nacionaliniam teismui, remiantis su aplinkos apsauga susijusiu privalomuoju pagrindu, gali būti leidžiama išimties tvarka pasinaudoti nacionalinės teisės nuostata, suteikiančia jam teisę palikti galioti tam tikrus nacionalinės teisės akto, panaikinto dėl Sąjungos teisės normos pažeidimo, padarinius [101].

98 2016 m. liepos 28 d. Sprendimo *Association France Nature Environnement* (C-379/15, EU:C:2016:603) 33 punktas.

99 Komisijos rašytinių pastabų 100 punktas.

100 Byla C-41/11, EU:C:2012:103.

101 2012 m. vasario 28 d. Sprendimo *Inter-Environnement Wallonie ir Terre wallonne* (C-41/11, EU:C:2012:103) 58 punktas. 2016 m. liepos 28 d. Sprendimo *Association France Nature Environnement* (C-379/15, EU:C:2016:603) 34 punkte Teisingumo Teismas, remdamasis šiuo teiginiu, padarė išvadą, kad „siek[iama] kiekvienu konkrečiu atveju įvertinus aplinkybes išimties tvarka pripažinti nacionalinio teismo įgaliojimus pakeisti nacionalinės teisės nuostatos, pripažintos nesuderinama su Sąjungos teise, panaikinimo padarinius“.

148. Ši jurisprudencija buvo patvirtinta 2019 m. liepos 29 d. Sprendime *Inter-Environnement Wallonie ir Bond Beter Leefmilieu Vlaanderen* [102]. Nesvarbu, ar sprendimas priimtas aplinkosaugos srityje, ar pagrįstas elektros tiekimo saugumu, nematau priežasčių jo netaikyti kitose Sąjungos teisės srityse, visų pirma srityje, kuri nagrinėjama šioje byloje.

149. Jeigu remiantis „su aplinkos apsauga susijusiu privalomuoju pagrindu“ ir galima pateisinti nacionalinių teismų galimybę išimties tvarka palikti galioti tam tikrus nacionalinės teisės nuostatos, neatitinkančios Sąjungos teisės, padarinius, taip yra dėl to, kad aplinkos apsauga – tai „vienas pagrindinių ir esminių Sąjungos tikslų, taikomas daugelyje sričių“ [103].

150. Taigi vienas iš Sąjungos tikslų taip pat yra saugumo erdvės sukūrimas (ESS 3 straipsnis), apimantis pagarbą esminėms valstybės funkcijoms, visų pirma funkcijoms, kurių tikslas – užtikrinti viešąją tvarką ir nacionalinį saugumą (ESS 4 straipsnio 2 dalis). Tai tikslas, kuris taip pat yra „taikomas daugelyje sričių ir esminis“, kaip ir aplinkos apsauga, nes jo įvykdymas yra būtina sąlyga siekiant sukurti teisinį pagrindą, leidžiantį užtikrinti, kad būtų veiksmingai naudojamasi pagrindinėmis teisėmis ir laisvėmis.

151. Manau, kad šioje byloje remiantis su nacionalinio saugumo apsauga susijusiais privalomaisiais pagrindais būtų galima pateisinti tai, kad Teisingumo Teismas išimties tvarka leistų prašymą priimti prejudicinį sprendimą pateikusiam teismui bent palikti galioti tam tikrus nagrinėjamo įstatymo padarinius.

152. Tam, kad paliktų galioti šiuos padarinius, prašymą priimti prejudicinį sprendimą pateikęs teismas, atsižvelgdamas į Teisingumo Teismo sprendimą, turėtų nacionalinės teisės aktą pripažinti neatitinkančiu Sąjungos teisės ir nuspręsti, kad padarytas labai neigiamas poveikis, dėl kurio, siekiant užtikrinti visuomenės saugumą ar valstybės saugumą, tas teisės aktas galėtų būti nedelsiant panaikintas (jeigu teisės aktas pagal nacionalinę teisę panaikinamas dėl to, kad pripažinta jo neatitiktis Sąjungos teisei) arba netaikomas.

153. Be to, norint laikinai palikti galioti nacionalinės teisės akto padarinius (visus ar dalį jų), reikėtų, kad:

– taip būtų siekiama išvengti teisinio vakuumo, kurio padariniai būtų tokie pat žalingi kaip ir atsiradę taikant nagrinėjamą teisės aktą, t. y. vakuumo, kurio nebūtų galima panaikinti kitomis priemonėmis ir dėl kurio nacionalinės institucijos netektų vertingos priemonės, siekdamos užtikrinti valstybės saugumą,

– tie padariniai būtų palikti galioti tik laikotarpiu, būtinai reikalingu siekiant priimti priemones, kurios leistų pašalinti nurodytą neatitiktį Sąjungos teisei [104].

154. Priimti tokį sprendimą taip pat reikėtų dėl to, kad nacionalinės teisės normas sunku suderinti su Sprendime *Tele2 Sverige ir Watson* įtvirtinta jurisprudencija [105] ir kad Belgijos teisės aktų leidėjas iš dalies pakeitė nacionalinės teisės aktus tam, kad būtų užtikrintas Sprendimo *Digital Rights* laikymasis. Šis precedentas leidžia manyti, kad 2016 m. gegužės 29 d. įstatymas (priimtas prieš sužinant apie Sprendimą *Tele2 Sverige ir Watson*) taip pat bus suderintas su šiame sprendime įtvirtinta jurisprudencija.

[102] Byla C-411/17 (EU:C:2019:622, 178 punktas).

[103] 2012 m. vasario 28 d. Sprendimo *Inter-Environnement Wallonie ir Terre wallonne* (C-41/11, EU:C:2012:103) 57 punktas.

[104] 2012 m. vasario 28 d. Sprendimo *Inter-Environnement Wallonie ir Terre wallonne* (C-41/11, EU:C:2012:103) 62 punktas.

[105] Danijos vyriausybės pastabų 45 punktas.

V. Išvada

155. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) pateikti tokį atsakymą:

1. 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 bei 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją:

   – draudžiamas nacionalinės teisės aktas, kuriame elektroninių ryšių paslaugų teikėjams ir operatoriams nustatyta pareiga bendrai ir nediferencijuotai saugoti visų abonentų ir naudotojų srauto ir vietos nustatymo duomenis, susijusius su visomis elektroninių ryšių priemonėmis,

   – šiai išvadai neturi įtakos tai, kad tuo nacionalinės teisės aktu siekiama ne tik nustatyti ir ištirti sunkias ar nesunkias nusikalstamas veikas ir vykdyti persekiojimą dėl jų, bet ir užtikrinti nacionalinį saugumą, ginti teritoriją, užtikrinti visuomenės saugumą, užkirsti kelią neleistinam elektroninių ryšių sistemos naudojimui ar įgyvendinti bet kurį kitą tikslą, numatytą 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) 23 straipsnio 1 dalyje,

   – šiai išvadai įtakos taip pat neturi tai, kad prieigai prie saugomų duomenų taikomos konkrečiai reglamentuojamos garantijos. Prašymą priimti prejudicinį sprendimą pateikęs teismas turi patikrinti, ar nacionalinės teisės akte, reglamentuojančiame sąlygas, kuriomis ši prieiga suteikiama kompetentingoms institucijoms, nustatyta, kad prieiga galima tik konkrečiais atvejais, dėl kurių rimtumo būtina imtis veiksmų; nurodyta, kad tokia prieiga suteikiama tik jeigu teismas arba nepriklausoma institucija atliko išankstinę kontrolę (išskyrus skubius atvejus); numatyta, kad duomenų subjektai būtų informuojami apie šią prieigą, jei toks informavimas nekenkia minėtų institucijų veiklai.

2. Europos Sąjungos pagrindinių teisių chartijos 4 ir 6 straipsniai neturi įtakos aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį, susijusią su minėtais kitais šios Chartijos straipsniais, taigi pagal juos negalima nustatyti, kad nacionalinės teisės aktas, kaip antai nagrinėjamas pagrindinėje byloje, neatitinka Sąjungos teisės.

3. Nacionalinis teismas gali, jei tai leidžiama pagal nacionalinę teisę, išimties tvarka palikti laikinai galioti teisės aktą, kaip antai nagrinėjamą pagrindinėje byloje, net jei tas teisės aktas neatitinka Sąjungos teisės, jeigu toks palikimas galioti pateisinamas privalomaisiais pagrindais, susijusiais su grėsmėmis visuomenės saugumui ar nacionaliniam saugumui, kurių negalima panaikinti taikant kitas priemones ar kitas alternatyvas. Palikti galioti teisės aktą galima tik tol, kol to neišvengiamai reikia minėtam nesuderinamumui su Sąjungos teise panaikinti.