



Teisingumo Teismas patvirtino, kad pagal Sąjungos teisę draudžiamas bendras ir nediferencijuotas elektroninių ryšių srauto ir vietos nustatymo duomenų saugojimas kovos su sunkiais nusikaltimais tikslais

Nacionalinis teismas negali apriboti negaliojančiu pripažinto nacionalinio teisės akto, nustatančio tokių duomenų saugojimą, poveikio laiko atžvilgiu

2015 m. kovo mėn. G.D. buvo nuteistas laisvės atėmimo bausme iki gyvos galvos dėl moters nužudymo Airijoje. Dėl jo nuteisimo Airijos apeliaciniame teisme pateiktame apeliaciniame skunde suinteresuotasis asmuo, be kita ko, priekaištavo pirmosios instancijos teismui, kad šis klaidingai srauto ir vietos nustatymo duomenis, susijusius su telefoniniais skambučiais, pripažino įrodymais. Kad vykstant baudžiamajam procesui galėtų ginčyti minėtų įrodymų priimtinumą, G.D. paraleliai Airijos aukštajame teisme pradėjo civilinį procesą dėl 2011 m. Airijos įstatymo, kuriuo reglamentuojamas šių duomenų saugojimas ir prieiga prie jų, kai kurių nuostatų pripažinimo negaliojančiomis, nes šiuo įstatymu pažeidžiamos Sąjungos teisės jam suteikiamos teisės. 2018 m. gruodžio 6 d. sprendimu Aukštasis teismas pritarė G.D. argumentams. Dėl šio sprendimo Airija pateikė apeliacinį skundą Airijos Aukščiausiąjame Teisme, kuris yra prašymą priimti prejudicinį sprendimą pateikęs teismas šioje byloje.

Prašymu priimti prejudicinį sprendimą Aukščiausiasis Teismas prašė išaiškinti Sąjungos teisės reikalavimus, taikomus saugant minėtus duomenis kovos su sunkiais nusikaltimais tikslais, bei būtinas garantijas, kurios turėtų būti taikomos prieigai prie tokių duomenų. Be to, jam taip pat kilo klausimas dėl teisės akto, kurį jis turėtų pripažinti nesuderinamu su Sąjungos teise, apimties ir poveikio laiko atžvilgiu, nes Airijos 2011 m. įstatymas buvo priimtas siekiant į nacionalinę teisę perkelti Direktyvą 2006/24/EB¹, kurią Teisingumo Teismas pripažino negaliojančia 2014 m. balandžio 8 d. Sprendimu *Digital Rights Ireland ir kt.*²

Savo sprendime Teisingumo Teismas (didžioji kolegija), pirma, patvirtino savo suformuotą jurisprudenciją³, kuria remiantis pagal Sąjungos teisę⁴ **draudžiamos nacionalinės teisėkūros priemonės, prevenciškai numatančios bendrą ir nediferencijuotą elektroninių ryšių srauto ir vietos nustatymo duomenų saugojimą kovos su sunkiais nusikaltimais tikslais.**

Iš tiesų Direktyva dėl privatumo ir elektroninių ryšių ne tik reglamentuojama prieiga prie tokių duomenų numatant garantijas, kuriomis siekiama užkirsti kelią piktnaudžiavimui, bet visų pirma

¹ 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB 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).

² 2014 m. balandžio 8 d. Sprendimas *Digital Rights Ireland*, [C-293/12](#), (žr. pranešimą spaudai [Nr. 54/14](#)).

³ 2014 m. balandžio 8 d. Sprendimas *Digital Rights Ireland*, [C-293/12](#); 2016 m. gruodžio 21 d. Sprendimas *Tele2 Sverige ir Watson ir kt.*, [C-203/15 ir C-698/15](#) (žr. pranešimą spaudai [Nr. 145/16](#)); 2020 m. spalio 6 d. sprendimai *Privacy International*, [C-623/17](#), *La Quadrature du Net ir kt.*, [C-511/18 ir C-512/18](#) bei *Ordre des barreaux francophones et germanophone ir kt.*, [C-520/18](#) (žr. pranešimą spaudai [Nr. 123/20](#)), ir 2021 m. kovo 2 d. Sprendimas *Prokuratuur (Prieigos prie elektroninių pranešimų duomenų sąlygos)*, [C-746/18](#) (žr. pranešimą spaudai [Nr. 29/21](#)).

⁴ 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. leidimas lietuvių k. 13 sk., 29 t., p. 514), iš dalies pakeista 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (OL L 337, 2009, p. 11) (toliau – Direktyva dėl privatumo ir elektroninių ryšių), siejama su Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi.

įtvirtinamas **draudimo saugoti** srauto ir vietos nustatymo duomenis **principas**. Taigi tokių duomenų saugojimas yra, pirma, draudimo saugoti tokius duomenis išimtis, ir, antra, Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą suvaržymas.

Nors Direktyva dėl privatumo ir elektroninių ryšių leidžia valstybėms narėms apriboti šias teises ir pareigas, be kita ko, kovos su nusikalstamomis veikomis tikslu, vis dėlto tokie apribojimai turi atitikti proporcingumo principą. Šis principas reikalauja, kad būtų laikomasi ne tik tinkamumo ir būtinumo reikalavimų, bet ir reikalavimo, kad tokios priemonės būtų **proporcingos** siekiamam tikslui. Taigi Teisingumo Teismas jau yra nusprendęs, kad vien kovos su sunkiais nusikaltimais tikslas, kad ir koks fundamentalus būtų, negali pateisinti to, kad bendro ir nediferencijuoto srauto ir vietos nustatymo duomenų saugojimo priemonė, kaip antai įtvirtintina Direktyvoje 2006/24, būtų laikoma būtina. Taip pat net valstybių narių pareigomis veikti, kurios susijusios su taisyklių, leidžiančių veiksmingai kovoti su nusikalstamomis veikomis, nustatymu, negalima pateisinti tokių didelių suvaržymų, kokie nustatyti nacionalinės teisės aktuose, numatančiuose beveik visų žmonių srauto ir vietos nustatymo duomenų saugojimą, kai negali būti nustatytas, bent jau netiesioginis, duomenų subjektų duomenų ir siekiamo tikslo ryšys.

Teisingumo Teismas priminė, kad pagal Chartiją viešosios valdžios institucijoms tenka įvairios pareigos veikti, pavyzdžiui, priimti teisines priemones, kuriomis siekiama apsaugoti privatų ir šeimos gyvenimą, būsto neliečiamybę, komunikacijos slaptumą bei asmenų fizinę ir psichinę neliečiamybę ar nustatyti kankinimo, nežmoniško ir žeminamo elgesio draudimus. Tokios institucijos turi **suderinti įvairius nagrinėjamus interesus ir teises**. Iš tiesų bendrojo intereso tikslo negalima siekti neatsižvelgiant į tai, kad jis turi būti derinamas su pagrindinėmis teisėmis, kurioms taikoma priemonė, **nustatant pusiausvyrą** tarp, viena vertus, bendrojo intereso tikslo ir, kita vertus, nagrinėjamų teisių, tikrinant, ar šio tikslo svarba atitinka tokia priemone nustatyto suvaržymo dydį.

Atsižvelgiant į tai, Teisingumo Teismas visų pirma atmetė argumentą, kad ypač sunkūs nusikaltimai galėtų būti prilyginti grėsmei nacionaliniam saugumui, kuri yra tikra, esama ar numatoma ir kuria gali būti apibrėžtu laikotarpiu pateisinama bendro ir nediferencijuoto srauto ir vietos nustatymo duomenų saugojimo priemonė. Iš tiesų tokia grėsmė savo pobūdžiu, dydžiu ir ją supančių aplinkybių specifika skiriasi nuo bendros ir nuolatinės rizikos, susijusios su įtampa ar sutrikimais, net dideliais, visuomenės saugumui, ar sunkių nusikaltimų rizikos.

Antra, Teisingumo Teismas patvirtino savo ankstesnę jurisprudenciją ir nusprendė, kad pagal Sąjungos teisę nedraudžiamos teisėkūros priemonės, kuriomis, siekiant kovoti su sunkiomis nusikalstamomis veikomis ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatomas:

- **tikslinis srauto ir vietos nustatymo duomenų saugojimas**, atsižvelgiant į duomenų subjektų kategorijas arba geografinius kriterijus;
- **bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas**;
- **bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas** ir
- operatyvus (anglų k. *quick freeze*) srauto ir vietos nustatymo duomenų, kuriuos turi paslaugų teikėjai, **saugojimas**.

Teisingumo Teismas pateikė paaiškinimus dėl šių skirtingų priemonių kategorijų.

Visų pirma kompetentingos nacionalinės valdžios institucijos gali taikyti tikslinę saugojimo priemonę, pagrįstą geografiniu kriterijumi, kaip antai vidutiniu nusikalstamumo lygiu geografinėje zonoje, ir nebūtinai turi turėti konkrečių įrodymų dėl sunkių nusikaltimų rengimo ar vykdymo atitinkamose teritorijose. Jis pridūrė, kad tikslinio duomenų saugojimo priemonė, susijusi su vietomis ar infrastruktūra, kuriose reguliariai lankosi labai didelis asmenų skaičius, ar su strateginėmis vietomis, kaip antai oro uostais, stotimis, jūrų uostais ar rinklių zonomis, leidžia

kompetentingoms institucijoms rinkti be kita ko, informaciją apie asmenų, kurie naudojami elektroninių ryšių priemone vienoje iš šių vietų ar geografinių zonų, buvimą ir daryti išvadas dėl jų buvimo ir veiklos šiose vietose ar geografinėse teritorijose, siekiant kovoti su sunkiais nusikaltimais.

Be to, Teisingumo Teismas nurodė, kad nei pagal Direktyvą dėl privatumo ir elektroninių ryšių, nei pagal kokį nors kitą Sąjungos teisės aktą nedraudžiami nacionalinės teisės aktai, kuriais siekiama kovoti su sunkiais nusikaltimais ir pagal kuriuos elektroninių ryšių priemonės, kaip antai iš anksto apmokėtos SIM kortelės, įsigijimas siejamas su sąlyga, kad patikrinami oficialūs dokumentai, patvirtinantys pirkėjo tapatybę, ir kad pardavėjas registruoja juose esančią informaciją – pardavėjas prirėkęs privalo suteikti kompetentingoms nacionalinėms institucijoms prieigą prie tokios informacijos.

Teisingumo Teismas pabrėžė, kad pagal Direktyvą dėl privatumo ir elektroninių ryšių kompetentingoms nacionalinėms institucijoms nedraudžiama taikyti operatyvaus duomenų saugojimo priemonės nuo pat pirmojo tyrimo, susijusio su didele grėsme visuomenės saugumui arba galimu sunkiu nusikalstamu, etapo, t. y. nuo momento, kai šios institucijos pagal atitinkamas nacionalinės teisės nuostatas gali pradėti tokį tyrimą. Tokia priemonė gali apimti kitų asmenų nei tie, kurie įtariami planavę arba padarę sunkią nusikalstamą veiką ar keliantys grėsmę nacionaliniam saugumui, srauto ir vietos nustatymo duomenis, jeigu tie duomenys, remiantis objektyviais ir nediskriminaciniais veiksniais, gali padėti išaiškinti tokią nusikalstamą veiką ar grėsmę nacionaliniam saugumui; tai gali būti, pavyzdžiui, tokios nusikalstamos veikos aukos, jos socialinės ar profesinės aplinkos duomenys.

Šios priemonės, atsižvelgiant į nacionalinio įstatymų leidėjo pasirinkimą ir laikantis to, kas griežtai būtina, gali būti taikomos kartu.

Teisingumo Teismas atmetė argumentą, kad kompetentingos nacionalinės institucijos, siekdamos kovoti su sunkiais nusikaltimais, turėtų turėti prieigą prie srauto ir vietos nustatymo duomenų, kurie bendrai ir nediferencijuojant buvo saugomi, remiantis suformuota jurisprudencija, kad užkirstų kelią didelei grėsmei nacionaliniam saugumui, kai tokia grėsmė yra tikra, esama arba numatoma. Iš tikrųjų remiantis šiuo argumentu tokia prieiga priklausytų nuo su tikslu kovoti su sunkiais nusikaltimais nesusijusių aplinkybių. Be to, remiantis šiuo argumentu, prieiga gali būti pateisinama mažesnės svarbos tikslu, nei saugojimą pateisinant tikslas, t. y. nacionalinio saugumo užtikrinimu, o tai prieštarautų bendrojo intereso tikslų hierarchijai, į kurią atsižvelgiant turi būti vertinamas duomenų saugojimo priemonės proporcingumas. Be to, suteikus tokią prieigą, kiltų pavojus, kad draudimas bendrai ir nediferencijuotai saugoti duomenis kovos su sunkiais nusikaltimais tikslais taptų neveiksmingas.

Trečia, Teisingumo Teismas patvirtino, kad pagal Sąjungos teisę draudžiami nacionalinės teisės aktai, pagal kuriuos, tiriant sunkius nusikaltimus ir vykdant baudžiamąjį persekiojimą už juos, policijos pateiktus prašymus leisti susipažinti su saugomais duomenimis centralizuotai tvarko policijos pareigūnas, net kai jam padeda policijoje įsteigtas padalinys, turintis tam tikrą autonomiją vykdant savo pareigas ir kurio sprendimams vėliau gali būti taikoma teisminė kontrolė. Teisingumo Teismas šiuo klausimu patvirtino savo jurisprudenciją, pagal kurią siekiant praktiškai užtikrinti visišką prieigos prie asmens duomenų (pavyzdžiui, srauto ir vietos nustatymo duomenų) sąlygų laikymąsi, būtina, kad prieš suteikiant kompetentingoms nacionalinėms institucijoms prieigą prie saugomų duomenų teismas arba nepriklausomas administracinis subjektas atliktų išankstinę kontrolę, o toks teismas ar toks subjektas savo sprendimą priimtų gavę motyvuotą tų institucijų prašymą, kurį jos pateiktų, be kita ko, vykdydamos prevencijos, atskleidimo arba baudžiamojo persekiojimo procedūras. Vis dėlto policijos pareigūnas nėra teismas ir nesuteikia visų nepriklausomumo ir nešališkumo garantijų, kad būtų galima jį kvalifikuoti nepriklausomu administraciniu subjektu.

Galiausiai, ketvirta, Teisingumo Teismas patvirtino savo jurisprudenciją, kuria remiantis pagal Sąjungos teisę nacionaliniam teismui draudžiama apriboti laiko atžvilgiu jo paties pagal nacionalinę teisę pripažinto negaliojančiu nacionalinės teisės akto, kuriuo elektroninių ryšių paslaugų teikėjai

įpareigojami bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis, poveikį, kai toks teisės aktas nesuderinamas su Direktyva dėl privatumo ir elektroninių ryšių.

Vis dėlto Teisingumo Teismas priminė, kad remiantis valstybių narių procesinės autonomijos principu, taip saugant duomenis gautų įrodymų priimtino klausimas sprendžiamas pagal nacionalinę teisę, laikantis, be kita ko, lygiavertiškumo ir veiksmingumo principų.

PASTABA: Prašyme priimti prejudicinį sprendimą valstybių narių teismai, nagrinėdami juose iškeltą bylą, gali pateikti Teisingumo Teismui klausimus dėl Sąjungos teisės išaiškinimo ar Sąjungos teisės akto galiojimo. Teisingumo Teismas nenagrinėja nacionalinės bylos. Remdamasis Teisingumo Teismo sprendimu šią bylą turi išspręsti nacionalinis teismas. Šis sprendimas taip pat privalomas kitiems nacionaliniams teismams, nagrinėjantiems panašias problemas.

Žiniasklaidai skirtas neoficialus dokumentas, neįpareigojantis Teisingumo Teismo.

[Visas sprendimo tekstas](#) nuo jo paskelbimo dienos prieinamas CURIA tinklalapyje.

Kontaktinis asmuo: Marta Osleja ☎ (+352) 4303 6005

Nuotraukas iš sprendimo paskelbimo posėdžio galima rasti „[Europe by Satellite](#)“ ☐ ☎ (+32) 2 2964106