



Prese un informācija

Eiropas Savienības Tiesa
PAZIŅOJUMS PRESEI Nr. 58/22
Luksemburgā, 2022. gada 5. aprīlī

Spriedums lietā C-140/20
Commissioner of the Garda Síochána u.c.

Tiesa apstiprina, ka ar elektroniskajām komunikācijām saistītās informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana smagu noziegumu apkarošanas nolūkā ir pretrunā Savienības tiesībām

Dalībvalsts tiesa nedrīkst ierobežot laikā sekas, kas izriet no tādu valsts tiesību aktu atzīšanas par spēkā neesošiem, kuri paredz šādu saglabāšanu

2015. gada martā personai G.D. tika piespriests mūža ieslodzījums par kādas sievietes slepkavību Īrijā. Pārsūdzot viņu notiesājošo spriedumu apelācijas kārtībā *Court of Appeal* (Apelācijas tiesa, Īrija), ieinteresētā persona tostarp pārmeta pirmās instances tiesai, ka tā esot kļūdaini pieļāvusi pierādījumus, kas izriet no informācijas par datu plūsmu un atrašanās vietas datiem attiecībā uz tālruna zvaniem. Lai kriminālprocesā varētu apstrīdēt minēto pierādījumu pieļaujamību, G.D. līdztekus vērsās arī *High Court* (Augstā tiesa, Īrija) ar civilprasību atzīt par spēkā neesošām vairākas normas šo datu saglabāšanu un piekļuvi tiem reglamentējošajā Īrijas 2011. gada likumā, pamatojoties uz to, ka ar šo likumu ir pārkāptas šīs personas no Savienības tiesību aktiem izrietošās tiesības. Ar 2018. gada 6. decembra nolēmumu Augstā tiesa šo G.D. prasību apmierināja. Īrija šo nolēmumu pārsūdzēja *Supreme Court* (Augstākā tiesa, Īrija), kas šajā lietā ir iesniedzējtiesa.

Lūgumā sniegt prejudiciālu nolēmumu Augstākā tiesa lūdza sniegt skaidrojumu par prasībām, kādas Savienības tiesībās ir noteiktas attiecībā uz minēto datu saglabāšanu smagu noziegumu apkarošanas nolūkos, kā arī par garantijām, kas nepieciešamas, lai varētu gūt piekļuvi šiem datiem. Turklāt tā vaicā par to, kāds tvērums un sekas laikā būtu iespējamam nolēmumam par Īrijas 2011. gada likuma nesaderīguma atzīšanu, kas tai būtu jāpasludina tāpēc, ka šis likums bija pieņemts tālab, lai transponētu Direktīvu 2006/24/EK ¹, kuru Tiesa 2014. gada 8. aprīļa spriedumā *Digital Rights Ireland* u.c. ir atzinusi par spēkā neesošu ².

Šajā spriedumā Tiesa virspalātas sastāvā, pirmām kārtām, apstiprina savu pastāvīgās judikatūras ³ atziņu, ka Savienības tiesībām ⁴ ir pretrunā tādi valsts legīslatīvie pasākumi, kuros smagu noziegumu apkarošanai preventīvi tiek paredzēta ar elektroniskajām komunikācijām saistītās informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana.

¹ Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK (OV 2006, L 105, 54. lpp.).

² Spriedums, 2014. gada 8. aprīlis, *Digital Rights Ireland*, C-293/12, (skat. PP Nr. 54/14).

³ Spriedums, 2014. gada 8. aprīlis, *Digital Rights Ireland*, C-293/12; spriedums, 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c., C-203/15 un C-698/15 (skat. PP Nr. 145/16); spriedumi, 2020. gada 6. oktobris, *Privacy International*, C-623/17, un *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18 (skat. PP Nr. 123/20); un spriedums, 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi), C-746/18 (skat. PP Nr. 29/21).

⁴ Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), redakcijā ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (turpmāk tekstā – “Direktīva par privāto dzīvi un elektronisko komunikāciju”), lasot to Eiropas Savienības Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā.

Proti, Direktīvā par privāto dzīvi un elektronisko komunikāciju piekļuve šiem datiem ir ne tikai pakārtota garantijām, kuru mērķis ir novērst ļaunprātīgu izmantošanu, bet arī it īpaši nostiprināts princips, ka informāciju par datu plūsmu un atrašanās vietas datus **uzglabāt ir aizliegts**. Tādējādi šo datu saglabāšana ir gan atkāpe no šā uzglabāšanas aizlieguma, gan iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību.

Lai arī Direktīvā par privāto dzīvi un elektronisko komunikāciju dalībvalstīm tiek ļauts ierobežot šīs tiesības un šos pienākumus, piemēram, tālab, lai apkarotu noziedzīgus nodarījumus, šiem ierobežojumiem ir jāatbilst tostarp samērīguma principam. Šis princips prasa, lai tiktu izpildītas ne tikai piemērotības un nepieciešamības prasības, bet arī prasība par šo pasākumu **samērīgumu** ar izvirzīto mērķi. Tiesa jau ir nospriedusi, ka smagu noziegumu apkarošanas mērķis, lai cik būtisks tas arī nebūtu, pats par sevi nevar attaisnot to, ka tāds informācijas par datu plūsmu un atrašanās vietas datu visaptverošas un nediferencētas saglabāšanas pasākums kā ar Direktīvu 2006/24/EK noteiktais tiek uzskatīts par nepieciešamu. Ar šādu pašu domu – pat dalībvalstu pozitīvie pienākumi, kuri attiecas uz tādu noteikumu ieviešanu, kas ļauj efektīvi apkarot noziedzīgus nodarījumus, nevar attaisnot tik nopietnu no valsts tiesību aktiem, kuros ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, izrietošo iejaukšanos gandrīz visu iedzīvotāju pamattiesībās, ja attiecīgo personu datiem nav – kaut vai tikai netiešas – saiknes ar izvirzīto mērķi.

Tiesa arī atgādina, ka saskaņā ar Hartu valsts iestādēm ir dažādi pozitīvi pienākumi, kas izpaužas, piemēram, kā juridisku pasākumu veikšana privātās un ģimenes dzīves aizsardzībai, mājoķļa un saziņas aizsardzībai, kā arī personu fiziskās un garīgās neaizskaramības aizsardzībai un arī spīdzināšanas un necilvēcīgas vai pazemojošas izturēšanās aizlieguma ievērošanas nodrošināšanai. Tāpēc tām ir jāveic **dažādo iesaistīto leģitīmo interešu un tiesību salāgošana**. Proti, vispārējo interešu mērķa sasniegšanā nevar neņemt vērā to, ka tas ir jāsalāgo ar šā pasākuma skartajām pamattiesībām, **līdzsvarojot** šo vispārējo interešu mērķi ar attiecīgajām tiesībām un vienlaikus arī pārbaudot, vai šā mērķa nozīmīgums ir atbilstošs no šāda pasākuma izrietošās iejaukšanās smagumam.

Šo apsvērumu dēļ Tiesa noraida konkrēti argumentu, ka īpaši smagā noziedzība varētu tikt pielīdzināta draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, un var uz noteiktu laiku attaisnot informācijas par datu plūsmu un atrašanās vietas datu visaptverošas un nediferencētas saglabāšanas pasākumu. Proti, šādi draudi pēc sava rakstura, smaguma un to veidojošo apstākļu specifiskuma atšķiras no vispārīgā un pastāvīgā riska, ka varētu rasties spriedze vai traucēta, pat nopietni traucēta, sabiedrības drošība, kā arī izdarīti smagi noziegumi.

Otrām kārtām un apstiprinot savu līdzšinējo judikatūru, Tiesa nospriež, ka Savienības tiesībām savukārt nav pretrunā leģislatīvi pasākumi, kas smagu noziegumu apkarošanas un nopietnu sabiedrības drošības apdraudējumu novēršanas nolūkos ar šajā spriedumā minētajiem nosacījumiem paredz:

- **mērķorientētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu** atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju;
- **savienojuma avotam piešķirto IP adresu visaptverošu un nediferencētu saglabāšanu;**
- **elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu visaptverošu un nediferencētu saglabāšanu** un
- šo pakalpojumu sniedzēju rīcībā esošo informācijas par datu plūsmu un atrašanās vietas datu operatīvo **saglabāšanu** (*quick freeze*).

Tiesa sniedz sīkākus paskaidrojumus par šīm dažādajām pasākumu kategorijām.

Pirmkārt, kompetentās valsts iestādes drīkst veikt mērķorientētas saglabāšanas pasākumu, pamatojoties uz ģeogrāfisku kritēriju, piemēram, vidējo noziedzības rādītāju kādā konkrētā

ģeogrāfiskajā zonā, un tālab nav obligāti nepieciešams, lai tām būtu zināmas konkrētas pazīmes, kas liecina par to, ka attiecīgajās zonās notiek gatavošanās smagu noziegumu izdarīšanai vai tie tiek izdarīti. Tā piebilst, ka šāds saglabāšanas pasākums, kas tiek veikts attiecībā uz vietām vai infrastruktūru, ko regulāri apmeklē ļoti liels personu skaits, vai arī stratēģiskām vietām, piemēram, lidostām, dzelzceļa stacijām, jūras ostām vai autoceļu nodevas iekasēšanas vietām, ļauj kompetentajām iestādēm iegūt informāciju par to, ka šajās vietās vai ģeogrāfiskajās zonās atrodas personas, kuras tur lieto elektroniskās komunikācijas līdzekli, un smagu noziegumu apkarošanas nolūkā no tās izdarīt secinājumus par šo personu atrašanos un aktivitātēm šajās vietās vai ģeogrāfiskajās zonās.

Otrkārt, Tiesa norāda, ka nedz Direktīvai par privāto dzīvi un elektronisko komunikāciju, nedz kādam citam Savienības tiesību aktam nav pretrunā valsts tiesību akti, kuru mērķis ir smagu noziegumu apkarošana un saskaņā ar kuriem elektroniskās komunikācijas līdzekļa, piemēram, priekšapmaksas SIM kartes iegāde, ir pakārtota prasībai par pircēja identitāti apliecināšu oficiālu dokumentu pārbaudi un pārdevēja pienākumu reģistrēt no tās izrietošo informāciju, un pārdevējam vajadzības gadījumā ir pienākums dot kompetentajām valsts iestādēm piekļuvi šai informācijai.

Visbeidzot treškārt, Tiesa norāda, ka Direktīvai par privāto dzīvi un elektronisko komunikāciju nav pretrunā tas, ka kompetentās valsts iestādes izdod rīkojumu veikt operatīvo saglabāšanu jau kopš brīža, kad tiek sākta izmeklēšana jautājumā par nopietnu sabiedriskās drošības apdraudējumu vai iespējamu smagu noziegumu, proti, līdzko šīs iestādes saskaņā ar piemērojamām valsts tiesību normām var sākt šādu izmeklēšanu. Šāds pasākums var tikt attiecināts arī uz informāciju par datu plūsmu un atrašanās vietas datiem saistībā ar personām, kas nav tās, kuras tiek turētas aizdomās par to, ka tās ir plānojušas vai izdarījušas smagu noziegumu vai veikušas valsts drošības apdraudējumu, ciktāl šie dati, pamatojoties uz objektīviem un nediskriminējošiem elementiem, var veicināt šāda noziedzīga nodarījuma vai šāda valsts drošības apdraudējuma atklāšanu, piemēram, cietušās personas datus, kā arī datus par tās sociālo vai profesionālo vidi veidojošo personu loku.

Šie dažādie pasākumi atkarībā no valsts likumdevēja izvēles un ievērojot absolūti nepieciešamā robežas var tikt piemēroti kopā.

Tiesa arī noraida argumentāciju, ka atbilstoši tās judikatūrai kompetentajām valsts iestādēm smagu noziegumu apkarošanas nolūkos būtu jāvar piekļūt visaptveroši un nediferencēti saglabātajai informācijai par datu plūsmu un atrašanās vietas datiem, lai rīkotos attiecībā pret nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami. Proti, šī argumentācija padara šo piekļuvi atkarīgu no apstākļiem, kuriem nav nekā kopīga ar smagu noziegumu apkarošanas mērķi. Turklāt atbilstoši šai argumentācijai piekļuve varētu tikt attaisnota ar mērķi, kurš nav tik svarīgs kā šo saglabāšanu pamatojušais mērķis, proti, valsts drošības aizsardzība, savukārt tas būtu pretrunā vispārējo interešu mērķu hierarhijai, kuras ietvaros ir vērtējams saglabāšanas pasākuma samērīgums. Turklāt, atļaujot šādu piekļuvi, iespējami tiktu atņemta visa lietderīgā iedarbība aizliegumam šādu visaptverošu un nediferencētu saglabāšanu veikt smagu noziegumu apkarošanas nolūkā.

Trešām kārtām, Tiesa apstiprina, ka Savienības tiesībām ir pretrunā tādi valsts tiesību akti, saskaņā ar kuriem policijas pieprasījumus par piekļuvi elektronisko komunikāciju pakalpojumu sniedzēju saglabātajiem datiem saistībā ar smagu noziegumu izmeklēšanu un kriminālvajāšanu par tiem centralizēti izskata kāda policijas amatpersona, pat ja tai palīdz kāda policijā izveidota struktūrvienība, kura ir apveltīta ar zināma apjoma autonomiju sava uzdevuma veikšanai, un attiecībā uz kuras lēmumiem vēlāk var tikt veikta pārbaude tiesā. Proti, šajā ziņā Tiesa apstiprina savu judikatūras atziņu, ka, lai praksē nodrošinātu, ka pilnībā tiek ievēroti stingrie nosacījumi, kādos var notikt piekļuve tādiem personas datiem kā informācija par datu plūsmu un atrašanās vietas datus, kompetento valsts iestāžu piekļuvei saglabātajiem datiem ir jābūt pakļautai iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, un šīs tiesas vai iestādes lēmumam ir jābūt pieņemtam, pamatojoties uz šo iestāžu pieteikumu tostarp saistībā ar procedūrām šā noziedzīgā nodarījuma novēršanai, atklāšanai vai kriminālvajāšanai par to. Taču policijas amatpersona nav tiesa un nenodrošina visas neatkarības un objektivitātes garantijas, kas ir vajadzīgas, lai to varētu uzskatīt par neatkarīgu administratīvu iestādi.

Visbeidzot ceturtām kārtām, Tiesa apstiprina savu judikatūras atziņu, ka Savienības tiesībām ir pretrunā tas, ka dalībvalsts tiesa ierobežo laikā sekas, kas izriet no apstākļa, ka tā, pildot savu valsts tiesībās paredzēto uzdevumu, par spēkā neesošiem ir atzinusi valsts tiesību aktus – kuros elektronisko komunikāciju pakalpojumu sniedzējiem ir uzlikts pienākums visaptveroši un nediferencēti saglabāt informāciju par datu plūsmu un atrašanās vietas datus – tāpēc, ka šie tiesību akti ir nesaderīgi ar Direktīvu par privāto dzīvi un elektronisko komunikāciju.

Tomēr Tiesa atgādina, ka atbilstoši dalībvalstu procesuālās autonomijas principam jautājums par šādas saglabāšanas ceļā iegūto pierādījumu pieļaujamību ir vērtējams saskaņā ar valsts tiesībām, ja vien tiek ievēroti tostarp līdzvērtības un efektivitātes principi.

ATGĀDINĀJUMS. Lūgums sniegt prejudiciālu nolēmumu ļauj dalībvalstu tiesām to tiesvedības ietvaros uzdot jautājumus Tiesai par Savienības tiesību interpretāciju vai Savienības akta spēkā esamību. Tiesa neiztiesā strīdus, ko izskata valstu tiesas. Valsts tiesai ir jāatrisina lieta saskaņā ar Tiesas nolēmumu. Šis nolēmums līdzīgā veidā ir saistošs citām valstu tiesām, kurām ir jāatrisina līdzīgas problēmas.

Neoficiāls dokuments plašsaziņas līdzekļu vajadzībām, kas Tiesai nav saistošs.

[Pilns sprieduma teksts](#) tiek publicēts CURIA tīmekļvietnē pasludināšanas dienā.

Kontaktpersona presei: Marta Ošleja ☎ (+352) 4303 6005

Sprieduma pasludināšanas attēli ir pieejami "[Europe by Satellite](#)" ☎ (+32) 2 2964106