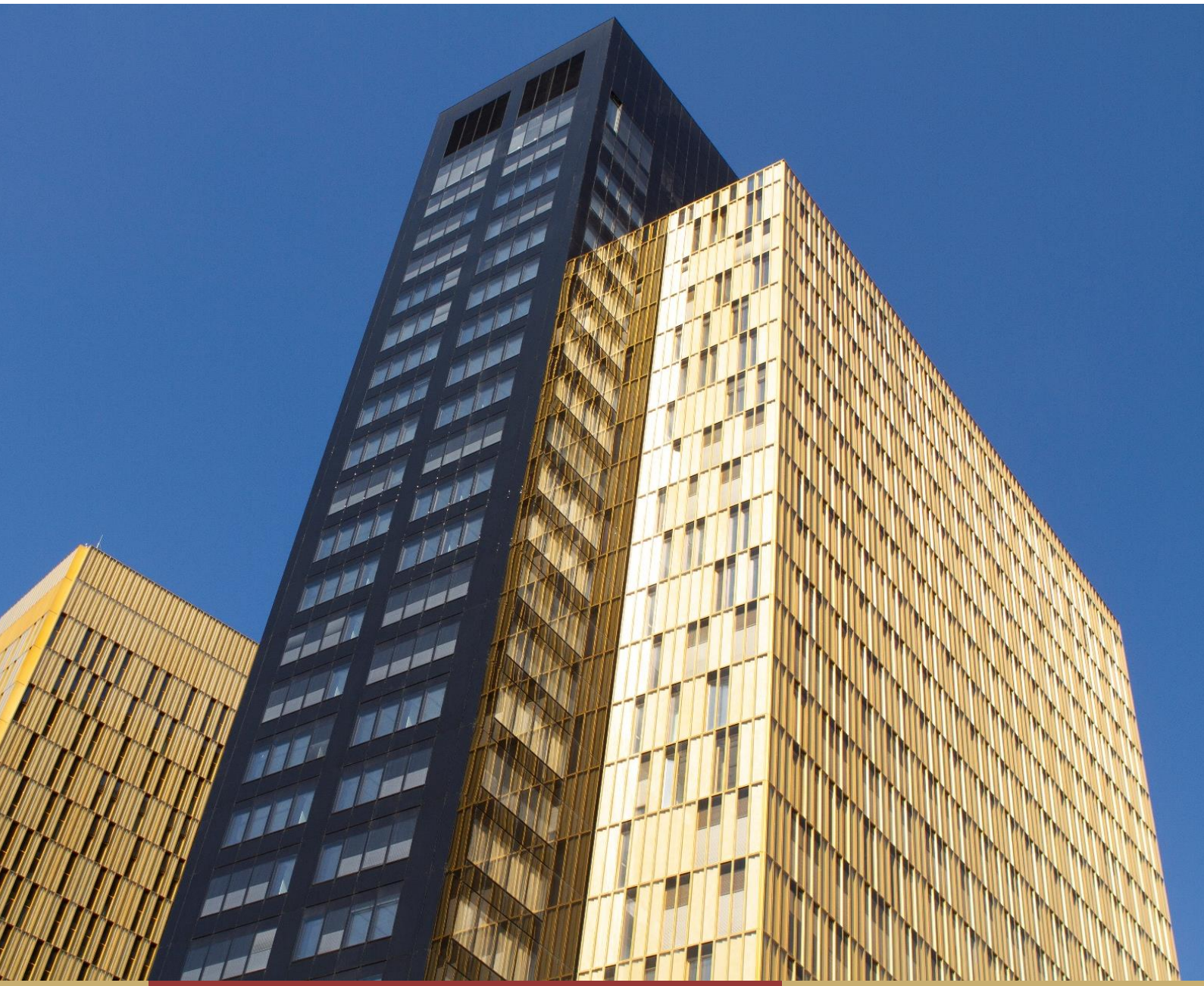
EIROPAS SAVIENĪBAS
TIESA

LV



Tematisks pārskats

Personas datu aizsardzība

Pētniecības un dokumentācijas direkcija

curia.europa.eu

Priekšvārds

Tiesības uz personas datu aizsardzību ir pamattiesības, kuru ievērošana ir nozīmīgs Eiropas Savienības mērķis.

Tās ir nostiprinātas primārajās tiesībās, tostarp Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 8. pantā, kā arī Līguma par Eiropas Savienības darbību (LESD) 16. panta 1. punktā. Šīs pamattiesības turklāt ir cieši saistītas ar tiesībām uz privātās un ģimenes dzīves neaizskaramību, kas ir nostiprinātas Hartas 7. pantā.

Atvasināto tiesību jomā kopš 90. gadu vidus Eiropas Kopiena ir izveidojusi vairākus instrumentus, lai nodrošinātu personas datu aizsardzību. Galvenais Savienības tiesību akts šajā jomā bija Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [1], kas atcelta kopš 2018. gada.

Pēc tam, lai papildinātu Direktīvu 95/46, tika pieņemta Direktīva 2002/58/EK [2], saskaņojot dalībvalstu tiesību aktu noteikumus attiecībā uz tiesību uz privātās dzīves neaizskaramību konkrēti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē [3]. Jānorāda, ka, lai ņemtu vērā jauno tehnoloģisko un komerciālo attīstību, Savienības likumdevējs 2017. gadā ir uzsācis šīs direktīvas pārskatīšanu [4], kas šobrīd joprojām notiek [5].

2016. gadā Eiropas Savienība pārstrādāja šīs jomas vispārējo tiesisko regulējumu. Tālab tā pieņēma Regulu (ES) 2016/679 [6] par personas datu aizsardzību (turpmāk tekstā – "VDAR"), ar ko atceļ Direktīvu 95/46 un kas ir piemērojama kopš 2018. gada 25. maija, kā

---

1 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.), 2003. gada 20. novembra konsolidētā redakcija, atcelta no 2018. gada 25. maija (skat. 6. zemsvītras piezīmi).

2 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) (OV 2002, L 201, 37. lpp.), 2009. gada 19. decembra konsolidētā redakcija.

3 Direktīva 2002/58 tika grozīta ar Eiropas Parlamenta un Padomes Direktīvu 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.). 2014. gada 8. aprīļa spriedumā *Digital Rights Ireland* un *Seitlinger* u.c. (C-293/12 un C-594/12, EU:C:2014:238) Tiesa nosprieda, ka šī direktīva nav spēkā, jo tā nopietni aizskāra tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību (skat. šā pārskata I.1. sadaļu "Savienības atvasināto tiesību atbilstība tiesībām uz personas datu aizsardzību").

4 2017. gada 10. janvārī Komisija iesniedza priekšlikumu, lai šo direktīvu aizstātu ar regulu par privāto dzīvi un elektroniskajām komunikācijām.

5 2021. gada 10. februārī Eiropas Savienības Padome apstiprināja sarunu pilnvaras, lai pārskatītu privātās dzīves un konfidencialitātes aizsardzības noteikumus elektronisko sakaru pakalpojumu izmantošanā, kas ļāva uzsākt sarunas ar Eiropas Parlamentu. Priekšlikuma regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula) teksts ir pieejams šeit: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

6 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (OV 2016, L 119, 1. lpp.).

arī Direktīvu (ES) 2016/680 [7] par minēto datu aizsardzību kriminālllietu jomā, kuras normas ir jāpiemēro kopš 2018. gada 6. maija.

Savukārt ES iestāžu un struktūru apstrādāto personas datu aizsardzība kopš 2018. gada 11. decembra tiek nodrošināta konkrēti ar Regulu (ES) 2018/1725 [8]. Lai nodrošinātu saskaņotu pieeju personas datu aizsardzībai visā Savienībā, šīs regulas noteikumi ir veidoti tādējādi, lai tie būtu pēc iespējas pieskaņotāki ar VDAR izveidotajam regulējumam.

Visbeidzot, lai rastu risinājumu jauno tehnoloģiju radītajiem izaicinājumiem, Savienības likumdevējs kopš 2020. gada ir sācis pieņemt jaunu tiesisko regulējumu [9], kam ir saikne ar personas datu aizsardzību reglamentējošajām Savienības tiesību normām.

Ņemot vērā personas datu aizsardzības jomā esošo bagātīgo Tiesas judikatūru, šā tematiskā pārskata mērķis ir iepazīstināt ar vairākiem šajā jomā nozīmīgākajiem spriedumiem, kā arī spriedumiem, kas lielā mērā palīdzējuši šo judikatūru tālāk attīstīt, īpašu uzmanību pievēršot Tiesas virspalātas pasludinātajiem spriedumiem. Proti, šā pārskata mērķis ir aptvert gan judikatūru, kas attiecas uz vispārējo tiesisko regulējumu personas datu aizsardzības jomā, kas izriet no Direktīvas 95/46 un VDAR interpretācijas, gan judikatūru, kas attiecas uz nozares tiesisko regulējumu un it īpaši uz elektroniskajiem sakariem un krimināltiesībām. Šajā pārskatā ir paredzēts arī iepazīstināt ar vairākiem spriedumiem par transversāli piemērojamiem tiesiskajiem regulējumiem, vienlaikus jau no paša sākuma uzsverot Hartas lomu judikatūras attīstībā.

---

7 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV 2016, L 119, 89. lpp.).

8 Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV 2018, L 295, 39. lpp.).

9 Šajā ziņā it īpaši ir jāmin trīs likumdošanas iniciatīvas: *i)* Eiropas Parlamenta un Padomes Regula (ES) 2022/868 (2022. gada 30. maijs) par Eiropas datu pārvaldību un ar ko groza Regulu (ES) 2018/1724 (Datu pārvaldības akts) (OV 2022, L 152, 1. lpp.) un Eiropas Parlamenta un Padomes Regula (ES) 2023/2854 (2023. gada 13. decembris) par saskaņotiem noteikumiem par taisnīgu piekļuvi datiem un to lietošanu un ar ko groza Regulu (ES) 2017/2394 un Direktīvu (ES) 2020/1828 (Datu akts) (OV 2023, L 2854, 1. lpp.); *ii)* leģislatīvu aktu par digitālajiem pakalpojumiem un tirgiem pakete, kura sastāv no Eiropas Parlamenta un Padomes Regulas (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (OV 2022, L 277, 1. lpp.) un Eiropas Parlamenta un Padomes Regulas (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (OV 2022, L 265, 1. lpp.); un *iii)* pirmais leģislatīva akta priekšlikums, lai izveidotu tiesisko regulējumu mākslīgā intelekta jomā, kas materializējies Mākslīgā intelekta akta (OV 2024, L 1689) formā.

Satura rādītājs

PRIEKŠVĀRDS 3
I. TIESĪBAS UZ PERSONAS DATU AIZSARDZĪBU, KAS ATZĪTAS EIROPAS SAVIENĪBAS PAMATTIESĪBU HARTĀ 6
1. Savienības atvasināto tiesību atbilstība tiesībām uz personas datu aizsardzību . 6
2. Tiesību uz personas datu aizsardzību ievērošana, īstenojot Savienības tiesību aktus 16
II. PERSONAS DATU APSTRĀDE VISPĀRĒJĀ ŠĪS JOMAS TIESISKĀ REGULĒJUMA IZPRATNĒ 18
1. Vispārējā tiesiskā regulējuma piemērošanas joma 18
2. Jēdziens "personas dati" 23
3. Jēdziens "personas datu apstrāde" 26
4. Jēdziens "personas datu kartotēka" 30
5. Jēdziens "personas datu pārzinis" 30
6. Jēdziens "kopīgs pārzinis" 33
7. Personas datu apstrādes likumīguma nosacījumi 33
III. PERSONAS DATU APSTRĀDE NOZARES TIESISKĀ REGULĒJUMA IZPRATNĒ 39
1. Personas datu apstrāde elektronisko komunikāciju nozarē 39
2. Personas datu apstrāde kriminālliet ās 57
IV. PERSONAS DATU NOSŪTĪŠANA UZ TREŠĀM VALSTĪM 60
V. PERSONAS DATU AIZSARDZĪBA INTERNETĀ 67
1. Tiesības iebilst pret personas datu apstrādi ("tiesības tikt aizmirstam") 67
2. Personas datu apstrāde un intelektuālā īpašuma tiesības 68
3. Atsauču uz personas datiem atsaistīšana 71
4. Tīmekļvietnes lietotāja piekrišana informācijas uzglabāšanai 79
5. Personas datu apstrāde tiešsaistes sociālajos tīklos 81
VI. VALSTS UZRAUDZĪBAS IESTĀDES 84
1. Prasības par neatkarību tvērums 84
2. Piemērojamo tiesību un kompetentās uzraudzības iestādes noteikšana 86
3. Valstu uzraudzības iestāžu pilnvaras 87
4. Administratīvo naudas sodu piemērošanas nosacījumi 93
5. Valsts uzraudzības iestāžu pilnvaru saikne ar citu valsts iestāžu pilnvarām 96

I. Tiesības uz personas datu aizsardzību, kas atzītas Eiropas Savienības Pamattiesību hartā

1. Savienības atvasināto tiesību atbilstība tiesībām uz personas datu aizsardzību

2010. gada 9. novembra spriedums (virspalāta) Volker und Markus Schecke un Eifert (C-92/09 un C-93/09, EU:C:2010:662)

Šajā lietā notika pamattiesvedības starp lauksaimniekiem un *Land Hessen* [Hesenes federālo zemi] par viņu kā Eiropas Lauksaimniecības garantiju fonda (ELGF) un Eiropas Lauksaimniecības fonda lauku attīstībai (ELFLA) līdzekļu saņēmēju personas datu publicēšanu *Bundesanstalt für Landwirtschaft und Ernährung* (Federālā Lauksaimniecības un uztura aģentūra) tīmekļvietnē. Minētie lauksaimnieki iebilda pret šādu datu publicēšanu, apgalvojot, konkrēti, ka tā nav pamatota ar sevišķām sabiedrības interesēm. *Land Hessen* savukārt uzskatīja, ka pienākums publicēt minētos datus izriet no Regulas Nr. 1290/2005 [10] un Regulas Nr. 259/2008 [11], ar kurām ir reglamentēta kopējās lauksaimniecības politikas finansēšana un ir noteikta informācijas publicēšana par ELGF un ELFLA līdzekļu saņēmējiem.

Šajā saistībā *Verwaltungsgericht Wiesbaden* (Vīsbādenes Administratīvā tiesa, Vācija) uzdeva Tiesai vairākus jautājumus par to, vai ir spēkā vairākas Regulas Nr. 1290/2005 normas un Regula Nr. 259/2008, kas noteic pienākumu nodrošināt sabiedrībai piekļuvi šādai informācijai, tostarp izmantojot valsts aģentūru tīmekļvietnes.

Runājot par Hartā atzīto tiesību uz personas datu aizsardzību samērojamību ar pārredzamības principu Eiropas fondu jomā, Tiesa uzsvēra, ka konkrētas informācijas publicēšana tīmekļvietnē par fondu līdzekļu saņēmējiem, minot viņu uzvārdus un saņemtās summas, ņemot vērā, ka vietnei brīvi var piekļūt trešās personas, ir šo saņēmēju tiesību uz privātās dzīves neaizskaramību aizskārums vispār un viņu personas datu aizsardzības aizskārums konkrēti.

Lai šāds tiesību aizskārums būtu attaisnots, tam ir jābūt noteiktam tiesību aktos, tam ir jārespektē šo tiesību būtiskais saturs un, ievērojot samērīguma principu, tam ir jābūt nepieciešamam un patiešām jāatbilst Savienības atzītiem vispārējas nozīmes mērķiem; atkāpes no šīm tiesībām un to ierobežojumi jāīsteno tikai tiktāl, ciktāl tas ir absolūti

[10] Padomes Regula (EK) Nr. 1290/2005 (2005. gada 21. jūnijs) par kopējās lauksaimniecības politikas finansēšanu (OV 2005, L 209, 1. lpp.), kas tika atcelta ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1306/2013 (2013. gada 17. decembris) par kopējās lauksaimniecības politikas finansēšanu, pārvaldību un uzraudzību (OV 2013, L 347, 549. lpp.).

[11] Komisijas Regula (EK) Nr. 259/2008 (2008. gada 18. marts), ar ko nosaka sīki izstrādātus noteikumus par to, kā piemērot Padomes Regulu (EK) Nr. 1290/2005 attiecībā uz informācijas publicēšanu par ELGF un ELFLA līdzekļu saņēmējiem (OV 2008, L 76, 28. lpp.), kas tika atcelta ar Komisijas Īstenošanas regulu (ES) Nr. 908/2014 (2014. gada 6. augusts), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1306/2013 piemēro attiecībā uz maksājumu aģentūrām un citām struktūrām, finanšu pārvaldību, grāmatojumu noskaidrošanu, noteikumiem par pārbaudēm, nodrošinājumu un pārredzamību (OV 2014, L 255, 59. lpp.).

nepieciešams. Šajā situācijā Tiesa uzskatīja, ka, tā kā demokrātiskā sabiedrībā nodokļu maksātājiem ir tiesības saņemt informāciju par publisko līdzekļu izlietojumu, Padomei un Komisijai bija pienākums veikt līdzsvarotu dažādu attiecīgo interešu izsvēršanu, pirms strīdīgo noteikumu pieņemšanas pārbaudot, vai šo datu publicēšana tīmekļvietnē, kas ir vienīgā katrā dalībvalstī, nepārsniedz to, kas bija nepieciešams, lai īstenotu izvirzītos leģitīmos mērķus.

Tādējādi Tiesa atzina par spēkā neesošām vairākas Regulas Nr. 1290/2005 normas, kā arī Regulu Nr. 259/2008 kopumā, ciktāl ELGF un ELFLA atbalstu saņemošo fizisko personu gadījumā šīs normas noteic, ka jāpublicē personas dati par ikvienu saņēmēju, nenošķirot tos atbilstoši tādiem pienācīgiem kritērijiem kā laikposmi, kuros viņi ir saņēmuši šādu atbalstu, šā atbalsta saņemšanas biežums vai arī veids un apmērs. Tomēr Tiesa neapšaubīja tiesiskās sekas, kas izriet no valsts iestāžu veiktās šāda veida atbalsta saņēmēju sarakstu publicēšanas laikposmā pirms šā sprieduma pasludināšanas datuma.

2014. gada 8. aprīļa spriedums (virspalāta) Digital Rights Ireland un Seitlinger u.c. (apvienotās lietas C-293/12 un C-594/12, EU:C:2014:238).

Šā sprieduma pamatā ir Īrijas un Austrijas tiesās celtās prasības izvērtēt to, vai ir spēkā Direktīva 2006/24/EK par datu saglabāšanu, ņemot vērā pamattiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību. Lietā C-293/12 *High Court* (Augstā tiesa, Īrija) bija jāizspriež strīds starp sabiedrību *Digital Rights* un Īrijas iestādēm par to, vai ir tiesiski tādi valsts pasākumi, kas noteic ar elektroniskajām komunikācijām saistīto datu saglabāšanu. Lietā C-594/12 *Verfassungsgerichtshof* (Konstitucionālā tiesa, Austrija) izskatīja vairākas konstitucionālās prasības, kurās tika lūgts atcelt valsts tiesību normu, ar kuru Direktīva 2006/24 bija transponēta Austrijas tiesībās.

Lūgumos sniegt prejudiciālu nolēmumu Īrijas un Austrijas tiesas vaicāja Tiesai par Direktīvas 2006/24 spēkā esamību, ņemot vērā Hartas 7., 8. un 11. pantu. Proti, minētās tiesas jautāja Tiesai, vai saskaņā ar minēto direktīvu publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākums noteiktu laiku saglabāt datus par personas privāto dzīvi un saziņu un sniegt valsts kompetentajām iestādēm piekļuvi šiem datiem ir nepamatota iejaukšanās minētajās pamattiesībās. Runa ir tostarp par datiem, kas ir nepieciešami, lai izsekotu un identificētu komunikācijas avotu un tās galamērķi, noteiktu komunikācijas datumu, laiku, ilgumu un veidu, lietotāja komunikāciju aprīkojumu, kā arī lai noskaidrotu mobilo sakaru iekārtas atrašanās vietu, un šie dati ietver tostarp abonenta vai reģistrētā lietotāja vārdu vai nosaukumu, zvanītāja un zvana adresāta tālruņa numuru, kā arī attiecībā uz interneta pakalpojumiem – IP adresi. Šie dati ļauj konkrēti noskaidrot, kas ir persona, ar kuru abonents vai reģistrētais lietotājs ir sazinājies, un kādā veidā tie ir sazinājušies, kā arī noskaidrot komunikācijas laiku un vietu, no kurienes tā notikusi. Turklāt tie ļauj uzzināt, cik bieži abonents vai reģistrētais lietotājs noteiktā laikposmā ir sazinājies ar konkrētām personām.

Tiesa vispirms nosprieda, ka Direktīvas 2006/24 normas, kurās šiem piegādātājiem ir noteikti šādi pienākumi, rada sevišķi nopietnu iejaukšanos pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, kuras ir garantētas Hartas 7. un 8. pantā. Šajā kontekstā Tiesa konstatēja, ka šādu iejaukšanos patiešām var pamatot ar tāda vispārējo interešu mērķa īstenošanu kā, piemēram, organizētās noziedzības apkarošana. Šajā ziņā Tiesa norādīja, pirmkārt, ka direktīvā noteiktā datu saglabāšana nav tāda, kas varētu aizskart pamattiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību būtību, jo šī direktīva neļauj uzzināt pašu elektronisko komunikāciju saturu un paredz, ka pakalpojumu sniedzējiem vai tīklu operatoriem ir jāievēro noteikti datu aizsardzības un drošības principi. Otrkārt, Tiesa konstatēja, ka datu saglabāšana, lai tos nepieciešamības gadījumā nodotu kompetentām valsts iestādēm, palīdz efektīvi īstenot vispārējo interešu mērķi, proti, sekmēt cīņu pret smagiem noziegumiem, kā arī galu galā gādāt par sabiedrības drošību.

Tomēr Tiesa atzina, ka, pieņemot direktīvu par datu saglabāšanu, Savienības likumdevējs ir pārsniedzis robežas, kas noteiktas tālab, lai tiktu ievērots samērīguma princips. Tādējādi Tiesa atzina šo direktīvu par spēkā neesošu, jo tā rada plaša apjoma un īpaši būtisku iejaukšanos pamattiesībās, kas nav pietiekami sīki reglamentēta, lai nodrošinātu, ka tā patiešām aprobežojas ar absolūti nepieciešamo. Proti, Direktīva 2006/24 vispārīgā veidā aptvēra visas personas un visus elektronisko komunikāciju līdzekļus, kā arī visu informāciju par datu plūsmu bez jebkādām atšķirībām, ierobežojumiem vai izņēmumiem saistībā ar mērķi cīnīties pret smagiem noziegumiem. Turklāt direktīvā nebija paredzēti nekādi objektīvi kritēriji, kas ļautu ierobežot kompetento valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu vienīgi tādu noziegumu novēršanas, izmeklēšanas, atklāšanas vai kriminālvajāšanas mērķiem, kuri varētu tikt uzskatīti par pietiekami smagiem, lai attaisnotu šādu iejaukšanos, kā arī tajā nebija paredzēti šādas piekļuves vai izmantošanas materiāltiesiskie un procesuālie nosacījumi. Visbeidzot attiecībā uz datu saglabāšanas ilgumu direktīvā bija paredzēts pienākums tos saglabāt vismaz sešus mēnešus, nenosakot nekādas atšķirības starp datu kategorijām atkarībā no personām, uz kurām tie attiecas, vai to iespējamā noderīguma izvirzītā mērķa sasniegšanai.

Turklāt attiecībā uz prasībām, kas izriet no Hartas 8. panta 3. punkta, Tiesa konstatēja, ka Direktīvā 2006/24 nav paredzētas pietiekamas garantijas, kas ļautu nodrošināt datu efektīvu aizsardzību pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu, un tajā nav arī prasīta datu saglabāšana Savienības teritorijā.

Tādējādi minētā direktīva pilnībā nenodrošināja neatkarīgas iestādes kontroli pār aizsardzības un drošības prasību ievērošanu, kā tas skaidri prasīts Hartā.

2022. gada 21. jūnija spriedums (virspalāta) Ligue des droits humains (C-817/19, EU:C:2022:491)

PDR (pasažieru datu reģistra) dati ir informācija par biļešu rezervāciju, ko gaisa pārvadātāji glabā savās rezervācijas un izlidošanas kontroles sistēmās. PDR direktīva [12] šiem pārvadātājiem noteic pienākumu terorisma un smagu noziegumu apkarošanas vajadzībām nosūtīt datus par ikvienu pasažieri lidojumā starp kādu trešo valsti un Eiropas Savienību attiecīgā reisa ielidošanas vai izlidošanas dalībvalsts pasažieru informācijas nodaļai (turpmāk tekstā – "PIN"). Proti, šādi nosūtītos PDR datus PIN iepriekš izvērtē [13] un pēc tam tos saglabā, lai attiecīgās vai citas dalībvalsts kompetentās iestādes varētu veikt iespējamu vēlāku novērtējumu. Dalībvalstis var nolemt piemērot šo direktīvu arī attiecībā uz lidojumiem Savienības iekšienē [14].

Ligue des droits humains cēla prasību *Cour constitutionnelle* (Konstitucionālā tiesa, Beļģija), lūdzot atcelt Beļģijas likumu, ar kuru Beļģijas tiesībās ir transponēta gan PDR direktīva, gan IPI direktīva [15]. Prasītājas ieskatā šajā likumā netiek ievērotas tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību. Tā kritizē, pirmkārt, PDR datu ļoti plašo apjomu un, otrkārt, šo datu vākšanas, pārsūtīšanas un apstrādes visaptverošo raksturu. Ar šo likumu tiekot apdraudēta arī personu brīva pārvietošanās, jo ar šo likumu, attiecinot PDR sistēmu uz ES iekšējiem lidojumiem un cita veida pārvadājumiem Savienības iekšienē, netieši tiekot atjaunota robežkontrole.

Šajā kontekstā Beļģijas Konstitucionālā tiesa uzdeva Tiesai prejudiciālus jautājumus tostarp par PDR direktīvas spēkā esamību.

Ar virspalātas sastāvā taisīto spriedumu Tiesa apstiprina PDR direktīvas spēkā esamību, ciktāl tā var tikt interpretēta atbilstīgi Hartai.

Šajā ziņā Tiesa nospriež, ka, tā kā Tiesas veiktā PDR direktīvas normu interpretācija Hartas 7., 8. un 21. pantā, kā arī 52. panta 1. punktā [16] garantēto pamattiesību gaismā nodrošina šīs direktīvas atbilstīgumu minētajiem pantiem, izskatot uzdotos jautājumus, nav konstatēts nekas tāds, kas ietekmētu minētās direktīvas spēkā esamību.

---

[12] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/681 (2016. gada 27. aprīlis) par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem (OV 2016, L 119, 132. lpp.; turpmāk tekstā – "PDR direktīva").

[13] Šis iepriekšējais novērtējums tiek veikts, lai identificētu personas, attiecībā uz kurām kompetentajām iestādēm jāveic padziļināta pārbaude, ņemot vērā, ka šīs personas var būt iesaistītas teroristu nodarījumā vai smagā noziegumā. Tas tiek veikts sistemātiski un ar automatizētiem līdzekļiem, salīdzinot PDR datus ar "lietderīgām" datubāzēm vai tos apstrādājot saskaņā ar PDR direktīvas 6. panta 2. punkta a) apakšpunktā un 3. punktā noteiktajiem kritērijiem.

[14] Izmantojot PDR direktīvas 2. pantā paredzēto iespēju.

[15] Padomes Direktīva 2004/82/EK (2004. gada 29. aprīlis) par pārvadātāju pienākumu darīt zināmus datus par pasažieriem (OV 2004, L 261, 24. lpp.; turpmāk tekstā – "IPI direktīva"). Šajā direktīvā ir regulēta gaisa pārvadātāju veikta iepriekšējas informācijas par pasažieriem (piemēram, izmantotā ceļošanas dokumenta numurs un veids, kā arī pilsonība) nodošana kompetentajām valsts iestādēm, lai uzlabotu robežkontroli un cīnītos pret nelikumīgu imigrāciju.

[16] Atbilstoši šai tiesību normai visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem jābūt noteiktiem tiesību aktos un tiem jāievēro šo tiesību un brīvību būtība. Turklāt šo tiesību un brīvību izmantošanas ierobežojumus drīkst noteikt tikai tad, ja tie ir nepieciešami un patiešām atbilst Savienības atzītiem vispārējo interešu mērķiem vai vajadzībai aizsargāt citu personu tiesības un brīvības.

Vispirms tā atgādina, ka Savienības tiesību akts, ciktāl iespējams, ir jāinterpretē veidā, kas neliek apšaubīt tā spēkā esamību un atbilstīgi primāro tiesību aktiem kopumā, it īpaši Hartas normām, un tāpēc dalībvalstīm jārūpējas, lai tās nebalstītos uz tādu šā akta interpretāciju, kas būtu pretrunā Savienības tiesību sistēmā aizsargātajām pamattiesībām vai citiem šajā tiesību sistēmā atzītajiem vispārējiem principiem. Par PDR direktīvu Tiesa paskaidro, ka liels skaits tās apsvērumu un normu prasa šādu atbilstīgu interpretāciju, uzsvērdama, kādu nozīmi Savienības likumdevējs, atsaucoties uz augstu datu aizsardzības līmeni, piešķir tam, lai pilnībā tiktu ievērotas Hartā nostiprinātās pamattiesības.

Tiesa konstatē, ka PDR direktīva ietver būtisku iejaukšanos Hartas 7. un 8. pantā garantētajās tiesībās, it īpaši, ciktāl tās mērķis ir nodibināt turpinātas, nemērķtiecīgas un sistemātiskas uzraudzības režīmu, ietverot visu aviotransporta pakalpojumus izmantojošo personu personas datu novērtēšanu. Tā atgādina, ka dalībvalstu iespēja attaisnot šādu iejaukšanos jāvērtē, izsverot tās būtiskumu un pārliecinoties, ka izvirzītais vispārējo interešu mērķis ir samērīgs ar iejaukšanās būtiskumu.

Tiesa secina – var uzskatīt, ka šajā direktīvā noteikto PDR datu nosūtīšana, apstrāde un glabāšana var tikt uzskatītas par tādām, kas aprobežojas ar to, kas ir absolūti nepieciešams, lai cīnītos pret teroristu nodarījumiem un smagiem noziegumiem, ja vien minētajā direktīvā noteiktās pilnvaras tiek interpretētas šauri. Šajā ziņā minētajā spriedumā ir teikts tostarp sekojošais:

- Ar PDR direktīvu izveidotā sistēma var attiekties tikai uz skaidri identificējamu un tās I pielikuma posteņos uzskaitītu informāciju saistībā ar veikto lidojumu un attiecīgo pasažieri, un atsevišķu šā pielikuma posteņu gadījumā tas nozīmē, ka šī sistēma aptver vienīgi tajos skaidri norādītās ziņas [17].

- Ar PDR direktīvu izveidotā sistēma jāpiemēro tikai un vienīgi attiecībā uz tiem teroristu nodarījumiem un smagiem noziegumiem, kam ir objektīva, kaut arī tikai netieša, saikne ar pasažieru aviotransportu. Runājot par šiem noziegumiem – šīs sistēmas piemērošanu nevar attiecināt uz noziedzīgiem nodarījumiem, kas, lai gan tie atbilst šajā direktīvā paredzētajam kritērijam par smaguma slieksni un ir tieši norādīti tās II pielikumā, ir uzskatāmi par parastiem noziedzīgiem nodarījumiem, ņemot vērā valsts krimināltiesību sistēmas īpatnības.

- Iespējamai PDR direktīvas piemērošanai attiecībā uz visiem ES iekšējiem lidojumiem vai daļu no tiem – ko dalībvalsts var izlemt veikt, izmantojot šajā direktīvā paredzētās pilnvaras, – ir jāaprobežojas ar to, kas ir absolūti nepieciešams. Šajā ziņā jābūt iespējamai efektīvai tiesas vai neatkarīgas

[17] Tādējādi it īpaši "maksājumu informācija" (pielikuma 6. punkts) ir jāierobežo ar maksāšanas kārtību un rēķinu par aviobiļeti, izslēdzot jebkādu citu informāciju, kurai nav tiešas saistības ar lidojumu, un "vispārīgās piezīmes" (12. punkts) var attiekties tikai uz šajā punktā tieši uzskaitīto informāciju, kas attiecas uz nepilngadīgiem pasažieriem.

administratīvas iestādes kontrolei, kuras lēmums ir saistošs. Šajā ziņā Tiesa precizē:

- Tikai tad, ja minētā dalībvalsts konstatē, ka pastāv pietiekami konkrēti apstākļi, lai uzskatītu, ka tā saskaras ar terorisma draudiem, kas, iespējams, ir reāli un esoši vai paredzami, šīs direktīvas piemērošana visiem ES iekšējiem lidojumiem no minētās dalībvalsts vai uz to laikposmā, kas ir ierobežots līdz absolūti nepieciešamajam, bet ir pagarināms, nepārsniedz absolūti nepieciešamo [18].

- Ja nav šādu terorisma draudu, minētā direktīva ir piemērojama nevis attiecībā uz visiem ES iekšējiem lidojumiem, bet gan tikai uz tiem, kuri ir saistīti tostarp ar noteiktiem gaisa satiksmes maršrutiem vai ceļojumu modeļiem vai arī noteiktām lidostām, par kurām attiecīgās dalībvalsts vērtējumā pastāv norādes, kas var pamatot šo piemērošanu. Šīs piemērošanas šādi izvēlētiem ES iekšējiem lidojumiem absolūta nepieciešamība regulāri jāpārbauda atkarībā no izmaiņām apstākļos, kas pamato to izvēli.

- Lai iepriekš novērtētu PDR datus ar mērķi identificēt personas, attiecībā uz kurām jāveic padziļināta pārbaude pirms viņu ieceļošanas vai izceļošanas, ko vispirms veic, izmantojot automātisku apstrādi, PIN, pirmkārt, šos datus var salīdzināt tikai ar datubāzēm par meklējamām personām vai objektiem vai arī personām, par kurām saņemts brīdinājums [19]. Šīm datubāzēm jābūt nediskriminējošām, un tās jāpārvalda kompetentajām iestādēm saistībā ar cīņu pret teroristu nodarījumiem un smagiem noziegumiem, kuri objektīvi, kaut arī netieši, ir saistīti ar pasažieru aviotransportu. Attiecībā, otrkārt, uz iepriekšēju novērtēšanu ar iepriekš noteiktu kritēriju palīdzību jāteic, ka PIN nevar izmantot mākslīgā intelekta tehnoloģijas pašmācīšanās (*machine learning*) sistēmā, kas bez cilvēka iesaistīšanās un kontroles var mainīt novērtēšanas procesu un it īpaši novērtēšanas kritērijus, uz kuriem tiek balstīts šī procesa piemērošanas rezultāts, kā arī šo kritēriju izsvēršanu. Minētie kritēriji jānosaka tādā veidā, lai to piemērošana būtu vērsta specifiski uz indivīdiem, kas varētu pamatoti tikt turēti aizdomās par līdzdalību teroristu nodarījumos vai smagos noziegumos, un lai tiktu ņemti vērā gan "apsūdzošie", gan "attaisnojošie" elementi, neradot tiešu vai netiešu diskrimināciju [20].

---

[18] Proti, šādu draudu esamība pati par sevi var radīt saikni starp attiecīgo datu nosūtīšanu un apstrādi, no vienas puses, un cīņu pret terorismu, no otras puses. Tādējādi, paredzot PDR direktīvas piemērošanu uz noteiktu laiku visiem ES iekšējiem lidojumiem no attiecīgās dalībvalsts vai uz to, netiek pārsniegtas absolūti nepieciešamā robežas, ja lēmumu, kurā paredzēta šī piemērošana, ir jābūt iespējai pārbaudīt tiesā vai neatkarīgā valsts pārvaldes iestādē.

[19] Proti, datubāzes, kas attiecas uz meklējamām personām vai objektiem vai arī personām, par kurām saņemts brīdinājums PDR direktīvas 6. panta 3. punkta a) apakšpunkta izpratnē. Savukārt analīze, pamatojoties uz dažādām datubāzēm, varētu izpausties kā datu izpēte (*data mining*), un tā varētu radīt šo datu nesamērīgu izmantošanu, kas ļautu noteikto šo datu subjektu precīzu profilu tāpēc vien, ka tām ir nodoms ceļot ar gaisa transportu.

[20] Iepriekš noteiktajiem kritērijiem jābūt mērķorientētiem, samērīgiem un konkrētiem, un tie regulāri ir jāpārskata (PDR direktīvas 6. panta 4. punkts). Iepriekšējs novērtējums, ņemot vērā iepriekš noteiktus kritērijus, jāveic nediskriminējošā veidā. Saskaņā ar PDR direktīvas 6. panta

- Ņemot vērā šādai PDR datu automātiskai apstrādei raksturīgo kļūdu īpatsvaru un samērā lielo to "kļūdaini pozitīvo" rezultātu skaitu, kuri iegūti tās piemērošanas laikā 2018. un 2019. gadā, ar PDR direktīvu izveidotās sistēmas piemērotība izvirzīto mērķu sasniegšanai galvenokārt ir atkarīga no tā, cik sekmīga ir šajā apstrādē iegūto pozitīvo rezultātu otrreizējā pārbaude, ko PIN veic ar neautomatizētiem līdzekļiem. Šajā ziņā dalībvalstīm jāparedz skaidri un precīzi noteikumi, uz kuriem PIN darbinieki, kas veic šo individuālo atkārtoto pārbaudi, balstītu savu analīzi, lai nodrošinātu Hartas 7., 8. un 21. pantā nostiprināto pamattiesību pilnīgu ievērošanu un it īpaši garantētu saskanīgu administratīvu praksi PIN, ievērojot diskriminācijas aizlieguma principu. It īpaši tām jānodrošina, ka PIN nosaka objektīvus pārskatīšanas kritērijus, kas tās darbiniekiem ļautu pārbaudīt, pirmkārt, vai un kādā mērā pozitīva atbilsme (*hit*) tiešām attiecas uz indivīdu, kas var būt iesaistīts teroristu nodarījumos vai smagos noziegumos, kā arī, otrkārt, automātiskās apstrādes nediskriminējošo raksturu. Šajā ziņā Tiesa vēl arī uzsver – kompetentajām iestādēm jānodrošina, ka ieinteresētā persona var saprast iepriekš noteikto novērtēšanas kritēriju un programmu, ar kurām šie kritēriji tiek piemēroti, darbības veidu, lai apzināti varētu izlemt izmantot vai neizmantot tiesības uz efektīvu tiesību aizsardzību tiesā. Tāpat arī saistībā ar šādu pārsūdzību tiesa, kas kontrolē kompetento iestāžu pieņemtā lēmuma likumību, kā arī, izņemot draudu valsts drošībai gadījumu, pati ieinteresētā persona var iepazīties gan ar visiem iemesliem, gan pierādījumiem, uz kuriem pamatojoties šis lēmums ir pieņemts, tostarp ar iepriekš noteiktajiem novērtēšanas kritērijiem un to programmu darbību, kuras piemēro šos kritērijus.
- PDR datu turpmāka izpaušana un novērtēšana, proti, pēc datu subjekta ieceļošanas vai izceļošanas, var notikt vienīgi, pamatojoties uz jauniem apstākļiem un objektīviem elementiem, kas vai nu var radīt pamatotas aizdomas par šīs personas iesaistīšanos smagos noziegumos, kuri objektīvi, kaut arī netieši, ir saistīti ar pasažieru aviotransportu, vai arī ļauj uzskatīt, ka šie dati konkrētajā gadījumā varētu faktiski palīdzēt cīņā pret teroristu nodarījumiem, kam ir šāda saikne. PDR datu paziņošana, lai veiktu šādu vēlāku novērtējumu, izņemot pienācīgi pamatotas steidzamības gadījumu, principā var notikt pēc iepriekšējas pārbaudes, ko veic vai nu tiesa, vai arī neatkarīga administratīva iestāde pēc kompetento iestāžu pamatota pieprasījuma, un tas tā ir neatkarīgi no tā, vai šis pieprasījums iesniegts, kamēr vēl nav vai jau ir pagājuši seši mēneši kopš šo datu nosūtīšanas PIN [21].

4. punkta ceturto teikumu kritēriji nekādā gadījumā nedrīkst būt balstīti uz personas rasi vai etnisko izcelsmi, politiskajiem uzskatiem, reliģiju vai filozofisko pārliecību, dalību arodbiedrībās, veselību, seksuālo dzīvi vai dzimumorientāciju.

[21] Saskaņā ar PDR direktīvas 12. panta 1. un 3. punktu šāda kontrole ir tieši paredzēta tikai attiecībā uz pieprasījumiem izpaust PDR datus, kas iesniegti pēc tam, kad pagājis sešu mēnešu termiņš kopš šo datu pārsūtīšanas PIN.

2022. gada 22. novembra spriedums (virspalāta) Luxembourg Business Registers (C-37/20 un C-601/20, EU:C:2022:912)

Lai apkarotu un novērstu noziedzīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu, Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīva [22] dalībvalstīm noteic pienākumu uzturēt reģistru, kurā ir informācija par to teritorijā reģistrētu sabiedrību un citu juridisko vienību patiesajiem labuma guvējiem [23]. Pēc grozījumiem šajā direktīvā, kas izdarīti ar Direktīvu 2018/843 [24], noteikta daļa šīs informācijas vienmēr jādara pieejama ikvienam sabiedrības loceklim. Atbilstoši šādi grozītajai Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvai (turpmāk tekstā – "grozītā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīva") ar Luksemburgas tiesību aktiem tika izveidots patieso labuma guvēju reģistrs (turpmāk tekstā – "PLGR"), lai saglabātu un darītu pieejamu virkni informācijas par reģistrēto juridisko vienību patiesajiem labuma guvējiem, ar kuru var iepazīties ikviens interesents.

Šajā kontekstā *Tribunal d'arrondissement de Luxembourg* (Luksemburgas apgabaltiesa) tika ierosinātas divas lietas, kurās WM un *Sovim SA* iebilda pret to, ka *Luxembourg Business Registers*, kas pārvalda PLGR, ir noraidījis to pieprasījumus liegt plašai sabiedrībai piekļuvi informācijai, kas attiecas – pirmajā lietā – uz WM kā nekustamā īpašuma sabiedrības patieso labuma guvēju un – otrajā lietā – uz *Sovim SA* patieso labuma guvēju. Saistībā ar šīm divām lietām Luksemburgas apgabaltiesa, šaubīdamās par to, vai Savienības tiesību normas, ar kurām izveidota informācijas par patiesajiem labuma guvējiem publiskas pieejamības sistēma, ir spēkā, vērsās Tiesā ar prejudiciālu jautājumu par spēkā esamības vērtējumu.

Virspalātas sastāvā pasludinātajā spriedumā Tiesa atzīst par spēkā neesošu Direktīvu 2018/843, ciktāl Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīva ar to grozīta tādējādi, ka dalībvalstīm ir jānodrošina, lai informācija par to teritorijā reģistrētu sabiedrību un citu juridisko vienību patiesajiem labuma guvējiem vienmēr būtu pieejama ikvienam sabiedrības loceklim [25].

Pirmām kārtām, Tiesa konstatē, ka ikviena sabiedrības locekļa piekļuve informācijai par patiesajiem labuma guvējiem, kas paredzēta grozītajā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvā, ir smaga iejaukšanās Hartas attiecīgi 7. un 8. pantā

---

22 Eiropas Parlamenta un Padomes Direktīva (ES) 2015/849 (2015. gada 20. maijs) par to, lai nepieļautu finanšu sistēmas izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai vai teroristu finansēšanai, un ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) Nr. 684/2012 un atceļ Eiropas Parlamenta un Padomes Direktīvu 2005/60/EK un Komisijas Direktīvu 2006/70/EK (OV 2015, L 141, 73. lpp.; turpmāk tekstā – "Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīva").

23 Saskaņā ar šīs direktīvas 3. panta 6. punktu patiesie labuma guvēji ir jebkura(-as) fiziska(-as) persona(-as), kurai(-ām) faktiski pieder klients vai kura(-as) šo klientu kontrolē, un/vai fiziska(-as) persona(-as), kuras vārdā darījums vai darbība tiek veikta.

24 Eiropas Parlamenta un Padomes Direktīva (ES) 2018/843 (2018. gada 30. maijs), ar ko groza Direktīvu (ES) 2015/849 par to, lai nepieļautu finanšu sistēmas izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai vai teroristu finansēšanai, un ar ko groza Direktīvas 2009/138/EK un 2013/36/ES (OV 2018, L 156, 43. lpp.).

25 Direktīvas 2018/843 1. panta 15. punkta c) apakšpunkta spēkā neesamība, ciktāl ar šo normu ir grozīta Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvas 30. panta 5. punkta pirmā daļa.

nostiprinātajās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību.

Šajā ziņā Tiesa norāda, ka – tā kā attiecīgie dati satur informāciju par identificētām fiziskām personām, proti, dalībvalstu teritorijā reģistrētu sabiedrību un citu juridisko vienību patiesajiem labuma guvējiem, – ikviena sabiedrības locekļa piekļuve informācijai skar pamattiesības uz privātās dzīves neaizskaramību. Turklāt tās publiskošana ir personas datu apstrāde. Tā piebilst, ka šāda publiskošana ir iejaukšanās abās iepriekš minētajās pamattiesībās, lai kāda arī būtu izpaustās informācijas vēlākā izmantošana.

Attiecībā uz šīs iejaukšanās smagumu Tiesa norāda, ka, ciktāl publiskotā informācija attiecas uz patiesā labuma guvēja identitāti, kā arī viņa faktiskās līdzdalības veidu un apmēru uzņēmumos vai citās juridiskajās vienībās, tā var ļaut izveidot profilu, kas attiecas uz noteiktiem personas identifikācijas datiem, datu subjekta mantisko stāvokli, kā arī konkrētām ekonomikas nozarēm, valstīm un uzņēmumiem, kuros tas ir veicis ieguldījumus. Turklāt šī informācija kļūst pieejama potenciāli neierobežotam personu skaitam, un tādējādi šāda personas datu apstrāde var ļaut arī personām, kuras ar šī pasākuma mērķi nesaistītu iemeslu dēļ vēlas noskaidrot tostarp patiesā labuma guvēja materiālo un finansiālo situāciju, brīvi piekļūt minētajai informācijai. Šī iespēja izrādās vēl jo vienkāršāka, ja ar attiecīgajiem datiem var iepazīties internetā. Turklāt varbūtējās sekas datu subjektiem, kādas rodas iespējamas to datu ļaunprātīgas izmantošanas dēļ, saasina fakts, ka, tiklīdz šie dati ir darīti pieejami ikvienam sabiedrības loceklim, tos ne tikai var brīvi iegūt, bet arī saglabāt un izplatīt un tādējādi datu subjektiem kļūst grūtāk vai pat iluzori efektīvi aizstāvēt sevi pret ļaunprātīgām darbībām.

Otrām kārtām, pārbaudot attiecīgās iejaukšanās attaisnojumu, pirmkārt, Tiesa atzīmē, ka šajā lietā ir ievērots tiesiskuma princips. Proti, iepriekš minēto pamattiesību izmantošanas ierobežojums, kas izriet no ikviena sabiedrības locekļa piekļuves informācijai par patiesajiem labuma guvējiem, ir paredzēts leģislatīvā aktā, proti, grozītajā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvā. Turklāt, no vienas puses, šajā direktīvā ir precizēts, ka šai informācijai ir jābūt adekvātai, pareizai un aktuālai, un tajā ir skaidri uzskaitīti konkrēti dati, kuriem ir jāpiešķir publiska piekļuve. No otras puses, tajā ir paredzēti nosacījumi, ar kādiem dalībvalstis var paredzēt atkāpes no šādas piekļuves.

Otrkārt, tā precizē, ka attiecīgā iejaukšanās neapdraud Hartas 7. un 8. pantā garantēto pamattiesību būtību. Lai gan grozītajā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvā patiešām nav ietverts izsmeļošs to datu uzskaitījums, kuriem ir jāļauj piekļūt ikvienam sabiedrības loceklim, un dalībvalstīm ir tiesības sniegt piekļuvi papildu informācijai, tomēr iegūt, saglabāt un tādējādi potenciāli darīt publiski pieejamu var vienīgi “adekvātu” informāciju par patiesajiem labuma guvējiem un to faktisko līdzdalību, kas izslēdz tostarp informāciju, kurai nav adekvātas saiknes ar grozītās Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvas mērķiem. Tomēr nešķiet, ka informācijas, kam ir šāda saikne, izpaušana ikvienam sabiedrības loceklim jebkādā veidā apdraudētu minēto pamattiesību būtību.

Treškārt, Tiesa uzsver, ka, paredzot ikviena sabiedrības locekļa piekļuvi informācijai par patiesajiem labuma guvējiem, Savienības likumdevējs vēlas novērst noziedzīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu, radot vidi ar lielāku pārredzamību, kurā ir mazāka iespēja, ka to izmantos šiem mērķiem, un tas ir vispārējo interešu mērķis, ar ko var attaisnot pat smagu iejaukšanos Hartas 7. un 8. pantā nostiprinātajās pamattiesībās.

Ceturtkārt, pārbaudot attiecīgās iejaukšanās piemērotību, nepieciešamību un samērīgumu, Tiesa konstatē, ka ikviena sabiedrības locekļa piekļuve informācijai par patiesajiem labuma guvējiem patiešām ir piemērota šī mērķa sasniegšanai.

Tomēr tā uzskata, ka šo iejaukšanos nevar uzskatīt par tādu, kas aprobežojas ar absolūti nepieciešamo. No vienas puses, minētās iejaukšanās absolūto nepieciešamību nevar pierādīt, pamatojoties uz to, ka kritēriju par ikvienas personas, kura vēlas piekļūt informācijai par patiesajiem labuma guvējiem, "leģitīmo interešu" esamību saskaņā ar Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvu, redakcijā, kas bija spēkā pirms tās grozīšanas ar Direktīvu 2018/843, bija grūti īstenot un ka tā piemērošana varēja izraisīt patvaļīgus lēmumus. Proti, iespējamās grūtības tiesību aktos precīzi noteikt gadījumus un apstākļus, kādos sabiedrība var piekļūt informācijai par patiesajiem labuma guvējiem, nevar attaisnot to, ka Savienības likumdevējs piekļuvi šai informācijai paredz ikvienam sabiedrības loceklim.

No otras puses, arī ar Direktīvā 2018/843 ietvertajiem skaidrojumiem nevar pierādīt attiecīgās iejaukšanās absolūtu nepieciešamību [26]. Tā kā saskaņā ar šiem skaidrojumiem ikviena sabiedrības locekļa piekļuvei informācijai par patiesajiem labuma guvējiem ir jāļauj pilsoniskajai sabiedrībai, tostarp presei un pilsoniskās sabiedrības organizācijām, labāk kontrolēt informāciju, Tiesa norāda, ka gan presei, gan pilsoniskās sabiedrības organizācijām, kurām ir saikne ar noziedzīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanu un apkarošanu, ir leģitīmas intereses piekļūt attiecīgajai informācijai. Tas pats attiecas uz personām, kas vēlas uzzināt sabiedrības vai citas juridiskas vienības patiesā labuma guvēja identitāti tāpēc, ka tās gatavojas noslēgt darījumus ar šīm sabiedrībām vai vienībām, vai arī finanšu iestādēm un iestādēm, kas iesaistītas noziedzīgi iegūtu līdzekļu legalizēšanas vai terorisma finansēšanas apkarošanā.

Turklāt attiecīgā iejaukšanās nav arī samērīga. Šajā ziņā Tiesa konstatē, ka materiālo tiesību normas, kas reglamentē šo iejaukšanos, neatbilst skaidrības un precizitātes prasībai. Proti, grozītajā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvā ir paredzēta ikvienas sabiedrības daļas piekļuve "vismaz" šajā direktīvā minētajiem datiem un dalībvalstīm ir dota iespēja sniegt piekļuvi papildu informācijai, kas ietver "vismaz" attiecīgā patiesā labuma guvēja dzimšanas datumu vai kontaktinformāciju. No vārda

[26] Runa ir par Direktīvas 2018/843 30. apsvērumā minētajiem skaidrojumiem.

"vismaz" lietojuma izriet, ka šī direktīva ļauj darīt pieejamus sabiedrībai datus, kas nav nedz pietiekami definēti, nedz identificējami.

Turklāt attiecībā uz šīs iejaukšanās smaguma samērošanu ar izvirzītā vispārējo interešu mērķa nozīmīgumu Tiesa atzīst, ka, ņemot vērā šā mērķa nozīmīgumu, tas var attaisnot pat smagu iejaukšanos Hartas 7. un 8. pantā nostiprinātajās pamattiesībās.

Tomēr, pirmkārt, cīņa pret noziedzīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu galvenokārt ir jāveic publiskajām iestādēm, kā arī tādām struktūrām kā kredītiestādēm vai finanšu iestādēm, kurām, ņemot vērā to darbību, šajā jomā ir noteikti īpaši pienākumi. Tieši šī iemesla dēļ grozītajā Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvā ir paredzēts, ka informācijai par patiesajiem labuma guvējiem vienmēr ir jābūt pieejamai kompetentajām iestādēm un finanšu ziņu vākšanas vienībām bez jebkādiem ierobežojumiem, kā arī atbildīgajiem subjektiem saistībā ar klienta uzticamības pārbaudi [27].

Otrkārt, salīdzinājumā ar agrāko sistēmu, kurā papildus kompetento iestāžu un noteiktu struktūru piekļuvei informācijai par patiesajiem labuma guvējiem bija paredzēta arī jebkuras tādas personas vai organizācijas piekļuve, kas var pierādīt leģitīmas intereses, ar Direktīvu 2018/843 ieviestā sistēma rada ievērojami smagāku Hartas 7. un 8. pantā garantēto pamattiesību aizskārumu, taču šo smagumu nevar atsvērt iespējamie ieguvumi, ko attiecībā uz cīņu pret noziedzīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu šī otrā sistēma varētu radīt salīdzinājumā ar pirmo.

2. Tiesību uz personas datu aizsardzību ievērošana, īstenojot Savienības tiesību aktus

2016. gada 21. decembra spriedums (virspalāta) Tele2 Sverige (apvienotās lietas C-203/15 un C-698/15, EU:C:2016:970)

Pēc tam, kad Tiesa spriedumā *Digital Rights Ireland* un *Seitlinger* u.c. bija atzinusi Direktīvu 2006/24 par spēkā neesošu (skat. iepriekš), tajā tika ierosinātas divas lietas par elektronisko sakaru pakalpojumu sniedzējiem Zviedrijā un Apvienotajā Karalistē noteiktu vispārēju pienākumu saglabāt ar šo saziņu saistītos datus, kuru saglabāšana bija paredzēta par spēkā neesošu atzītajā direktīvā.

Nākamajā dienā pēc sprieduma *Digital Rights Ireland* un *Seitlinger* u.c. pasludināšanas telekomunikāciju uzņēmums *Tele2 Sverige* paziņoja Zviedrijas Pasta un telekomunikāciju uzraudzības iestādei par savu lēmumu pārtraukt datu glabāšanu un nodomu dzēst jau

[27] Grozītās Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas direktīvas 30. panta 5. punkta pirmās daļas a) un b) apakšpunkts.

saglabātos datus (lieta C-203/15). Proti, Zviedrijas tiesību aktos elektronisko sakaru pakalpojumu sniedzējiem bija paredzēts pienākums sistemātiski un nepārtraukti, neizdarot nevienu izņēmumu, saglabāt visus datus attiecībā uz visu abonentu un reģistrēto lietotāju datu plūsmu un atrašanās vietu saistībā ar visiem elektronisko sakaru līdzekļiem. Lietā C-698/15 trīs personas bija cēlušas prasību, apstrīdot Apvienotajā Karalistē pastāvošo datu saglabāšanas kārtību, kas ļāva iekšlietu ministram noteikt publisko telekomunikāciju operatoriem pienākumu saglabāt visus saziņas datus ne ilgāk kā divpadsmit mēnešus, tomēr šīs saziņas satura saglabāšana netika atļauta.

Kammarrätten i Stockholm (Administratīvā apelācijas tiesa Stokholmā, Zviedrija) un *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta), Apvienotā Karaliste) lūdza Tiesu lemt par to, kā ir interpretējams Direktīvas 2002/58 (direktīva par privāto dzīvi un elektronisko komunikāciju) 15. panta 1. punkts, kas ļauj dalībvalstīm ieviest dažus izņēmumus no šajā direktīvā noteiktā pienākuma nodrošināt elektroniskās saziņas un attiecīgās informācijas par datu plūsmu konfidencialitāti.

Šajā spriedumā Tiesa vispirms nosprieda, ka Direktīvas 2002/58 15. panta 1. punktam – interpretētam Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā – pretrunā ir tāds valsts tiesiskais regulējums kā Zviedrijā pastāvošais, kurā noziedzības apkarošanas nolūkā ir paredzēta visaptveroša un nediferencēta visas informācijas saglabāšana par datu plūsmu un atrašanās vietu attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko sakaru līdzekļiem. Saskaņā ar Tiesas viedokli šāds tiesiskais regulējums pārsniedz to, kas ir absolūti nepieciešams, un tas nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā to prasa minētais 15. panta 1. punkts, lasot to minēto Hartas pantu gaismā.

Šai pašai tiesību normai – interpretētai minēto Hartas pantu gaismā – pretrunā ir arī tāds valsts tiesiskais regulējums, ar ko reglamentē informācijas par datu plūsmu un atrašanās vietas datu aizsardzību un drošību, it īpaši kompetento valsts iestāžu piekļuvi saglabātajiem datiem, noziedzības apkarošanas ietvaros neierobežojot šo piekļuvi vienīgi ar smagās noziedzības apkarošanas mērķiem, nepakļaujot šo piekļuvi iepriekšējai tiesas vai neatkarīgas valsts iestādes kontrolei un neprasot, lai konkrētie dati tiktu saglabāti Savienības teritorijā.

Tiesa savukārt atzina, ka Direktīvas 2002/58 15. panta 1. punktam nav pretrunā tāds tiesiskais regulējums, ar ko preventīvi atļauts saglabāt iepriekš definētu informāciju par šāda veida datiem smagu noziegumu apkarošanas nolūkā ar nosacījumu, ka datu saglabāšana attiecībā uz saglabājamo datu kategorijām, iepriekš identificētiem saziņas līdzekļiem, datu subjektiem, kā arī noteikto saglabāšanas ilgumu aptver tikai absolūti nepieciešamo. Lai izpildītu šīs prasības, valsts tiesiskajā regulējumā, pirmkārt, ir jāparedz skaidri un precīzi noteikumi, kuri ļautu datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Konkrēti tajā ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem datu saglabāšanas pasākums var preventīvi tikt veikts, tādējādi nodrošinot, ka šāds pasākums aprobežojas ar absolūti nepieciešamo. Otrkārt, attiecībā

uz substanciālajiem nosacījumiem, kuriem ir jāatbilst valsts tiesiskajam regulējumam, lai nodrošinātu, ka tas aprobežojas ar absolūti nepieciešamo, datu saglabāšanai ir vienmēr jāatbilst objektīviem kritērijiem, ar kuriem konstatē saikni starp saglabājamiem datiem un sasniedzamo mērķi. It īpaši, šādiem nosacījumiem praktiski ir jābūt tādiem, kas faktiski ierobežo pasākuma vērienu un secīgi arī attiecīgo personu loku. Attiecībā uz šādu ierobežošanu valsts tiesiskajam regulējumam ir jābūt balstītam uz objektīviem apstākļiem, kas ļauj definēt personu loku, kuru datiem var būt kaut vai netieša saikne ar smagiem noziegumiem, vienā vai otrā veidā dot ieguldījumu smagu noziegumu apkarošanā vai novērst būtisku apdraudējumu sabiedrības drošībai.

II. Personas datu apstrāde vispārējā šīs jomas tiesiskā regulējuma izpratnē

1. Vispārējā tiesiskā regulējuma piemērošanas joma

2006. gada 30. maija spriedums (virspalāta) Parlaments/Padome (C-317/04 un C-318/04, EU:C:2006:346)

Pēc 2001. gada 11. septembra teroristu uzbrukumiem Amerikas Savienotās Valstis pieņēma tiesisko regulējumu, kas noteic, ka gaisa pārvadājumu uzņēmumiem, kas nodrošina lidojumus uz Amerikas Savienotajām Valstīm, no tām vai pāri to teritorijai, ir pienākums ASV iestādēm dot elektronisku pieeju datiem, kuri ir ietverti to rezervēšanas un izlidošanas kontroles sistēmās, ko sauc par Pasažieru datu reģistru (PDR).

Uzskatot, ka šie noteikumi varētu būt pretrunā ES un dalībvalstu tiesību aktiem datu aizsardzības jomā, Komisija uzsāka sarunas ar ASV iestādēm. Šo sarunu rezultātā Komisija 2004. gada 14. maijā pieņēma Lēmumu 2004/535/EK [28], kurā konstatēts, ka Amerikas Savienoto Valstu Muitas un robežapsardzes birojs (*United States Bureau of Customs and Border Protection*, turpmāk tekstā – "*CBP*") nodrošina atbilstošu aizsardzību *PNR* iekļautajiem datiem, kas nosūtīti no Kopienas (turpmāk tekstā – "lēmums par atbilstību"). Pēc tam Padome 2004. gada 17. maijā pieņēma Lēmumu 2004/496/EK [29], ar ko apstiprina nolīguma noslēgšanu starp Eiropas Kopienu un Amerikas Savienotajām Valstīm attiecībā uz PDR datu apstrādi un pārsūtīšanu *CBP*, ko veic Kopienas dalībvalstu teritorijā reģistrētie aviopārvadātāji.

[28] Komisijas Lēmums 2004/535/EK (2004. gada 14. maijs) par pietiekamu aizsardzību *Passenger Name Record* iekļautajiem lidmašīnu pasažieru personas datiem, kas nosūtīti Amerikas Savienoto Valstu Muitas un robežapsardzes birojam (OV 2004, L 235, 11. lpp.).

[29] Padomes Lēmums 2004/496/EK (2004. gada 17. maijs) par nolīguma noslēgšanu starp Eiropas Kopienu un Amerikas Savienotajām Valstīm attiecībā uz personas datu apstrādi un pārsūtīšanu, ko aviopārvadātāji veic ASV Nacionālās drošības ministrijas Muitas un robežsardzes departamentam (OV 2004, L 183, 83. lpp.).

Eiropas Parlaments lūdza Tiesu atcelt abus iepriekš minētos lēmumus, apgalvojot tostarp, ka lēmums par atbilstību tika pieņemts *ultra vires*, ka EKL 95. pants (tagad LESD 114. pants) nav bijis atbilstošs juridiskais pamats lēmumam, ar ko apstiprina nolīguma noslēgšanu, un ka abos gadījumos ir pārkāptas pamattiesības.

Attiecībā uz lēmumu par atbilstību Tiesa vispirms pārbaudīja, vai Komisija varēja likumīgi pieņemt lēmumu, balstoties uz Direktīvu 95/46. Šajā situācijā tā konstatēja, ka no lēmuma par atbilstību izriet, ka PDR datu nosūtīšana *CBP* ir uzskatāma par apstrādi, kuras mērķis ir sabiedriskā drošība un valsts pasākumi krimināltiesību jomā. Saskaņā ar Tiesas viedokli, lai gan aviosabiedrības sākumā apkopo PDR datus tādu pasākumu ietvaros, kuri paredzēti Savienības tiesībās, proti, lidmašīnas biļešu pārdošanai, kas dod tiesības uz pakalpojumu sniegšanu, tomēr datu apstrādei, kura paredzēta lēmumā par atbilstību, ir pavisam cits raksturs. Proti, šis lēmums neattiecās uz datu apstrādi, kas ir nepieciešama pakalpojumu sniegšanai, bet gan uz datu apstrādi, kas ir nepieciešama, lai nodrošinātu sabiedrisko drošību, un represīvos nolūkos.

Šajā ziņā Tiesa norādīja, ka tas, ka privātie uzņēmēji ir apkopojuši PDR datus komercdarbības nolūkā un organizē to pārsūtīšanu uz trešām valstīm, nav pretrunā tam, ka šāda pārsūtīšana tiek uzskatīta par datu apstrādi, kas neietilpst direktīvas piemērošanas jomā. Proti, šī pārsūtīšana ietilpst sabiedriskās drošības nolūkos valsts varas noteiktajos ietvaros. Tāpēc Tiesa secināja, ka lēmums par atbilstību neietilpst direktīvas piemērošanas jomā, jo tas attiecas uz personas datu apstrādi, kas no tās ir izslēgta. Līdz ar to Tiesa lēmumu par atbilstību atcēla.

Attiecībā uz Padomes lēmumu Tiesa konstatēja, ka EKL 95. pants, lasot to kopā ar Direktīvas 95/46 25. pantu, nevar radīt Kopienas kompetenci noslēgt minēto nolīgumu ar ASV. Proti, šis nolīgums attiecās uz to pašu datu pārsūtīšanu, uz ko attiecās lēmums par atbilstību, un tādējādi – uz datu apstrādi, kas ir izslēgta no direktīvas piemērošanas jomas. Tādēļ Tiesa atcēla Padomes lēmumu, ar ko tika apstiprināta nolīguma noslēgšana.

2014. gada 13. maija spriedums (virspalāta) Google Spain un Google (C-131/12, EU:C:2014:317)

2010. gadā kāds Spānijas valstspiederīgais iesniedza *Agencia Española de Protección de Datos* (Spānijas Datu aizsardzības aģentūra, turpmāk tekstā – "*AEPD*") sūdzību pret *La Vanguardia Ediciones SL*, kas ir Spānijā plaši pazīstama dienas laikraksta redakcija, kā arī pret *Google Spain* un *Google*. Šī persona apgalvoja, ka, ja interneta lietotāji ievada viņa vārdu *Google* grupas meklētājprogrammā, rezultātu sarakstā parādās saites uz divām dienas laikraksta *La Vanguardia* lappusēm, kas datētas ar 1998. gadu, sakarā ar nekustamas mantas izsoli saistībā ar apķīlāšanu šīs personas parādu dēļ. Ar savu sūdzību minētā persona lūdza, pirmkārt, lai *La Vanguardia* tiktu uzdots vai nu dzēst, vai izmainīt šīs lapas, vai arī izmantot noteiktus rīkus, kas pieejami interneta meklētājprogrammās, šo datu aizsargāšanai. Otrkārt, tā lūdza, lai vai nu *Google Spain*, vai

Google tiktu uzdots dzēst vai aizklāt viņa personas datus, lai tie vairs neparādītos meklēšanas rezultātos un vairs nebūtu *La Vanguardia* saitēs.

AEPD sūdzību noraidīja, ciktāl tā attiecās uz *La Vanguardia*, uzskatot, ka tās veiktā attiecīgās informācijas publicēšana bija tiesiski pamatota, taču šī pati sūdzība tika apmierināta, ciktāl tā bija vērsta pret *Google Spain* un *Google*, un šiem abiem uzņēmumiem tika likts izdzēst no sava indeksa attiecīgos personas datus un liegt turpmāku piekļuvi šiem datiem. Tā kā minētie uzņēmumi iesniedza divas apelācijas sūdzības *Audiencia Nacional* (Valsts mēroga lietu tiesa, Spānija), lai panāktu *AEPD* lēmuma atcelšanu, Spānijas tiesa vērsās Tiesā ar vairākiem prejudiciāliem jautājumiem.

Šajā spriedumā Tiesa ir arī lēmusi par Direktīvas 95/46 teritoriālās piemērošanas jomu.

Tādējādi Tiesa nosprieda, ka personas datu apstrāde tiek veikta par šo apstrādi dalībvalsts teritorijā atbildīgā nodibinājuma darbības ietvaros Direktīvas 95/46 izpratnē, ja meklētājprogrammas pakalpojumu sniedzējs, lai gan tā juridiskā adrese ir reģistrēta trešā valstī, dalībvalstī izveido filiāli vai meitasuzņēmumu, kas ir paredzēts reklāmas laukumu meklētājprogrammā reklamēšanai un pārdošanai un kura darbība ir vērsta uz šīs dalībvalsts iedzīvotājiem.

Proti, šādos apstākļos meklētājprogrammas pakalpojumu sniedzēja darbības ir nesaraujami saistītas un šā pakalpojumu sniedzēja attiecīgajā dalībvalstī esošā nodibinājuma darbībām, jo darbības saistībā ar reklāmas laukumiem ir līdzeklis, lai padarītu attiecīgo meklētājprogrammu ekonomiski rentablu, un šī programma tajā pašā laikā ir līdzeklis, kas ļauj paveikt šīs darbības.

2014. gada 11. decembra spriedums Ryneš (C-212/13, EU:C:2014:2428).

Reaģējot uz vairākkārtējiem uzbrukumiem, *F. Ryneš* savai mājai uzstādīja novērošanas kameru. Pēc atkārtota uzbrukuma viņa mājai ar kameras ieraksta palīdzību tika identificēti divi aizdomās turētie, pret kuriem tika uzsākti kriminālprocesi. Tā kā viens no aizdomās turētajiem apstrīdēja videonovērošanas kameras ierakstīto datu apstrādes likumīgumu Čehijas Republikas Personas datu aizsardzības birojā, šis birojs konstatēja, ka *F. Ryneš* ir pārkāpis noteikumus par personas datu aizsardzību, un uzlika viņam naudas sodu.

Tā kā *Městský soud v Praze* (Prāgas pilsētas tiesa, Čehijas Republika) lēmumu, ar ko Biroja lēmums tika atstāts negrozīts, *F. Ryneš* pārsūdzēja *Nejvyšší správní soud* (Augstākā administratīvā tiesa), šī tiesa uzdeva Tiesai jautājumu, vai *F. Ryneš* veiktais videonovērošanas ieraksts ar nolūku aizsargāt savu dzīvību, veselību un īpašumu ir uzskatāms par datu apstrādi, uz kuru neattiecas Direktīva 95/46, tādēļ, ka šo ierakstu veikusi fiziska persona tikai un vienīgi personiskām vai sadzīviskām vajadzībām minētās direktīvas 3. panta 2. punkta otrā ievilkuma izpratnē.

Tiesa nosprieda, ka tādas kameras sistēmas izmantošana, ar kuru tiek veikts personu vizuālais ieraksts, kas tiek uzglabāts cirkulējošā ieraksta iekārtā, proti, cietajā diskā, un

kuru fiziska persona ir uzstādījusi pie savas ģimenes mājas ar mērķi aizsargāt mājas īpašnieku īpašumu, veselību un dzīvību, bet ar šo sistēmu tiek uzraudzīta arī publiskā telpa, nav datu apstrāde tikai un vienīgi personiskām vai sadzīviskām vajadzībām.

Šajā ziņā tā atgādināja, ka Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību aizsardzības pamatā ir prasība, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti tikai tik lielā mērā, cik tas ir absolūti nepieciešams. Ciktāl Direktīvas 95/46 tiesību normas, tā kā tajās ir reglamentēta personas datu apstrāde, kas var kaitēt pamatbrīvībām un it īpaši tiesībām uz privātās dzīves neaizskaramību, noteikti ir jāinterpretē, ievērojot minētajā Hartā nostiprinātās pamattiesības, šīs direktīvas 3. panta 2. punkta otrajā ievilkumā paredzētā atkāpe ir jāinterpretē šauri. Turklāt pats šīs tiesību normas formulējums izslēdz no Direktīvas 95/46 piemērošanas jomas datu apstrādi "tikai un vienīgi" personiskām vai sadzīviskām vajadzībām. Tomēr, ciktāl videonovērošana kaut vai daļēji aptver publisko telpu un tādēļ ir vērsta ārpus personas, kura ar šo līdzekli veic datu apstrādi, privātās sfēras, to nevar uzskatīt par darbību tikai un vienīgi "personiskām vai sadzīviskām vajadzībām" minētās tiesību normas izpratnē.

2024. gada 16. janvāra spriedums (virspalāta) Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Iespējamās politiskās ietekmes uz *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (Federālais konstitucionālās kārtības aizsardzības un terorisma apkarošanas birojs, Austrija) [30] noskaidrošanai *Nationalrat* (Nacionālā padome, Austrija) izveidoja izmeklēšanas komisiju (turpmāk tekstā – "*BVT* izmeklēšanas komisija"). Šī komisija uzklausīja WK kā liecinieku. Lai arī viņš bija izteicis lūgumu par anonimizāciju, *Parlament Österreich* (Austrijas parlaments) tīmekļvietnē tika publiskots šīs uzklausīšanas protokols, kurā bija pilnībā norādīts viņa vārds un uzvārds. Apgalvojot, ka šāda viņa identitātes izpaušana ir pretrunā VDAR un Austrijas tiesību aktiem, WK iesniedza sūdzību *Österreichische Datenschutzbehörde* (Datu aizsardzības iestāde, Austrija; turpmāk tekstā – "*Datenschutzbehörde*"). Ar 2019. gada 18. septembra lēmumu *Datenschutzbehörde* atzina, ka tās kompetencē nav lemt par šo sūdzību tāpēc, ka varas dalīšanas princips liedzot šai iestādei kā izpildvaras orgānam kontrolēt likumdošanas varai piederīgo *BVT* izmeklēšanas komisiju.

Pēc tam, kad *Bundesverwaltungsgericht* (Federālā administratīvā tiesa, Austrija) ar nolēmumu bija apmierinājusi WK prasību un atcēlusi *Datenschutzbehörde* lēmumu, šī nupat minētā iestāde vērsās Augstākajā administratīvajā tiesā ar revīzijas sūdzību par šo Federālās administratīvās tiesas nolēmumu.

[30] 2021. gada 1. decembrī šī struktūra pārtapa par "Direktion Staatsschutz und Nachrichtendienst" (Valsts drošības un izlūkošanas dienesta direkcija, Austrija).

Šajā kontekstā iesniedzējtiesa jautāja Tiesai, vai dalībvalsts parlamenta izveidotas izmeklēšanas komisijas darbības ietilpst VDAR piemērošanas jomā un vai šī regula ir piemērojama situācijā, kad šīs darbības attiecas uz valsts drošības aizsardzību.

Pirmām kārtām, Tiesa atgādina, ka VDAR 2. panta 2. punkta a) apakšpunkta – kas noteic, ka šo regulu nepiemēro personas datu apstrādei, kas veikta tādas darbības gaitā, kas neietilpst Savienības tiesību piemērošanas jomā – vienīgais mērķis ir izslēgt no minētās regulas piemērošanas jomas tādu personas datu apstrādi, ko valsts iestādes veic uz valsts drošības aizsardzību vērstas vai arī šajā pašā kategorijā iekļaujamas darbības ietvaros. Tādējādi ar to vien, ka darbība ir raksturīga valstij vai valsts iestādei, nepietiek, lai automātiski izslēgtu VDAR piemērojamību šādai darbībai.

Šo interpretāciju – kas izriet jau no tā, ka netiek veikta nošķiršana atkarībā no attiecīgās apstrādes veicēja identitātes – apstiprina VDAR 4. panta 7. punkts [31].

Tiesa precizē, ka *BVT* izmeklēšanas komisijas parlamentārā iedaba nenozīmē, ka tās darbības būtu izslēgtas no VDAR piemērošanas jomas. Proti, šīs regulas 2. panta 2. punkta a) apakšpunktā paredzētais izņēmums attiecas nevis uz personu kategorijām, bet gan tikai uz darbību kategorijām, kas savas iedabas dēļ neietilpst Savienības tiesību piemērošanas jomā. Līdz ar to apstāklis, ka personas datu apstrādi veic izmeklēšanas komisija, ko dalībvalsts parlaments izveidojis, izmantojot savas tiesības īstenot kontroli pār izpildvaru, pats par sevi neļauj konstatēt, ka šī apstrāde tiek veikta tādas darbības ietvaros, kas neietilpst Savienības tiesību piemērošanas jomā.

Otrām kārtām, Tiesa norāda, ka, lai gan dalībvalstu ziņā ir noteikt savas būtiskās drošības intereses un veikt pienācīgus pasākumus, lai šo drošību garantētu [32], tas vien, ka valsts pasākums ir veikts valsts drošības aizsardzības nolūkā, nevar izraisīt Savienības tiesību nepiemērojamību un atbrīvot dalībvalstis no obligātās šo tiesību ievērošanas. Savukārt VDAR 2. panta 2. punkta a) apakšpunktā paredzētais izņēmums attiecas tikai uz tādām darbību kategorijām, kas savas iedabas dēļ neietilpst Savienības tiesību piemērošanas jomā. Šajā ziņā apstāklis, ka pārzinis ir publiska iestāde, kuras pamatdarbība ir garantēt valsts drošību, pats par sevi nav pietiekams, lai no VDAR piemērošanas jomas izslēgtu personas datu apstrādi, ko šī iestāde veic saistībā ar citām tās veiktajām darbībām.

Šajā gadījumā *BVT* izmeklēšanas komisijas veiktā politiskā kontrole pati par sevi nešķiet esam darbība, kas vērsta uz valsts drošības aizsardzību, vai tāda, kas būtu iekļaujama tajā pašā kategorijā. Tāpēc – ja vien iesniedzējtiesas veicamajā pārbaudē netiek konstatēts citādi – šī darbība nav izslēgta no VDAR piemērošanas jomas.

[31] Tajā jēdziens "pārzinis" ir definēts kā "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus".

[32] Saskaņā ar LES 4. panta 2. punktu.

Taču parlamentārā izmeklēšanas komisija savā darbā var piekļūt personas datiem, kam valsts drošības apsvērumu dēļ jānodrošina īpaša aizsardzība. Šajā ziņā VDAR paredzētos pienākumus un tiesības var ierobežot ar leģislatīviem pasākumiem tostarp tālab, lai garantētu valsts drošību [33]. Tādējādi ar šādu pamatojumu var tikt attaisnoti ierobežojumi attiecībā uz personas datu vākšanu, datu subjektu informēšanu un viņu piekļuvi minētajiem datiem vai arī šo datu izpaušanu bez datu subjektu piekrišanas personām, kas nav pārzinis, ja vien ar šādiem ierobežojumiem tiek ievērota datu subjektu pamattiesību un pamatbrīvību būtība un ja vien tie demokrātiskā sabiedrībā ir nepieciešami un samērīgi.

Tomēr Tiesa norāda, ka no tās rīcībā esošās informācijas neizriet, ka *BVT* izmeklēšanas komisija būtu apgalvojusi, ka datu subjekta personas datu izpaušana bija nepieciešama valsts drošības aizsardzībai un balstīta uz tālab paredzētu valsts leģislatīvu pasākumu; to gan pārbaudīt vajadzības gadījumā ir iesniedzējtiesas ziņā.

2. Jēdziens "personas dati"

2016. gada 19. oktobra spriedums Breyer (C-582/14, EU:C:2016:779)

P. Breyer Vācijas civillietu tiesās cēla prasību par to, lai Vācijas Federatīvajai Republikai tiktu aizliegts pēc katras Vācijas federālo dienestu interneta vietņu aplūkošanas saglabāt vai likt trešām personām saglabāt nodotos informātikas datus. Lai novērstu uzbrukumus un darītu iespējamu krimināltiesiskas vajāšanas uzsākšanu pret "uzbrucējiem", Vācijas federālo dienestu tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ierakstīja datus, kas satur "dinamisko" IP adresi – IP adresi, kas mainās līdz ar katru jaunu pievienošanos internetam, – kā arī vietnes aplūkošanas datumu un laiku. Atšķirībā no statiskajām IP adresēm dinamiskās IP adreses *a priori* nedod iespēju, izmantojot sabiedrībai pieejamas datnes, noteikt saikni starp konkrētu datoru un interneta piekļuves pakalpojumu sniedzēja izmantotu fizisku pieslēgumu tīklam. Tikai ierakstītie dati paši par sevi tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējam nedod iespēju identificēt lietotāju. Savukārt interneta piekļuves pakalpojumu sniedzējam ir papildu informācija, kura, ja tā tiktu kombinēta ar šo IP adresi, ļautu identificēt minēto lietotāju.

Šajā saistībā *Bundesgerichtshof* (Federālā augstākā tiesa, Vācija), kurā tika iesniegta sūdzība "Revision" kārtībā, uzdeva Tiesai jautājumu, vai IP adrese, ko tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ieraksta saistībā ar piekļuvi tā tīmekļvietnei, attiecībā uz to ir uzskatāma par personas datiem.

[33] Atbilstoši VDAR 23. pantam.

Tiesa vispirms norādīja, ka, lai datus varētu kvalificēt kā "personas datus" Direktīvas 95/46 2. panta a) punkta izpratnē, netiek prasīts, lai visa informācija, kas ļauj identificēt datu subjektu, atrastos tikai vienas personas rīcībā. Tādējādi ar to, ka papildu informācija, kas ir vajadzīga, lai identificētu tīmekļvietnes lietotāju, ir nevis tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja, bet šā lietotāja interneta piekļuves pakalpojumu sniedzēja rīcībā, nevar izslēgt, ka tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzēja ierakstītās dinamiskās IP adreses attiecībā uz to ir personas dati Direktīvas 95/46 2. panta a) punkta izpratnē.

Tāpēc Tiesa konstatēja, ka dinamiskā IP adrese, ko tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs ieraksta saistībā ar personas piekļuvi šā pakalpojumu sniedzēja publiskai lietošanai paredzētai tīmekļvietnei, attiecībā uz minēto pakalpojumu sniedzēju ir uzskatāma par personas datiem Direktīvas 95/46 2. panta a) punkta izpratnē, ja tā rīcībā ir tiesiski līdzekļi, kas tam ļauj likt identificēt datu subjektu, izmantojot šā subjekta interneta piekļuves pakalpojumu sniedzēja rīcībā esošo papildu informāciju par šo subjektu.

2017. gada 20. decembra spriedums Nowak (C-434/16, EU:C:2017:994)

P. Nowak, grāmatvedības praktikantam, neizdevās nokārtot Īrijas Zvērinātu grāmatvežu institūta rīkotu eksāmenu. Viņš iesniedza pieteikumu nodrošināt piekļuvi saskaņā ar Datu aizsardzības likuma 4. pantu visiem personas datiem, kas attiecībā uz viņu atradās Zvērinātu grāmatvežu institūta rīcībā. Institūts nosūtīja *P. Nowak* dažus dokumentus, taču atteicās izsniegt viņa pārbaudes darba kopiju, kā pamatojumu minot, ka pārbaudes darbā neesot ietverti ar viņu saistīti "personas dati" Datu aizsardzības likuma izpratnē.

Kad Datu aizsardzības uzraudzītājs to pašu iemeslu dēļ arī nesniedza pozitīvu atbildi uz viņa pieteikumu par piekļuvi, *P. Nowak* vērsās valsts tiesās. *Supreme Court* (Augstākā tiesa, Īrija), kurā *P. Nowak* iesniedza pārsūdzību, vērsās Tiesā ar jautājumu, vai Direktīvas 95/46 2. panta a) punkts ir jāinterpretē tādējādi, ka tādos apstākļos kā pamatlietā aplūkotie rakstiskās atbildes, kuras eksaminējamā persona sniedz profesionāla kvalifikācijas eksāmena laikā, un iespējamas eksaminētāju piezīmes par šo pārbaudījumu ir eksaminējamās personas dati šīs tiesību normas izpratnē.

Pirmkārt, Tiesa norādīja, ka, lai datus varētu uzskatīt par "personas datiem" Direktīvas 95/46 2. panta a) punkta izpratnē, netiek prasīts, lai visa informācija, kas ļauj identificēt datu subjektu, atrastos tikai vienas personas rīcībā. Turklāt gadījumā, ja pārbaudījuma atbilžu vērtēšanas laikā eksaminētājam nav zināma eksaminējamās personas identitāte, iestādes, kas rīko šos pārbaudījumus, – šajā gadījumā Zvērinātu grāmatvežu institūta – rīcībā savukārt ir visa nepieciešamā informācija, lai bez jebkādām grūtībām vai šaubām identificētu šo eksaminējamo personu pēc tās reģistrācijas numura, kas ir norādīts uz pārbaudījuma darba vai vāka titullapas, un tādējādi attiecinātu atbildes uz šo personu.

Otrkārt, Tiesa konstatēja, ka eksaminējamās personas sniegtās rakstiskās atbildes profesionālās kvalifikācijas eksāmena laikā ir informācija, kas uz to attiecas. Proti, šo atbilžu saturs atspoguļo eksaminējamās personas zināšanu līmeni un kompetenci minētajā jomā, kā arī attiecīgā gadījumā tās domāšanas procesu, spriestspēju un kritisko domāšanu. Turklāt minēto atbilžu apkopošanas mērķis ir novērtēt eksaminējamās personas profesionālās zināšanas un piemērotību veicamajam amatam. Papildus tam šīs informācijas izmantošana, kas it īpaši atspoguļo attiecīgās eksaminējamās personas veiksmīgus vai neveiksmīgus pārbaudījuma rezultātus, var ietekmēt personas tiesības un intereses, jo tā var noteikt vai ietekmēt, piemēram, personas iespējas strādāt vēlamajā profesijā vai amatā. Konstatējumu, ka eksaminējamās personas sniegtās rakstiskās atbildes profesionālās kvalifikācijas eksāmenā ir informācija, kas attiecas uz šo personu tās satura, mērķa un ietekmes dēļ, var attiecināt arī uz pārbaudījumu, kurā ir iespēja izmantot konkrētus materiālus.

Treškārt, runājot par eksaminētāja piezīmēm par eksaminējamās personas sniegtajām atbildēm, Tiesa uzskatīja, ka tās tāpat kā personas pārbaudījuma darbā sniegtās atbildes ir informācija par šo eksaminējamo personu, jo tās atspoguļo eksaminētāja viedokli vai vērtējumu par šīs personas individuālu sniegumu pārbaudījuma laikā un it īpaši par tās zināšanām un kompetenci attiecīgajā jomā. Turklāt šo piezīmju konkrētais mērķis ir dokumentēt eksaminētāja vērtējumu par eksaminējamās personas sniegumu, un tās, iespējams, varētu šai personai radīt sekas.

Ceturtkārt, Tiesa nosprieda, ka rakstiskās atbildes, ko eksaminējamā persona sniegusi profesionālās kvalifikācijas eksāmenā, un jebkādas eksaminētāja piezīmes par tām var tikt novērtētas precizitātes un vajadzības tās saglabāt ziņā Direktīvas 95/46 6. panta 1. punkta d) un e) apakšpunkta izpratnē un tās var tikt labotas vai dzēstas šīs direktīvas 12. panta b) punkta izpratnē. Tas, ka eksaminējamai personai tiek dotas tiesības piekļūt šīm atbildēm un piezīmēm saskaņā ar šīs direktīvas 12. panta a) punktu, atbilst minētās direktīvas mērķim garantēt, ka ar šo eksaminējamo personu saistīto datu apstrādes ziņā šīs personas tiesības uz privātās dzīves neaizskaramību tiek aizsargātas neatkarīgi no tā, vai šai eksaminējamai personai šādas piekļuves tiesības ir vai nav arīdzan saskaņā ar eksāmena procedūrai piemērojamo valsts tiesisko regulējumu. Tomēr Tiesa uzsvēra, ka tiesības uz piekļuvi datiem un to labošanu saskaņā ar Direktīvas 95/46 12. panta a) un b) punktu neattiecas uz eksāmena jautājumiem, kuri paši par sevi nav uzskatāmi par eksaminējamās personas datiem.

Ņemot vērā šos elementus, Tiesa secināja, ka tādos apstākļos kā pamatlietā eksaminējamās personas profesionālās kvalifikācijas eksāmenā sniegtās rakstiskās atbildes un iespējamas eksaminētāja piezīmes par šīm atbildēm ir personas dati Direktīvas 95/46 2. panta a) punkta izpratnē.

3. Jēdziens "personas datu apstrāde"

2003. gada 6. novembra spriedums (virspalāta) Lindqvist (C-101/01, EU:C:2003:596)

B. Lindqvist, brīvprātīgā darbiniece protestantu baznīcas draudzē Zviedrijā, no sava personīgā datora izveidoja tīmekļvietnes, kurās publicēja personas datus par vairākiem cilvēkiem, kas tāpat kā viņa brīvprātīgi strādāja minētajā draudzē. *B. Lindqvist* tika piespriests samaksāt naudas sodu, jo viņa bija veikusi automātisku personas datu apstrādi, pirms tam neiesniedzot rakstveida paziņojumu Zviedrijas *Datainspektion* (valsts iestāde elektroniski pārraidītu datu aizsardzībai), bez atļaujas šos personas datus pārsūtījusi uz trešām valstīm un veikusi sensitīvu personas datu apstrādi.

Tā kā *B. Lindqvist* par šo lēmumu iesniedza apelācijas sūdzību *Göta hovrätt* (Jetas apelācijas tiesa, Zviedrija), šī tiesa uzdeva Tiesai prejudiciālus jautājumus, lai noskaidrotu, vai *B. Lindqvist* ir veikusi "personas datu apstrādi pilnībā vai daļēji ar automatizētiem līdzekļiem" Direktīvas 95/46 izpratnē.

Tiesa konstatēja, ka darbība, kuras ietvaros interneta mājaslapā tiek norādītas vairākas personas un tās identificētas, vai nu norādot viņu uzvārdu, vai citā veidā, piemēram, norādot viņu tālruņa numuru vai informāciju par viņu darba apstākļiem un vaļaspriekiem, ir uzskatāma par "personas datu apstrādi pilnībā vai daļēji ar automatizētiem līdzekļiem" šīs direktīvas izpratnē. Uz šādu personas datu apstrādi, kas veikta brīvprātīgu vai reliģiska rakstura darbību īstenošanas nolūkā, neattiecas neviens no izņēmumiem no direktīvas piemērošanas jomas, jo tā neietilpst ne tādu darbību kategorijā, kuras attiecas uz sabiedrisko drošību, ne arī tādu darbību kategorijā, kas veiktas tikai un vienīgi personiskām vai sadzīviskām vajadzībām un līdz ar to neietilpst direktīvas piemērošanas jomā.

2014. gada 13. maija spriedums (virspalāta) Google Spain un Google (C-131/12, EU:C:2014:317)

Šajā spriedumā (skat. arī II.1. sadaļu "Vispārējā tiesiskā regulējuma piemērošanas joma") Tiesai bija iespēja precizēt jēdzienu "personas datu apstrāde" internetā, ņemot vērā Direktīvu 95/46.

Tiesa nosprieda, ka meklētājprogrammas darbība, kura izpaužas kā publicētās vai trešo personu internetā ievietotās informācijas atrašana, to automātiski indeksējot, to īslaicīgi uzglabājot un visbeidzot to nododot interneta lietotāju rīcībā noteiktā svarīguma secībā, ir jākvalificē kā personas datu apstrāde, ja šī informācija ietver personas datus. Turklāt Tiesa atgādināja, ka direktīvā norādītās darbības ir jākvalificē kā šāda apstrāde arī gadījumā, ja tās attiecas vienīgi uz tādu informāciju kā medijos jau publicētā. Vispārēja atkāpe no direktīvas piemērošanas šajā gadījumā lielā mērā padarītu šo direktīvu bezjēdzīgu.

2018. gada 10. jūlija spriedums (virspalāta) Jehovan todistajat (C-25/17, EU:C:2018:551)

Somijas datu aizsardzības iestāde pieņēma lēmumu, ar kuru Jehovas liecinieku kopienai aizliedz vākt vai apstrādāt personas datus saistībā ar sludināšanu, ko veic tās locekļi, apstaigājot mājas, ja nav izpildīti Somijas tiesību aktos par šādu datu apstrādi paredzētie nosacījumi. Proti, šīs kopienas locekļi, sludinādami apstaigājot mājas, veic piezīmes par tikšanos ar personām, ar kurām ne viņi paši, ne minētā kopiena nav pazīstami. Šie dati tiek vākti kā atgādinošas piezīmes, lai tās varētu atrast iespējamiem vēlākiem apmeklējumiem, un datu subjekti tam nav nedz piekrituši, nedz arī ir par to tikuši informēti. Šajā ziņā Jehovas liecinieku kopiena saviem locekļiem ir sniegusi pamatnostādnes par šādu piezīmju veikšanu, un šīs pamatnostādnes ir ietvertas vismaz vienā no tās publikācijām, kas veltītas sludināšanas darbībai.

Tiesa nosprieda, ka personas datu vākšanu, ko veic reliģiskas kopienas locekļi, sludinādami apstaigājot mājas, un šo datu vēlāku apstrādi neaptver izņēmumi no Direktīvas 95/46 piemērošanas jomas, ņemot vērā, ka minētās darbības nav uzskatāmas nedz par personas datu apstrādi, kas veikta, īstenojot šīs direktīvas 3. panta 2. punkta pirmajā ievilkumā paredzētās darbības, nedz par personas datu apstrādi, ko veic fiziskas personas tikai un vienīgi personiskām vai sadzīviskām vajadzībām minētās direktīvas 3. panta 2. punkta otrā ievilkuma izpratnē.

2021. gada 22. jūnija spriedums (virspalāta) Latvijas Republikas Saeima (Pārkāpumu uzskaites punkti) (C-439/19, EU:C:2021:504)

Fiziskai personai B par vienu vai vairākiem ceļu satiksmes noteikumu pārkāpumiem tika reģistrēti pārkāpumu uzskaites punkti. Šos pārkāpumu uzskaites punktus Ceļu satiksmes drošības direkcija (Latvija) (turpmāk tekstā – "CSDD") reģistrēja transportlīdzekļu un to vadītāju valsts reģistrā.

Saskaņā ar Latvijas tiesisko regulējumu ceļu satiksmes jomā [34] informācija par pārkāpumu uzskaites punktiem, kuri transportlīdzekļu vadītājiem reģistrēti šajā reģistrā, ir vispārpieejama un CSDD to izpauž ikvienai personai, kura to pieprasa – un tai nav jāpierāda konkrēta interese iegūt šādu informāciju –, tostarp nodod komersantiem atkalizmantošanas nolūkā. Tā kā B bija šaubas par šā regulējuma tiesiskumu, viņš iesniedza konstitucionālu sūdzību Latvijas Republikas Satversmes tiesā, lūdzot izvērtēt šā regulējuma atbilstību tiesībām uz privātās dzīves neaizskaramību.

Satversmes tiesa uzskatīja, ka tai, izvērtējot šīs konstitucionālās tiesības, ir jāņem vērā VDAR. Tādējādi tā lūdza Tiesu skaidrot vairāku VDAR normu tvērumu, lai noteiktu Latvijas tiesiskā regulējuma par ceļu satiksmi saderīgumu ar šo regulu.

[34] 1997. gada 1. oktobra Ceļu satiksmes likuma 14[1]. panta otrā daļa (Latvijas Vēstnesis, 1997, Nr. 274/276).

Šajā virspalātas sastāvā pasludinātajā spriedumā Tiesa uzskata, ka personas datu par pārkāpumu uzskaites punktiem apstrāde ir "personas datu par sodāmību un pārkāpumiem apstrāde" [35], attiecībā uz kuru VDAR ir paredzēta pastiprināta aizsardzība attiecīgo datu īpaši sensitīvā rakstura dēļ.

Šajā ziņā tā vispirms norāda, ka informācija par pārkāpumu uzskaites punktiem ir personas dati un ka to izpaušana, ko CSDD veic trešām personām, ir apstrāde, kas ietilpst VDAR materiālās piemērošanas jomā. Proti, šī piemērošanas joma ir ļoti plaša, un uz šo apstrādi neattiecas izņēmumi no šīs regulas piemērojamības.

Tādējādi, pirmkārt, uz šo apstrādi neattiecas izņēmums par VDAR nepiemērojamību apstrādei, ko veic tādas darbības ietvaros, kura neietilpst Savienības tiesību aktu darbības jomā [36]. Šis izņēmums ir uzskatāms par tādu, kas ir domāts vienīgi tam, lai no šīs regulas piemērošanas jomas izslēgtu personas datu apstrādi, ko valsts iestādes veic tādas darbības ietvaros, kura vērsta uz valsts drošības aizsardzību, vai tādas darbības ietvaros, kura var tikt iekļauta tajā pašā kategorijā. Šīs darbības it īpaši aptver darbības, kuras vērstas uz valsts pamatfunkciju un sabiedrības pamatinterešu aizsardzību. Taču ar ceļu satiksmes drošību saistītajām darbībām nav šāda mērķa un līdz ar to tās nevar tikt iekļautas to darbību kategorijā, kuras vērstas uz valsts drošības aizsardzību.

Otrkārt, personas datu par pārkāpumu uzskaites punktiem izpaušana arī nav apstrāde, ko aptver izņēmums, kurš paredz VDAR nepiemērojamību personas datu apstrādei, ko kompetentās iestādes veic krimināltiesību jomā [37]. Proti, Tiesa konstatē, ka CSDD, veicot minēto izpaušanu, nevar tikt uzskatīta par šādu "kompetento iestādi" [38].

Lai noskaidrotu, vai piekļuve tādiem personas datiem par ceļu satiksmes noteikumu pārkāpumiem kā, piemēram, pārkāpumu uzskaites punkti, ir personas datu apstrāde par "pārkāpumiem" [39], uz kuru attiecas pastiprināta aizsardzība, Tiesa, balstoties tostarp uz VDAR rašanās vēsturi, konstatē, ka šis jēdziens attiecas tikai uz noziedzīgiem nodarījumiem. Tomēr tas, ka Latvijas tiesību sistēmā ceļu satiksmes noteikumu pārkāpumi tiek kvalificēti kā administratīvi pārkāpumi, nav noteicošais, izvērtējot, vai šie pārkāpumi ietilpst jēdzienā "noziedzīgs nodarījums", jo runa ir par autonomu Savienības tiesību jēdzienu, kura interpretācijai visā Savienībā jābūt autonomai un vienveidīgai. Tādējādi, atgādinājusi trīs atbilstošos kritērijus, lai vērtētu pārkāpuma noziedzīgo raksturu, proti, pārkāpuma juridisko kvalifikāciju valsts tiesībās, pārkāpuma raksturu un piemērotā soda smaguma pakāpi, Tiesa nospriež, ka attiecīgie ceļu satiksmes noteikumu pārkāpumi ietilpst jēdzienā "pārkāpums" VDAR izpratnē. Attiecībā uz pirmajiem diviem

[35] VDAR 10. pants.
[36] VDAR 2. panta 2. punkta a) apakšpunkts.
[37] VDAR 2. panta 2. punkta d) apakšpunkts.
[38] Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV 2016, L 119, 89. lpp.), 3. panta 7. punkts.
[39] VDAR 10. pants.

kritērijiem Tiesa konstatē, ka, pat ja pārkāpumi valsts tiesībās netiek kvalificēti kā "noziedzīgi", šāds raksturs var izrietēt no pārkāpuma iedabas un it īpaši no soda, ko var izraisīt šāds pārkāpums, represīvā mērķa. Tā, šajā lietā pārkāpumu uzskaites punktu reģistrēšanai par ceļu satiksmes noteikumu pārkāpumiem, tāpat kā citiem sodiem, kas var būt piemērojami šo pārkāpumu izdarīšanas rezultātā, tostarp ir šāds represīvs mērķis. Attiecībā uz trešo kritēriju Tiesa norāda, ka pārkāpumu uzskaites punkti tiek reģistrēti tikai noteikta smaguma ceļu satiksmes noteikumu pārkāpumu gadījumā un ka līdz ar to šādi pārkāpumi var izraisīt noteikta smaguma sodus. Turklāt pārkāpumu uzskaites punktu reģistrēšana parasti tiek veikta papildus piemērotajam sodam un šo punktu uzkrāšanās rada juridiskas sekas, kas var izpausties pat kā aizliegums vadīt transportlīdzekli.

2023. gada 5. decembra spriedums (virspalāta) Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Lai labāk pārvaldītu Covid-19 pandēmiju, Lietuvas iestādes 2020. gadā nolēma organizēt mobilās lietotnes iegādi. Šī lietotne bija paredzēta, lai atbalstītu epidemioloģisko uzraudzību, ļaujot reģistrēt un uzraudzīt datus par personām, kas saskārušās ar Covid-19 vīrusu.

Šajā nolūkā *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos* (Veselības ministrijas pakļautībā esošais Nacionālais sabiedrības veselības centrs, Lietuva; turpmāk tekstā – "NSVC"), kas bija atbildīgs par šo iegādi, sazinājās ar sabiedrību *UAB "IT sprendimai sėkmei"* (turpmāk tekstā – "sabiedrība *ITSS*"), lūdzot tai izstrādāt šādu mobilo lietotni. Pēc tam NSVC darbinieki šai sabiedrībai nosūtīja e-pasta vēstules par jautājumiem, kuriem bija jābūt ietvertiem šajā lietotnē.

Laikposmā no 2020. gada aprīļa līdz maijam sabiedrības *ITSS* izveidotā mobilā lietotne bija publiski pieejama. Līdz ar to šo lietotni izmantoja 3802 personas un sniedza par sevi dažādus šajā lietotnē prasītos datus. Tomēr finansējuma trūkuma dēļ NSVC nepiešķīra sabiedrībai *ITSS* publiskā iepirkuma līgumu par tās izstrādātās mobilās lietotnes oficiālu iegādi un izbeidza ar to saistīto iepirkuma procedūru.

Tikmēr valsts uzraudzības iestāde sāka izmeklēšanu par personas datu apstrādi, kas izriet no šīs lietotnes izmantošanas. Ar šīs iestādes lēmumu, kas pieņemts izmeklēšanas noslēgumā, administratīvie naudas sodi tika piemēroti gan NSVC, gan sabiedrībai *ITSS*, kura tika uzskatīta par kopīgu pārzini.

Šo lēmumu NSVC apstrīdēja *Vilniaus apygardos administracinis teismas* (Viļņas Administratīvā apgabaltiesa, Lietuva). Šaubīdamās par vairāku VDAR normu interpretāciju, šī tiesa vērsās Tiesā ar lūgumu sniegt prejudiciālu nolēmumu.

Šajā spriedumā Tiesa virspalātas sastāvā sniedz precizējumus tostarp par jēdzienu "apstrāde". Šajā ziņā tā norāda, ka personas datu izmantošana mobilās lietotnes testēšanas vajadzībām ir "apstrāde" VDAR izpratnē. Taču savādāk ir, ja šādi dati ir

anonimizēti tiktāl, ka šo datu subjekts vai vairs nav identificējams, vai ja runa ir par fiktīviem datiem, kas neattiecas uz reālu fizisku personu.

Proti, pirmkārt, jautājums, vai personas dati tiek izmantoti lietotnes testēšanas vajadzībām vai citam nolūkam, neietekmē attiecīgās darbības kvalificēšanu par "apstrādi". Otrkārt, tikai apstrāde, kas attiecas uz personas datiem, var tikt kvalificēta par "apstrādi" VDAR izpratnē. Taču fiktīvi vai anonīmi dati nav personas dati.

4. Jēdziens "personas datu kartotēka"

2018. gada 10. jūlija spriedums (virspalāta) Jehovan todistajat (C-25/17, EU:C:2018:551)

Šajā spriedumā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"") Tiesa ir precizējusi Direktīvas 95/46 2. panta c) punktā paredzēto jēdzienu "kartotēka".

Tādējādi, atgādinājusi, ka šī direktīva attiecas uz personas datu manuālu apstrādi tikai tad, ja apstrādātie dati veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, Tiesa nosprieda, ka minētais jēdziens aptver personas datu kopumu, kas ievākti saistībā ar sludināšanu, apstaigājot mājas, un kas ietver kontaktēto personu vārdus un adreses, kā arī citu informāciju par tām, ja šie dati ir sakārtoti saskaņā ar noteiktiem kritērijiem, kas praksē ļauj tos viegli atrast to vēlākas izmantošanas nolūkā. Lai uz šādu datu kopumu attiektos šis jēdziens, nav nepieciešams, lai tas ietvertu reģistrus, īpašus sarakstus vai citas meklēšanas metodes.

5. Jēdziens "personas datu pārzinis"

2018. gada 10. jūlija spriedums (virspalāta) Jehovan todistajat (C-25/17, EU:C:2018:551)

Šajā lietā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"" un II.4. sadaļu "Jēdziens "personas datu kartotēka"") Tiesa lēma par kādas reliģiskas kopienas atbildību par personas datu apstrādi, kas veikta saistībā ar sludināšanas darbību, apstaigājot mājas, ko organizē, koordinē un veicina šī kopiena.

Tiesa uzskatīja, ka ikvienas personas pienākums ievērot Savienības tiesību normas par personas datu aizsardzību nevar tikt uzskatīts par iejaukšanos reliģisko kopienu organizatoriskajā autonomijā. Šajā ziņā tā secināja, ka Direktīvas 95/46 2. panta d) punkts, to aplūkojot Hartas 10. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tas ļauj reliģisko kopienu – kopā ar tās locekļiem, kuri veic sludināšanu, – uzskatīt par pārzini attiecībā uz personas datu apstrādi, ko šie locekļi veic tādas sludināšanas gaitā, apstaigājot mājas, kuru organizē, koordinē un veicina šī kopiena, un nav nepieciešams

ne tas, lai minētajai kopienai būtu piekļuve šiem datiem, ne arī – lai tiktu konstatēts, ka tā saviem locekļiem ir sniegusi rakstveida pamatnostādnes vai ieteikumus par šo apstrādi.

2018. gada 5. jūnija spriedums (virspalāta) Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)

Vācijas datu aizsardzības iestāde kā uzraudzības iestāde Direktīvas 95/46 28. panta izpratnē lika kādai Vācijas komercsabiedrībai, kas ir specializējusies izglītības jomā, piedāvājot apmācības pakalpojumus, izmantojot "fanu lapu", kas tiek mitināta sociālā tīkla *Facebook* vietnē, deaktivizēt šo lapu. Minētā iestāde uzskata, ka nedz šī sabiedrība, nedz *Facebook* nebija informējuši "fanu lapas" apmeklētājus par to, ka pēdējā minētā, izmantojot sīkdatnes, apkopoja ar viņiem saistīto personiska rakstura informāciju un ka minētā sabiedrība un *Facebook* pēc tam šo informāciju apstrādāja.

Šādā kontekstā Tiesa precizēja personas datu "pārziņa" jēdzienu. Šajā ziņā tā uzskatīja, ka *Facebook* mitinātas "fanu lapas" uzturētājs, kāda ir pamatlietā aplūkotā sabiedrība, iestatot parametrus (atbilstoši tostarp savai mērķauditorijai, kā arī savas darbības vadības vai reklāmas mērķiem), piedalās šīs lapas apmeklētāju personas datu apstrādes nolūku un līdzekļu noteikšanā. Tiesa uzskata, ka šis uzturētājs ir jākvalificē kā Savienībā kopīgi ar *Facebook Ireland* (Amerikas Savienoto Valstu sabiedrības *Facebook* meitasuzņēmums Savienībā) par šādu apstrādi atbildīgais pārzinis Direktīvas 95/46 2. panta d) punkta izpratnē.

2019. gada 29. jūlija spriedums Fashion ID (C-40/17, EU:C:2019:629)

Šajā lietā Tiesai bija iespēja sīkāk definēt jēdzienu "pārzinis" saistībā ar "spraudņa" iestrādāšanu tīmekļvietnē.

Šajā gadījumā *Fashion ID*, kas ir Vācijas uzņēmums, kurš nodarbojas ar modes apģērbu tirdzniecību tiešsaistē, savā tīmekļvietnē bija iestrādājis sociālā tīkla *Facebook* piedāvāto sociālo spraudni "Patīk". Šīs iestrādāšanas rezultāts ir tāds, ka, līdzko kāds apmeklētājs aplūko *Fashion ID* tīmekļvietni, šā apmeklētāja personas dati tiek pārsūtīti *Facebook Ireland*. Izrādās, ka šī pārsūtīšana notiek, minētajam apmeklētājam par to nezinot un neatkarīgi no tā, vai viņš ir sociālā tīkla *Facebook* lietotājs un vai viņš ir nospiedis *Facebook* pogu "Patīk".

Verbraucherzentrale NRW, kas ir Vācijas sabiedriskā labuma organizācija, kas nodarbojas ar patērētāju interešu aizsardzību, pārmet *Fashion ID*, ka tā esot pārsūtījusi *Facebook Ireland* savas tīmekļvietnes apmeklētāju personas datus, pirmkārt, bez šo personu piekrišanas un, otrkārt, neizpildot informēšanas pienākumus, kas paredzēti tiesību normās par personas datu aizsardzību. Saņēmusi izskatīšanai lietu, *Oberlandesgericht Düsseldorf* (Federālās zemes Augstākā tiesa Diseldorfā, Vācija) lūdza Tiesu interpretēt vairākas Direktīvas 95/46 normas.

Vispirms Tiesa konstatēja, ka tāds tīmekļvietnes pārvaldītājs kā *Fashion ID* var tikt uzskatīts par personas datu [pārzini] Direktīvas 95/46 2. panta d) punkta izpratnē. Tomēr šī atbildība attiecas tikai uz to personas datu apstrādes darbību vai šādu darbību kopumu, kuru nolūkus un līdzekļus tā faktiski nosaka, proti, attiecīgo datu vākšanu un atklāšanu, tos pārsūtot. Turpretim Tiesa uzskata, ka pirmšķietami ir izslēgts, ka *Fashion ID* noteiktu nolūkus, kādiem, un līdzekļus, ar kādiem personas datu turpmākās apstrādes darbības veic *Facebook Ireland* pēc tam, kad tai šie dati tiek pārsūtīti, un tāpēc *Fashion ID* nav uzskatāma par personas datu [pārzini] attiecībā uz šīm darbībām šā 2. panta d) punkta izpratnē.

Tiesa turklāt uzsvēra, ka tīmekļvietnes pārvaldītājam un sociālā spraudņa piedāvātājam, piemēram, *Facebook Ireland*, šīs apstrādes darbības, lai tās viņu gadījumā būtu attaisnotas, ir jāveic [leģitīmās] interesēs Direktīvas 95/46 7. panta f) punkta izpratnē.

Visbeidzot Tiesa precizēja, ka datu subjekta piekrišana, kas ir paredzēta Direktīvas 95/46 2. panta h) punktā un 7. panta a) punktā, tīmekļvietnes pārvaldītājam ir jāiegūst tikai saistībā ar personas datu apstrādi, kuras nolūkus un līdzekļus nosaka šis pārvaldītājs. Šādā situācijā šīs direktīvas 10. pantā paredzētais informēšanas pienākums ir arī minētajam pārvaldītājam, taču informācijai, kas tam ir jāsniedz datu subjektam, ir jāattiecas tikai uz to personas datu apstrādes darbību vai šādu darbību kopumu, kuru nolūkus un līdzekļus tas nosaka.

2023. gada 5. decembra spriedums (virspalāta) Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Šajā lietā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"") Tiesa nosprie ž, ka struktūru, kas uzdevusi uzņēmumam izstrādāt mobilo lietotni un šajā kontekstā piedalījusies ar šo lietotni veicamās datu apstrādes nolūku un līdzekļu noteikšanā, var uzskatīt par pārzini [40]. Šo apsvērumu neatspēko fakts, ka šī struktūra apstrādes darbības nav veikusi pati, nav skaidri devusi savu piekrišanu konkrētu šādas apstrādes darbību veikšanai vai minētās mobilās lietotnes publiskošanai un nav iegādājusies šo mobilo lietotni, ja vien pirms šīs publiskošanas minētā struktūra nav skaidri iebildusi pret to un no tās izrietošo personas datu apstrādi.

[40] VDAR 4. panta 7. punkta izpratnē.

6. Jēdziens "kopīgs pārzinis"

2023. gada 5. decembra spriedums (virspalāta) Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Šajā lietā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"" un II.5. sadaļu "Jēdziens "personas datu pārzinis"") Tiesa norāda, ka, lai divas struktūras kvalificētu par kopīgiem pārziņiem, nav nepieciešams, lai šīs struktūras būtu noslēgušas vienošanos par personas datu apstrādes nolūku un līdzekļu noteikšanu, ne arī, lai tās būtu noslēgušas vienošanos, kurā paredzēti nosacījumi attiecībā uz kopīgu atbildību par apstrādi. Protams, saskaņā ar VDAR [41] kopīgajiem pārziņiem, savstarpēji vienojoties, pārredzamā veidā ir jānosaka attiecīgie pienākumi, lai izpildītu šajā regulā noteiktās saistības. Tomēr šādas vienošanās esamība ir nevis priekšnosacījums, lai divas vai vairākas struktūras varētu kvalificēt kā "kopīgus pārziņus", bet gan pienākums, kas VDAR ir noteikts kopīgajiem pārziņiem, tiklīdz tie par tādiem ir kvalificēti, lai nodrošinātu, ka tie ievēro šīs regulas prasības. Tādējādi šī kvalifikācija izriet tikai no tā vien, ka apstrādes nolūku un līdzekļu noteikšanā ir piedalījušās vairākas struktūras.

Attiecībā uz to, ka attiecīgās struktūras kopīgi nosaka apstrādes nolūkus un līdzekļus, Tiesa precizē, ka to dalība šajā noteikšanā var izpausties dažādās formās un izrietēt gan no to kopīgā lēmuma, gan no to saskaņotiem lēmumiem. Pēdējā minētajā gadījumā šiem lēmumiem ir jābūt savstarpēji papildinošiem tādējādi, ka katram no tiem ir konkrēta ietekme uz apstrādes nolūku un līdzekļu noteikšanu.

7. Personas datu apstrādes likumīguma nosacījumi

2008. gada 16. decembra spriedums (virspalāta) Huber (C-524/06, EU:C:2008:724)

Federālā migrācijas un bēgļu pārvalde (*Bundesamt für Migration und Flüchtlinge*, Vācija) nodrošina ārvalstnieku centrālā reģistra pārvaldību, kurā ir apkopoti noteikti personas dati par ārvalstniekiem, kas uzturas Vācijas teritorijā ilgāk nekā trīs mēnešus. Reģistrs tiek izmantots statistikas mērķiem un gadījumos, kad drošības dienesti, policija un tiesu iestādes īsteno savu kompetenci ar kriminālām vai valsts drošību apdraudošām darbībām saistītas vajāšanas vai izmeklēšanas jomā.

H. Huber, Austrijas valstspiederīgais, Vācijā ieradās 1996. gadā, lai tur strādātu par pašnodarbinātu apdrošināšanas aģentu. *H. Huber*, uzskatīdams, ka tiek diskriminēts

[41] VDAR 26. panta 1.punkts, lasot to šīs regulas 79. apsvēruma gaismā.

saistībā ar minētajā reģistrā ietverto datu apstrādi, it īpaši tāpēc, ka šādas datubāzes par Vācijas pilsoņiem nav, lūdza šos datus dzēst.

Šajā situācijā *Oberverwaltungsgericht für das Land Nordrhein-Westfalen* (Ziemeļreinas-Vestfālenes Augstākā administratīvā tiesa, Vācija), kurā tika iesniegta sūdzība, uzdeva Tiesai jautājumu par minētajā reģistrā veiktās personas datu apstrādes saderību ar Savienības tiesībām.

Tiesa vispirms atgādināja, ka Savienības pilsoņa uzturēšanās tiesības tādas dalībvalsts teritorijā, kuras valstspiederīgais viņš nav, nav beznosacījuma un šīm tiesībām var tikt noteikti ierobežojumi. Līdz ar to šāda reģistra izmantošana, lai palīdzētu iestādēm, kurām ir uzticēts piemērot uzturēšanās tiesības nosakošu tiesisko regulējumu, principā ir leģitīma un, ņemot vērā tās raksturu, saderīga ar EKL 12. panta 1. punktā (tagad LESD 18. panta pirmā daļa) ietverto aizliegumu diskriminēt valstspiederības dēļ. Tomēr šādā reģistrā var iekļaut tikai tādu informāciju, kas ir vajadzīga šim mērķim direktīvas par personas datu aizsardzību izpratnē.

Runājot par apstrādes "vajadzības" jēdzienu Direktīvas 95/46 7. panta e) punkta izpratnē, Tiesa vispirms atgādināja, ka tas ir autonoms Savienības tiesību jēdziens, kas ir jāinterpretē tā, lai tas pilnībā atbilstu Direktīvas 95/46 mērķim, kas ir noteikts tās 1. panta 1. punktā. Turpinājumā tā konstatēja, ka personas datu apstrādes sistēma atbilst Savienības tiesībām, ja tajā iekļauti tikai tādi dati, kas ir vajadzīgi, lai minētās iestādes varētu piemērot šo regulējumu, un ja tās centralizētais raksturs veicina šā regulējuma efektīvāku piemērošanu attiecībā uz tādu Savienības pilsoņu, kas nav šīs dalībvalsts valstspiederīgie, uzturēšanās tiesībām.

Katrā ziņā nevar uzskatīt par vajadzīgu Direktīvas 95/46 7. panta e) punkta izpratnē identificētu personas datu saglabāšanu un apstrādi šādā reģistrā statistikas mērķiem.

Turklāt attiecībā uz jautājumu par reģistrā iekļauto datu izmantošanu cīņā pret noziedzību Tiesa īpaši uzsvēra, ka šis mērķis ir vērsts uz izdarīto noziegumu un kriminālpārkāpumu izmeklēšanu neatkarīgi no to izdarītāju valstspiederības. Tāpēc cīņas pret noziedzību aspektā dalībvalstī tās valstspiederīgo situācijai nevajadzētu atšķirties no to Savienības pilsoņu situācijas, kas nav šīs dalībvalsts valstspiederīgie un dzīvo tās teritorijā. Tāpēc atšķirīga attieksme pret šiem valstspiederīgajiem un šiem Savienības pilsoņiem, ko rada sistemātiska tikai to Savienības pilsoņu, kas nav attiecīgās dalībvalsts valstspiederīgie, personas datu apstrāde, lai cīnītos pret noziedzību, ir EKL 12. panta 1. punktā aizliegta diskriminācija.

2016. gada 19. oktobra spriedums Breyer (C-582/14, EU:C:2016:779)

Šajā spriedumā (skat. arī II.2. sadaļu "Jēdziens "personas dati"") Tiesa arī lēma par jautājumu, vai ar Direktīvas 95/46 7. panta f) punktu netiek pieļauta valsts tiesību norma, atbilstoši kurai tiešsaistes plašsaziņas līdzekļu pakalpojumu sniedzējs lietotāja personas datus bez viņa piekrišanas var iegūt un izmantot tikai tad, kad tas ir nepieciešams, lai

nodrošinātu tiešsaistes plašsaziņas līdzekļa konkrētu lietošanu attiecīgajam lietotājam un veiktu ar to saistītos norēķinus, un atbilstoši kurai mērķis nodrošināt vispārēju tiešsaistes plašsaziņas līdzekļa funkcionēšanas spēju nevar attaisnot datu izmantošanu pēc attiecīgā lietošanas procesa beigām.

Tiesa nosprieda, ka ar Direktīvas 95/46 7. panta f) punktu netiek pieļauts aplūkojamais regulējums. Saskaņā ar šo noteikumu personas datu apstrāde šā noteikuma izpratnē ir likumīga, ja tā ir vajadzīga pārziņa vai trešo personu, kurām dati tiek atklāti, likumīgo interešu īstenošanai, ja vien pār tām neprevalē datu subjekta pamattiesību un pamatbrīvību intereses. Taču šajā lietā Vācijas regulējumā kategoriski un vispārīgi ir tikusi izslēgta iespēja apstrādāt atsevišķas personas datu kategorijas, neļaujot konkrētajā gadījumā izsvērt attiecīgās pretstatītās tiesības un intereses. Tādējādi ar to nelikumīgi tika sašaurināta Direktīvas 95/46 7. panta f) punktā paredzētā principa piemērošanas joma, izslēdzot to, ka tiešsaistes plašsaziņas līdzekļa vispārējas funkcionēšanas spējas nodrošināšanas mērķi var samērot ar lietotāju interesēm vai pamattiesībām un pamatbrīvībām.

2017. gada 27. septembra spriedums Puškár (C-73/16, EU:C:2017:725)

Pamatlietā *P. Puškár* iesniedza prasību *Najvyšší súd Slovenskej republiky* (Slovākijas Republikas Augstākā tiesa) uzdot *Finančné riaditel'stvo* (Finanšu pārvalde), visiem tai pakļautajiem nodokļu birojiem un *Kriminálny úrad finančnej správy* (Noziedzīgu nodarījumu finanšu jomā apkarošanas birojs) neiekļaut viņa vārdu personu, ko Finanšu pārvalde uzskata par fiktīvām amatpersonām, sarakstā, kuru tā ir sagatavojusi saistībā ar nodokļu iekasēšanu un kura aktualizāciju nodrošina Finanšu pārvalde, kā arī Noziedzīgu nodarījumu finanšu jomā apkarošanas birojs (turpmāk tekstā – "strīdīgais saraksts"). Turklāt viņš lūdza svītrot jebkādas norādes uz viņu no šiem sarakstiem un no finanšu administrācijas informātikas sistēmas.

Šajos apstākļos *Najvyšší súd Slovenskej republiky* (Slovākijas Republikas Augstākā tiesa) uzdeva Tiesai jautājumu, vai tiesības uz privātās un ģimenes dzīves, dzīvokļa un saziņas neaizskaramību, kas ir noteiktas Hartas 7. pantā, un tiesības uz personas datu aizsardzību, kas noteiktas tās 8. pantā, var tikt interpretētas tādējādi, ka dalībvalsts bez datu subjekta atļaujas nevar sagatavot personas datu sarakstus nodokļu iekasēšanas nolūkos, proti, ka personas datu ieguve valsts iestāžu rīcībā, lai cīnītos pret krāpšanu nodokļu jomā, pati par sevi ir riskanta.

Tiesa secināja, ka Direktīvas 95/46 7. panta e) punkts neaizliedz personas datu apstrādi, ko dalībvalsts iestādes veic nodokļu iekasēšanas nolūkos un lai cīnītos pret krāpšanu nodokļu jomā un kas tiek veikta, izveidojot tādu personu sarakstu kā pamatlietā aplūkotais, bez datu subjektu piekrišanas, ar nosacījumu, pirmkārt, ka šīm iestādēm ar valsts tiesību aktiem ir uzticēti sabiedrības interesēs realizējami uzdevumi šīs tiesību normas izpratnē, ka šī saraksta izveidošana un datu subjektu vārdu iekļaušana tajā ir patiešām piemērota un nepieciešama izvirzīto mērķu sasniegšanai un ka pastāv

pietiekamas norādes, lai prezumētu, ka datu subjekti šajā sarakstā ir iekļauti pamatoti, un, otrkārt, ka ir izpildīti visi Direktīvā 95/46 paredzētie personas datu apstrādes likumīguma nosacījumi.

Šajā ziņā Tiesa norādīja, ka valsts tiesai arī jāpārbauda, vai strīdīgā saraksta izveidošana ir vajadzīga sabiedrības interesēs realizējama uzdevuma, par kuru ir runa pamatlietā, izpildei, ņemot vērā it īpaši strīdīgā saraksta izveides precīzu mērķi, juridiskās sekas, kādas rodas tajā ietvertajām personām, un šī saraksta publisko raksturu vai tāda neesamību. Turklāt, ņemot vērā samērīguma principu, valsts tiesai ir jāpārbauda, vai strīdīgā saraksta izveidošana un datu subjektu vārdu iekļaušana tajā ir piemērota, lai sasniegtu izvirzītos mērķus, un vai nepastāv citi mazāk ierobežojoši līdzekļi šo mērķu sasniegšanai.

Turklāt Tiesa konstatēja, ka tas, ka persona tiek iekļauta strīdīgajā sarakstā, var aizskart dažas no tās tiesībām. Iekļaušana šajā sarakstā var kaitēt tās reputācijai un ietekmēt tās attiecības ar nodokļu iestādēm. Tāpat šī iekļaušana var ietekmēt šīs personas nevainīguma prezumpciju, kas ir noteikta Hartas 48. panta 1. punktā, kā arī ar strīdīgajā sarakstā iekļautajām fiziskajām personām saistīto juridisko personu darījumdarbības brīvību, kas ir ietverta Hartas 16. pantā. Tādēļ šāda iejaukšanās var būt atbilstīga tikai tad, ja ir pietiekams iemesls aizdomām, ka attiecīgā persona fiktīvi ieņem vadošus amatus ar viņu saistītu juridisku personu uzņēmumos un tādējādi apdraud nodokļu iekasēšanu un cīņu pret krāpšanu nodokļu jomā.

Turklāt Tiesa atzina, ka, ja pastāvētu iemesli saskaņā ar Direktīvas 95/46 13. pantu ierobežot dažas no šīs direktīvas 6. un 10.–12. pantā paredzētajām tiesībām, piemēram, datu subjekta tiesības uz informāciju, šādam ierobežojumam būtu jābūt vajadzīgam, lai aizsargātu kādas šā 13. panta 1. punktā minētās intereses, piemēram, svarīgas ekonomiskās un finansiālās intereses, un ir jābūt balstītam uz tiesību aktiem.

2020. gada 11. novembra spriedums Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA ir mobilo telekomunikāciju pakalpojumu sniedzējs Rumānijas tirgū. 2018. gada 28. martā *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (*ANSPDCP*) (Personas datu apstrādes uzraudzības valsts iestāde, Rumānija) uzlika tai naudas sodu par tās klientu personu apliecinošo dokumentu kopiju vākšanu un saglabāšanu bez skaidras viņu piekrišanas.

ANSPDCP norāda, ka laikposmā no 2018. gada 1. marta līdz 26. martam *Orange România* noslēdza līgumus par mobilo telekomunikāciju pakalpojumu sniegšanu, kurā ir ietverta klauzula, saskaņā ar kuru klienti ir tikuši informēti un ir piekrituši viņu personu apliecinošā dokumenta kopijas vākšanai un saglabāšanai identifikācijas mērķiem. Izvēles rūtiņu, kas attiecas uz šo klauzulu, datu pārzinis pirms līguma parakstīšanas ir atzīmējis ar ķeksīti.

Šādos apstākļos *Tribunalul București* (Bukarestes apgabaltiesa, Rumānija) lūdza Tiesu precizēt nosacījumus, saskaņā ar kuriem klientu piekrišana personas datu apstrādei var tikt uzskatīta par pienācīgi sniegtu.

Vispirms Tiesa atgādina, ka Savienības tiesībās [42] ir paredzēts to situāciju saraksts, kurās personas datu apstrādi var uzskatīt par likumīgu. Konkrēti – datu subjekta piekrišanai ir jābūt brīvi sniegtai, konkrētai, apzinātai un viennozīmīgai [43]. Šajā ziņā piekrišanu nevar uzskatīt par pienācīgi dotu klusēšanas, iepriekš atzīmētu rūtiņu vai atturēšanās no darbības gadījumos.

Turklāt, ja datu subjekta piekrišanu dod saistībā ar rakstisku deklarāciju, kas attiecas arī uz citiem jautājumiem, šai deklarācijai jābūt sniegtai saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Lai nodrošinātu datu subjektam patiesu izvēles brīvību, līguma noteikumi nedrīkst viņu maldināt par iespēju noslēgt līgumu pat tad, ja viņš atsakās dot piekrišanu savu datu apstrādei.

Tiesa precizē, ka, tā kā *Orange România* ir personas datu pārzinis, tai ir jāspēj pierādīt šo datu apstrādes likumību un līdz ar to, šajā gadījumā, to, ka tās klienti ir devuši pienācīgu piekrišanu. Šajā ziņā, ņemot vērā, ka attiecīgie klienti, šķiet, paši nav atzīmējuši rūtiņu par viņu personu apliecinošo dokumentu kopiju vākšanu un saglabāšanu, tas vien, ka šī rūtiņa ir atzīmēta ar ķeksīti, neļauj konstatēt pozitīvu piekrišanas izpausmi. Valsts tiesai šajā ziņā ir jāveic nepieciešamās pārbaudes.

Tāpat Tiesa uzskata, ka valsts tiesai ir jāizvērtē, vai aplūkotie līguma noteikumi varēja vai nevarēja maldināt konkrētos klientus attiecībā uz iespēju noslēgt līgumu, neraugoties uz atteikumu piekrist savu datu apstrādei, ja nav sniegti precizējumi par šo iespēju. Turklāt gadījumā, ja klients atsakās piekrist savu datu apstrādei, Tiesa norāda, ka *Orange România* pieprasīja, lai viņš rakstveidā paziņotu, ka viņš nepiekrīt ne viņa personu apliecinošā dokumenta kopijas vākšanai, ne saglabāšanai. Tiesa uzskata, ka šāda papildu prasība var nepamatoti ietekmēt brīvu izvēli iebilst pret šādu vākšanu un saglabāšanu. Katrā ziņā, tā kā minētajai sabiedrībai ir jāpierāda, ka tās klienti ar aktīvu rīcību ir norādījuši piekrišanu savu personas datu apstrādei, šī sabiedrība nevar pieprasīt, lai tie aktīvi paustu atteikumu.

Līdz ar to Tiesa secina, ka līgums par telekomunikāciju pakalpojumu sniegšanu, kurā ir ietverta klauzula, saskaņā ar kuru datu subjekts ir ticis informēts un piekritis sava personu apliecinošā dokumenta kopijas vākšanai un saglabāšanai identifikācijas mērķiem, nevar pierādīt, ka šī persona ir pienācīgi sniegusi piekrišanu šai vākšanai un saglabāšanai, ja datu pārzinis pirms līguma parakstīšanas ir atzīmējis ar ķeksīti izvēles rūtiņu, kas attiecas uz šo klauzulu, ja minētā līguma noteikumi var maldināt datu subjektu attiecībā uz iespēju noslēgt attiecīgo līgumu pat tad, ja tas atsakās piekrist savu

[42] Direktīvas 95/46 7. pants un VDAR 6. pants.
[43] Direktīvas 95/46 2. panta h) punkts un VDAR 4. panta 11. punkts.

datu apstrādei, vai ja šis pārzinis netaisnīgi ir ietekmējis brīvu izvēli iebilst pret šo vākšanu un saglabāšanu, ciktāl viņš pieprasa, lai datu subjekts, paužot savu atteikšanos dot piekrišanu šai apstrādei, aizpildītu papildu veidlapu, kurā norādīts šis atteikums.

2021. gada 22. jūnija spriedums (virspalāta) Latvijas Republikas Saeima (Pārkāpumu uzskaites punkti) (C-439/19, EU:C:2021:504)

Šajā spriedumā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"") Tiesa nospriež, ka VDAR nepieļauj tādu tiesisko regulējumu, ar kuru Ceļu satiksmes drošības direkcijai (Latvija) (turpmāk tekstā – "CSDD") ir noteikts pienākums padarīt publiski pieejamus datus par transportlīdzekļu vadītājiem par ceļu satiksmes noteikumu pārkāpumiem reģistrētajiem soda punktiem, neliekot personai, kura pieprasa šādu piekļuvi, pamatot konkrētu interesi šo datu iegūšanā. Tā konstatē, ka nepieciešamība, it īpaši, ņemot vērā Latvijas valdības norādīto ceļu satiksmes drošības uzlabošanas mērķi, izpaust personas datus par pārkāpumu uzskaites punktiem, kuri reģistrēti par ceļu satiksmes noteikumu pārkāpumiem, nav pierādīta. Turklāt Tiesa uzskata, ka ne sabiedrības tiesības piekļūt oficiāliem dokumentiem, ne tiesības uz informācijas brīvību neattaisno šādu tiesisko regulējumu.

Šajā kontekstā Tiesa uzsver, ka Latvijas tiesiskajā regulējumā paredzētā ceļu satiksmes drošības uzlabošana ir Savienības atzīts vispārējo interešu mērķis un tātad dalībvalstis var kvalificēt ceļu satiksmes drošību kā "uzdevumu sabiedrības interesēs" [44]. Tomēr Latvijā noteiktās ar pārkāpumu uzskaites punktiem saistīto personas datu izpaušanas kārtības nepieciešamība nav pierādīta. Proti, pirmkārt, Latvijas likumdevējam ir pieejami vairāki rīcības veidi, kas tam ļautu sasniegt šo mērķi ar citiem līdzekļiem, kuri mazāk aizskartu datu subjektu pamattiesības. Otrkārt, ir jāņem vērā personas datu par pārkāpumu uzskaites punktiem sensitīvais raksturs un fakts, ka to izpaušana sabiedrībai var radīt smagu iejaukšanos tiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, jo tā var izraisīt sabiedrības nosodījumu un būt par pamatu datu subjekta stigmatizācijai.

Turklāt Tiesa uzskata, ka, ņemot vērā šo datu sensitīvo raksturu un šīs iejaukšanās šajās divās pamattiesībās smagumu, šīs tiesības ir pārākas gan par sabiedrības interesēm piekļūt tādiem oficiāliem dokumentiem kā transportlīdzekļu un to vadītāju valsts reģistrs, gan arī par tiesībām uz informācijas brīvību.

Tādu pašu iemeslu dēļ Tiesa arī nospriež, ka VDAR pretrunā ir arī Latvijas tiesiskais regulējums, ciktāl ar to CSDD ir atļauts datus par transportlīdzekļu vadītājiem par ceļu satiksmes noteikumu pārkāpumiem reģistrētajiem pārkāpumu uzskaites punktiem nodot komersantiem, lai tie varētu tos atkalizmantot un izpaust sabiedrībai.

[44] Saskaņā ar VDAR 6. panta 1. punkta e) apakšpunktu personas datu apstrāde ir likumīga, ja tā ir "vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs [..]".

Visbeidzot Tiesa precizē, ka Savienības tiesību pārākuma princips nepieļauj, ka iesniedzējtiesa, kas izskata sūdzību par Latvijas tiesisko regulējumu, ko Tiesa ir kvalificējusi kā nesaderīgu ar Savienības tiesībām, nolemj saglabāt šā tiesiskā regulējuma tiesiskās sekas līdz dienai, kad pasludināts minētās tiesas galīgais spriedums.

III. Personas datu apstrāde nozares tiesiskā regulējuma izpratnē

1. Personas datu apstrāde elektronisko komunikāciju nozarē

2018. gada 2. oktobra spriedums (virspalāta) Ministerio Fiscal (C-207/16, EU:C:2018:788)

Šajā lietā Spānijas izmeklēšanas tiesnesis noraidīja pieprasījumu, kas bija iesniegts saistībā ar izmeklēšanu par naudasmaka un mobilā tālruņa nolaupīšanu. Konkrētāk, kriminālpolicija minētajam tiesnesim lūdza sniegt tai piekļuvi uz divpadsmit dienu laikposmu, skaitot no nolaupīšanas brīža, tālruņa numuru, kas bija aktivizēti no nolaupītā tālruņa, lietotāju identifikācijas datiem. Noraidījums bija balstīts uz pamatojumu, ka fakti, kas bija kriminālizmeklēšanas pamatā, neveidoja "smagu" noziedzīgu nodarījumu, proti, saskaņā ar Spānijas tiesībām – nodarījumu, par kuru soda ar brīvības atņemšanu uz laiku, kas ilgāks par pieciem gadiem, jo piekļuve identifikācijas datiem ir iespējama tikai attiecībā uz šāda veida nodarījumiem.

Norādījusi, ka valsts iestāžu piekļuve elektronisko komunikāciju pakalpojumu sniedzēju saglabātajiem personas datiem kriminālizmeklēšanas ietvaros ietilpst Direktīvas 2002/58 piemērošanas jomā, Tiesa atzina, ka piekļuve datiem, ar ko var identificēt personas, kurām pieder SIM kartes, kas aktivizētas ar nozagtu mobilo tālruni, tādiem kā šo personu vārds, uzvārds un, attiecīgā gadījumā, adrese, rada iejaukšanos Hartā aizsargātajās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, pat ja nav apstākļu, kas ļautu šo iejaukšanos kvalificēt kā "smagu", un nav nozīmes tam, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas neērtības minētās iejaukšanās dēļ. Tomēr Tiesa uzsvēra, ka šī iejaukšanās nav tik smaga, ka piekļuve noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomās būtu jāierobežo ar smagas noziedzības apkarošanu. Proti, pat ja Direktīvā 2002/58 ir izsmeļoši uzskaitīti mērķi, kas var pamatot tādu valsts tiesisko regulējumu, kurā ir reglamentēta valsts iestāžu piekļuve attiecīgajiem datiem un ar kuru tiek izdarīta atkāpe no elektronisko komunikāciju konfidencialitātes principa, un šai piekļuvei patiešām un stingri ir jāatbilst kādam no šiem mērķiem, Tiesa norāda, ka attiecībā uz noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu Direktīvas 2002/58 formulējums neierobežo šo mērķi vienīgi ar smagu noziegumu apkarošanu, bet gan attiecas uz "noziedzīgiem nodarījumiem" vispārīgi.

Šādā kontekstā Tiesa precizēja, ka, pat ja spriedumā *Tele2 Sverige* un *Watson* u.c. [45] tā ir nospriedusi, ka vienīgi smagu noziegumu apkarošana var pamatot valsts iestāžu piekļuvi komunikāciju pakalpojumu sniedzēju saglabātajiem personas datiem, kuri, ja tiek apkopoti, ļauj izdarīt konkrētus secinājumus par to personu privāto dzīvi, kuru dati tiek skarti, šāda interpretācija ir pamatota ar apstākli, ka tiesiskā regulējuma, kas reglamentē šo piekļuvi, mērķim ir jābūt atbilstošam šīs darbības rezultātā radītajam attiecīgo pamattiesību aizskāruma smagumam. Tādējādi atbilstoši samērīguma principam šajā jomā smagu iejaukšanos var pamatot vienīgi ar cīņu pret noziedzību, kas arī jākvalificē kā "smaga". Turpretim, ja iejaukšanās nav smaga, minēto piekļuvi var pamatot ar "noziedzīgu nodarījumu" novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vispārīgā veidā.

Runājot par šo lietu, Tiesa uzskatīja, ka piekļuvi tikai aplūkotajā pieprasījumā minētajiem datiem nevar kvalificēt kā "smagu" iejaukšanos attiecīgo datu subjektu pamattiesībās, jo šie dati neļauj izdarīt precīzus secinājumus par viņu privāto dzīvi. Tiesa no tā secināja, ka iejaukšanās, ko rada piekļuve šādiem datiem, tādējādi ir pamatojama ar "noziedzīgu nodarījumu" novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi vispārīgā veidā, un nav nepieciešams, lai šie nodarījumi būtu kvalificējami kā "smagi".

2020. gada 6. oktobra spriedumi (virspalāta) Privacy International (C-623/17, EU:C:2020:790) un La Quadrature du Net u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791)

Judikatūra par personas datu saglabāšanu un piekļuvi personas datiem elektronisko komunikāciju jomā, īpaši spriedums *Tele2 Sverige* un *Watson* u.c., kurā Tiesa tostarp uzskatīja, ka dalībvalstis elektronisko komunikāciju pakalpojumu sniedzējiem nedrīkst noteikt pienākumu veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu, izraisīja atsevišķu valstu bažas – tās uztraucās par to, ka tām tiek liegts instruments, kuru tās uzskata par nepieciešamu valsts drošības aizsardzībai un noziedzības apkarošanai.

Šajā kontekstā *Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesā, Apvienotā Karaliste) (*Privacy International*, C-623/17), *Conseil d'État* (Valsts padomē, Francija) (*La Quadrature du Net* u.c., apvienotās lietas C-511/18 un C-512/18), kā arī *Cour constitutionnelle* (Konstitucionālajā tiesā, Beļģija) (*Ordre des barreaux francophones et germanophone* u.c., C-520/18) tika celtas prasības saistībā ar tāda tiesiskā regulējuma likumību, kuru atsevišķas dalībvalstis bija pieņēmušas šajās jomās, konkrētāk, paredzot pienākumu elektronisko komunikāciju pakalpojumu sniedzējiem nodot valsts iestādei vai visaptverošā un nediferencētā veidā saglabāt ar lietotājiem saistīto informāciju par datu plūsmu un atrašanās vietas datus.

[45] Tiesas spriedums, 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970).

Ar diviem virspalātas sastāvā 2020. gada 6. oktobrī pasludinātiem spriedumiem Tiesa vispirms nosprież, ka valsts tiesiskie regulējumi, kuros elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums saglabāt informāciju par datu plūsmu un atrašanās vietu datus vai arī nodot šos datus valsts drošības un izlūkdienestu iestādēm šim nolūkam, ietilpst Direktīvas 2002/58 piemērošanas jomā.

Turpinājumā Tiesa atgādina, ka Direktīva 2002/58 [46] nepieļauj, ka atkāpe no principiālā pienākuma nodrošināt elektronisko komunikāciju un ar to saistīto datu konfidencialitāti un atkāpe no aizlieguma uzglabāt šos datus kļūtu par normu. Tas nozīmē, ka šī direktīva ļauj dalībvalstīm, tostarp valsts drošības mērķiem, pieņemt tiesību aktus ar nolūku ierobežot šajā direktīvā paredzēto tiesību un pienākumu, tostarp pienākuma nodrošināt komunikāciju un informācijas par datu plūsmu konfidencialitāti [47], piemērošanas jomu vienīgi tad, ja tās ievēro vispārējos Savienības tiesību principus, tostarp samērīguma principu, un Hartā garantētās pamattiesības [48].

Šajā ziņā Tiesa, pirmkārt, lietā *Privacy International* uzskata, ka Direktīva 2002/58, lasot to Hartas kontekstā, nepieļauj tādu tiesisko regulējumu, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem valsts drošības aizsardzības nolūkos ir noteikts pienākums veikt informācijas par datu plūsmu un atrašanās vietas datu visaptverošu un nediferencētu nodošanu drošības dienestiem un izlūkdienestiem. Otrkārt, apvienotajās lietās *La Quadrature du Net* u.c., kā arī lietā *Ordre des barreaux francophones et germanophone* u.c. Tiesa uzskata, ka šī pati direktīva nepieļauj tiesību aktus, ar kuriem elektronisko komunikāciju pakalpojumu sniedzējiem ir preventīvi noteikts pienākums veikt informācijas par datu plūsmu un atrašanās vietas datu visaptverošu un nediferencētu saglabāšanu.

Proti, šādi šo datu nodošanas un visaptverošas un nediferencētas saglabāšanas pienākumi ir uzskatāmi par īpaši nopietnu iejaukšanos Hartas garantētajās pamattiesībās, jo to personu rīcībai, attiecībā uz kuru datiem tā tiek veikta, nav saiknes ar aplūkotajā tiesiskajā regulējumā izvirzīto mērķi. Analoģiski arī VDAR 23. panta 1. punktu, lasot to Hartas gaismā, Tiesa interpretē tādējādi, ka tas nepieļauj tādu valsts tiesisko regulējumu, ar kuru piekļuves publiskiem tiešsaistes komunikāciju pakalpojumiem sniedzējiem un mitināšanas pakalpojumu sniedzējiem ir noteikts pienākums veikt visaptverošu un nediferencētu ar šiem pakalpojumiem saistīto personas datu saglabāšanu.

Turpretī Tiesa uzskata, ka situācijās, kad dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami, Direktīva 2002/58, lasot to Hartas gaismā, neliedz rīkojumā uzdot elektronisko komunikāciju pakalpojumu sniedzējiem visaptverošā un nediferencētā veidā saglabāt informāciju par datu plūsmu

[46] Direktīvas 2002/58 15. panta 1. un 3. punkts.
[47] Direktīvas 2002/58 5. panta 1. punkts.
[48] It īpaši Hartas 7., 8. un 11. pants, kā arī 52. panta 1. punkts.

un atrašanās vietas datus. Šādā kontekstā Tiesa precizē, ka lēmumam, kurā ir paredzēts šāds rīkojums uz laiku, kas nepārsniedz absolūti nepieciešamo, ir jābūt pakļautam efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē, kuras lēmumam ir saistoša iedarbība, lai pārliecinātos, vai pastāv kāda no šādām situācijām, kā arī vai ir ievēroti paredzētie nosacījumi un garantijas. Ar šādiem pašiem nosacījumiem minētā direktīva pieļauj arī visu elektroniskās komunikācijas līdzekļu lietotāju datu, tostarp informācijas par datu plūsmu un atrašanās vietas datu, automatizētu analīzi.

Tiesa piebilst, ka Direktīvai 2002/58, lasot to Hartas kontekstā, nav pretrunā leģislatīvi pasākumi, ar kuriem tiek atļauta tādas informācijas par datu plūsmu un atrašanās vietas datu mērķorientēta saglabāšana uz laiku, kas nav ilgāks par absolūti nepieciešamo, kura ir ierobežota ar objektīviem un nediskriminējošiem elementiem, ņemot vērā datu subjektu kategorijas vai izmantojot ģeogrāfisko kritēriju. Tāpat šī direktīva neliedz šādos tiesību aktos paredzēt komunikācijas avotam piešķirto IP adrešu visaptverošu un nediferencētu saglabāšanu, ja saglabāšanas ilgums nepārsniedz absolūti nepieciešamo, vai arī šādu elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu saglabāšanu, pēdējā minētajā gadījumā nenosakot dalībvalstīm pienākumu saglabāšanu ierobežot laikā. Minētajai direktīvai nav pretrunā arī leģislatīvs pasākums, kas ļauj operatīvi saglabāt pakalpojumu sniedzēju rīcībā esošos datus, ja rodas situācijas, kurās ir nepieciešams saglabāt minētos datus pēc tiesību aktos noteiktajiem termiņiem datu saglabāšanai, lai atklātu smagus noziedzīgus nodarījumus vai valsts drošības apdraudējumu, ja šie noziedzīgie nodarījumi vai šis apdraudējums jau ir ticis konstatēts vai arī ja par to esamību var rasties pamatotas aizdomas.

Turklāt Tiesa nospriež, ka Direktīva 2002/58, lasot to Hartas kontekstā, pieļauj tādu valsts tiesisko regulējumu, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums reāllaikā vākt tostarp informāciju par datu plūsmu un atrašanās vietas datus, ja šī vākšana attiecas tikai uz tādām personām, par kurām ir pamatots iemesls aizdomām, ka tās kaut kādā veidā ir iesaistītas terorisma darbībās, un ja tas ir pakļauts iepriekšējai pārbaudei tiesā vai neatkarīgā administratīvā iestādē, kuras lēmumam ir saistoša iedarbība, lai pārliecinātos, ka šāda vākšana reāllaikā ir atļauta vienīgi absolūti nepieciešamā apmērā. Neatliekamības gadījumos pārbaude jāveic īsā laikā.

Noslēgumā Tiesa pievēršas jautājumam par valsts tiesiskā regulējuma, kurš ir atzīts par neatbilstīgu Savienības tiesībām, seku saglabāšanu laikā. Šajā ziņā tā nospriež, ka valsts tiesa nedrīkst piemērot valsts tiesību normu, ar kuru tā ir pilnvarota ierobežot laikā tāda konstatējuma par prettiesiskumu iedarbību, kas tai ir jāveic attiecībā uz valsts tiesību aktiem, ar kuriem elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums visaptveroši un nediferencēti saglabāt informāciju par datu plūsmu un atrašanās vietas datus un kuri ir atzīti par nesaderīgiem ar Direktīvu 2002/58, lasot to Hartas kontekstā.

Tomēr, lai sniegtu lietderīgu atbildi valsts tiesai, Tiesa atgādina, ka pierādījumu, kuri iegūti, saglabājot datus neatbilstoši Savienības tiesībām, pieļaujamība un izvērtēšana

kriminālprocesā, kas sākts pret smaga noziegumu izdarīšanā aizdomās turētām personām, pašreizējā Savienības tiesību attīstības posmā ir nosakāma vienīgi saskaņā ar valsts tiesībām. Tomēr Tiesa precizē, ka Direktīva 2002/58, interpretējot to efektivitātes principa kontekstā, pieprasa, lai valsts krimināllietu tiesa šādā kriminālprocesā neņemtu vērā pierādījumus, kas – pretrunā Savienības tiesībām – ir iegūti, visaptveroši un nediferencēti saglabājot informāciju par datu plūsmu un atrašanās vietas datus, ja personas, kuras tiek turētas aizdomās par noziegumu, nevar efektīvi paust nostāju par šiem pierādījumiem.

2021. gada 2. marta spriedums (virspalāta), Prokuratuur (Piekļuves elektronisko komunikāciju datiem nosacījumi) (C-746/18, EU:C:2021:152)

Igaunijā tika ierosināta krimināllieta pret H. K. par zādzībām, citas personas bankas kartes izmantošanu un vardarbību pret tiesas procesa dalībniekiem. Par šiem nodarījumiem pirmās instances tiesa piesprieda H. K brīvības atņemšanu uz diviem gadiem. Šis spriedums tika atstāts negrozīts apelācijas instancē. Protokoli, uz kuriem pamatojas šo noziedzīgo nodarījumu konstatācija, ir sagatavoti, balstoties tostarp uz personas datiem, kas ir iegūti saistībā ar elektronisko komunikāciju pakalpojumu sniegšanu. *Riigikohus* (Augstākā tiesa, Igaunija), kura izskata H. K. iesniegto kasācijas sūdzību, pauž šaubas par to, vai ar Savienības tiesībām ir saderīgi [49] nosacījumi, ar kādiem izmeklēšanas dienestiem bija piešķirta piekļuve šiem datiem.

Šīs šaubas, pirmām kārtām, ir par to, vai laikposma ilgums, attiecībā uz kuru izmeklēšanas dienestiem bija piekļuve datiem, ir kritērijs, kas ļauj izvērtēt to, cik smaga ir šīs piekļuves izraisītā iejaukšanās datu subjektu pamattiesībās. Tādējādi iesniedzējtiesa vēlas noskaidrot, vai cīņa pret noziedzību kopumā – nevis tikai cīņa pret smagiem noziegumiem – var pamatot šādu iejaukšanos, ja šis laikposms ir ļoti īss vai ja ievākto datu apjoms ir ļoti neliels. Otrām kārtām, iesniedzējtiesai ir šaubas par to, vai Igaunijas Republikas Prokuratūra, ņemot vērā dažādos tai valsts tiesiskajā regulējumā uzticētos uzdevumus, ir "neatkarīga" administratīva iestāde sprieduma *Tele2 Sverige* un *Watson* u.c. izpratnē [50], kas var ļaut izmeklēšanas iestādei piekļūt attiecīgajiem datiem.

Šajā virspalātas sastāvā pasludinātajā spriedumā Tiesa nosprież, ka Direktīvai 2002/58, lasot to kopsakarā ar Hartu, pretrunā ir tāds valsts tiesiskais regulējums, ar kuru noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkā valsts iestādēm ir atļauts piekļūt informācijai par datu plūsmu vai atrašanās vietas datiem, kas var sniegt ziņas par saziņu, ko lietotājs veicis, izmantojot elektronisku komunikācijas līdzekli, vai par viņa izmantotās galiekārtas atrašanās vietu un no kā var izdarīt precīzus secinājumus par viņa privāto dzīvi, ja šī piekļuve neaprobežojas ar procedūrām smagas noziedzības apkarošanai vai smagu sabiedrības drošības

[49] Konkrēti ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā.
[50] Spriedums, 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970, 120. punkts).

apdraudējumu novēršanai. Tiesa uzskata, ka tā laikposma ilgumam, par kuru ir lūgta piekļuve šiem datiem, un par šādu laikposmu pieejamo datu apjomam vai raksturam šajā ziņā nav nozīmes. Turklāt Tiesa uzskata, ka šai pašai direktīvai, lasot to kopsakarā ar Hartu, ir pretrunā valsts tiesiskais regulējums, ar kuru prokuratūrai ir piešķirta kompetence atļaut valsts iestādei piekļūt datiem par datu plūsmu un atrašanās vietas datiem nolūkā veikt kriminālizmeklēšanu.

Attiecībā uz noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi, kas izvirzīts ar aplūkoto tiesisko regulējumu, Tiesa uzskata, ka saskaņā ar samērīguma principu vienīgi smagu noziegumu apkarošana un nopietnu valsts drošības apdraudējumu novēršana var pamatot valsts iestāžu piekļuvi visai informācijai par datu plūsmu vai atrašanās vietas datiem, no kuriem var izdarīt precīzus secinājumus par datu subjektu privāto dzīvi; savukārt citi ar piekļuves pieprasījuma samērīgumu saistīti faktori, piemēram, tā laikposma ilgums, par kuru tiek prasīta piekļuve šādiem datiem, nevar būt iemesls, lai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķis varētu attaisnot šādu piekļuvi.

Attiecībā uz prokuratūrai piešķirto kompetenci atļaut valsts iestādei piekļūt informācijai par datu plūsmu un atrašanās vietas datiem, lai vadītu kriminālizmeklēšanu, Tiesa atgādina, ka nosacījumus – kādos elektronisko komunikāciju pakalpojumu sniedzējiem ir jāļauj kompetentajām valsts iestādēm piekļūt to rīcībā esošajiem datiem – paredzēt ir valsts tiesiskā regulējuma ziņā. Taču, lai izpildītu samērīguma prasību, šajā tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi gan par attiecīgā pasākuma tvērumu un piemērošanu, gan par minimālajām prasībām, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šim tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās, un tajā ir jānorāda, kādos apstākļos un saskaņā ar kādiem materiāltiesiskajiem un procesuālajiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamā robežās.

Tiesa uzskata, ka, lai praksē nodrošinātu šo nosacījumu ievērošanu pilnībā, ir būtiski, ka kompetento valsts iestāžu piekļuve saglabātajiem datiem principā ir pakļauta iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, un ka šīs tiesas vai administratīvās iestādes lēmums tiek pieņemts, pamatojoties uz pieteicējas iestādes pamatotu pieteikumu, tostarp saistībā ar noziedzīga nodarījuma novēršanu, atklāšanu vai kriminālvajāšanas procedūrām. Pienācīgi pamatotos neatliekamības gadījumos pārbaude ir jāveic īsā laikā.

Šajā ziņā Tiesa precizē, ka šai iepriekšējai pārbaudei tostarp ir nepieciešams, lai tiesai vai iestādei, kurai ir jāveic minētā pārbaude, būtu visas pilnvaras un lai tā sniegtu visas garantijas, kas nepieciešamas, lai nodrošinātu dažādo attiecīgo interešu un tiesību salāgošanu. Runājot konkrētāk par kriminālizmeklēšanu, šādai pārbaudei ir vajadzīgs, lai šī tiesa vai iestāde spētu nodrošināt taisnīgu līdzsvaru starp interesēm, kas saistītas ar izmeklēšanas vajadzībām cīņā pret noziedzību, no vienas puses, un personu, kuru

datiem tiek piekļūts, pamattiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību, no otras puses. Ja šo pārbaudi veic nevis tiesa, bet gan neatkarīga administratīva iestāde, šai iestādei ir jāpiemīt tādam statusam, kas tai savu uzdevumu izpildē ļauj rīkoties objektīvi, un tālab tā nedrīkst būt pakļauta jebkādai ārējai ietekmei.

Tiesas ieskatā – no minētā izriet, ka neatkarības prasība, kam ir jāatbilst iestādei, kurai ir jāveic iepriekšējā pārbaude, nozīmē, ka šai iestādei ir jābūt nesaistītai ar piekļuvi datiem lūdzošo struktūru, lai tā spētu īstenot šo pārbaudi objektīvi un neatkarīgi no jebkādas ārējas ietekmes. Konkrēti krimināltiesību jomā neatkarības prasība nozīmē, ka iestāde, kas ir atbildīga par šo iepriekšējo pārbaudi, pirmkārt, nav iesaistīta attiecīgajā kriminālizmeklēšanā un, otrkārt, tai attiecībā pret kriminālprocesa dalībniekiem ir jābūt neitrālai. Tā tas nav gadījumā, kad izmeklēšanu vada un attiecīgā gadījumā valsts apsūdzību uztur prokuratūra, kā tas ir Igaunijas prokuratūras gadījumā. No tā izriet, ka prokuratūra nevar veikt iepriekšējo pārbaudi.

2022. gada 5. aprīļa spriedums (virspalāta), Commissioner of An Garda Síochána u.c. (C-140/20, EU:C:2022:258)

Šajā lietā lūgumu sniegt prejudiciālu nolēmumu iesniedza *Supreme Court* (Augstākā tiesa, Īrija), izskatot prasību civillietā, ko cēlusi kāda persona, kas notiesāta ar mūža ieslodzījumu par Īrijā izdarītu slepkavību. Šī persona apstrīdēja, ka ar Savienības tiesībām ir saderīgas vairākas valsts likuma par elektronisko komunikāciju gaitā radīto datu saglabāšanu normas. Pamatojoties uz šo likumu, elektronisko komunikāciju pakalpojumu sniedzēji bija saglabājuši un policijas iestādēm nodevuši informāciju par datu plūsmu un atrašanās vietas datus saistībā ar apsūdzētās personas tālruņa zvaniem. Iesniedzējtiesa šaubījās konkrēti par to, vai ar Direktīvu 2002/58, lasot to Hartas gaismā, ir saderīgs regulējums par šo datu visaptverošu un nediferencētu saglabāšanu saistībā ar smagu noziegumu apkarošanu.

Virspalātas sastāvā pasludinātajā spriedumā Tiesa apstiprina judikatūru, kas izriet no sprieduma *La Quadrature du Net* u.c. [51], vienlaikus precizējot tās tvērumu un atgādinot, ka smagu noziegumu apkarošanas un nopietnu valsts drošības apdraudējumu novēršanas nolūkos nav atļauts veikt ar elektroniskajām komunikācijām saistītās informācijas par datu plūsmu un atrašanās vietas datu visaptverošu un nediferencētu saglabāšanu. Tā apstiprina arī to, ka no sprieduma *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi) izrietošā judikatūra [52] – konkrēti jautājumā par to, ka kompetento valsts iestāžu piekļuve šiem saglabātajiem datiem ir jāpakārto iepriekšējai pārbaudei, ko veic vai nu tiesa, vai neatkarīga administratīva iestāde, – ir attiecināma arī uz policijas amatpersonu.

[51] Spriedums, 2020. gada 6. oktobris, *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791).
[52] Spriedums, 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi) (C-746/18, EU:C:2021:152).

Tiesa nospriež, pirmām kārtām, ka Direktīvai 2002/58, lasot to Hartas gaismā, ir pretrunā tādi valsts leģislatīvie pasākumi, kuros smagu noziegumu apkarošanai un nopietnu valsts drošības apdraudējumu novēršanai preventīvi tiek paredzēta ar elektroniskajām komunikācijām saistītās informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana. Proti, ņemot vērā, pirmkārt, atturošo ietekmi uz pamattiesību izmantošanu [53], kādu šī saglabāšana var izraisīt, un, otrkārt, šīs saglabāšanas radītās iejaukšanās smagumu, šādai saglabāšanai ir jābūt izņēmumam no šīs direktīvas radītās sistēmas, nevis tās normai tā, lai šie dati nedrīkstētu tikt saglabāti sistemātiski un nepārtraukti. Noziedzība, pat ja tā ir īpaši smaga, nav pielīdzināma valsts drošības apdraudējumam, jo šādas pielīdzināšanas rezultātā iespējami tiktu radīta starpkategorija starp valsts drošību un sabiedrības drošību, lai uz otro no tām attiecinātu prasības, kādas ir noteiktas saistībā ar pirmo.

Savukārt Direktīvai 2002/58, lasot to Hartas gaismā, nav pretrunā leģislatīvi pasākumi, kas smagu noziegumu apkarošanas un nopietnu sabiedrības drošības apdraudējumu novēršanas nolūkos paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu saglabāšanu, kura ir ierobežota ar objektīviem un nediskriminējošiem elementiem, ņemot vērā datu subjektu kategorijas vai izmantojot ģeogrāfisko kritēriju, uz laikposmu, kas nepārsniedz absolūti nepieciešamo, taču kuru ir iespējams pagarināt. Tā piebilst, ka šāds saglabāšanas pasākums, kas tiek veikts attiecībā uz vietām vai infrastruktūru, kuru 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 tā izdarīt secinājumus par šo personu atrašanos un aktivitātēm šajās vietās vai ģeogrāfiskajās zonās. Katrā ziņā iespējamās grūtības precīzi noteikt gadījumus, kad var tikt veikta mērķorientēta saglabāšana, un nosacījumus, saskaņā ar kuriem tā veicama, neattaisno to, ka dalībvalstis paredz informācijas par datu plūsmu un atrašanās vietas datu visaptverošu un nediferencētu saglabāšanu.

Šai direktīvai, lasot to Hartas gaismā, nav pretrunā arī leģislatīvi pasākumi, kuri šajos pašos nolūkos paredz uz laiku, kas nepārsniedz absolūti nepieciešamo, visaptveroši un nediferencēti saglabāt savienojuma avotam piešķirtās IP adreses, kā arī elektronisko komunikāciju līdzekļu lietotāju personas identitātes datus. Attiecībā uz pēdējo minēto aspektu Tiesa precizē, ka nedz Direktīvai 2002/58, nedz kādam citam Savienības tiesību aktam nav pretrunā tādi valsts tiesību akti, kuru mērķis ir smagu noziegumu apkarošana un saskaņā ar kuriem gan elektronisko komunikāciju līdzekļa, piemēram, priekšapmaksas SIM kartes, iegāde ir pakārtota prasībai par pircēja identitāti apliecinošu oficiālu dokumentu pārbaudi un pārdevēja pienākumam reģistrēt no tās izrietošo

[53] Kas nostiprinātas Hartas 7.–11. pantā.

informāciju, un pārdevējam vajadzības gadījumā ir pienākums dot kompetentajām valsts iestādēm piekļuvi šai informācijai.

Tas pats attiecas uz leģislatīvajiem pasākumiem, kuri šajos pašos smagu noziegumu apkarošanas un nopietnu sabiedrības drošības apdraudējumu nolūkos paredz ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, noformēta rīkojuma izdošanu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt ("*quick freeze*") šo pakalpojumu sniedzēju rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus. Proti, šāda saglabāšana var būt attaisnojama tikai ar mērķi apkarot smagus noziegumus un *a fortiori* – aizsargāt valsts drošību, ja vien šis pasākums, kā arī piekļuve saglabātajiem datiem aprobežojas ar to, kas ir absolūti nepieciešams. Tiesa atgādina, ka šāds operatīvās saglabāšanas 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 gatavojušās smaga nozieguma izdarīšanai vai to izdarījušas, vai arī 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 dati, kā arī dati par tās sociālo vai profesionālo vidi veidojošo personu loku.

Tomēr turpinājumā Tiesa norāda, ka visos iepriekš minētajos leģislatīvajos pasākumos ar skaidriem un precīziem noteikumiem ir jānodrošina, ka attiecīgo datu saglabāšana ir pakārtota piemērojamo materiāltiesisko un procesuālo nosacījumu ievērošanai un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku. Dažādie informācijas par datu plūsmu un atrašanās vietas datu saglabāšanas pasākumi, ievērojot absolūti nepieciešamā robežas, pēc valsts likumdevēja izvēles var tikt piemēroti kopā.

Turklāt Tiesa precizē, ka smagu noziegumu apkarošanas nolūkā atļaut piekļuvi šādiem datiem, kas ir visaptveroši un nediferencēti saglabāti tālab, lai reaģētu uz nopietniem draudiem valsts drošībai, būtu pretrunā hierarhijai, kas pastāv starp vispārējo interešu mērķiem, ar kuriem var attaisnot saskaņā ar Direktīvu 2002/58 veiktu pasākumu. Proti, tas nozīmētu pieļaut, ka piekļuve tiek attaisnota ar mērķi, kurš nav tik svarīgs kā šo saglabāšanu attaisnojošais mērķis, proti, valsts drošības aizsardzība, tādējādi iespējami liedzot visu lietderīgo iedarbību aizliegumam veikt visaptverošu un nediferencētu saglabāšanu smagu noziegumu apkarošanas nolūkā.

Otrām kārtām, Tiesa nospriež, ka Direktīvai 2002/58, lasot to Hartas gaismā, ir pretrunā tāds valsts tiesiskais regulējums, saskaņā ar kuru 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, pirmkārt, šāda amatpersona neatbilst neatkarības un objektivitātes prasībām, kurām ir jāatbilst administratīvajai iestādei, kura veic iepriekšēju kontroli attiecībā uz kompetento valsts iestāžu

iesniegtajiem pieprasījumiem saņemt piekļuvi datiem, jo tā nav nepiederīga šīm iestādēm. Otrkārt, lai arī šādas amatpersonas lēmums var būt pakļauts *a posteriori* pārbaudei tiesā, šī pārbaude nevar aizstāt neatkarīgu un, izņemot pienācīgi pamatotus steidzamības gadījumus, iepriekš veiktu pārbaudi.

Visbeidzot trešām 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 2002/58. 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.

2022. gada 20. septembra spriedums (virspalāta) VD un SR (C-339/20 un C-397/20, EU:C:2022:703)

Autorité des marchés financiers (Finanšu tirgus uzraudzības iestāde (*AMF*), Francija) veiktās pārbaudes rezultātā tika uzsākti kriminālprocesi pret divām fiziskām personām, proti, VD un SR, kas bija apsūdzētas šādu noziedzīgu nodarījumu izdarīšanā: iekšējās informācijas ļaunprātīga izmantošana, iekšējās informācijas ļaunprātīgas izmantošanas slēpšana, līdzdalība minētajos nodarījumos, korupcija un nelikumīgi iegūtu līdzekļu legalizēšana. Šajā izmeklēšanā *AMF* bija izmantojusi personas datus, kuri iegūti no VD un SR veiktajiem tālruņa zvaniem un kuri elektronisko komunikāciju pakalpojumu sniegšanas ietvaros iegūti saskaņā ar *code des postes et des communications électroniques* (Pasta un elektronisko sakaru kodekss) .

Tā kā par aizdomās turētajiem viņi tika atzīti, pamatojoties uz *AMF* sniegto informāciju par datu plūsmu, VD un SR katrs vērsās *cour d'appel de Paris* (Parīzes apelācijas tiesa, Francija) ar prasību, izvirzot tostarp pamatu par to, ka esot pārkāpts Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā. Konkrēti, atsaucoties uz judikatūru, kas izriet no sprieduma *Tele2 Sverige* un *Watson* u.c. [54], VD un SR apstrīdēja, ka *AMF* ir tiesīga vākt minētos datus, pamatojoties uz aplūkotajām valsts tiesību normām, tāpēc, ka, viņuprāt, šīs normas, pirmkārt, nav saderīgas ar Savienības tiesībām, jo paredz savienojuma datu visaptverošu un nediferencētu glabāšanu, un, otrkārt, tajās nav nekādi ierobežotas *AMF* izmeklētāju pilnvaras pieprasīt tiem nosūtīt glabātos datus.

[54] Spriedums, 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970).

Ar diviem 2018. gada 20. decembra un 2019. gada 7. marta spriedumiem *cour d'appel de Paris* (Parīzes apelācijas tiesa) noraidīja VD un SR prasības. Iepriekš minēto prasības pamatu šīs lietas pēc būtības izskatošie tiesneši noraidīja, pamatojoties tostarp uz apstākli, ka Tirgus ļaunprātīgas izmantošanas regula [55] ļauj kompetentajām iestādēm – ciktāl tas atļauts ar valsts tiesību aktiem – pieprasīt elektronisko komunikāciju pakalpojumu operatoru rīcībā esošos datu plūsmas ierakstus, ja ir pamatotas aizdomas par iekšējās informācijas izmantošanas tirdzniecībā aizlieguma pārkāpumu un ja šādi ieraksti var būt vajadzīgi šā pārkāpuma izmeklēšanai.

Tad VD un SR iesniedza kasācijas sūdzību *Cour de cassation* (Kasācijas tiesa, Francija), kas ir iesniedzējtiesa šajās lietās.

Šajā kontekstā iesniedzējtiesa vaicā, kā Direktīvas 2002/58 15. panta 1. punkts – lasot to Hartas gaismā – būtu salāgojams ar prasībām, kas izriet no Tirgus ļaunprātīgas izmantošanas direktīvas [56] 12. panta 2. punkta a) un d) apakšpunkta un Tirgus ļaunprātīgas izmantošanas regulas 23. panta 2. punkta g) un h) apakšpunkta. Šā jautājuma pamatā ir pamatlietās aplūkotie leģislatīvie pasākumi, kuros tirgus ļaunprātīgas izmantošanas noziegumu – kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos elektronisko komunikāciju pakalpojumu operatoriem tiek noteikts pienākums preventīvā kārtā veikt informācijas par datu plūsmu visaptverošu un nediferencētu glabāšanu gadu pēc tās ierakstīšanas. Ja Tiesa atzītu, ka pamatlietās aplūkotie tiesību akti par savienojuma datu glabāšanu neatbilst Savienības tiesībām, iesniedzējtiesa vaicā par šo tiesību aktu seku provizorisku atstāšanu spēkā, lai novērstu tiesisko nedrošību un ļautu līdz šim ievāktos un glabātos datus izmantot iekšējās informācijas ļaunprātīgas izmantošanas konstatēšanai un kriminālvajāšanai par to.

Virspalātas sastāvā pasludinātajā spriedumā Tiesa nospriež, ka elektronisko komunikāciju pakalpojumu operatoriem nav atļauts tirgus ļaunprātīgas izmantošanas nodarījumu apkarošanas nolūkos preventīvā kārtā visaptveroši un nediferencēti glabāt informāciju par datu plūsmu gadu pēc tās ierakstīšanas. Turklāt tā apstiprina savu judikatūru, ka Savienības tiesībām ir pretrunā, ka dalībvalsts tiesa ierobežo laikā sekas, kas izriet no apstākļa, ka tā, pildot savu uzdevumu, par spēkā neesošām ir atzinusi ar Savienības tiesībām nesaderīgas valsts tiesību normas.

Tiesa vispirms atgādina, ka, interpretējot Savienības tiesību normu, ir jāņem vērā ne tikai tās teksts, bet arī konteksts un šo normu ietverošā tiesiskā regulējuma mērķi.

Attiecībā uz prejudiciālajos jautājumos minēto tiesību normu formulējumu Tiesa konstatē, ka Tirgus ļaunprātīgas izmantošanas direktīvas 12. panta 2. punkta

[55] Eiropas Parlamenta un Padomes Regula (ES) Nr. 596/2014 (2014. gada 16. aprīlis) par tirgus ļaunprātīgu izmantošanu (tirgus ļaunprātīgas izmantošanas regula) un ar ko atceļ Eiropas Parlamenta un Padomes Direktīvu 2003/6/EK un Komisijas Direktīvas 2003/124/EK, 2003/125/EK un 2004/72/EK (OV 2014, L 173, 1. lpp.).

[56] Eiropas Parlamenta un Padomes Direktīva 2003/6/EK (2003. gada 28. janvāris) par iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām (tirgus ļaunprātīgu izmantošanu) (OV 2003, L 96, 16. lpp.).

d) apakšpunktā ir norādīts uz *AMF* pilnvarām "pieprasīt esošo[s] telefonsarunu ierakstus un esošos datu plūsmas ierakstus", savukārt Tirgus ļaunprātīgas izmantošanas regulas 23. panta 2. punkta g) un h) apakšpunktā ir norādīts uz šīs iestādes pilnvarām pieprasīt, pirmkārt, "ieguldījumu brokeru sabiedrību, kredītiestāžu vai citu finanšu iestāžu rīcībā esošo[s] [..] datu plūsmas ierakstus" un, otrkārt, "ciktāl to atļauj valsts tiesību akti, pieprasīt telekomunikāciju operatora rīcībā esošos datu plūsmas ierakstus". Tiesa atzīst, ka no šo tiesību normu formulējuma nepārprotami izriet, ka tajās ir vienīgi noteikti ietvari *AMF* pilnvarām "pieprasīt" šo operatoru rīcībā esošos datus, un tas nozīmē piekļuvi šiem datiem. Turklāt norāde uz minēto operatoru "rīcībā" "esošajiem" ierakstiem ļauj noprast, ka Savienības likumdevējs nav vēlējies reglamentēt valsts likumdevēja iespēju noteikt pienākumu šādus ierakstus saglabāt. Tiesas ieskatā šo interpretāciju turklāt apstiprina gan minēto normu konteksts, gan šo normu veidotā tiesiskā regulējuma mērķi.

Attiecībā uz prejudiciālajos jautājumos minēto tiesību normu kontekstu Tiesa norāda – lai gan saskaņā ar attiecīgajām Tirgus ļaunprātīgas izmantošanas direktīvas un Tirgus ļaunprātīgas izmantošanas regulas normām [57] Savienības likumdevējs ir vēlējies likt dalībvalstīm veikt pasākumus, kas vajadzīgi tālab, lai finanšu jomā kompetento iestāžu rīcībā būtu iedarbīgu instrumentu, pilnvaru un resursu kopums, kā arī uzraudzības un izmeklēšanas pilnvaru kopums, lai nodrošinātu to uzdevumu izpildes efektivitāti, šajās normās nav nekas teikts nedz par dalībvalstu varbūtējo iespēju tālab noteikt elektronisko komunikāciju pakalpojumu operatoriem pienākumu visaptveroši un nediferencēti glabāt informāciju par datu plūsmu, nedz par nosacījumiem, ar kādiem šiem operatoriem būtu jāglabā šie dati, lai tos vajadzības gadījumā iesniegtu kompetentajām iestādēm.

Runājot par attiecīgā tiesiskā regulējuma mērķiem, Tiesa norāda, ka gan no Tirgus ļaunprātīgas izmantošanas direktīvas, gan no Tirgus ļaunprātīgas izmantošanas regulas [58] izriet, ka šo tiesību aktu mērķis ir nodrošināt Savienības finanšu tirgu integritāti un vairot ieguldītāju uzticēšanos šiem tirgiem, savukārt šī uzticēšanās balstās tostarp uz pārliecību, ka pret viņiem būs vienlīdzīga attieksme un viņi tiks aizsargāti no iekšējās informācijas prettiesiskas izmantošanas. Minētajās tiesību normās [59] noteiktā iekšējās informācijas ļaunprātīgas izmantošanas aizlieguma mērķis tātad ir nodrošināt līgumslēdzēju vienlīdzību biržas darījumos, izvairoties no tā, ka kāds no tiem, kura rīcībā ir iekšējā informācija un kurš tādēļ ir labvēlīgākā situācijā attiecībā pret citiem ieguldītājiem, gūst labumu uz to personu rēķina, kas šo informāciju nezina. Lai arī saskaņā ar Tirgus ļaunprātīgas izmantošanas regulu [60] savienojuma datu ieraksti ir būtiski un dažreiz vienīgie pierādījumi, kas ļauj konstatēt un pierādīt iekšējās

[57] Attiecīgi ar Tirgus ļaunprātīgas izmantošanas direktīvas 12. panta 1. punktu un Tirgus ļaunprātīgas izmantošanas regulas 23. panta 3. punktu, lasot kopsakarā ar šīs regulas 62. apsvērumu.

[58] Attiecīgi – no Tirgus ļaunprātīgas izmantošanas direktīvas 2. un 12. apsvēruma un no Tirgus ļaunprātīgas izmantošanas regulas 1. panta, lasot to kopsakarā ar tās 2. un 24. apsvērumu.

[59] Tirgus ļaunprātīgas izmantošanas direktīvas 2. panta 1. punkts un Tirgus ļaunprātīgas izmantošanas regulas 8. panta 1. punkts.

[60] Tirgus ļaunprātīgas izmantošanas regulas 62. apsvērums.

informācijas izmantošanu un tirgus manipulācijas, tomēr šajā regulā ir minēti tikai elektronisko komunikāciju pakalpojumu operatoru "rīcībā" esošie ieraksti, kā arī finanšu jomā kompetentās iestādes pilnvaras "pieprasīt" no šiem operatoriem "esošos" datus. Tādējādi no šā akta teksta nekādi neizriet, ka Savienības likumdevējs būtu šādi vēlējies atzīt dalībvalstīm tiesības noteikt elektronisko komunikāciju pakalpojumu operatoriem vispārīgu pienākumu glabāt datus. No tā izriet, ka nedz Tirgus ļaunprātīgas izmantošanas direktīva, nedz Tirgus ļaunprātīgas izmantošanas regula nevar būt juridiskais pamats vispārīgam pienākumam glabāt elektronisko komunikāciju pakalpojumu operatoru rīcībā esošos datu plūsmas ierakstus tālab, lai finanšu jomā kompetentā iestāde varētu īstenot tai saskaņā ar šiem tiesību aktiem piešķirtās pilnvaras.

Turpinājumā Tiesa atgādina, ka jautājumā par datu saglabāšanu un – plašāk – par personas datu apstrādi elektronisko komunikāciju jomā atsauces regulējums rodams Direktīvā 2002/58, un tāpēc tas, kā Tiesa interpretē šo direktīvu, ir attiecināms arī uz elektronisko komunikāciju pakalpojumu operatoru rīcībā esošajiem plūsmas datu ierakstiem, kurus finanšu jomā kompetentās iestādes Tirgus ļaunprātīgas izmantošanas direktīvas un Tirgus ļaunprātīgas izmantošanas regulas izpratnē [61] var tiem pieprasīt. Tādēļ elektronisko komunikāciju pakalpojumu operatoru rīcībā esošo ierakstu apstrādes likumīgums [62] jāvērtē to nosacījumu kontekstā, kas paredzēti Direktīvā 2002/58, kā arī atbilstoši tam, kā šo direktīvu savā judikatūrā interpretē Tiesa.

Tādējādi Tiesa nospriež, ka Tirgus ļaunprātīgas izmantošanas direktīvai un Tirgus ļaunprātīgas izmantošanas regulai – kopsakarā ar Direktīvu 2002/58 un lasot tās Hartas gaismā – ir pretrunā leģislatīvi pasākumi, kuros tirgus ļaunprātīgas izmantošanas nodarījumu – kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos elektronisko komunikāciju pakalpojumu operatoriem tiek paredzēts pienākums preventīvā kārtā uz noteiktu laiku, proti, gadu pēc tās ierakstīšanas, taču visaptveroši un nediferencēti glabāt informāciju par datu plūsmu.

Visbeidzot Tiesa apstiprina savu judikatūras atziņu, ka Savienības tiesībām ir pretrunā, ka dalībvalsts tiesa ierobežo laikā sekas, kas izriet no apstākļa, ka tā atbilstoši valsts tiesībām par spēkā neesošām ir atzinusi valsts tiesību normas – ar kurām, pirmkārt, elektronisko komunikāciju pakalpojumu operatoriem ir noteikts pienākums visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un, otrkārt, ir atļauts sniegt šo informāciju finanšu jomā kompetentajai iestādei, iepriekš nesaņemot tiesas vai neatkarīgas administratīvas iestādes atļauju –, jo šīs tiesību normas ir nesaderīgas ar Direktīvu 2002/58, lasot to Hartas gaismā. Tomēr Tiesa atgādina, ka atbilstoši dalībvalstu procesuālās autonomijas principam šādas glabāšanas ceļā iegūto pierādījumu pieļaujamību reglamentē valsts tiesības, ja vien tiek ievēroti tostarp līdzvērtības un

[61] Attiecīgi – Tirgus ļaunprātīgas izmantošanas direktīvas 11. panta un Tirgus ļaunprātīgas izmantošanas regulas 22. panta izpratnē.

[62] Tirgus ļaunprātīgas izmantošanas direktīvas 12. panta 2. punkta d) apakšpunkta un Tirgus ļaunprātīgas izmantošanas regulas 23. panta 2. punkta g) un h) apakšpunkta izpratnē.

efektivitātes principi. Efektivitātes princips prasa, lai valsts kriminālllietu tiesa neņemtu vērā informāciju un pierādījumus, kas iegūti, izmantojot ar Savienības tiesībām nesaderīgu visaptverošu un nediferencētu glabāšanu, ja datu subjekti nespēj efektīvi paust nostāju par šo informāciju un šiem pierādījumiem, kuri ir saistīti ar jomu, ko tiesa nepārzina, un kuri var būtiski ietekmēt faktu vērtējumu.

2024. gada 30. aprīļa spriedums (plēnums), La Quadrature du Net u.c. (Personas dati un intelektuālā īpašuma tiesību pārkāpumu apkarošana) (C-470/21, EU:C:2024:370)

Izskatīdams lūgumu sniegt prejudiciālu nolēmumu, ko tai iesniegusi *Conseil d'État* (Valsts padome, Francija), Tiesas plēnums pilnveido judikatūru par Direktīvu 2002/58, sniedzot sīkākus paskaidrojumus, pirmkārt, par nosacījumiem, kādos elektronisko komunikāciju pakalpojumu sniedzēju veiktā IP adrešu visaptveroša glabāšana var arī nebūt uzskatāma par tādu, kas izraisa smagu iejaukšanos Hartā garantētajās tiesībās uz privātās dzīves neaizskaramību, personas datu aizsardzību, kā arī vārda brīvību [63], un, otrkārt, par publiskas iestādes iespēju piekļūt noteiktiem personas datiem, kas glabāti saskaņā ar šiem nosacījumiem, tiešsaistē izdarītu intelektuālā īpašuma tiesību pārkāpumu apkarošanas vajadzībām.

Šajā gadījumā četras apvienības iesniedza *Premier ministre* (premjerministrs, Francija) lūgumu atcelt dekrētu par personas datu automatizētu apstrādi [64]. Tā kā šis lūgums tika atstāts bez izskatīšanas, šīs apvienības vērsās *Conseil d'État* (Valsts padome) ar prasību atcelt šo netieši izteikto noraidošo lēmumu. Tās uzskata, ka šis dekrēts, kā arī tiesību normas, kas veido tā juridisko pamatu [65], ir pretrunā Savienības tiesībām.

Saskaņā ar Francijas tiesību aktiem, lai varētu identificēt personas, kuras ir atbildīgas par tiešsaistē izdarītiem autortiesību vai blakustiesību pārkāpumiem, *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (Augstā iestāde darbu izplatīšanai un tiesību aizsardzībai internetā, turpmāk tekstā – "*Hadopi*") ir atļauts piekļūt noteiktiem datiem, kuri elektronisko komunikāciju pakalpojumu sniedzējiem ir jāglabā. Šie dati attiecas uz datu subjekta identitāti, kas piesaistīta tā IP adresei, kuru iepriekš ir ievākušas tiesību īpašnieku organizācijas. Tiklīdz ir identificēts par šādu pārkāpumu kvalificējamām darbībām izmantotās IP adreses īpašnieks, *Hadopi* veic tā saukto "pakāpeniskās reakcijas" procedūru. Konkrēti, tā ir tiesīga šai personai nosūtīt divus ieteikumus, kas līdzinās brīdinājumiem, un, ja šīs darbības turpinās – arī vēstuli, kurā šai personai tiek paziņots, ka par viņas darbībām var iespējami tikt veikta kriminālvajāšana.

---

[63] Hartas 7., 8. un 11. pants.

[64] 2010. gada 5. marta Dekrēts Nr. 2010-236 par personas datu automatizētu apstrādi, kas ir atļauta ar Intelektuālā īpašuma kodeksa L. 331-29. pantu un saukta par "Vadības sistēmu pasākumiem darbu aizsardzībai internetā") (2010. gada 7. marta *JORF* Nr. 56, teksts Nr. 19), redakcijā ar grozījumiem, kas izdarīti ar 2017. gada 6. maija Dekrētu Nr. 2017-924 par autortiesību un blakustiesību pārvaldību, ko veic tiesību pārvaldījuma organizācija, un ar ko groza Intelektuālā īpašuma kodeksu (2017. gada 10. maija *JORF* Nr. 109, teksts Nr. 176).

[65] Konkrēti Intelektuālā īpašuma kodeksa L. 331-21. panta trešā līdz piektā daļa.

Visbeidzot tā ir tiesīga vērsties prokuratūrā, lai veiktu minētās personas kriminālvajāšanu [66].

Šajā kontekstā *Conseil d'État* (Valsts padome) uzdeva Tiesai jautājumus par to, kā interpretējama Direktīva 2002/58, lasot to Hartas gaismā [67].

Pirmām kārtām, attiecībā uz personas identitātes datu un tām piesaistīto IP adrešu glabāšanu Tiesa uzsver, ka visaptveroša un nediferencēta IP adrešu glabāšana ne vienmēr izraisa smagu iejaukšanos Hartā garantētajās tiesībās uz privātās dzīves neaizskaramību, personas datu aizsardzību, kā arī vārda brīvību.

Pienākums nodrošināt šādu glabāšanu var būt attaisnojams ar mērķi apkarot noziedzīgus nodarījumus vispārīgi, ja ir faktiski izslēgts, ka šī glabāšana var izraisīt smagu iejaukšanos datu subjekta privātajā dzīvē tādēļ, ka par šo subjektu ir iespējams izdarīt precīzus secinājumus, tostarp sasaistot šīs IP adreses ar informācijas par datu plūsmu vai atrašanās vietas datu kopumu.

Līdz ar to dalībvalstij, kura vēlas noteikt elektronisko komunikāciju pakalpojumu sniedzējiem šādu pienākumu, ir jānodrošina, ka šo datu glabāšanas kārtība ir tāda, kas izslēdz iespēju izdarīt precīzus secinājumus par datu subjektu privāto dzīvi.

Tiesa precizē, ka glabāšanas kārtībai tālab jāaptver pati šīs glabāšanas strukturēšana, kas būtībā jāorganizē tā, lai nodrošinātu dažādo glabāto datu kategoriju faktisku izolētību. Tādējādi valsts tiesību normām par šo kārtību ir jānodrošina, ka katra datu kategorija, tostarp personas identitātes dati un IP adreses, tiek glabāta pilnīgi nošķirti no citām glabāto datu kategorijām, un šie dati tiek patiešām izolēti viens no otra, izmantojot drošu un uzticamu datoraprīkojumu. Turklāt, ciktāl šajos noteikumos ir paredzēta iespēja noziedzīgu nodarījumu apkarošanas nolūkos sasaistīt šādi glabātās IP adreses ar datu subjekta identitāti, šie noteikumi drīkst šādu sasaistīšanu atļaut tikai tad, ja tiek izmantots efektīvs tehnoloģisks process, kas nerada šaubas par šo datu kategoriju striktas izolētības efektivitāti. Šīs izolētības uzticamība ir regulāri jāpārbauda citai nepiederīgai publiskai iestādei. Ciktāl piemērojamos valsts tiesību aktos ir paredzētas šādas stingras prasības, no šīs IP adrešu glabāšanas izrietošā iejaukšanās nav kvalificējama kā "smaga".

Līdz ar to Tiesa secina, ka, ja ir normatīvais regulējums, kas garantē, ka nekāda datu kombinācija neļaus izdarīt precīzus secinājumus par to personu privāto dzīvi, kuru dati tiek glabāti, Direktīvai 2002/58, lasot to Hartas gaismā, nav pretrunā, ka dalībvalsts nosaka pienākumu visaptveroši un nediferencēti glabāt IP adreses uz laiku, kas nepārsniedz absolūti nepieciešamo, nolūkā apkarot noziedzīgus nodarījumus vispārīgi.

---

[66] Kopš 2022. gada 1. janvāra *Hadopi* tika apvienota ar *Conseil supérieur de l'audiovisuel* (Audiovizuālās nozares uzraudzības padome, *CSA*), citu neatkarīgu publisku iestādi, un kļuva par *Autorité de régulation de la communication audiovisuelle et numérique* (Audiovizuālās un digitālās komunikācijas regulatīvā iestāde, *ARCOM*). Taču pakāpeniskās reakcijas procedūra būtībā palika nemainīga.

[67] Direktīvas 2002/58 15. panta 1. punkts.

Otrām kārtām, attiecībā uz piekļuvi IP adresēm piesaistītajiem personas identitātes datiem Tiesa nospriež, ka Direktīvai 2002/58, lasot to Hartas gaismā, principā nav pretrunā tāds valsts tiesiskais regulējums, kurā publiskai iestādei ir ļauts piekļūt šiem datiem, kurus elektronisko komunikāciju pakalpojumu sniedzēji glabā nošķirti un faktiski izolēti, tikai tālab, lai šī iestāde varētu identificēt šo adrešu īpašniekus, par kuriem ir aizdomas, ka tie ir atbildīgi par internetā izdarītiem autortiesību un blakustiesību pārkāpumiem, un attiecībā uz viņiem veikt pasākumus. Šādā gadījumā valsts tiesiskajā regulējumā ir jāaizliedz amatpersonām, kurām ir šāda piekļuve, pirmkārt, jebkādā veidā izpaust informāciju par šo īpašnieku apmeklēto datņu saturu, izņemot, ja tas tiek darīts, lai vērstos prokuratūrā, otrkārt, veikt jebkādu šo īpašnieku tīklklejošanas izsekošanu un, treškārt, izmantot šīs IP adreses citiem mērķiem, nevis šo pasākumu veikšanai.

Šajā kontekstā Tiesa tostarp atgādina, ka, lai arī vārda brīvība un personas datu konfidencialitāte ir primārās rūpes, šīs pamattiesības tomēr nav absolūtas. Proti, samērojot attiecīgās tiesības un intereses, šīm tiesībām un interesēm dažkārt ir jāpiekāpjas citām pamattiesībām un tādiem vispārējo interešu apsvērumiem kā sabiedriskās kārtības aizsardzība un noziedzīgu nodarījumu novēršana vai citu personu tiesību un brīvību aizsardzība. Tā tas konkrēti ir gadījumā, kad prioritāte, kas piešķirta minētajām primārajām rūpēm, var traucēt kriminālizmeklēšanas efektivitātei, tostarp padarot neiespējamu vai pārmērīgi apgrūtinot noziedzīga nodarījuma izdarītāja faktisku identificēšanu un viņa sodīšanu.

Šajā pašā kontekstā Tiesa atsaucas arī uz savu judikatūru, atbilstoši kurai apstāklis, ka saistībā ar cīņu pret tiešsaistē izdarītiem autortiesību vai blakustiesību pārkāpumu noziedzīgiem nodarījumiem piekļuve IP adresēm var būt vienīgais izmeklēšanas līdzeklis, kas ļauj identificēt attiecīgo personu, apstiprina, ka šo adrešu glabāšana un piekļuve tām ir absolūti nepieciešamas, lai sasniegtu izvirzīto mērķi, un tādējādi atbilst samērīguma prasībai. Šādas piekļuves nepieļaušana radītu arī reālu sistēmiskas nesodāmības risku attiecībā uz tādiem noziedzīgiem nodarījumiem, kas izdarīti tiešsaistē vai kuru izdarīšanu vai sagatavošanu internetam raksturīgās iezīmes atvieglo. Savukārt šāda riska esamība ir nozīmīgs apstāklis, kas ņemams vērā, kad, samērojot dažādas iesaistītās tiesības un intereses, tiek novērtēts, vai iejaukšanās tiesībās uz privātās dzīves neaizskaramību, personas datu aizsardzību, kā arī vārda brīvību ir pasākums, kas ir samērīgs ar mērķi apkarot noziedzīgus nodarījumus.

Trešām kārtām, spriežot par to, vai publiskās iestādes piekļuve IP adresei piesaistītajiem personas identitātes datiem jāpakārto iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, Tiesa uzskata, ka prasība par šādu pārbaudi ir jāievēro tad, ja valsts tiesiskā regulējuma kontekstā šī piekļuve rada risku, ka notiks smaga iejaukšanās datu subjekta pamattiesībās tādā ziņā, ka tā varētu ļaut šai publiskajai iestādei izdarīt precīzus secinājumus par šā subjekta privāto dzīvi un vajadzības gadījumā izveidot šā subjekta detalizētu profilu. Šī iepriekšējas pārbaudes prasība turpretim nav piemērojama tad, ja iejaukšanās pamattiesībās nav kvalificējama kā smaga.

Šajā ziņā Tiesa precizē, ka gadījumā, ja ir ieviesta tāda glabāšanas kārtība, kas nodrošina dažādu glabāto datu kategoriju faktisku izolētību, publiskās iestādes piekļuve IP adresēm piesaistītajiem personas identitātes datiem principā nav pakārtota prasībai par iepriekšēju pārbaudi. Proti, šāda piekļuve ar vienu vienīgu mērķi identificēt IP adreses īpašnieku parasti nav kvalificējama kā smaga iejaukšanās iepriekš minētajās tiesībās.

Tomēr Tiesa neizslēdz, ka netipiskos gadījumos var būt risks, ka tādā procedūrā kā pamatlietā aplūkotā pakāpeniskās reakcijas procedūra publiskā iestāde var izdarīt precīzus secinājumus par datu subjekta privāto dzīvi, it īpaši tad, ja šī persona veic autortiesības vai blakustiesības pārkāpjošas darbības vienādranga (*peer-to-peer*) tīklos atkārtoti vai pat lielā apmērā saistībā ar konkrēta veida aizsargātajiem darbiem, ar kuru palīdzību var tikt atklāta iespējami sensitīva informācija par minētās personas privāto dzīvi.

Šajā gadījumā IP adreses īpašnieks var būt īpaši pakļauts šādam riskam, ja publiskajai iestādei ir jālemj, vai vērsties vai nevērsties prokuratūrā, lai attiecībā uz šo īpašnieku veiktu kriminālvajāšanu. Proti, tiesību uz privātās dzīves neaizskaramību aizskāruma intensitāte var pieaugt līdz ar secīgā procesā balstītās pakāpeniskās reakcijas procedūras virzību dažādos tās posmos. Šajā gadījumā kompetentās iestādes piekļuve visiem datu subjekta datiem, kas ievākti dažādos šīs procedūras posmos, var ļaut izdarīt precīzus secinājumus par šā subjekta privāto dzīvi. Līdz ar to valsts tiesiskajā regulējumā jāparedz tāda iepriekšēja pārbaude, kurai jānotiek, pirms publiskā iestāde var personas identitātes datus sasaistīt ar šādu datu kopumu un pirms iespējamās paziņojuma vēstules nosūtīšanas, kurā ir konstatēts, ka šī persona ir iesaistījusies nodarījumos, par kuriem var tikt veikta kriminālvajāšana. Šai pārbaudei turklāt jānodrošina pakāpeniskās reakcijas procedūras efektivitāte, it īpaši ļaujot identificēt attiecīgās pārkāpjošās rīcības iespējamās atkārtotības gadījumus. Tālab šī procedūra ir jāorganizē un jāstrukturē tā, lai personas, kas ir atbildīgas par faktu pārbaudi kompetentajā publiskajā iestādē, automātiski nevarētu personas identitātes datus, kas piesaistīti iepriekš internetā ievāktām IP adresēm, sasaistīt ar informāciju, kas jau ir šīs iestādes rīcībā un kas varētu ļaut izdarīt precīzus secinājumus par šīs personas privāto dzīvi.

Turklāt attiecībā uz iepriekšējās pārbaudes priekšmetu Tiesa norāda, ka gadījumos, kad datu subjekts tiek turēts aizdomās par to, ka tas ir izdarījis nodarījumu, kas ir piederīgs vispārīgiem noziedzīgiem nodarījumiem, tiesai vai neatkarīgajai administratīvajai iestādei, kas ir atbildīga par šo pārbaudi, ir jāatsaka piekļuve, ja šī piekļuve ļautu publiskajai iestādei izdarīt precīzus secinājumus par minētā subjekta privāto dzīvi. Savukārt pat tāda piekļuve, kas sniedz iespēju izdarīt šādus precīzus secinājumus, būtu jāatļauj gadījumos, kad datu subjekts tiek turēts aizdomās par to, ka tas ir izdarījis noziedzīgus nodarījumus, kurus dalībvalsts uzskata par sabiedrības pamatintereses apdraudošiem un tādējādi par tādiem, kas ir pieskaitāmi smagai noziedzībai.

Tiesa arī precizē, ka iepriekšēja pārbaude nekādā gadījumā nedrīkst būt pilnībā automatizēta, jo kriminālizmeklēšanas gadījumā šāda pārbaude prasa, lai ar noziedzības

apkarošanu saistītās leģitīmās intereses tiktu samērotas ar privātās dzīves neaizskaramību un personas datu aizsardzību. Šai samērošanai ir vajadzīga fiziskas personas iesaistīšanās, kura ir vēl jo vairāk nepieciešama tāpēc, ka attiecīgās datu apstrādes automātiskums un plašais vēriens rada privātās dzīves aizskāruma riskus.

Tādējādi Tiesa secina, ka iespēja personām, kurām publiskajā iestādē ir jāpārbauda fakti, sasaistīt IP adresei piesaistītus personas identitātes datus ar datnēm, kurās ir informācija, kas ļauj uzzināt to aizsargāto darbu nosaukumu, kuru publiskošana internetā ir attaisnojusi tiesību īpašnieku organizāciju veikto IP adrešu ievākšanu, ir jāpakārto – gadījumā, kad viena un tā pati persona atkārtoti veic darbību, ar kuru tiek pārkāptas autortiesības vai blakustiesības – tiesas vai neatkarīgas administratīvas iestādes veiktai pārbaudei. Šī pārbaude nedrīkst būt pilnībā automatizēta, un tai jānotiek pirms šādas sasaistīšanas, kas šādos gadījumos var ļaut izdarīt precīzus secinājumus par minētās personas, kuras IP adrese ir tikusi izmantota darbībām, ar kurām iespējami pārkāptas autortiesības vai blakustiesības, privāto dzīvi.

Visbeidzot ceturtām kārtām, Tiesa norāda, ka publiskās iestādes izmantotā datu apstrādes sistēma regulāri jākontrolē ar šo publisko iestādi nesaistītai neatkarīgai struktūrai. Šīs kontroles mērķis ir pārbaudīt sistēmas integritāti, tostarp to, vai tajā ir paredzētas efektīvas garantijas pret ļaunprātīgas vai nelikumīgas piekļuves šiem datiem un šo datu ļaunprātīgas vai nelikumīgas izmantošanas riskiem, kā arī tās efektivitāti un uzticamību iespējamo pārkāpumu konstatēšanai.

Šajā ziņā Tiesa norāda, ka šajā gadījumā personas datu automatizētā apstrāde, ko publiskā iestāde veic, pamatojoties uz tiesību īpašnieku organizāciju konstatēto informāciju par intelektuālā īpašuma tiesību pārkāpumiem, var ietvert zināmu skaitu kļūdaini pozitīvu rezultātu un it īpaši risku, ka trešās personas ļaunprātīgos vai nelikumīgos nolūkos prettiesiski izmantos potenciāli ļoti lielu skaitu personas datu; un šis apstāklis izskaidro šādas pārbaudes nepieciešamību. Tā arī piebilst, ka šai apstrādei ir jāatbilst īpašajiem personas datu aizsardzības noteikumiem, kas paredzēti Direktīvā 2016/680. Proti, šajā gadījumā, pat ja tā sauktās pakāpeniskās reakcijas procedūras ietvaros publiskajai iestādei nav pašai savu lēmumpieņemšanas pilnvaru, tā ir kvalificējama kā “publiska iestāde”, kas iesaistīta noziedzīgu nodarījumu novēršanā un atklāšanā un tādējādi ietilpst šīs direktīvas piemērošanas jomā. Tādējādi šādā procedūrā iesaistītajām personām ir jāsaņem visas Direktīvā 2016/680 noteiktās materiāltiesiskās un procesuālās garantijas; to, vai šīs garantijas ir paredzētas valsts tiesību aktos, pārbauda iesniedzējtiesa.

2. Personas datu apstrāde krimināllietās

2021. gada 12. maija spriedums (virspalāta) Bundesrepublik Deutschland (Interpola sarkanais paziņojums) (C-505/19, EU:C:2021:376)

2012. gadā Starptautiskā kriminālpolicijas organizācija (turpmāk tekstā – "Interpols") pēc Amerikas Savienoto Valstu lūguma, pamatojoties uz šīs valsts iestāžu izsniegtu apcietināšanas orderi, publicēja sarkano paziņojumu par Vācijas pilsoni WS, lai viņš varētu tikt izdots. Ja persona, uz kuru attiecas šāds paziņojums, atrodas Interpola dalībvalstī, šai dalībvalstij principā ir jāveic šīs personas pagaidu aizturēšana vai jāuzrauga vai jāierobežo tās pārvietošanās.

Tomēr pat pirms šā sarkanā paziņojuma publicēšanas Vācijā pret WS tika sākta izmeklēšanas procedūra, kas, pēc iesniedzējtiesas domām, attiecās uz tiem pašiem nodarījumiem kā tie, kuri bija šā paziņojuma pamatā. Šī procedūra tika galīgi pabeigta 2010. gadā pēc tam, kad WS bija samaksājis naudas summu saskaņā ar īpašu izlīguma procedūru, kas paredzēta Vācijas krimināltiesībās. Pēc tam *Bundeskriminalamt* (Federālais kriminālpolicijas birojs, Vācija) informēja Interpolu, ka tas uzskata, ka šīs iepriekšējās procedūras dēļ šajā lietā ir piemērojams princips *ne bis in idem*. Ar šo principu, kas ir nostiprināts gan Konvencijas, ar ko īsteno Šengenas nolīgumu [68], 54. pantā, gan Hartas 50. pantā, it īpaši ir aizliegts atkārtoti saukt pie kriminālatbildības par to pašu nodarījumu personu, attiecībā uz kuru jau ir pasludināts galīgs spriedums.

2017. gadā WS cēla prasību pret Vācijas Federatīvo Republiku *Verwaltungsgericht Wiesbaden* (Vīsbādenes Administratīvā tiesa, Vācija), lai šai dalībvalstij tiktu uzdots veikt vajadzīgos pasākumus šā sarkanā paziņojuma atsaukšanai. Šajā ziņā WS norāda ne tikai uz principa *ne bis in idem* pārkāpumu, bet arī uz LESD 21. pantā viņam garantēto tiesību uz brīvu pārvietošanos pārkāpumu, jo viņš nevarot doties uz valsti, kas ir Šengenas nolīguma līgumslēdzēja valsts vai dalībvalsts, neriskējot tikt aizturēts. Viņš arī uzskata, ka šo pārkāpumu dēļ sarkanajā paziņojumā ietverto viņa personas datu apstrāde ir pretrunā Direktīvai 2016/680 par personas datu aizsardzību krimināllietās [69].

Šādos apstākļos Vīsbādenes Administratīvā tiesa nolēma uzdot Tiesai jautājumu par principa *ne bis in idem* piemērošanu un, precīzāk, par personas, uz kuru attiecas sarkanais paziņojums, pagaidu aizturēšanas iespēju tādā situācijā, kāda ir šajā lietā. Turklāt šā principa piemērojamības gadījumā šī tiesa vēlas noskaidrot, kā tas ietekmē dalībvalstu iespējas veikt šādā paziņojumā ietverto personas datu apstrādi.

---

[68] Konvencija, ar ko īsteno Šengenas nolīgumu (1985. gada 14. jūnijs) starp Beniluksa Ekonomikas savienības valstu valdībām, Vācijas Federatīvās Republikas valdību un Francijas Republikas valdību par pakāpenisku kontroles atcelšanu pie kopīgām robežām (OV 2000, L 239, 19. lpp.; turpmāk tekstā – "KĪŠN").

[69] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV 2016, L 119, 89. lpp.).

Virspalātas sastāvā pasludinātajā spriedumā Tiesa tostarp nosprieda, ka Direktīvas 2016/680 normas, lasot tās saistībā ar KĪŠN 54. pantu un Hartas 50. pantu, ir jāinterpretē tādējādi, ka tās pieļauj tādu personas datu apstrādi, kuri ietverti Interpola izdotā sarkanajā paziņojumā, ja vien ar attiecīgu tiesas nolēmumu netiek konstatēts, ka attiecībā uz nodarījumiem, kas ir šā paziņojuma pamatā, ir piemērojams princips *ne bis in idem*, ja vien šāda apstrāde atbilst šajā direktīvā paredzētajiem nosacījumiem.

Par Interpola sarkanajā paziņojumā iekļautiem personas datiem Tiesa norāda, ka jebkāda darbība ar šiem datiem, piemēram, reģistrācija dalībvalstu datubāzēs, ir "apstrāde", uz ko attiecas Direktīva 2016/680 [70]. Turklāt tā uzskata, pirmkārt, ka šai apstrādei ir leģitīms nolūks un, otrkārt, ka to nevar uzskatīt par nelikumīgu tāpēc vien, ka nodarījumiem, uz ko attiecas sarkanais paziņojums [71], varētu būt piemērojams princips *ne bis in idem*. Turklāt dalībvalstīm var būt jāveic šāda apstrāde tieši tālab, lai pārbaudītu, vai minētais princips ir piemērojams.

Šādos apstākļos Tiesa arī nospriež, ka Direktīva 2016/680, lasot to saistībā ar KĪŠN 54. pantu un Hartas 50. pantu, pieļauj sarkanajā paziņojumā ietvertu personas datu apstrādi, ja vien ar galīgu nolēmumu nav konstatēts, ka šajā lietā ir piemērojams princips *ne bis in idem*. Tomēr šādai apstrādei ir jāatbilst šajā direktīvā paredzētajiem nosacījumiem. Tālab šai apstrādei ir jābūt nepieciešamai valsts kompetento iestāžu uzdevuma izpildei, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un sauktu pie atbildības par tiem vai izpildītu kriminālsodus [72].

Turpretim, ja ir piemērojams princips *ne bis in idem*, reģistrēt dalībvalstu datubāzēs Interpola sarkanajā paziņojumā ietvertus personas datus vairs nav nepieciešams, ņemot vērā, ka attiecīgā persona vairs nav saucama pie atbildības par nodarījumiem, uz kuriem attiecas minētais paziņojums, un līdz ar to – nav aizturama par šiem pašiem nodarījumiem. No tā izriet, ka datu subjektam ir jābūt iespējai lūgt savu datu dzēšanu. Ja tomēr dati tiek glabāti, tiem ir jāpievieno norāde, ka attiecīgo personu vairs nevar saukt pie atbildības dalībvalstī vai līgumslēdzējā valstī par tiem pašiem nodarījumiem saskaņā ar principu *ne bis in idem*.

2022. gada 21. jūnija spriedums (virspalāta) Ligue des droits humains (C-817/19, EU:C:2022:491)

Šajā lietā (skat. arī I.1. sadaļu "Savienības atvasināto tiesību atbilstība tiesībām uz personas datu aizsardzību"), konstatējusi PDR direktīvas spēkā esamību, Tiesa sniedz precizējumus par dažu šīs direktīvas normu interpretāciju [73].

[70] Skat. Direktīvas 2016/680 2. panta 1. punktu un 3. panta 2. punktu.
[71] Skat. Direktīvas 2016/680 4. panta 1. punkta b) apakšpunktu un 8. panta 1. punktu.
[72] Skat. Direktīvas 2016/680 1. panta 1. punktu un 8. panta 1. punktu.
[73] It īpaši PDR direktīvas 2. pants ("[..] [direktīvas] piemērošana ES iekšējiem lidojumiem"), 6. pants ("PDR datu apstrāde") un 12. pants ("Datu glabāšanas termiņš un depersonalizēšana").

Pirmkārt, tā norāda, ka direktīvā ir izsmeļoši uzskaitīti PDR datu apstrādes mērķi. Tādējādi šai direktīvai pretrunā ir tāds valsts tiesiskais regulējums, kurā ir atļauta PDR datu apstrāde citos nolūkos, kas nav cīņa pret teroristu nodarījumiem un smagiem noziegumiem. Tādējādi valsts tiesību aktos, kuros kā PDR datu apstrādes nolūks ir atzīta arī izlūkošanas un drošības dienestu darbība, iespējami netiek ievērots šā uzskaitījuma izsmeļošais raksturs. Tāpat arī ar PDR direktīvā izveidotā sistēma nav izmantojama tālab, lai uzlabotu robežkontroli un cīņu ar nelegālo imigrāciju. No minētā izriet arī, ka PDR datus nevar glabāt vienā datubāzē, ar kuru var iepazīties, lai sasniegtu gan PDR direktīvas mērķus, gan citus mērķus.

Otrkārt, Tiesa izskaidro neatkarīgas valsts iestādes jēdzienu, kurai ir kompetence pārbaudīt, vai PDR datu izpaušanas nosacījumi to vēlākai novērtēšanai ir izpildīti, un apstiprināt šādu izpaušanu. Konkrēti iestādi, kas ir izveidota kā PIN, nevar par tādu uzskatīt, jo tai nav trešās personas statusa attiecībā pret iestādi, kas lūdz piekļuvi datiem. Proti, tā kā tās darbinieki var būt darbinieki, kurus ir norīkojušas darbā iestādes, kam ir tiesības lūgt šādu piekļuvi, PIN visdrīzāk noteikti ir saistīta ar šīm iestādēm. Tādējādi PDR direktīvai pretrunā ir tāds valsts tiesiskais regulējums, saskaņā ar kuru iestādei, kas ir izveidota kā PIN, ir arī valsts kompetentās iestādes statuss, kura ir pilnvarota apstiprināt PDR datu izpaušanu sešus mēnešus pēc šo datu nosūtīšanas PIN.

Treškārt, attiecībā uz PDR datu glabāšanas termiņu Tiesa nospriež, ka PDR direktīvas 12. pantam, skatītam Hartas 7. un 8. panta, kā arī 52. panta 1. punkta gaismā, ir pretrunā valsts tiesiskais regulējums, kurā paredzēts vispārējais šo datu glabāšanas termiņš pieci gadi, kas ir vienādi piemērojams visiem aviopasažieriem.

Proti, Tiesas ieskatā pēc sākotnējā sešu mēnešu glabāšanas termiņa beigām PDR datu glabāšana visdrīzāk neaprobežojas ar absolūti nepieciešamo, ja tie attiecas uz aviopasažieriem, par kuriem ne iepriekšējais vērtējums, ne iespējamā sākotnējā sešu mēnešu glabāšanas laikā veiktās pārbaudes, ne jebkāds cits apstāklis nav atklājis, ka pastāvētu objektīvi elementi – piemēram, tas, ka attiecīgo pasažieru PDR dati ir snieguši pozitīvu atbilsmi, kas pārbaudīta iepriekšējā novērtējumā –, kuri varētu radīt teroristu nodarījumu vai smagu noziegumu risku, kam būtu objektīva, kaut arī netieša saikne ar šo pasažieru veikto avioceļojumu. Turpretī Tiesa uzskata, ka sākotnējā sešu mēnešu perioda laikā visu aviopasažieru, uz kuriem attiecas ar šo direktīvu izveidotā sistēma, PDR datu glabāšana principā nepārsniedz to, kas ir absolūti nepieciešams.

Ceturtkārt, Tiesa sniedz norādes par PDR direktīvas iespējamo piemērošanu – teroristu nodarījumu un smagu noziegumu apkarošanas nolūkā – attiecībā uz citiem pasažieru transportēšanas veidiem Savienībā. Direktīvai, skatītai kopsakarā ar LES 3. panta 2. punktu, LESD 67. panta 2. punktu un Hartas 45. pantu, ir pretrunā tādu PDR datu pārsūtīšanas un apstrādes sistēma, kas attiecas uz visiem pārvadājumiem, kas veikti Savienības iekšienē ar citiem līdzekļiem, ja nav reālu un aktuālu vai paredzamu terorisma draudu, ar kuriem sastapusies attiecīgā dalībvalsts. Šādā situācijā, tāpat kā ES iekšējo lidojumu gadījumā, ar PDR direktīvu izveidotā sistēma ir jāpiemēro tikai PDR datiem par pārvadājumiem, kas attiecas it īpaši uz atsevišķiem savienojumiem vai

ceļojumu plāniem vai arī noteiktām stacijām vai ostām, par kurām pastāv norādes, kas pamato šo piemērošanu. Attiecīgajai dalībvalstij ir jāizvēlas pārvadājumi, attiecībā uz kuriem šādas norādes pastāv, un regulāri jāpārskata šī piemērošana atkarībā no to nosacījumu attīstības, kuri ir bijuši to izvēles pamatā.

IV. Personas datu nosūtīšana uz trešām valstīm

2003. gada 6. novembra spriedums (virspalāta) Lindqvist (C-101/01, EU:C:2003:596)

Šajā lietā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"") iesniedzējtiesa vēlējās it īpaši uzzināt, vai *B. Lindqvist* bija veikusi datu pārsūtīšanu uz trešām valstīm PDR direktīvas izpratnē.

Tiesa nosprieda, ka "personas datu pārsūtīšana uz trešajām valstīm" Direktīvas 95/46 25. panta izpratnē nepastāv, ja persona, kas atrodas dalībvalstī, interneta mājaslapā, kura tiek glabāta pie fiziskas vai juridiskas personas, kas uztur tīmekļvietni, no kuras var piekļūt mājaslapai un kura ir izveidota šajā pašā valstī vai citā dalībvalstī, ievada personas datus, tos tādējādi padarot pieejamus ikvienai personai, kas ir pieslēgusies internetam, tostarp personām, kuras atrodas trešās valstīs.

Ņemot vērā, pirmkārt, interneta attīstības pakāpi Direktīvas 95/46 izstrādes laikā un, otrkārt, to, ka tās IV nodaļā, kur ir ietverts 25. pants, kura mērķis ir nodrošināt dalībvalstu kontroli par personas datu pārsūtīšanu trešām valstīm un aizliegt šādu pārsūtīšanu, ja tās nenodrošina atbilstošu aizsardzības līmeni, nav paredzēti kritēriji par interneta lietošanu, nevar prezumēt, ka Kopienu likumdevējam būtu bijis nolūks nākotnē iekļaut jēdzienā "datu pārsūtīšana uz trešajām valstīm" šādu datu ievadīšanu interneta mājaslapā, pat ja tādējādi šie dati ir padarīti pieejami trešo valstu personām, kuru rīcībā ir tehniskie līdzekļi, lai tiem piekļūtu.

2015. gada 6. oktobra spriedums (virspalāta) Schrems (C-362/14, EU:C:2015:650)

M. Schrems, Austrijas valstspiederīgais un sociālā tīkla *Facebook* lietotājs, bija iesniedzis sūdzību *Data Protection Commissioner* (datu aizsardzības komisārs, Īrija) par to, ka *Facebook Ireland* savu lietotāju personas datus pārsūta uz Amerikas Savienotajām Valstīm un tos saglabā serveros, kas atrodas šajā valstī, kur tiek veikta šo datu apstrāde. Saskaņā ar *M. Schrems* viedokli ASV tiesības un prakse nenodrošina pienācīgu aizsardzības līmeni pret uzraudzību, ko veic valsts iestādes attiecībā uz šo valsti

pārsūtītajiem datiem. *Data Protection Commissioner* atteicās izskatīt šo sūdzību, to pamatojot īpaši ar to, ka Komisija Lēmumā 2000/520/EK [74] uzskatīja, ka tā dēvētās "drošības zonas" (angļu val. "safe harbour") [75] shēmas ietvaros ASV pārsūtītajiem personas datiem tiek nodrošināts pienācīgs aizsardzības līmenis.

Šajā kontekstā *High Court* (Augstā tiesa, Īrija) lūdza Tiesu interpretēt Direktīvas 95/46 25. panta 6. punktu, saskaņā ar kuru Komisija var atzīt, ka trešā valsts nodrošina pārsūtīto datu pienācīgu aizsardzības līmeni, kā arī būtībā uzdeva jautājumu par Lēmuma 2000/520, kuru Komisija pieņēma, pamatojoties uz minēto Direktīvas 95/46 25. panta 6. punktu, spēkā esamību.

Tiesa Komisijas lēmumu atzina par spēkā neesošu kopumā, uzsverot, pirmkārt, ka tā pieņemšanai bija nepieciešams Komisijas pienācīgi pamatots secinājums, ka attiecīgā trešā valsts faktiski nodrošina tādu pamattiesību aizsardzības līmeni, kas būtībā ir līdzvērtīgs tam, kāds tiek garantēts Savienības tiesību sistēmā. Taču, tā kā Komisija savā Lēmumā 2000/520 to nav darījusi, šā lēmuma 1. pantā nav ievērotas Direktīvas 95/46 25. panta 6. punktā, to lasot kopā ar Hartu, noteiktās prasības un tādēļ tas nav spēkā. Šos "drošības zonas" principus piemēro tikai pašsertificētām ASV organizācijām, kas personas datus saņem no Savienības, neizvirzot prasību, lai ASV iestādes minētos principus ievērotu. Turklāt ar Lēmumu 2000/520 ir radīta iespēja iejaukties to personu pamattiesībās, kuru personas dati ir vai var tikt pārsūtīti no Savienības uz ASV, un tajā nav secinājuma par to, ka ASV ir spēkā valsts tiesību akti, kuru mērķis ir ierobežot iespējamo iejaukšanos šajās pamattiesībās, un nav runas par efektīvas tiesiskās aizsardzības pret šāda veida iejaukšanos esamību.

Turklāt Tiesa atzina par spēkā neesošu Lēmuma 2000/520 3. pantu, ciktāl ar to valsts uzraudzības iestādēm tiek atņemtas kontroles pilnvaras, kas tām atbilstoši Direktīvas 95/46 28. pantam ir piešķirtas gadījumā, kad persona izvirza apsvērumus, ar kuriem var tikt apšaubīts tāda Komisijas lēmuma saderīgums ar privātās dzīves neaizskaramības un personu pamatbrīvību un pamattiesību aizsardzību, kurā ir konstatēts, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni. Tiesa secināja, ka Lēmuma 2000/520 1. un 3. panta spēkā neesamības rezultātā spēku zaudē arī lēmums kopumā.

Attiecībā uz neiespējamību pamatot šādu iejaukšanos Tiesa vispirms norādīja, ka Savienības tiesību aktā, kurā ir ietverta iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās, ir jāparedz skaidri un precīzi noteikumi, kas reglamentētu pasākuma apjomu un piemērošanu un noteiktu minimālās prasības tādējādi, lai personām, kuru personas dati ir tikuši skarti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu

[74] Komisijas Lēmums 2000/520/EK (2000. gada 26. jūlijs) atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija (OV 2000, L 215, 7. lpp.).

[75] "Drošības zonas" shēma ietver virkni personas datu aizsardzības principu, kurus ASV uzņēmumi var brīvprātīgi apņemties ievērot.

piekļuvi šiem datiem un to nelikumīgu izmantošanu. Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves risks šiem datiem.

Turklāt un galvenokārt pamattiesību uz privātās dzīves neaizskaramību aizsardzībai Savienības līmenī pamatā ir prasība, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti absolūti nepieciešamā ietvaros. Tādējādi ar absolūti nepieciešamo neaprobežojas tāds tiesiskais regulējums, saskaņā ar kuru vispārīgi tiek pieļauta visu to personu personas datu saglabāšana, kuru dati no Savienības ir pārsūtīti – nešķirojot, bez ierobežojumiem vai izņēmumiem saistībā ar mērķi, kam tie kalpo, vai neparedzot objektīvus kritērijus, kas valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu ļauj ierobežot precīziem, stingri ierobežotiem un tādiem mērķiem, kas pamato iejaukšanos, ar kuru ir saistīta gan piekļuve šiem datiem, gan arī to izmantošana. It īpaši tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam, apdraud pamattiesību uz privātās dzīves neaizskaramību būtību. Tāpat tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu, nav ņemta vērā Hartas 47. pantā iedibināto pamattiesību uz efektīvu tiesību aizsardzību tiesā būtība.

2017. gada 26. jūlija atzinums 1/15 (ES un Kanādas PDR nolīgums) (virspalāta) (EU:C:2017:592)

Tiesa 2017. gada 26. jūlijā pirmoreiz sprieda par starptautiska nolīguma projekta saderīgumu ar Hartu un it īpaši ar noteikumiem, kas saistīti ar privātās dzīves neaizskaramību, kā arī personas datu aizsardzību.

Eiropas Savienība un Kanāda vienojās par nolīgumu attiecībā uz pasažieru datu reģistra datu pārsūtīšanu un apstrādi (PDR nolīgums), kas tika parakstīts 2014. gadā. Kad Eiropas Savienības Padome aicināja Eiropas Parlamentu to apstiprināt, tas nolēma vērsties Tiesā ar jautājumu, vai paredzētais nolīgums ir saderīgs ar Savienības tiesībām.

Paredzētais nolīgums pieļauj sistemātisku un pastāvīgu visu aviopasažieru PDR datu pārsūtīšanu kādai Kanādas iestādei, lai tos izmantotu un saglabātu, kā arī iespējami pārsūtītu tālāk citām iestādēm un citām trešām valstīm, lai cīnītos pret terorismu un smagiem starptautiskiem noziegumiem. Šim nolūkam paredzētajā nolīgumā tostarp ir noteikta datu uzglabāšana piecus gadus un ir noteiktas īpašas prasības attiecībā uz drošību un PDR integritāti, piemēram, tūlītēja sensitīvu datu maskēšana, tāpat tajā ir paredzētas tiesības uz piekļuvi datiem, to labošanu un dzēšanu un iespēja izmantot tiesību aizsardzību administratīvā kārtībā vai tiesā.

Paredzētajā nolīgumā minētie PDR dati tostarp ietver ne tikai aviopasažiera vai aviopasažieru vārdus un uzvārdus, bet arī rezervācijai vajadzīgo informāciju, piemēram, paredzētā ceļojuma datumus un ceļojuma maršrutu, informāciju par biļetēm, personu grupas, kas ir reģistrētas ar vienu un to pašu rezervācijas numuru, informāciju par

maksāšanas līdzekļiem vai rēķiniem, informāciju par bagāžu, kā arī vispārējas piezīmes par pasažieriem.

Atzinumā Tiesa nosprieda, ka PDR nolīgumu nevar noslēgt tā pašreizējā formā, jo daži tā noteikumi nav saderīgi ar Savienības atzītām pamattiesībām.

Tiesa vispirms konstatēja, ka gan PDR datu pārsūtīšana no Savienības Kanādas kompetentajai iestādei, gan Savienības un Kanādas nolīgtā kārtība par nosacījumiem attiecībā uz šo datu saglabāšanu, izmantošanu, kā arī to iespējamo vēlāku pārsūtīšanu citām Kanādas iestādēm, Eiropolam, *Eurojust*, dalībvalstu tiesu vai policijas iestādēm vai arī citu trešo valstu iestādēm ir iejaukšanās Hartas 7. pantā garantētajās tiesībās. Šīs darbības ir arī iejaukšanās Hartas 8. pantā garantētajās pamattiesībās uz personas datu aizsardzību, jo tās ietver personas datu apstrādi.

Turklāt tā uzsver, ka, lai arī daži PDR dati, aplūkoti atsevišķi, nešķiet esam tādi, kas varētu atklāt būtisku informāciju par attiecīgo personu privāto dzīvi, tas nemaina faktu, ka, aplūkoti kopā, minētie dati var atklāt tostarp pilnīgu ceļojuma maršrutu, ceļošanas paradumus, esošās attiecības starp divām vai vairākām personām, kā arī informāciju par aviopasažieru finansiālo stāvokli, viņu ēšanas paradumiem vai veselības stāvokli, un tie pat varētu sniegt par šiem pasažieriem sensitīvu informāciju, kas ir definēta paredzētā nolīguma 2. panta e) punktā (informācija, kas atklāj rases vai etnisko izcelsmi, politiskos uzskatus, reliģisko pārliecību u.c.).

Šajā ziņā Tiesa uzskatīja, ka, lai gan attiecīgā iejaukšanās varētu būt attaisnojama ar vēlmi sasniegt sabiedrības vispārējo interešu mērķi (lai nodrošinātu sabiedrisko drošību cīņā pret teroristu nodarījumiem un smagiem starptautiskiem noziegumiem), vairāki nolīguma noteikumi nav ierobežoti absolūti nepieciešamā apmērā un neparedz skaidrus un precīzus noteikumus.

It īpaši Tiesa norādīja, ka, ņemot vērā diskriminācijas aizlieguma principam pretējas datu apstrādes risku, sensitīvu datu pārsūtīšanai uz Kanādu būtu vajadzīgs precīzs un īpaši stingrs pamatojums, kas balstīts uz citiem pamatiem, nevis sabiedrības drošības aizsardzību pret terorismu un smagiem starptautiskiem noziegumiem. Taču šajā gadījumā šāda pamatojuma nav. Tādējādi Tiesa secināja, ka nolīguma noteikumi par sensitīvu datu pārsūtīšanu uz Kanādu, kā arī šo datu apstrādi un saglabāšanu nav saderīgi ar pamattiesībām.

Otrkārt, Tiesa uzskatīja, ka visu aviopasažieru PDR datu pastāvīga uzglabāšanu pēc viņu izceļošanas no Kanādas, kas ir atļauta nolīgumā, neaprobežojas ar absolūti nepieciešamo. Runājot par aviopasažieriem, saistībā ar kuriem terorisma vai smagu starptautisko noziegumu risks nav identificēts, kad viņi ieradušies Kanādā un līdz viņu izceļošanai no šīs valsts, nešķiet, ka pēc viņu izceļošanas būtu kāda saikne, kaut vai netieša, starp viņu PDR datiem un paredzētajā nolīgumā izvirzīto mērķi, kas pamatotu šo datu saglabāšanu. Turpretī, ja tiek konstatētas objektīvas pazīmes, kas liecina, ka noteikti aviopasažieri pat pēc izceļošanas no Kanādas varētu radīt risku saistībā ar cīņu pret

terorismu un smagiem starptautiskiem noziegumiem, ir pieļaujama viņu PDR datu uzglabāšana pēc viņu uzturēšanās Kanādā, pat piecu gadu periodā.

Treškārt, Tiesa konstatēja, ka pamattiesības uz privātās dzīves neaizskaramību, kas ir garantētas Hartas 7. pantā, nozīmē, ka attiecīgā persona var pārliecināties, ka tās personas dati ir apstrādāti pareizi un likumīgi. Lai varētu veikt vajadzīgās pārbaudes, šai personai ir jābūt tiesībām iepazīties ar datiem, kas uz to attiecas un kas tiek apstrādāti.

Šajā ziņā tā uzsvēra, ka paredzētajā nolīgumā ir svarīgi, lai aviopasažieri tiktu informēti par viņu PDR datu pārsūtīšanu uz attiecīgo trešo valsti un šo datu izmantošanu no brīža, kad šāda izpaušana nevar traucēt paredzētajā nolīgumā minēto valsts iestāžu veiktajai izmeklēšanai. Šāda informācija izrādās faktiski nepieciešama, lai aviopasažieriem dotu iespēju izmantot savas tiesības pieprasīt piekļuvi datiem, kas uz viņiem attiecas, un vajadzības gadījumā lūgt izdarīt tajos labojumus, kā arī izmantot tiesības uz efektīvu tiesību aizsardzību tiesā saskaņā ar Hartas 47. panta pirmo daļu.

Līdz ar to gadījumos, kad ir objektīvas pazīmes, kas pamato pasažieru datu izmantošanu, lai cīnītos pret terorismu un smagiem starptautiskiem noziegumiem, un tiek prasīta tiesas vai neatkarīgas administratīvas iestādes iepriekšēja atļauja, aviopasažieru individuāla informēšana ir nepieciešama. Tas pats attiecas uz gadījumiem, kad aviopasažieru PDR dati tiek izpausti citām valsts iestādēm vai privātpersonām. Taču šādai informēšanai ir jānotiek tikai no brīža, kad tā nevar traucēt izmeklēšanai, kuru veic paredzētajā nolīgumā minētās valsts iestādes.

2020. gada 16. jūlija spriedums (virspalāta) Facebook Ireland un Schrems (C-311/18, EU:C:2020:559)

VDAR ir noteikts, ka personas datu nosūtīšana uz trešām valstīm principā var notikt tikai tad, ja attiecīgā trešā valsts nodrošina pietiekamu šo datu aizsardzības līmeni. Saskaņā ar šo regulu Komisija var konstatēt, ka trešā valsts, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tā uzņēmusies, nodrošina pietiekamu aizsardzības līmeni [76]. Ja nav šāda lēmuma par aizsardzības līmeņa pietiekamību, minēto pārsūtīšanu drīkst veikt tikai tad, ja Savienībā reģistrētais personas datu nosūtītājs sniedz atbilstošas garantijas, kas tostarp var izpausties kā Komisijas pieņemtas datu aizsardzības standartklauzulas, un ja datu subjektiem tiek nodrošinātas īstenojamas tiesības un efektīvi tiesiskās aizsardzības līdzekļi [77]. Turklāt VDAR ir ietverti precīzi nosacījumi, ar kādiem šāda pārsūtīšana var notikt, ja nav lēmuma par aizsardzības līmeņa pietiekamību vai atbilstošu garantiju [78].

[76] VDAR 45. pants.
[77] VDAR 46. panta 1. punkts un 2. punkta c) apakšpunkts.
[78] VDAR 49. pants.

Maximillian Schrems, Austrijā dzīvojošs šīs pašas valsts pilsonis, ir *Facebook* lietotājs kopš 2008. gada. *M. Schrems*, gluži kā pārējo Savienībā dzīvojošo lietotāju, personas datus vai daļu no tiem *Facebook Ireland* pārsūta uz *Facebook Inc*. serveriem, kas atrodas ASV teritorijā, kur tie tiek apstrādāti. *M. Schrems* vērsās ar sūdzību Īrijas uzraudzības iestādē, būtībā vēloties panākt šīs nosūtīšanas aizliegumu. Viņš apgalvoja, ka ASV tiesiskais regulējums un prakse nenodrošina uz šo valsti nosūtīto personas datu pietiekamu aizsardzību pret publisko iestāžu piekļuvi. Šī sūdzība tika noraidīta, pamatojoties konkrēti uz to, ka Komisija Lēmumā 2000/520 [79] bija konstatējusi, ka ASV nodrošina pietiekamu aizsardzības līmeni. Ar 2015. gada 6. oktobra spriedumu Tiesa, atbildot uz *High Court* (Augstā tiesa, Īrija) uzdoto prejudiciālo jautājumu, atzina šo lēmumu par spēkā neesošu (turpmāk tekstā – "spiedums *Schrems I*") [80].

Pēc sprieduma *Schrems I* pasludināšanas un tam sekojošās lēmuma, ar ko tika noraidīta *M. Schrems* sūdzība, atcelšanas Īrijas tiesā Īrijas uzraudzības iestāde aicināja viņu pārformulēt savu sūdzību, ņemot vērā, ka Tiesa Lēmumu 2000/520 bija atzinusi par spēkā neesošu. Pārformulētajā sūdzībā *M. Schrems* uzskata, ka ASV nenodrošina uz šo valsti pārsūtīto datu pietiekamu aizsardzību. Viņš lūdz nākotnē apturēt vai aizliegt viņa personas datu pārsūtīšanu no Savienības uz ASV, ko *Facebook Ireland* pašlaik veic, pamatojoties uz Lēmuma 2010/87/ES [81] pielikumā ietvertajām aizsardzības standartklauzulām. Uzskatīdama, ka *M. Schrems* sūdzības risinājums tostarp ir atkarīgs no Lēmuma 2010/87 spēkā esamības, Īrijas uzraudzības iestāde uzsāka procedūru *High Court* (Augstā tiesa), lai tā vērstos Tiesā ar lūgumu sniegt prejudiciālu nolēmumu. Pēc tam, kad šī procedūra bija sākta, Komisija pieņēma Lēmumu (ES) 2016/1250 par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs [82].

Ar lūgumu sniegt prejudiciālu nolēmumu iesniedzējtiesa vaicā Tiesai par VDAR piemērojamību tādai personas datu pārsūtīšanai, kas pamatota ar Lēmumā 2010/87 ietvertajām aizsardzības standartklauzulām, par šajā regulā prasīto aizsardzības līmeni šādai pārsūtīšanai un par uzraudzības iestāžu pienākumiem šajā ziņā. *High Court* arī izvirza jautājumu gan par Lēmuma 2010/87, gan Lēmuma 2016/1250 spēkā esamību.

Tiesa konstatē, ka Lēmuma 2010/87 pārbaudē – attiecībā pret Hartu – nav atklājies neviens elements, kas ietekmētu tā spēkā esamību. Taču Lēmumu 2016/1250 tā atzīst par spēkā neesošu.

Vispirms Tiesa norāda, ka Savienības tiesības, it īpaši VDAR, ir piemērojamas personas datu pārsūtīšanai komerciālos mērķos, ko veicis dalībvalstī reģistrēts tirgus dalībnieks

---

[79] Komisijas lēmums (2000. gada 26. jūlijs) atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem[,] un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija (OV 2000, L 215, 7. lpp.).

[80] Tiesas spriedums, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650.

[81] Komisijas lēmums (2010. gada 5. februāris) par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (OV 2010, L 39, 5. lpp.), kas grozīta ar Komisijas Īstenošanas lēmumu (ES) 2016/2297 (2016. gada 16. decembris) (OV 2016, L 344, 100. lpp.).

[82] Komisijas īstenošanas lēmums (2016. gada 12. jūlijs) saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs (OV 2016, L 207, 1. lpp.).

citam, trešā valstī reģistrētam tirgus dalībniekam, pat ja šīs pārsūtīšanas laikā vai pēc tam šos datus sabiedrības drošības, aizsardzības un valsts drošības nolūkos var apstrādāt attiecīgās trešās valsts publiskās iestādes. Tā precizē, ka šāda veida datu apstrāde, ko veic trešās valsts iestādes, šādu pārsūtīšanu neizslēdz no VDAR piemērošanas jomas.

Attiecībā uz šādai pārsūtīšanai nepieciešamo aizsardzības līmeni Tiesa atzīst, ka VDAR normās šajā ziņā paredzētās prasības, kas saistītas ar atbilstošām garantijām, īstenojamām tiesībām un efektīviem tiesību aizsardzības līdzekļiem, ir jāinterpretē tādējādi, ka to personu tiesībām, kuru personas dati tiek pārsūtīti uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām, ir jāpiemēro būtībā līdzvērtīgs aizsardzības līmenis tam, kāds ir garantēts Savienībā ar šo regulu, lasot to kopā ar Hartu. Šādā kontekstā tā precizē, ka, izvērtējot šo aizsardzības līmeni, ir jāņem vērā gan līguma noteikumi, par kuriem ir panākta vienošanās starp Savienībā reģistrēto datu nosūtītāju un attiecīgajā trešā valstī reģistrēto pārsūtīto datu saņēmēju, gan arī – attiecībā uz šīs trešās valsts publisko iestāžu iespējamo piekļuvi šādi nosūtītajiem datiem – šīs trešās valsts tiesību sistēmas atbilstošie elementi.

Attiecībā uz uzraudzības iestāžu pienākumiem šādas pārsūtīšanas kontekstā Tiesa nospriež – ja vien Komisija nav juridiski pamatoti pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, šīm iestādēm ir pienākums apturēt vai aizliegt personas datu pārsūtīšanu uz trešo valsti, ja tās, ņemot vērā visus ar šo pārsūtīšanu saistītos apstākļus, uzskata, ka datu aizsardzības standartklauzulas šajā trešā valstī netiek vai nevar tikt ievērotas un ka Savienības tiesībās prasīto pārsūtīto datu aizsardzību nav iespējams nodrošināt ar citiem līdzekļiem, ja Savienībā reģistrētais datu nosūtītājs pats nav apturējis vai izbeidzis pārsūtīšanu.

Turpinājumā Tiesa izvērtē Lēmuma 2010/87 spēkā esamību. Tiesa norāda, ka šī lēmuma spēkā esamību neietekmē tikai tas vien, ka tajā ietvertās datu aizsardzības standartklauzulas to līgumiskā rakstura dēļ nav saistošas tādu trešo valstu iestādēm, uz kurām personas dati var tikt pārsūtīti. Šī spēkā esamība turpretim ir atkarīga no tā, vai minētais lēmums ietver efektīvus mehānismus, kas praksē ļauj nodrošināt, ka tiek ievērots Savienības tiesībās prasītais aizsardzības līmenis un ka pamatojoties uz šīm klauzulām īstenotā personas datu pārsūtīšana šo klauzulu pārkāpuma gadījumā tiek apturēta vai aizliegta. Tiesa konstatē, ka Lēmumā 2010/87 šādi mehānismi ir ietverti. Šajā ziņā tā jo īpaši uzsver, ka ar minēto lēmumu datu nosūtītājam un to saņēmējam ir noteikts pienākums vispirms pārbaudīt, vai attiecīgajā trešā valstī ir ievērots šis aizsardzības līmenis, un saņēmējam ir noteikts pienākums informēt datu nosūtītāju, ka tas, iespējams, nevarēs izpildīt aizsardzības standartklauzulu prasības un nosūtītājam tādējādi ir pienākums apturēt datu pārsūtīšanu un/vai izbeigt ar saņēmēju noslēgto līgumu.

Visbeidzot Tiesa veic Lēmuma 2016/1250 spēkā esamības pārbaudi saistībā ar prasībām, kas izriet no VDAR, lasot tās to Hartas normu kontekstā, kurās garantēta privātās un ģimenes dzīves neaizskaramība, personas datu aizsardzība un tiesības uz efektīvu

tiesību aizsardzību tiesā. Šajā ziņā Tiesa norāda, ka minētajā lēmumā, gluži kā Lēmumā 2000/520, ir iedibināts ar valsts drošību, sabiedrības interesēm un ASV tiesiskā regulējuma ievērošanu saistīto prasību pārākums, tādējādi padarot iespējamu iejaukšanos to personu pamattiesībās, kuru dati tiek pārsūtīti uz šo trešo valsti. Tiesa norāda, ka personas datu aizsardzības ierobežojumi, kuri izriet no ASV tiesiskā regulējuma par ASV publisko iestāžu piekļuvi no Savienības uz trešo valsti pārsūtītiem personas datiem un šādu datu izmantošanu un kurus Komisija ir izvērtējusi Lēmumā 2016/1250, nav formulēti tādā veidā, lai atbilstu prasībām, kas būtībā ir līdzvērtīgas tām, kuras Savienības tiesībās ir izvirzītas ar samērīguma principu, jo uz šo tiesisko regulējumu balstītās uzraudzības programmas neaprobežojas ar absolūti nepieciešamo. Pamatodamās uz šajā lēmumā ietvertajiem konstatējumiem, Tiesa norāda, ka attiecībā uz atsevišķām uzraudzības programmām no minētā tiesiskā regulējuma nekādā veidā neizriet, ka pastāvētu tajā paredzētie pilnvaru ierobežojumi attiecībā uz šo uzraudzības programmu īstenošanu, ne arī garantiju esamība personām, kuras nav ASV pilsoņi un kuras potenciāli skar šīs programmas. Tiesa piebilst – lai gan šajā pašā tiesiskajā regulējumā ir paredzētas prasības, kuras ASV iestādēm ir jāievēro, īstenojot attiecīgās uzraudzības programmas, tomēr tajā datu subjektiem nav piešķirtas tiesības, kuras tās varētu īstenot tiesās pret ASV iestādēm.

Attiecībā uz aizsardzību tiesā Tiesa nospriež, ka – pretēji Komisijas paustajam Lēmumā 2016/1250 – ar šo lēmumu izveidotajā ombuda mehānismā nav paredzēti iestādē izmantojami tiesību aizsardzības līdzekļi, kas sniegtu garantijas, kuras būtībā ir līdzvērtīgas Savienības tiesībās prasītajām, lai nodrošinātu gan šajā mehānismā paredzēto ombuda neatkarību, gan to, ka pastāv normas, kas pilnvaro šo ombudu pieņemt ASV izlūkdienestiem saistošus lēmumus. Visu šo iemeslu dēļ Tiesa Lēmumu 2016/1250 pasludina par spēkā neesošu.

V. Personas datu aizsardzība internetā

1. Tiesības iebilst pret personas datu apstrādi (“tiesības tikt aizmirstam”)

2014. gada 13. maija spriedums (virspalāta) Google Spain un Google (C-131/12, EU:C:2014:317)

Šajā spriedumā (skat. arī II.1. sadaļu “Vispārējā tiesiskā regulējuma piemērošanas joma” un II.3. sadaļu “Jēdziens “personas datu apstrāde””) Tiesa precizēja, kāds tvērums ir Direktīvā 95/46 paredzētajām tiesībām piekļūt internetā publicētiem personas datiem un tiesībām iebilst pret šādu datu apstrādi.

Tādējādi, lemjot par jautājumu attiecībā uz interneta meklētājprogrammas pakalpojumu sniedzēja atbildības apjomu, Tiesa būtībā nosprieda, ka, lai ievērotu piekļuves tiesības un tiesības iebilst pret personas datu apstrādi, kas ir garantētas Direktīvas 95/46 12. panta b) punktā un 14. panta pirmās daļas a) punktā, un ja šajos pantos minētie nosacījumi ir izpildīti, tam konkrētos apstākļos ir jāizdzēš no rezultātu saraksta – kas parādās tad, ja ir veikts meklējums pēc personas vārda – saites uz tīmekļa lapām, kuras ir publicējušas trešās personas un kurās ir informācija saistībā ar šo personu. Tiesa precizēja, ka šāds pienākums var pastāvēt arī gadījumā, ja šis vārds vai šī informācija nav iepriekš vai vienlaicīgi tikusi izdzēsta no šīm tīmekļa lapām, attiecīgajā gadījumā – pat ja to publicēšana šajās lapās ir likumīga.

Turklāt, atbildot uz jautājumu, vai direktīva ļauj datu subjektam lūgt, lai saites uz tīmekļa mājaslapām tiktu dzēstas no šāda rezultātu saraksta, pamatojoties uz viņa vēlēšanos, lai tajās ietvertā informācija par viņa personu pēc noteiktā laika "tiktu aizmirsta", Tiesa vispirms norāda, ka pat sākotnēji likumīga pareizu datu apstrāde ar laiku var kļūt nesaderīga ar šo direktīvu, ja šie dati vairs nav nepieciešami saistībā ar mērķiem, kādēļ tie tikuši ievākti vai apstrādāti. Tā it īpaši ir gadījumā, ja tie izrādās neadekvāti, neatbilstoši vai vairs neatbilstoši, vai pārmērīgi saistībā ar šiem mērķiem vai ar pagājušo laiku. Līdz ar to, ja pēc datu subjekta lūguma tiek konstatēts, ka šo saišu iekļaušana sarakstā pašreizējā stadijā ir nesaderīga ar direktīvu, tad informācija un saites, kas ir iekļautas šajā sarakstā, ir jāizdzēš. Šajā kontekstā konstatācija, saskaņā ar kuru datu subjektam ir tiesības, lai informācija, kas saistīta ar tā personu, vairs netiktu saistīta ar tā vārdu ar rezultātu saraksta palīdzību, nenozīmē, ka šādas attiecīgās informācijas iekļaušana rezultātu sarakstā rada kaitējumu datu subjektam.

Visbeidzot Tiesa precizēja, ka, tā kā datu subjekts, ņemot vērā tā pamattiesības atbilstoši Hartas 7. un 8. pantam, var lūgt, lai attiecīgā informācija vairs netiktu sniegta plašai sabiedrībai, to iekļaujot šādā rezultātu sarakstā, šīs tiesības principā ir svarīgākas ne tikai par meklētājprogrammas pakalpojumu sniedzēja ekonomisko interesi, bet arī šīs sabiedrības interesi atrast šo informāciju, veicot meklēšanu, izmantojot šīs personas vārdu. Tomēr tas tā nebūtu gadījumā, ja tādu īpašu iemeslu dēļ kā minētās personas loma sabiedriskajā dzīvē izrādītos, ka iejaukšanās tās pamattiesībās ir attaisnota ar īpašām minētās sabiedrības interesēm saņemt piekļuvi attiecīgajai informācijai, pateicoties šai iekļaušanai.

2. Personas datu apstrāde un intelektuālā īpašuma tiesības

2008. gada 29. janvāra spriedums (virspalāta) Promusicae (C-275/06, EU:C:2008:54)

Promusicae, Spānijas bezpeļņas asociācija, kas apvieno mūzikas ierakstu, kā arī audiovizuālo ierakstu producentus un izdevējus, bija vērsusies Spānijas tiesās, lai tās noteiktu pienākumu *Telefónica de España SAU* (komercsabiedrība, kura tostarp sniedz

piekļuves internetam pakalpojumus) atklāt atsevišķu personu, kam tā nodrošina piekļuvi internetam un kam ir zināma IP adrese, kā arī pievienošanās datums un laiks, identitāti un faktisko adresi. Kā norāda *Promusicae*, šīs personas izmanto arhīvu apmaiņas programmu, sauktu "peer-to-peer" jeb "P2P" (kas ir pārskatāms līdzeklis, kā dalīties ar saturu; tas ir neatkarīgs un decentralizēts, un tam ir paplašinātas meklēšanas un lejuplādēšanas funkcijas), kas ļauj to personālā datora kopīgajā direktorijā piekļūt fonogrammām, kuru izmantošanas īpašumtiesības ir *Promusicae* biedriem. Tā līdz ar to lūdza sniegt minēto informāciju, lai varētu uzsākt civilo tiesvedību pret attiecīgajām personām.

Šajos apstākļos *Juzgado de lo Mercantil no 5 de Madrid* (Madrides Komerctiesa Nr. 5, Spānija) uzdeva Tiesai jautājumu, vai Eiropas tiesību akti, lai nodrošinātu autortiesību efektīvu aizsardzību, noteic dalībvalstīm pienākumu paziņot personas datus civilā tiesvedībā.

Tiesa uzskata, ka minētais lūgums sniegt prejudiciālu nolēmumu izvirza jautājumu par nepieciešamību saskaņot prasības attiecībā uz dažādu pamattiesību aizsardzību, proti, pirmkārt, tiesību uz privātās dzīves neaizskaramību un, otrkārt, tiesību uz īpašuma aizsardzību un efektīvu tiesību aizsardzību.

Šajā ziņā Tiesa secināja, ka Direktīva 2000/31/EK par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) [83], Direktīva 2001/29/EK par dažu autortiesību un blakustiesību aspektu saskaņošanu informācijas sabiedrībā [84], Direktīva 2004/48/EK par intelektuālā īpašuma tiesību piemērošanu [85] un Direktīva 2002/58 neliek dalībvalstīm tādā situācijā kā pamatlietā aplūkotā paredzēt pienākumu paziņot personas datus, lai nodrošinātu autortiesību efektīvu aizsardzību civilā tiesvedībā. Tomēr Savienības tiesības pieprasa, lai minētās dalībvalstis, transponējot šīs direktīvas, pamatotos uz tādu minēto direktīvu interpretāciju, kas ļauj nodrošināt atbilstošu līdzsvaru starp dažādām Kopienu tiesību sistēmā aizsargātām pamattiesībām. Līdz ar to, īstenojot minēto direktīvu transponēšanas pasākumus, dalībvalstu iestādēm un tiesām ir ne tikai jāinterpretē savas valsts tiesības ar šīm pašām direktīvām saskanīgā veidā, bet arī jānodrošina, lai tās nebūtu pamatotas ar tādu šo direktīvu interpretāciju, kas nonāk konfliktā ar minētajām pamattiesībām vai citiem Kopienu tiesību vispārējiem principiem, tādiem kā samērīguma princips.

[83] Eiropas Parlamenta un Padomes Direktīva 2000/31/EK (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) (OV 2000, L 178, 1. lpp.).

[84] Eiropas Parlamenta un Padomes Direktīva 2001/29/EK (2001. gada 22. maijs) par dažu autortiesību un blakustiesību aspektu saskaņošanu informācijas sabiedrībā (OV 2001, L 167, 10. lpp.).

[85] Eiropas Parlamenta un Padomes Direktīva 2004/48/EK (2004. gada 29. aprīlis) par intelektuālā īpašuma tiesību piemērošanu (OV 2004, L 157, 45. lpp.).

2012. gada 19. aprīļa spriedums Bonnier Audio u.c. (C-461/10, EU:C:2012:219)

Högsta domstolen (Augstākā tiesa, Zviedrija) uzdeva Tiesai prejudiciālus jautājumus par to, kā interpretēt Direktīvu 2002/58 un Direktīvu 2004/48 tiesvedībā starp *Bonnier Audio AB*, *Earbooks AB*, *Norstedts Förlagsgrupp AB*, *Piratförlaget AB* un *Storyside AB* (turpmāk tekstā – "*Bonnier Audio* u.c.") un *Perfect Communication Sweden AB* (turpmāk tekstā – "*ePhone*") par pēdējās minētās sabiedrības iebildumiem pret *Bonnier Audio* u.c. iesniegto pieprasījumu izdot rīkojumu sniegt datus.

Šajā lietā *Bonnier Audio* u.c. ir izdevējas sabiedrības, kurām tostarp pieder ekskluzīvas tiesības reproducēt, izdot un padarīt pieejamus sabiedrībai 27 darbus, kas ir audiogrāmatu formātā. Tās apgalvoja, ka ir aizskartas to ekskluzīvās tiesības, jo bez to piekrišanas šie 27 darbi ir publiski izplatīti, izmantojot *FTP* ("file transfer protocol" jeb "datņu pārsūtīšanas protokols") serveri, kas ļauj veikt datņu koplietošanu un datu nosūtīšanu starp internetam pieslēgtiem datoriem. Tādēļ tās vērsās Zviedrijas tiesās ar pieprasījumu izdot rīkojumu paziņot tās personas vārdu vai nosaukumu un adresi, kas lieto IP adresi, no kuras attiecīgās datnes ir tikušas nosūtītas.

Šajā kontekstā *Högsta domstolen*, kurā tika iesniegta kasācijas sūdzība, uzdeva jautājumu Tiesai, vai Savienības tiesību akti nepieļauj tāda valsts tiesību noteikuma piemērošanu, kas ir ieviests, pamatojoties uz Direktīvas 2004/48 8. pantu, un kas, lai identificētu abonentu, ļauj izdot rīkojumu interneta piekļuves nodrošinātājam civilās tiesvedības ietvaros paziņot autortiesību īpašniekam vai tā tiesību pārņēmējam tā abonenta identitāti, kuram ir piešķirta IP adrese, kas ir tikusi izmantota, lai pārkāptu minētās tiesības. Šis jautājums ir balstīts uz pieņēmumu, ka, pirmkārt, prasītājs ir iesniedzis reālus pierādījumus par attiecīgo autortiesību pārkāpumu un, otrkārt, ka lūgtais pasākums ir samērīgs.

Tiesa vispirms atgādināja, ka Direktīvas 2004/48 8. panta 3. punktam, skatot to kopsakarā ar Direktīvas 2002/58 15. panta 1. punktu, nav pretrunā tas, ka dalībvalstis ievieš pienākumu nodot privātpersonām personas datus, lai civillietu tiesās varētu ierosināt lietu par autortiesību aizskārumu, taču tas arī nenosaka, ka šīm valstīm būtu obligāti jāparedz šāds pienākums. Tomēr dalībvalstu iestādēm un tiesām ir ne tikai jāinterpretē savas valsts tiesības šīm pašām direktīvām atbilstošā veidā, bet arī jānodrošina, lai tās nebūtu pamatotas ar tādu šo direktīvu interpretāciju, kas nonāk konfliktā ar minētajām pamattiesībām vai citiem Savienības tiesību vispārējiem principiem, tādiem kā samērīguma princips.

Šajā ziņā tā konstatēja, ka attiecīgajā valsts tiesību aktā it īpaši ir noteikts, ka, lai varētu izdot rīkojumu sniegt attiecīgos datus, ir jābūt reālam pierādījumam par darba intelektuālā īpašuma tiesību aizskārumu, pieprasītajai informācijai ir jāspēj veicināt izmeklēšanu par autortiesību pārkāpumu vai šādu tiesību aizskārumu un šī rīkojuma mērķim ir jāatsver neērtības vai cits kaitējums, kas saistībā ar šo pasākumu var rasties tā adresātam vai jebkurām citām atšķirīgām interesēm.

Līdz ar to Tiesa secināja, ka Direktīva 2002/58 un Direktīva 2004/48 pieļauj tādu valsts tiesību aktu kā pamatlietā aplūkotais, ciktāl ar šo tiesību aktu valsts tiesai, kas no personas, kurai ir tiesības celt prasību, ir saņēmusi pieprasījumu izdot rīkojumu sniegt personas datus, ir atļauts – ņemot vērā katra konkrētā gadījuma apstākļus un pienācīgi ievērojot prasības, kas izriet no samērīguma principa, – izvērtēt attiecīgajā gadījumā pastāvošās atšķirīgās intereses.

3. Atsauču uz personas datiem atsaistīšana

2019. gada 24. septembra spriedums (virspalāta) GC u.c. (Atsauču uz sensitīviem datiem atsaistīšana) (C-136/17, EU:C:2019:773)

Šajā spriedumā Tiesas virspalāta konkretizēja meklētājprogrammas pakalpojumu sniedzēja pienākumus saistībā ar pieprasījumu atsaistīt atsauces uz sensitīviem datiem.

Google bija atteikusies apmierināt četru personu pieprasījumus no rezultātu saraksta, kas meklētājprogrammā parādās, veicot meklēšanu pēc šo personu vārda, atsaistīt vairākas atsauces uz trešo personu publicētām tīmekļa lapām, tostarp uz presē publicētiem rakstiem. Šo četru personu sūdzības saņēmusī *Commission nationale de l'informatique et des libertés* (*CNIL*) (Valsts informātikas un brīvību komisija, Francija) atteicās pieprasīt, lai *Google* veiktu lūgto atsauču atsaistīšanu. Lietu izskatošā *Conseil d'État* (Valsts padome, Francija) lūdza Tiesu konkretizēt, kādi ir meklētājprogrammas pakalpojumu sniedzēja pienākumi, kad tas izskata pieprasījumu atsaistīt atsauces saskaņā ar Direktīvu 95/46.

Pirmkārt, Tiesa atgādināja, ka apstrādāt tādus personas datus, kas atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī datus par veselību vai seksuālo dzīvi, – ar zināmiem izņēmumiem un atkāpēm – ir aizliegts [86]. Savukārt datus par noziedzīgiem nodarījumiem, kriminālsodāmību vai drošības pasākumiem principā var apstrādāt tikai valsts iestādes kontrolē vai tad, ja attiecīgās valsts tiesībās ir paredzētas atbilstīgas speciālas garantijas [87].

Tiesa nosprieda, ka aizliegums apstrādāt šo īpašo kategoriju personas datus un šādas apstrādes ierobežojumi ir piemērojami meklētājprogrammas pakalpojumu sniedzējam gluži tāpat kā ikvienam citam personas datu pārzinim. Proti, šo aizliegumu un ierobežojumu mērķis ir nodrošināt ciešāku aizsardzību pret tādu apstrādi, kas šo datu īpašās sensitivitātes dēļ iespējami varētu radīt īpaši smagu iejaukšanos pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību.

[86] Direktīvas 95/46 8. panta 1. punkts un Regulas 2016/679 9. panta 1. punkts.
[87] Direktīvas 95/46 8. panta 5. punkts un Regulas 2016/679 10. pants.

Tomēr meklētājprogrammas pakalpojumu sniedzējs ir atbildīgs nevis tāpēc, ka personas dati atrodas kādas trešās personas publicētā tīmekļa lapā, bet gan tāpēc, ka tas sasaista atsauces uz šo lapu. Šajos apstākļos aizliegums apstrādāt sensitīvos datus vai šādas apstrādes ierobežojumi šim meklētājprogrammas pakalpojumu sniedzējam ir piemērojami tikai šīs atsauču sasaistīšanas dēļ, un tātad tas darāms, kompetento valsts iestāžu uzraudzībā veicot pārbaudi pēc datu subjekta pieprasījuma.

Otrkārt, Tiesa uzskatīja, ka meklētājprogrammas pakalpojumu sniedzējam, saņemot pieprasījumu atsaistīt atsauces uz sensitīviem datiem, šis pieprasījums – ar zināmiem izņēmumiem – principā ir jāapmierina. Runājot par šiem izņēmumiem, jāteic, ka pakalpojumu sniedzējs var noraidīt šādu pieprasījumu, piemēram, ja viņš konstatē, ka attiecīgās saites novirza uz datiem, kurus acīmredzami ir publiskojis pats datu subjekts [88], ar nosacījumu, ka šo atsauču sasaistīšana atbilst pārējiem personas datu apstrādes likumīguma nosacījumiem un ja vien šim subjektam nav tiesību iebilst pret minēto atsauču sasaistīšanu ar viņa īpašo situāciju saistītu iemeslu dēļ [89].

Katrā ziņā, saņemot pieprasījumu atsaistīt atsauces, meklētājprogrammas pakalpojumu sniedzējam ir jāpārbauda, vai saites uz tīmekļa lapu, kurā ir publicēti sensitīvi dati, iekļaušana rezultātu sarakstā, kas parādās, veicot meklēšanu pēc šā subjekta vārda, izrādās esam absolūti nepieciešama, lai aizsargātu informācijas brīvību to interneta lietotāju gadījumā, kuri varētu būt ieinteresēti piekļūt šai tīmekļa lapai, veicot šādu meklēšanu. Šajā ziņā Tiesa uzsvēra, ka, lai gan tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību principā ir pārākas par interneta lietotāju informācijas brīvību, šis samērs tomēr īpašos gadījumos var būt atkarīgs no attiecīgās informācijas būtības un no tā, cik šī informācija ir sensitīva datu subjekta privātās dzīves aspektā, kā arī no sabiedrības interesēm saņemt šo informāciju, kas savukārt var atšķirties tostarp atkarībā no attiecīgā subjekta lomas sabiedriskajā dzīvē.

Treškārt, Tiesa nosprieda, ka meklētājprogrammas pakalpojumu sniedzējam, saņemot pieprasījumu atsaistīt atsauces uz datiem par tiesvedību krimināllietā pret datu subjektu, kuri attiecas uz šīs tiesvedības agrāku posmu un vairs neatbilst pašreizējai situācijai, ir jāizvērtē, vai – ņemot vērā visus attiecīgās lietas apstākļus – šim subjektam ir tiesības uz to, lai attiecīgā informācija pašreiz vairs netiktu saistīta ar viņa vārdu rezultātu sarakstā, kas parādās, veicot meklēšanu pēc šā vārda. Tomēr, lai arī tā tas nav tāpēc, ka attiecīgās saites iekļaušana izrādās esam absolūti nepieciešama, lai datu subjekta tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību salāgotu ar iespējami ieinteresēto interneta lietotāju informācijas brīvību, pakalpojumu sniedzējam – vēlākais, saņemot pieprasījumu atsaistīt atsauces – ir jāpārveido rezultātu saraksts tādējādi, lai interneta lietotāja gūtā kopaina atspoguļotu pašreizējo tieslietu situāciju, un tālab ir

[88] Direktīvas 95/46 8. panta 2. punkta e) apakšpunkts un Regulas 2016/679 9. panta 2. punkta e) apakšpunkts.
[89] Direktīvas 95/46 14. panta pirmās daļas a) punkts un Regulas 2016/679 21. panta 1. punkts.

vajadzīgs tostarp, lai saites uz tīmekļa lapām, kurās ir rodama informācija par šo jautājumu, parādītos šā saraksta sākumā.

2019. gada 24. septembra spriedums (virspalāta) Google (Atsauču atsaistīšanas teritoriālā piemērojamība) (C-507/17, EU:C:2019:772)

Commission nationale de l'informatique et des libertés (*CNIL*) (Valsts informātikas un brīvību komisija, Francija) izteica brīdinājumu sabiedrībai *Google*, pieprasot, lai tā – apmierinot pieprasījumu atsaistīt atsauces – no rezultātu saraksta, kas parādās, veicot meklēšanu pēc datu subjekta vārda, izņemtu saites uz tīmekļa lapām, kurās ir šā subjekta personas dati, visos savas meklētājprogrammas domēna nosaukuma paplašinājumos. Tā kā *Google* atteicās izpildīt šo prasību, *CNIL* šai sabiedrībai uzlika sodu 100 000 EUR apmērā. *Google* prasību izskatošā *Conseil d'État* (Valsts padome, Francija) lūdza Tiesu konkretizēt, kāda teritoriālā piemērojamība ir meklētājprogrammas pakalpojumu sniedzēja pienākumam nodrošināt tiesību uz atsauču atsaistīšanu izmantošanu saskaņā ar Direktīvu 95/46.

Vispirms Tiesa atgādināja par iespēju fiziskām personām, pamatojoties uz Savienības tiesībām, izmantot savas tiesības uz atsauču atsaistīšanu attiecībā pret meklētājprogrammas pakalpojumu sniedzēju, kuram ir viens vai vairāki dibinājumi Savienības teritorijā, neatkarīgi no tā, vai personas datu apstrāde (šajā gadījumā – saišu uz tīmekļa lapām, kurās ir šīs tiesības izmantojošā datu subjekta personas dati) notiek Savienībā vai ārpus tās [90].

Jautājumā par to, kāds ir tiesību uz atsauču atsaistīšanu tvērums, Tiesa atzina, ka meklētājprogrammas pakalpojumu sniedzējam ir pienākums veikt atsauču atsaistīšanu nevis visās savas meklētājprogrammas versijās, bet gan visās dalībvalstīm paredzētajās savas meklētājprogrammas versijās. Šajā ziņā tā norādīja, ka, lai arī ar atsauču vispārēju atsaistīšanu, ņemot vērā interneta un meklētājprogrammu raksturiezīmes, tiktu pilnībā sasniegts Savienības likumdevēja mērķis nodrošināt personas datu aizsardzību augstā līmenī visā Savienībā, tomēr no Savienības tiesībām [91] nekādi neizriet, ka šā mērķa sasniegšanai likumdevējs būtu izvēlējies tiesībām uz atsauču atsaistīšanu piešķirt tvērumu, kas būtu plašāks par dalībvalstu teritoriju. Konkrēti, Savienības tiesībās ir paredzēti mehānismi dalībvalstu uzraudzības iestāžu sadarbībai, lai, no vienas puses, samērojušas tiesības uz privātās dzīves un personas datu aizsardzību ar dažādu dalībvalstu sabiedrības interesēm piekļūt informācijai, tās varētu panākt kopīgu lēmumu, taču šādi mehānismi pašreiz nav paredzēti attiecībā uz atsauču atsaistīšanas tvērumu ārpus Savienības.

[90] Direktīvas 95/46 4. panta 1. punkta a) apakšpunkts un Regulas 2016/679 3. panta 1. punkts.
[91] Direktīvas 95/46 12. panta b) punkts un 14. panta pirmās daļas a) punkts un Regulas 2016/679 17. panta 1. punkts.

Pašreizējā Savienības tiesību attīstības stadijā meklētājprogrammas pakalpojumu sniedzējam lūgtā atsauču atsaistīšana ir jāveic nevis vienīgi tajā meklētājprogrammas versijā, kas ir paredzēta dalībvalstij, kurā atrodas atsauču atsaistīšanu prasīt tiesīgās personas dzīvesvieta, bet gan visās dalībvalstīm paredzētajās meklētājprogrammas versijās, tostarp tālab, lai nodrošinātu konsekventu un augsta līmeņa aizsardzību visā Savienībā. Turklāt šādam meklētājprogrammas pakalpojumu sniedzējam ir pienākums vajadzības gadījumā veikt pietiekami iedarbīgus pasākumus, lai Savienībā esošajiem interneta lietotājiem liegtu piekļuvi – piemēram, no kādai trešai valstij paredzētas meklētājprogrammas versijas – saitēm, uz kurām attiecas atsauču atsaistīšana, vai vismaz viņus nopietni atturētu no šādas piekļūšanas, un valsts tiesai ir jāpārbauda, vai pakalpojumu sniedzēja veiktie pasākumi atbilst šai prasībai.

Visbeidzot Tiesa uzsvēra, ka, lai arī Savienības tiesībās netiek prasīts, lai meklētājprogrammas pakalpojumu sniedzējs veiktu atsauču atsaistīšanu visās savas meklētājprogrammas versijās, taču tas arīdzan netiek aizliegts. Tāpēc dalībvalsts uzraudzības iestādes vai tiesas kompetencē joprojām ir attiecīgajā valstī esošo pamattiesību aizsardzības standartu gaismā veikt datu subjekta tiesību uz privātās dzīves neaizskaramību un savu personas datu aizsardzību samērošanu ar tiesībām uz informācijas brīvību un šīs samērošanas iznākumā vajadzības gadījumā likt šīs meklētājprogrammas pakalpojumu sniedzējam veikt atsauču atsaistīšanu visās šīs meklētājprogrammas versijās.

2022. gada 8. decembra spriedums (virspalāta) Google (Atsauču uz apgalvoti nepatiesu saturu atsaistīšana) (C-460/20, EU:C:2022:962)

Par prasītājiem pamatlietā, proti, TU, kas ieņem atbildīgus amatus un kam pieder kapitāldaļas dažādās sabiedrībās, un RE, kas bija viņa dzīvesbiedre un līdz 2015. gada maijam – vienas no šīm sabiedrībām prokūriste, bija trīs raksti, kurus 2015. gadā kādā tīmekļvietnē publicēja šīs tīmekļvietnes redaktore *G LLC*. Šajos rakstos, no kuriem viens tika ilustrēts ar četrām fotogrāfijām, kurās attēloti prasītāji un kuras vedina domāt, ka viņi dzīvo greznībā, bija kritiski aplūkots vairāku viņu sabiedrību ieguldījumu modelis. Piekļuve šiem rakstiem bija iespējama, *Google LLC* (turpmāk tekstā – "*Google*") pārvaldītajā meklētājprogrammā ievadot prasītāju vārdus un uzvārdus gan atsevišķi, gan kopā ar konkrētu sabiedrību nosaukumiem. Rezultātu sarakstā bija saite uz šiem rakstiem, kā arī uz fotogrāfijām sīktēlu (*thumbnails*) formā.

Prasītāji pamatlietā pieprasīja *Google* kā tās meklētājprogrammas veiktās personas datu apstrādes pārzini, pirmkārt, no meklēšanas rezultātu saraksta atsaistīt atsauces uz attiecīgajiem rakstiem, pamatojoties uz to, ka šajos rakstos esot ietverti nepatiesi apgalvojumi un apmelojoši viedokļi, un, otrkārt, no meklēšanas rezultātu saraksta izņemt sīktēlus. *Google* atteicās apmierināt šo pieprasījumu.

Tā kā gan pirmajā instancē, gan apelācijas instancē prasītājiem pamatlietā spriedums nebija labvēlīgs, tie vērsās *Bundesgerichtshof* (Federālā augstākā tiesa, Vācija) ar revīzijas

(*Revision*) sūdzību, saistībā ar kuras izskatīšanu *Bundesgerichtshof* ir vērsusies Tiesā ar prejudiciālajiem jautājumiem par VDAR un Direktīvas 95/46 [92] interpretāciju.

Ar virspalātas sastāvā pasludināto spriedumu Tiesa tālāk attīsta savu judikatūru par nosacījumiem, kas piemērojami atsauču atsaistīšanas pieprasījumiem, kuri adresēti meklētājprogrammas pakalpojumu sniedzējam, pamatojoties uz noteikumiem par personas datu aizsardzību. Konkrēti tā pārbauda, pirmkārt, to pienākumu un atbildības apjomu, kas ir meklētājprogrammas pakalpojumu sniedzējam, izskatot atsaistīšanas pieprasījumu, kurš pamatots ar piesaistītajā saturā atrodamās informācijas apgalvotu nepatiesumu, un, otrkārt, datu subjekta pienākumu pierādīt šīs informācijas nepatiesumu. Turklāt tā arī spriež par to, vai, izskatot pieprasījumu no meklēšanas rezultātu saraksta izņemt sīktēlu formā esošās fotogrāfijas, ir jāņem vērā sākotnējais konteksts, kurā šīs fotogrāfijas ir publicētas internetā.

Pirmām kārtām, Tiesa nospriež, ka saistībā ar tiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību samērošanu ar tiesībām uz vārda un informācijas brīvību [93], kas veicama, izskatot meklētājprogrammas pakalpojumu sniedzējam adresētu pieprasījumu no meklēšanas rezultātu saraksta izņemt atsauci uz saturu ar apgalvoti nepatiesu informāciju, šāda atsaistīšana nav pakārtota nosacījumam, ka jautājumam par atsaucēs piesaistītā satura patiesumu jābūt vismaz provizoriski atrisinātam tiesvedībā, ko šā pieprasījuma iesniedzējs uzsācis pret satura izplatītāju.

Ievadam, lai izvērtētu, kādos apstākļos meklētājprogrammas pakalpojumu sniedzējam ir jāapmierina atsaistīšanas pieprasījums un tātad no rezultātu saraksta, kas parādās, veicot meklēšanu pēc datu subjekta vārda, jādzēš saite uz tīmekļvietni, kurā atrodas apgalvojumi, kurus minētā persona uzskata par nepatiesiem, Tiesa citastarp atgādina, ka:

• ciktāl meklētājprogrammas darbība var būtiski un vēl papildus interneta vietņu redaktoru darbībai ietekmēt pamattiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību, šādas meklētājprogrammas pakalpojumu sniedzējam kā personai, kas nosaka šīs darbības nolūkus un līdzekļus, savas atbildības, pilnvaru un iespēju robežās ir jānodrošina, lai Direktīvā 95/46 un VDAR paredzētās garantijas varētu tikt pilnībā nodrošinātas un lai faktiski varētu tikt īstenota datu subjektu efektīva un pilnīga aizsardzība;

• meklētājprogrammas pakalpojumu sniedzējam, kas saņēmis pieprasījumu atsaistīt atsauces, ir jāpārbauda, vai saites uz attiecīgo tīmekļvietni iekļaušana rezultātu sarakstā ir vajadzīga, lai izmantotu ar tiesībām uz vārda brīvību un informāciju aizsargāto informācijas brīvību to interneta lietotāju gadījumā, kuri varētu būt ieinteresēti piekļūt šai tīmekļvietnei, veicot šādu meklēšanu;

[92] Attiecīgi VDAR 17. panta 3. punkta a) punkts un Direktīvas 95/46 12. panta b) punkts un 14. panta pirmās daļas a) punkts.
[93] Pamattiesības, kas garantētas attiecīgi Hartas 7., 8. un 11. pantā.

• VDAR ir skaidri noteikta prasība veikt pamattiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību samērošanu ar pamattiesībām uz informācijas brīvību.

Vispirms Tiesa norāda, ka, lai gan datu subjekta tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību vispārīgi ir pārākas par interneta lietotāju tiesībām piekļūt attiecīgajai informācijai, šis samērs tomēr var būt atkarīgs no katra gadījuma īpašajiem apstākļiem, tostarp – šīs informācijas veida un tā, cik šī informācija ir sensitīva saistībā ar datu subjekta privāto dzīvi, kā arī no sabiedrības interesēm saņemt šo informāciju, kuras var atšķirties citastarp atkarībā no attiecīgā subjekta lomas sabiedriskajā dzīvē.

Jautājums, vai piesaistītais saturs ir vai nav patiess, arī ir būtisks elements šajā vērtējumā. Tādējādi noteiktos apstākļos interneta lietotāju tiesības uz informāciju un satura izplatītāja vārda brīvība var prevalēt pār tiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību, it īpaši, ja datu subjektam ir loma sabiedriskajā dzīvē. Tomēr šī pakārtotība kļūst pretēja, ja vismaz daļa no atsaistīšanas pieprasījumā norādītās informācijas, kura nav maznozīmīga uz visa satura fona, izrādās esam nepatiesa. Šādā gadījumā tiesības informēt un tiesības tikt informētam nevar tikt ņemtas vērā, jo tās nevar ietvert tiesības izplatīt šādu informāciju un piekļūt tai.

Turpinājumā, runājot, pirmkārt, par pienākumiem saistībā ar konstatējumu par to, vai informācija, kas ietverta piesaistītajā saturā, ir vai nav patiesa, Tiesa precizē, ka personai, kas lūdz atsaistīt atsauces šādas informācijas nepatiesuma dēļ, ir jāpierāda, ka šī informācija vai vismaz daļa no šīs informācijas, kura nav maznozīmīga uz visa šā satura fona, ir acīmredzami nepatiesa. Tomēr, lai izvairītos, ka šai personai tiek uzlikts pārmērīgs slogs, kas varētu kaitēt tiesību uz atsaistīšanu efektivitātei, šai personai ir pienākums iesniegt tikai tādus pierādījumus, ko tai var pamatoti prasīt sameklēt, ņemot vērā konkrētās lietas apstākļus. Šai personai principā nevar prasīt, lai tā pirmstiesas posmā, pamatojot savu atsaistīšanas pieprasījumu, iesniegtu tiesas nolēmumu, kas kaut pagaidu noregulējuma posmā pieņemts pret tīmekļvietnes redaktoru.

Otrkārt, attiecībā uz meklētājprogrammas pakalpojumu sniedzēja pienākumiem un atbildību Tiesa uzsver – lai pārbaudītu, vai pēc atsaistīšanas pieprasījuma saņemšanas attiecīgo saturu var joprojām iekļaut tā meklētājprogrammas sniegto meklējumu rezultātu sarakstā, pakalpojumu sniedzējam ir jāņem vērā visas iesaistītās tiesības un intereses un visi konkrētās lietas apstākļi. Taču šim pakalpojumu sniedzējam nevar prasīt, lai tas noskaidrotu faktus un šajā nolūkā organizētu uz sacīkstes principu balstītu saziņu ar satura izplatītāju nolūkā iegūt trūkstošo informāciju par atsaucēs piesaistītā satura patiesumu. Pienākums piedalīties atsaucēs piesaistītā satura patiesuma noskaidrošanā pakalpojumu sniedzējam radītu slogu, kas pārsniedz to, ko no tā var saprātīgi gaidīt, ņemot vērā šā pakalpojumu sniedzēja atbildību, pilnvaras un iespējas. Šāds risinājums radītu nopietnu risku, ka saturs, kas atbilst leģitīmai un prevalējošai sabiedrības vajadzībai pēc informācijas, tiktu atsaistīts no rezultātu saraksta un tādējādi kļūtu grūti atrodams internetā. Tādējādi, ja šis pakalpojumu sniedzējs gandrīz sistemātiski veiktu atsaistīšanu no rezultātu saraksta, lai izvairītos no pienākuma

noskaidrot attiecīgos faktus par norādītā satura patiesumu, pastāvētu reāls risks, ka personas varētu tikt atturētas no vārda un informācijas brīvības izmantošanas.

Tāpēc gadījumā, ja atsaistīšanas pieprasījuma iesniedzējs sniedz pierādījumus tam, ka piesaistītajā saturā ietvertā informācija vai vismaz daļa no šīs informācijas, kura nav maznozīmīga uz visa šā satura fona, ir acīmredzami nepatiesa, meklētājprogrammas pakalpojumu sniedzējam ir jāapmierina šis pieprasījums. Tāpat ir gadījumā, kad pieprasījuma iesniedzējs iesniedz tiesas nolēmumu, kas pieņemts pret tīmekļvietnes redaktoru un kas ir balstīts uz konstatējumu, ka atsaucēs piesaistītajā saturā ietvertā informācija, kura uz visa šā satura fona nav maznozīmīga, vismaz pirmšķietami ir nepatiesa. Savukārt, ja no pieprasījuma iesniedzēja sniegtajiem pierādījumiem uzskatāmi neizriet, ka šī informācija ir nepatiesa, meklētājprogrammas pakalpojumu sniedzējam nav pienākuma apmierināt atsaistīšanas pieprasījumu, ja nav šāda tiesas nolēmuma. Ja attiecīgā informācija var veicināt sabiedriski nozīmīgu diskusiju, tad, ņemot vērā visus konkrētās lietas apstākļus, īpaša nozīme ir jāpiešķir tiesībām uz vārda un informācijas brīvību.

Visbeidzot Tiesa piebilst, ka tad, ja meklētājprogrammas pakalpojumu sniedzējs atsaistīšanas pieprasījumu atstāj bez virzības, datu subjektam ir jābūt iespējai vērsties uzraudzības iestādē vai tiesu iestādē, lai tā veiktu nepieciešamās pārbaudes un uzdotu pārzinim veikt vajadzīgās darbības. Šajā ziņā tieši tiesu iestādēm ir jānodrošina konfliktējošo interešu izsvēršana, jo tās vislabāk var veikt kompleksu un padziļinātu izsvēršanu, kurā tiek ņemti vērā visi kritēriji un faktori, kas ir noteikti atbilstošajā judikatūrā.

Otrām kārtām, Tiesa nospriež, ka, samērojot iepriekš minētās pamattiesības, lai izvērtētu atsaistīšanas pieprasījumu, ar kuru lūgts no attēlu meklēšanas, kas veikta pēc fiziskas personas vārda, dzēst rezultātus ar fotogrāfijām sīktēlu formā, kurās attēlota šī persona, jāņem vērā šo fotogrāfiju informatīvā nozīme neatkarīgi no sākotnējā konteksta, kādā tās publicētas tīmekļvietnē, no kuras tās izgūtas. Taču ir jāņem vērā visi teksta elementi, kuri šīm fotogrāfijām tieši pievienoti meklēšanas rezultātu sarakstā un kuri var viest skaidrību par šo fotogrāfiju informatīvo nozīmi.

Lai pamatotu šo secinājumu, Tiesa uzsver, ka attēlu meklēšanai, kas veikta interneta meklētājprogrammā, ievadot kādas personas vārdu, tiek piemēroti tādi paši principi kā interneta vietņu un tajās ietvertās informācijas meklēšanai. Tā norāda, ka datu subjekta fotogrāfiju parādīšana sīktēlu formā, veicot meklēšanu pēc personvārda, var būt īpaši nopietna iejaukšanās šīs personas tiesībās uz privātās dzīves neaizskaramību un uz personas datu aizsardzību.

Tāpēc, ja meklētājprogrammas pakalpojumu sniedzējam ir iesniegts atsaistīšanas pieprasījums dzēst tādas attēlu meklēšanas rezultātus, kas veikta, ievadot personas vārdu un iegūstot šīs personas fotogrāfijas sīktēlu formā, tam ir jāpārbauda, vai attiecīgo fotogrāfiju parādīšana ir nepieciešama, lai varētu tikt izmantotas tādu interneta lietotāju

tiesības uz informācijas brīvību, kuriem, iespējams, ir interese piekļūt šīm fotogrāfijām, veicot šādu meklēšanu.

Tā kā meklētājprogramma datu subjekta fotogrāfijas parāda ārpus konteksta, kādā tās publicētas ar atsauci piesaistītajā tīmekļvietnē, visbiežāk, lai ilustrētu šajā lapā ietvertos teksta elementus, jānoskaidro, vai šis konteksts tomēr ir jāņem vērā veicamajā konfliktējošo tiesību un interešu izsvēršanā. Šajā ziņā tas, vai minētajā vērtējumā jāiekļauj arī tās tīmekļvietnes saturs, kurā ir ietverta fotogrāfija, kuras parādīšanu sīktēla formā tiek prasīts izbeigt, ir atkarīgs no attiecīgās apstrādes priekšmeta un rakstura.

Pirmkārt, attiecībā uz šīs apstrādes priekšmetu Tiesa norāda, ka fotogrāfiju kā neverbāla komunikācijas līdzekļa publicēšanai var būt lielāka ietekme uz interneta lietotājiem nekā tekstuālām publikācijām. Proti, fotogrāfijas pašas par sevi ir būtisks līdzeklis, lai piesaistītu interneta lietotāju uzmanību, un var izraisīt interesi piekļūt rakstiem, ko tās ilustrē. Tomēr, jo īpaši, ņemot vērā to, ka fotogrāfijas bieži vien var tikt interpretētas dažādi, to parādīšana meklēšanas rezultātu sarakstā sīktēlu formā var radīt īpaši nopietnu iejaukšanos datu subjekta tiesībās uz sava attēla aizsardzību, un tas ir jāņem vērā, izsverot konfliktējošās tiesības un intereses. Tādēļ atšķirīga izsvēršana jāveic atkarībā no tā, vai runa ir par tīmekļvietnes redaktora publicētiem rakstiem ar fotogrāfijām, kas, ievietotas to sākotnējā kontekstā, ilustrē šajos rakstos sniegto informāciju un tajos pausto viedokli, vai gluži otrādi par fotogrāfijām, kuras kā sīktēlus rezultātu sarakstā meklētājprogrammas pakalpojumu sniedzējs parāda ārpus konteksta, kurā tās publicētas sākotnējā tīmekļvietnē.

Šajā ziņā Tiesa atgādina, ka ne tikai iemesls, kas attaisno personas datu publicēšanu tīmekļvietnē, ne vienmēr sakrīt ar to, uz kā balstās meklētājprogrammas darbība, bet arī ka pat tad, ja tas tā ir, veicamās attiecīgo tiesību un interešu izsvēršanas rezultāts var atšķirties atkarībā no tā, vai apstrādi ir veicis meklētājprogrammas pakalpojumu sniedzējs vai šīs tīmekļvietnes redaktors. Pirmām kārtām, leģitīmās intereses, kas attaisno šo apstrādi, var būt atšķirīgas un, otrām kārtām, sekas, kādas ir šādai apstrādei attiecībā uz datu subjektu un it īpaši tā privāto dzīvi, ne vienmēr ir vienādas.

Otrkārt, attiecībā uz meklētājprogrammas pakalpojumu sniedzēja veiktās apstrādes raksturu Tiesa konstatē, ka, izgūstot internetā publicētās fizisko personu fotogrāfijas un parādot tās atsevišķi attēlu meklēšanas rezultātos sīktēlu formā, meklētājprogrammas pakalpojumu sniedzējs piedāvā pakalpojumu, kas ietver personas datu apstrādi, kura ir savrupa un atšķirīga no tās apstrādes, ko veic tās tīmekļvietnes redaktors, no kuras ir ņemtas fotogrāfijas, kā arī no apstrādes, par kuru šis pakalpojumu sniedzējs arī ir atbildīgs un kura attiecas uz atsauču piesaistīšanu šai vietnei.

Tāpēc darbība, ko meklētājprogrammas pakalpojumu sniedzējs veic, attēlu meklēšanas rezultātus parādot sīktēlu formā, ir jāvērtē savrupi, jo šādas darbības rezultātā radītais pamattiesību papildu aizskārums var būt īpaši spēcīgs tādēļ, ka, veicot meklēšanu pēc personvārda, tiek apkopota visa internetā atrodamā informācija par datu subjektu. Šajā savrupajā vērtējumā jāņem vērā, ka fotogrāfiju parādīšana pati par sevi ir interneta

lietotāja veiktās meklēšanas rezultāts neatkarīgi no tā, vai viņš pēc tam nolemj aplūkot vai neaplūkot sākotnējo saturu ietverošo tīmekļvietni.

Katrā ziņā Tiesa piebilst, ka šāda īpaša izsvēršana, kurā ņemts vērā meklētājprogrammas pakalpojumu sniedzēja veiktās apstrādes autonomais raksturs, neskar iespējamo to teksta elementu nozīmi, kuri var būt tieši pievienoti meklēšanas rezultātu sarakstā uzrādītajai fotogrāfijai, jo šādi elementi var viest skaidrību par šīs fotogrāfijas informatīvo nozīmi sabiedrībai un tādējādi ietekmēt attiecīgo tiesību un interešu izsvēršanu.

4. Tīmekļvietnes lietotāja piekrišana informācijas uzglabāšanai

2019. gada 1. oktobra spriedums (virspalāta) Planet49 (C-673/17, EU:C:2019:801)

Ar šo spriedumu Tiesa nosprieda, ka piekrišana tam, ka ar tīmekļvietnes lietotāja galiekārtā ievietotu sīkdatņu palīdzību tiek saglabāta un izgūta informācija, nav dota pienācīgi, ja atļauja to darīt izriet no iepriekš ar ķeksīti atzīmētas izvēles rūtiņas, neatkarīgi no tā, vai attiecīgā informācija ir vai nav personas dati. Tiesa turklāt precizēja, ka pakalpojumu sniedzējam ir jānorāda tīmekļvietnes lietotājam ziņas par sīkdatņu darbības ilgumu, kā arī to, vai trešām personām ir vai nav iespējams gūt piekļuvi šīm sīkdatnēm.

Pamatlieta bija par reklāmas loteriju, ko *Planet49* rīkoja tīmekļvietnē www.dein-macbook.de. Lai tajā varētu piedalīties, interneta lietotājiem bija jānorāda savs vārds un sava adrese tīmekļvietnē, kur atradās ar ķeksīti atzīmējamas izvēles rūtiņas. Izvēles rūtiņa, kurā tiek dota atļauja ievietot sīkdatnes, bija atzīmēta ar ķeksīti jau pēc noklusējuma. Vācijas Federālās patērētāju tiesību organizāciju un asociāciju apvienības iesniegto prasību izskatošā *Bundesgerichtshof* (Federālā augstākā tiesa, Vācija) šaubījās par to, vai veids, kādā lietotāju piekrišana tiek saņemta, izmantojot jau pēc noklusējuma ar ķeksīti atzīmētu izvēles rūtiņu, ir pienācīgs, kā arī par to, kāds ir apjoms pakalpojuma sniedzēja pienākumam sniegt informāciju.

Lūgums sniegt prejudiciālu nolēmumu būtībā bija par to, kā ir jāinterpretē "piekrišanas" jēdziens, kas ir paredzēts Direktīvā2002/58 [94], skatot to kopsakarā ar Direktīvu 95/46/EK [95], kā arī ar VDAR [96].

Pirmkārt, Tiesa konstatēja, ka Direktīvas 95/46 2. panta h) punktā – uz kuru ir izdarīta atsauce Direktīvas 2002/58 2. panta f) punktā – piekrišana ir definēta kā "jebkurš labprātīgi sniegts šīs personas vēlmju konkrēts un paziņots norādījum[s], ar kuru datu

[94] Direktīvas 2002/58, redakcijā ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (OV 2009, L 337, 11. lpp.), 2. panta f) punkts un 5. panta 3. punkts.
[95] Direktīvas 95/46 2. panta h) punkts.
[96] Regulas 2016/679 6. panta 1. punkta a) apakšpunkts.

subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei". Tā norādīja, ka prasība pēc datu subjekta vēlmju "norādījuma" skaidri liecina par aktīvu rīcību, nevis pasīvu izturēšanos. Savukārt, lai dotu piekrišanu, izmantojot iepriekš ar ķeksīti atzīmētu izvēles rūtiņu, tīmekļvietnes lietotājam nav aktīvi jārīkojas. Turklāt arī Direktīvas 2002/58 5. panta 3. punkta – kurā kopš grozījumu izdarīšanas ar Direktīvu 2009/136 ir paredzēts, ka lietotājam ir jābūt "[devušam] savu piekrišanu" sīkdatņu ievietošanai – rašanās vēsture liecina, ka lietotāja piekrišana turpmāk vairs nav prezumējama un tai ir jāizriet no šā lietotāja aktīvas rīcības. Visbeidzot aktīva piekrišana tagad ir paredzēta VDAR [97], kuras 4. panta 11. punktā ir prasīts, lai gribas izpaudums būtu veikts tostarp "skaidri apstiprinošas darbības" veidā, un kuras 32. apsvērumā ir skaidri izslēgts, ka par piekrišanu būtu jāuzskata "klusēšana, iepriekš atzīmēti laukumi vai atturēšanās no darbības".

Tāpēc Tiesa nosprieda, ka piekrišana nav dota pienācīgi tad, ja atļauja informācijas saglabāšanai tīmekļvietnes lietotāja galiekārtā vai piekļuvei tur jau uzglabātai informācijai tiek dota, izmantojot iepriekš ar ķeksīti atzīmētu izvēles rūtiņu, no kuras lietotājam, ja viņš nevēlas dot savu piekrišanu, ķeksītis ir jāizņem. Tā piebilda, ka ar to, ka lietotājs aktivizē pogu dalībai attiecīgajā reklāmas loterijā, nav pietiekami, lai varētu uzskatīt, ka lietotājs ir pienācīgi devis savu piekrišanu sīkdatņu ievietošanai.

Otrkārt, Tiesa konstatēja, ka Direktīvas 2002/58 5. panta 3. punkta mērķis ir aizsargāt lietotāju no iejaukšanās viņa privātajā dzīvē neatkarīgi no tā, vai šī iejaukšanās skar vai neskar personas datus. No tā izriet, ka jēdziens "piekrišana" nav jāinterpretē atšķirīgi atkarībā no tā, vai tīmekļvietnes lietotāja galiekārtā saglabātā vai no tās izgūtā informācija ir vai nav personas dati.

Treškārt, Tiesa norādīja, ka Direktīvas 2002/58 5. panta 3. punktā ir prasīts, lai lietotājs būtu devis savu piekrišanu, būdams nodrošināts ar skaidru un visaptverošu informāciju, tostarp par apstrādes nolūku. Skaidrai un visaptverošai informācijai ir jāļauj lietotājam viegli noprast sekas, kas iestātos viņa iespējami dotai piekrišanai, un jāgarantē, ka šī piekrišana tiek dota, pilnībā apzinoties visus apstākļus. Šajā ziņā Tiesa uzskatīja, ka skaidrajai un visaptverošajai informācijai, kas pakalpojumu sniedzējam ir jāsniedz lietotājam, ir jāietver ziņas arī par sīkdatņu funkcionēšanas ilgumu, kā arī par to, vai trešām personām ir iespēja piekļūt šīm sīkdatnēm vai arī tām šādas iespējas nav.

[97] Turpat.

5. Personas datu apstrāde tiešsaistes sociālajos tīklos

2023. gada 4. jūlija spriedums (virspalāta) Meta Platforms u.c. (Vispārīgie sociālā tīkla lietošanas noteikumi) (C-252/21, EU:C:2023:537)

Sabiedrībai *Meta Platforms* pieder tiešsaistes sociālais tīkls *Facebook*, kas privātiem lietotājiem ir bez maksas. Šā sociālā tīkla uzņēmējdarbības modeļa pamatā ir finansējums no tiešsaistes reklāmas, kas tiek pielāgota individuāliem lietotājiem. Tehniski šāda reklāma ir padarīta iespējama, automatizēti izveidojot detalizētus tīkla un *Meta* grupas līmenī piedāvāto tiešsaistes pakalpojumu lietotāju profilus. Tādējādi, lai varētu lietot minēto sociālo tīklu, lietotājiem reģistrācijas brīdī ir jāpiekrīt *Meta Platforms* vispārīgajiem noteikumiem, kuros norādīts uz šīs sabiedrības noteikto datu un sīkdatņu izmantošanas politiku. Saskaņā ar šo politiku papildus tiem datiem, ko lietotāji sniedz tiešā veidā reģistrācijas brīdī, *Meta Platforms* vāc arī datus par minēto lietotāju darbībām sociālajā tīklā un ārpus tā un tos sasaista ar attiecīgo lietotāju *Facebook* kontiem. Pēdējie minētie dati, saukti arī par *"off Facebook* datiem", ir, pirmkārt, dati par trešo personu tīmekļvietņu un lietotņu aplūkošanu un, otrkārt, dati par citu *Meta* grupai piederošu tiešsaistes pakalpojumu izmantošanu (tostarp *Instagram* un *WhatsApp*). Šādi ievāktie dati kopumā ļauj izdarīt detalizētus secinājumus par šo lietotāju izvēlēm un interesēm.

Ar 2019. gada 6. februāra lēmumu *Bundeskartellamt* (Federālais karteļu birojs, Vācija) aizliedza *Meta Platforms*, pirmkārt, saskaņā ar tobrīd spēkā esošajiem vispārīgajiem noteikumiem Vācijā dzīvojošu privātu lietotāju *Facebook* sociālā tīkla lietošanu pakārtot nosacījumam par viņu *off Facebook* datu apstrādi un, otrkārt, bez viņu piekrišanas veikt šo datu apstrādi. Turklāt Federālais karteļu birojs tai lika pielāgot šos vispārīgos noteikumus tādējādi, lai no tiem skaidri izrietētu, ka minētie dati netiks nedz vākti, nedz sasaistīti ar *Facebook* lietotāju kontiem, nedz izmantoti bez attiecīgo lietotāju piekrišanas. Visbeidzot šis birojs uzsvēra, ka šāda piekrišana nav derīga, ja tā ir nosacījums sociālā tīkla lietošanai. Savu lēmumu tas pamatoja ar apstākli, ka šī datu apstrāde, kas neatbilst VDAR, ir *Meta Platforms* dominējošā stāvokļa ļaunprātīga izmantošana tiešsaistes sociālo tīklu tirgū.

Meta Platforms šo lēmumu pārsūdzēja *Oberlandesgericht Düsseldorf* (Federālās zemes Augstākā tiesa Diseldorfā, Vācija). Tostarp šaubīdamās par vairāku VDAR normu interpretāciju un piemērošanu, Federālās zemes Augstākā tiesa Diseldorfā vērsās Tiesā ar lūgumu sniegt prejudiciālu nolēmumu.

Virspalātas sastāvā pasludinātajā spriedumā Tiesa sniedz precizējumus par iespēju sociālā tīkla operatoram apstrādāt "sensitīvus" šā tīkla lietotāju personas datus, par šā operatora veiktās datu apstrādes likumīgumu, kā arī par tādas piekrišanas derīgumu, ko

lietotāji šādas apstrādes nolūkiem devuši valsts tiešsaistes sociālo tīklu tirgū dominējošā stāvoklī esošam uzņēmumam.

Attiecībā uz īpašu kategoriju personas datu apstrādi [98] Tiesa uzskata, ka gadījumā, ja tiešsaistes sociālā tīkla lietotājs aplūko tīmekļvietnes vai lietotnes, kas attiecas uz vienu vai vairākām no šīm kategorijām, un attiecīgā gadījumā tajās ievada datus, reģistrējoties vai veicot pasūtījumus tiešsaistē, šā tiešsaistes sociālā tīkla operatora veiktā personas datu apstrāde [99] ir jāuzskata par "īpašu kategoriju personas datu apstrādi" VDAR 9. panta 1. punkta izpratnē, ja tā ļauj atklāt informāciju, kas ietilpst kādā no šīm īpašajām kategorijām, neatkarīgi no tā, vai šī informācija attiecas uz minētā tīkla lietotāju vai jebkuru citu fizisku personu. Šāda datu apstrāde principā ir aizliegta, atskaitot dažus izņēmumus [100].

Par pēdējo minēto aspektu Tiesa precizē, ka tad, ja tiešsaistes sociālā tīkla lietotājs apmeklē tīmekļvietnes vai izmanto lietotnes, kas saistītas ar vienu vai vairākām minētajām īpašajām datu kategorijām, viņš šā aplūkojuma datus, ko tiešsaistes sociālā tīkla operators ir apkopojis, izmantojot sīkdatnes vai līdzīgas datu vākšanas tehnoloģijas, apzināti nedara publiski pieejamus [101]. Turklāt, kad viņš ievada datus šādās tīmekļvietnēs vai lietotnēs vai kad viņš izmanto šajās tīmekļvietnēs un lietotnēs integrētās atlases pogas, piemēram, pogas "patīk" vai "dalīties", vai pogas, kas ļauj lietotājam identificēties šajās vietnēs vai lietotnēs, izmantojot pieslēgšanās datus, kas sasaistīti ar viņa sociālā tīkla lietotāja kontu, tālruņa numuru vai e-pasta adresi, lietotājs šādi ievadītos vai pēc šo pogu izmantošanas iegūtos datus apzināti publisko tikai tad, ja viņš iepriekš ir skaidri paudis savu izvēli – vajadzības gadījumā ar individuāliem iestatījumiem, kas veikti, pilnībā apzinoties situāciju, – savus datus padarīt pieejamus neierobežotam personu lokam.

Attiecībā uz personas datu apstrādes likumīguma nosacījumiem vispārīgākā tvērumā Tiesa atgādina, ka saskaņā ar VDAR datu apstrāde ir likumīga, ja un ciktāl datu subjekts ir piekritis šādu datu apstrādei vienam vai vairākiem konkrētiem nolūkiem [102]. Ja šādas piekrišanas nav vai ja šāda piekrišana nav dota brīvi, konkrēti, apzināti un viennozīmīgi,

---

98 Minētas VDAR 9. panta 1. punktā. Šajā normā ir noteikts, ka "ir aizliegta tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde".

99 Šī apstrāde ietver datu, kas iegūti no šo vietņu aplūkošanas un lietotņu izmantošanas, kā arī lietotāju ievadīto datu vākšanu, izmantojot integrētas saskarnes, sīkdatnes un līdzīgas datu vākšanas tehnoloģijas, visu šo datu sasaisti ar lietotāja sociālā tīkla kontu, kā arī to, ka šis operators minētos datus izmanto.

100 Paredzēti VDAR 9. panta 2. punktā. Minētajā tiesību normā ir noteikts: "Šā panta 1. punktu nepiemēro, ja ir piemērojams kāds no šādiem pamatojumiem:

a) datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot, ja Savienības vai dalībvalsts tiesību akti paredz, ka 1. punktā minēto aizliegumu datu subjekts nevar atcelt; [..]

e) apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis;

f) apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības, vai ikreiz, kad tiesas pilda savus uzdevumus;

[..]".

101 VDAR 9. panta 2. punkta e) apakšpunkta izpratnē.

102 Saskaņā ar VDAR 6. panta 1. punkta pirmās daļas a) apakšpunktu.

šāda apstrāde tomēr ir attaisnota, ja tā atbilst kādai no nepieciešamības prasībām [103], kas jāinterpretē šauri. Taču lietotāju personas datu apstrādi, ko veic tiešsaistes sociālā tīkla operators, var uzskatīt par nepieciešamu līguma, kura līgumslēdzējas puses ir šie lietotāji, izpildei tikai tad, ja šī apstrāde ir objektīvi nepieciešama, lai sasniegtu mērķi, kas ir lietotājiem paredzētā līgumiskā pakalpojuma neatņemama sastāvdaļa tādā ziņā, ka bez šīs apstrādes līguma galveno mērķi nevarētu sasniegt.

Turklāt Tiesa atzīst, ka attiecīgo datu apstrādi var uzskatīt par vajadzīgu pārziņa vai trešās personas leģitīmo interešu mērķiem tikai tad, ja operators lietotājiem, kuru dati ir ievākti, ir norādījis datu apstrādes pamatā esošās leģitīmās intereses, ja šī apstrāde tiek veikta šo leģitīmo interešu īstenošanai tikai absolūti nepieciešamajā apmērā un ja no pretnostatīto interešu samērošanas, kas veikta, ņemot vērā visus nozīmīgos apstākļus, izriet, ka lietotāju intereses vai pamattiesības un pamatbrīvības neprevalē pār minētajām pārziņa vai trešās personas leģitīmajām interesēm. Tiesa it īpaši uzskata, ka gadījumā, ja lietotāji nav devuši piekrišanu šādai apstrādei, viņu intereses un pamattiesības prevalē pār tiešsaistes sociālā tīkla operatora interesi personalizēt reklāmu, ar kuru tas finansē savu darbību.

Tiesa visbeidzot precizē, ka attiecīgā datu apstrāde ir pamatota, ja tā ir patiešām nepieciešama, lai izpildītu likumisku pienākumu, kas pārzinim uzlikts vai nu saskaņā ar Savienības, vai attiecīgās dalībvalsts tiesību normām, ja šis juridiskais pamats atbilst sabiedrības interešu mērķim un ir samērīgs ar izvirzīto leģitīmo mērķi un ja šī apstrāde tiek veikta tikai absolūti nepieciešamajā apmērā.

Runājot par attiecīgo lietotāju piekrišanas viņu datu apstrādei derīgumu saskaņā ar VDAR, Tiesa uzskata – apstāklis, ka tiešsaistes sociālā tīkla operatoram ir dominējošs stāvoklis tiešsaistes sociālo tīklu tirgū, pats par sevi nav šķērslis tam, ka šāda tīkla lietotāji var dot derīgu piekrišanu operatora veiktajai lietotāju personas datu apstrādei. Taču, ņemot vērā, ka šāds stāvoklis var ietekmēt šo lietotāju izvēles brīvību un radīt acīmredzamu nevienlīdzību starp tiem un minēto operatoru, tas ir būtisks elements, lai noteiktu, vai dotā piekrišana patiešām ir derīga un – it īpaši – sniegta brīvi, un tas ir jāpierāda operatoram [104].

Proti, šiem attiecīgā tiešsaistes sociālā tīkla lietotājiem ir jābūt iespējai līguma slēgšanas gaitā brīvi atteikties individuāli piekrist konkrētām datu apstrādes darbībām, kas nav nepieciešamas līguma izpildei, bez vajadzības vienlaikus pilnībā atteikties no šā tiešsaistes sociālā tīkla lietošanas, un tas nozīmē, ka minētajiem lietotājiem vajadzības gadījumā par atbilstošu atlīdzību ir jābūt piedāvātai līdzvērtīgai alternatīvai bez šādām

[103] Minētas VDAR 6. panta 1. punkta pirmās daļas b)–f) apakšpunktā. Saskaņā ar šīm tiesību normām apstrāde ir likumīga tikai tad un tiktāl, ciktāl apstrāde citastarp ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei (VDAR 6. panta 1. punkta pirmās daļas b) apakšpunkts), lai izpildītu pārzinim uzliktu likumisku pienākumu (VDAR 6. panta 1. punkta pirmās daļas c) apakšpunkts) vai lai ievērotu pārziņa vai trešās personas leģitīmās intereses (VDAR 6. panta 1. punkta pirmās daļas f) apakšpunkts).

[104] Atbilstoši VDAR 7. panta 1. punktam.

datu apstrādes darbībām. Turklāt ir jābūt iespējai sniegt atsevišķu piekrišanu *off Facebook* datu apstrādei.

VI. Valsts uzraudzības iestādes

1. Prasības par neatkarību tvērums

2010. gada 9. marta spriedums (virspalāta) Komisija/Vācija (C-518/07, EU:C:2010:125)

Ar savu prasības pieteikumu Komisija lūdza Tiesu atzīt, ka Vācijas Federatīvā Republika, pakļaujot dažādās federālajās zemēs valsts pārraudzībai uzraudzības iestādes, kuru kompetencē ir uzraudzīt personu datu apstrādi privātajā sektorā, un tādējādi kļūdaini transponējot prasību par iestāžu, kam ir jānodrošina šo datu aizsardzība, "pilnīgu neatkarību", nav izpildījusi pienākumus, kas tai paredzēti Direktīvas 95/46 28. panta 1. punkta otrajā daļā.

Vācijas Federatīvā Republika savukārt uzskatīja, ka Direktīvas 95/46 28. panta 1. punkta otrajā daļā ir paredzēta uzraudzības iestāžu funkcionāla neatkarība tādā ziņā, ka šīm iestādēm ir jābūt neatkarīgām no privātā sektora iestādēm, kas ir to uzraudzības objekts, un ka tām nav jābūt pakļautām ārējai ietekmei. Tomēr tā pauda viedokli, ka Vācijas federālajās zemēs īstenotā valsts pārraudzība nav šāda ārējā ietekme, bet administrācijas iekšējās uzraudzības mehānisms, kuru īsteno iestādes, kas ietilpst tajā pašā administratīvajā aparātā, kurā ir uzraudzības iestādes, un kam tāpat kā šīm uzraudzības iestādēm ir jāīsteno Direktīvas 95/46 mērķi.

Tiesa nosprieda, ka Direktīvā 95/46 paredzētās valsts uzraudzības iestāžu neatkarības garantijas mērķis ir nodrošināt efektīvu un uzticamu kontroli pār tiesību normu ievērošanu saistībā ar fizisko personu aizsardzību attiecībā uz personas datu apstrādi un tā ir jāinterpretē šī mērķa kontekstā. Šī neatkarības garantija ir iedibināta nevis tādēļ, lai piešķirtu minētajām iestādēm, kā arī to pārstāvjiem īpašu statusu, bet lai pastiprinātu personu un struktūru, kuras skar to lēmumi, aizsardzību, jo tādējādi uzraudzības iestādēm savu pienākumu izpildē ir jārīkojas objektīvi.

Tiesa uzskatīja, ka šīm uzraudzības iestādēm, kuru kompetencē ir uzraudzīt personas datu apstrādi privātajā sektorā, ir jābūt neatkarīgām tādā apjomā, kas tām ļauj veikt savus pienākumus bez ārējās ietekmes. Šī neatkarība izslēdz ne vien jebkādu ietekmi, ko īsteno uzraugāmās iestādes, bet arī jebkādus rīkojumus un cita veida ārējo ietekmi, tiešu vai netiešu, kura varētu apdraudēt minēto iestāžu pienākumu izpildi, kas ietver taisnīga līdzsvara izveidošanu starp tiesību uz privāto dzīvi aizsardzību un personas datu brīvu apriti. Iespēja vien, ka pārraudzības iestādes var īstenot politisku ietekmi pār kompetentu uzraudzības iestāžu lēmumiem, ir pietiekama, lai radītu šķēršļus neatkarīgai

to pienākumu izpildei. Pirmkārt, šīs iestādes varētu izrādīt "iepriekšēju pakļaušanos", ņemot vērā pārraudzības iestāžu lēmumu pieņemšanas praksi. Otrkārt, tiesību uz privāto dzīvi garanta loma, ko nodrošina minētās uzraudzības iestādes, nozīmē, ka to lēmumi un tātad pašas šīs iestādes ir ārpus jebkādām aizdomām par neobjektivitāti. Tiesa uzskatīja, ka valsts īstenotā pārraudzība pār valsts uzraudzības iestādēm nav saderīga ar prasību par neatkarību.

2012. gada 16. oktobra spriedums (virspalāta) Komisija/Austrija (C-614/10, EU:C:2012:631)

Savā prasības pieteikumā Komisija lūdza Tiesu konstatēt, ka, nepieņemot visus vajadzīgos noteikumus, lai Austrijā spēkā esošie tiesību akti atbilstu neatkarības kritērijam attiecībā uz *Datenschutzkommission* (Datu aizsardzības komisija), kas tika izveidota kā personas datu aizsardzības uzraudzības iestāde, Austrija nav izpildījusi Direktīvas 95/46 28. panta 1. punkta otrajā daļā paredzētos pienākumus.

Tiesa konstatēja, ka Austrija nav izpildījusi valsts pienākumus, būtībā uzskatot, ka uzraudzības iestādes neatkarības kritēriju, kurš noteikts ar Direktīvu 95/46, nav izpildījusi dalībvalsts, kas ievieš tiesisko regulējumu, saskaņā ar kuru minētās iestādes administrators ir valsts ierēdnis, kas pakļauts uzraudzībai, kura birojs ir iekļauts valsts valdības dienestos un attiecībā uz ko valsts valdības vadītājam ir beznosacījuma tiesības saņemt informāciju par jebkādiem minētās iestādes vadības aspektiem.

Tiesa vispirms atgādināja, ka Direktīvas 95/46 28. panta 1. punkta otrajā daļā minētais jēdziens "pilnīgi neatkarīgi" nozīmē, ka uzraudzības iestādēm ir jābūt neatkarīgām tādā apjomā, kas tām ļauj veikt savus pienākumus bez ārējas ietekmes. Šajā ziņā ar apstākli vien, ka šāda iestāde ir funkcionāli neatkarīga, jo tās locekļi ir neatkarīgi un, pildot savus pienākumus, tiem nav saistoši nekādi norādījumi, nepietiek, lai minēto uzraudzības iestādi pasargātu no jebkādas ārējas ietekmes. Taču šajos ietvaros pieprasītās neatkarības mērķis ir izslēgt ne tikai tiešu ietekmi, kas izpaužas norāžu veidā, bet arī jebkāda veida netiešu ietekmi, kas varētu iespaidot uzraudzības iestādes lēmumus. Turklāt, ņemot vērā tiesību uz privāto dzīvi garanta lomu, ko nodrošina uzraudzības iestādes, to lēmumiem un tātad pašām šīm iestādēm ir jābūt ārpus jebkādām aizdomām par neobjektivitāti.

Tiesa precizēja, ka valsts uzraudzības iestādei, lai tā atbilstu iepriekš minētajā Direktīvas 95/46 noteikumā paredzētajam neatkarības kritērijam, nav jābūt tādai atsevišķai budžeta pozīcijai kā tai, kas ir paredzēta Regulas Nr. 45/2001 43. panta 3. punktā. Dalībvalstīm faktiski nav pienākuma savos valsts tiesību aktos pārņemt noteikumus, kas ir analogi Regulas Nr. 45/2001 V nodaļā paredzētajiem, lai nodrošinātu savas(-u) uzraudzības iestādes(-žu) pilnīgu neatkarību, un tādējādi tās var paredzēt, ka no budžeta tiesību viedokļa uzraudzības iestāde ir pakļauta noteiktam ministrijas departamentam. Tomēr nepieciešamo cilvēku un materiālo resursu piešķiršana šādai iestādei nedrīkstētu tai traucēt pildīt savus pienākumus "pilnīgi neatkarīgi" Direktīvas 95/46 28. panta 1. punkta otrās daļas izpratnē.

2014. gada 8. aprīļa spriedums (virspalāta) Komisija/Ungārija (C-288/12, EU:C:2014:237)

Šajā lietā Komisija bija lūgusi Tiesu konstatēt, ka, priekšlaicīgi izbeidzot Personas datu aizsardzības uzraudzības iestādes pilnvaru termiņu, Ungārija nav izpildījusi pienākumus, kas tai ir noteikti Direktīvā 95/46.

Tiesa nosprieda, ka, priekšlaicīgi izbeidzot Personas datu aizsardzības uzraudzības iestādes pilnvaru termiņu, dalībvalsts nav izpildījusi pienākumus, kas tai ir noteikti Direktīvā 95/46/EK.

Tiesa uzskatīja, ka uzraudzības iestāžu, kuras atbild par minēto datu apstrādes uzraudzību, nepieciešamā neatkarība izslēdz it īpaši jebkādu rīkojumu došanu un jebkādu citu ārēju ietekmi – vai tā būtu tieša vai netieša –, kura varētu iespaidot to lēmumus un kura tādējādi varētu apdraudēt minēto iestāžu pienākumu izpildi, kas ietver taisnīga līdzsvara nodrošināšanu starp tiesību uz privāto dzīvi aizsardzību un personas datu brīvu apriti.

Turklāt Tiesa atgādināja, ka ar šādu funkcionālu neatkarību vien nepietiek, lai uzraudzības iestādes pasargātu no jebkādas ārējas ietekmes, jo iespēja vien, ka valsts pārraudzības iestādes var īstenot politisku ietekmi pār uzraudzības iestāžu lēmumiem, ir pietiekama, lai radītu šķēršļus tās neatkarīgai pienākumu izpildei. Tomēr, ja katrai dalībvalstij būtu atļauts pirms tās sākotnēji paredzētā termiņa izbeigt uzraudzības iestādes pilnvaras, neievērojot piemērojamos tiesību aktos šajā nolūkā iepriekš noteiktos noteikumus un garantijas, šādas priekšlaicīgas izbeigšanas draudi, kas šai iestādei pastāvētu visā tās pilnvaru termiņa laikā, varētu izraisīt to, ka tā zināmā veidā pakļaujas politiskajai varai, kas nav saderīgi ar minēto neatkarības prasību. Turklāt šādā situācijā uzraudzības iestādi nevarētu uzskatīt par spējīgu darboties jebkuros apstākļos, nepastāvot nekādām aizdomām par neobjektivitāti.

2. Piemērojamo tiesību un kompetentās uzraudzības iestādes noteikšana

2015. gada 1. oktobra spriedums Weltimmo (C-230/14, EU:C:2015:639)

Nemzeti Adatvédelmi és Információszabadság Hatóság (Valsts iestāde, kuras uzdevums ir datu un informācijas brīvības aizsardzība, Ungārija) piemēroja naudas sodu *Weltimmo*, kas ir Slovākijā reģistrēta sabiedrība un kas pārvalda tīmekļvietnes, kurās atrodami sludinājumi par Ungārijā esošiem nekustamā īpašuma objektiem, par to, ka tā, neraugoties uz sludinājumu ievietotāju pieprasījumiem, neizdzēsa viņu personas datus no šīm vietnēm un izpauda šos datus parādu piedziņas iestādēm, lai saņemtu neapmaksātajos rēķinos norādītās summas. Ungārijas uzraudzības iestāde uzskata, ka sabiedrība *Weltimmo*, šādi rīkojoties, ir pārkāpusi Ungārijas tiesību aktus, ar kuriem ir transponēta Direktīva 95/46.

Kúria (Augstākā tiesa, Ungārija), kurā tika iesniegta kasācijas sūdzība, bija šaubas par piemērojamām tiesībām un Ungārijas uzraudzības iestādes pilnvarām, ņemot vērā Direktīvas 95/46 4. panta 1. punktu un 28. pantu. Tādēļ tā uzdeva Tiesai vairākus prejudiciālus jautājumus.

Runājot par piemērojamiem valsts tiesību aktiem, Tiesa nosprieda, ka Direktīvas 95/46 4. panta 1. punkta a) apakšpunktā ir ļauts piemērot citas dalībvalsts, kas nav tā, kurā ir reģistrēts šo datu pārzinis, tiesību aktus par personas datu aizsardzību, ciktāl tas, izmantojot stabilu veidojumu šīs dalībvalsts teritorijā, veic reālu un faktisku darbību – pat ja tā ir minimāla –, kuras ietvaros notiek šī apstrāde. Lai noteiktu, vai tas tā ir, iesniedzējtiesa var it īpaši ņemt vērā faktu, ka, pirmkārt, attiecīgā pārziņa darbība, kuras ietvaros šī apstrāde notiek, izpaužas kā tādu nekustamā īpašuma sludinājumu interneta vietņu pārvaldīšana, kuras attiecas uz šīs dalībvalsts teritorijā esošiem nekustamā īpašuma objektiem un kuras ir šīs dalībvalsts valodā, un kuras tādējādi galvenokārt vai pat pilnībā ir vērstas uz minēto dalībvalsti. Iesniedzējtiesa var ņemt vērā, otrkārt, arī to, ka šim pārzinim minētajā dalībvalstī ir pārstāvis, kura uzdevums ir piedzīt no šīs darbības izrietošos prasījumus, kā arī to pārstāvēt administratīvajos procesos un tiesvedībās saistībā ar attiecīgo datu apstrādi. Tiesa savukārt precizēja, ka jautājumam par attiecīgo datu subjektu valstspiederību nav nozīmes.

Runājot par tās uzraudzības iestādes kompetenci un pilnvarām, kurā tiek iesniegtas sūdzības atbilstoši Direktīvas 95/46 28. panta 4. punktam, Tiesa uzskatīja, ka šī iestāde var izskatīt šīs sūdzības neatkarīgi no piemērojamām tiesībām un pat pirms tā zina, kuras valsts tiesības attiecīgajai apstrādei ir piemērojamas. Tomēr, ja šī iestāde secina, ka ir piemērojamas citas dalībvalsts tiesības, tā nevar piemērot sankcijas ārpus tās dalībvalsts teritorijas, kurai tā ir piederīga. Šādā situācijā tai, izpildot šīs direktīvas 28. panta 6. punktā paredzēto sadarbības pienākumu, ir jāpieprasa otras dalībvalsts uzraudzības iestādei konstatēt iespējamu šo tiesību pārkāpumu un piemērot sankcijas, ja šajās tiesībās tas ir atļauts, attiecīgā gadījumā balstoties uz informāciju, kuru šī iestāde tai būtu sniegusi.

3. Valstu uzraudzības iestāžu pilnvaras

2015. gada 6. oktobra spriedums (virspalāta) Schrems (C-362/14, EU:C:2015:650)

Šajā lietā (skat. arī IV sadaļu “Personas datu nosūtīšana uz trešām valstīm”) Tiesa tostarp nosprieda, ka valsts uzraudzības iestāžu kompetencē ietilpst personas datu pārsūtīšanas uz trešām valstīm uzraudzība.

Šajā saistībā Tiesa vispirms konstatēja, ka valsts uzraudzības iestādēm ir virkne pilnvaru un ka šīs pilnvaras, kuras neizsmeļošā veidā ir uzskaitītas Direktīvas 95/46 28. panta 3. punktā, ir līdzekļi, kas ir vajadzīgi šo iestāžu uzdevumu izpildē. Tādējādi minētajām

iestādēm ir tostarp izmeklēšanas pilnvaras, piemēram, pilnvaras ievākt visu tās uzraudzības pienākumu izpildei vajadzīgo informāciju, efektīvas iejaukšanās pilnvaras, piemēram, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, vai arī pilnvaras iesaistīties tiesvedībā.

Runājot par pilnvarām uzraudzīt personas datu pārsūtīšanu uz trešām valstīm, Tiesa nosprieda, ka no Direktīvas 95/46 28. panta 1. un 6. punkta, protams, izriet, ka valstu uzraudzības iestāžu pilnvaras attiecas uz personas datu apstrādi dalībvalsts teritorijā, kurā šīs iestādes atrodas, un, pamatojoties uz šo 28. pantu, to pilnvaras nesniedzas līdz šādu datu apstrādei, kas veikta trešās valsts teritorijā.

Tomēr darbība, kurā ietilpst personas datu pārsūtīšana no dalībvalsts uz trešo valsti, kā tāda ir personas datu apstrāde, kas veikta dalībvalsts teritorijā. Tādējādi valstu uzraudzības iestāžu ziņā saskaņā ar Hartas 8. panta 3. punktu un Direktīvas 95/46 28. pantu ir kontrolēt, vai tiek ievērotas Savienības tiesību normas par fizisku personu aizsardzību saistībā ar personas datu apstrādi, ikviena no tām tātad ir apveltīta ar pilnvarām pārbaudīt, vai šo datu pārsūtīšanā no dalībvalsts, kurā tā darbojas, uz trešo valsti ir ievērotas šajā direktīvā izvirzītās prasības.

2018. gada 5. jūnija spriedums (virspalāta) Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

Šajā spriedumā (skat. arī II.5. sadaļu "Jēdziens "personas datu pārzinis""), kas tostarp attiecas uz Direktīvas 95/46 4. un 28. panta interpretāciju, Tiesa sprieda par to iejaukšanās pilnvaru apmēru, kādas uzraudzības iestādēm ir attiecībā uz personas datu apstrādi, kurā ir iesaistīti vairāki dalībnieki.

Tādējādi Tiesa nosprieda, ka tad, ja ārpus Eiropas Savienības iedibinātam uzņēmumam (piemēram, ASV sabiedrībai *Facebook*) ir vairāki dažādās dalībvalstīs esoši dibinājumi, pilnvaras, kas kādas dalībvalsts uzraudzības iestādei ir piešķirtas šīs direktīvas 28. panta 3. punktā, šī iestāde ir tiesīga izmantot attiecībā uz šīs dalībvalsts teritorijā esošu šā uzņēmuma dibinājumu (šajā gadījumā *Facebook Germany*) pat tad, ja atbilstoši koncerna ietvaros esošajam uzdevumu sadalījumam, pirmkārt, šā dibinājuma pārziņā ir tikai reklāmas laukumu pārdošana un citas mārketinga darbības minētās dalībvalsts teritorijā un, otrkārt, ekskluzīvā atbildība par personas datu vākšanu un apstrādi visā Eiropas Savienības teritorijā ir dibinājumam, kas atrodas kādā citā dalībvalstī (šajā gadījumā *Facebook Ireland*).

Turklāt Tiesa precizēja, ka tad, ja dalībvalsts uzraudzības iestāde grasās attiecībā uz šīs dalībvalsts teritorijā iedibinātu struktūru izmantot Direktīvas 95/46 28. panta 3. punktā paredzētās iejaukšanās pilnvaras, tāpēc ka personas datu aizsardzības noteikumu pārkāpumu izdara kāda trešā persona, kura ir šo personas datu pārzinis un kuras juridiskā adrese ir kādā citā dalībvalstī (šajā gadījumā *Facebook Ireland*), šīs uzraudzības iestādes kompetencē ir neatkarīgi no šīs otras dalībvalsts (Īrijas) uzraudzības iestādes izvērtēt šādas apstrādes likumību un tā var īstenot savas iejaukšanās pilnvaras attiecībā

uz tās teritorijā iedibināto struktūru, iepriekš neaicinot otrās dalībvalsts uzraudzības iestādes iejaukties.

2021. gada 15. jūnija spriedums (virspalāta) Facebook Ireland u.c. (C-645/19, EU:C:2021:483)

2015. gada 11. septembrī Beļģijas Privātās dzīves aizsardzības komisijas (turpmāk tekstā – "PDzAK") priekšsēdētājs vērsās *Nederlandstalige rechtbank van eerste aanleg Brussel* (Briseles pirmās instances tiesa, kurā tiesvedība noris holandiešu valodā, Beļģija) pret *Facebook Ireland*, *Facebook Inc*. un *Facebook Belgium* ar prasību noteikt aizliegumu, lai panāktu, ka *Facebook* izbeidz apgalvotos datu aizsardzības tiesību aktu pārkāpumus. Konkrēti šie pārkāpumi izpaudās kā informācijas vākšana un izmantošana par Beļģijā esošo interneta lietotāju, kuriem ir vai nav *Facebook* konts, tīklklejošanas darbībām, izmantojot dažādas tehnoloģijas, piemēram, sīkdatnes, sociālos spraudņus [105] vai pikseļus.

2018. gada 16. februārī minētā tiesa atzina, ka izskatīt šo prasību ir tās kompetencē un, izskatījusi šo lietu pēc būtības, nosprieda, ka sociālais tīkls *Facebook* nav pietiekami informējis Beļģijā esošos interneta lietotājus par attiecīgās informācijas vākšanu un izmantošanu. Turklāt interneta lietotāju dotā piekrišana minētās informācijas ievākšanai un apstrādei tika atzīta par nederīgu.

2018. gada 2. martā *Facebook Ireland*, *Facebook Inc*. un *Facebook Belgium* pārsūdzēja šo spriedumu *Hof van beroep te Brussel* (Briseles apelācijas tiesa), kas ir iesniedzējtiesa šajā lietā. Minētajā tiesā Beļģijas Datu aizsardzības iestāde (turpmāk tekstā – "DAI") rīkojās kā PDzAK priekšsēdētāja tiesību pārņēmēja. Iesniedzējtiesa atzina, ka tās kompetencē ir lemt tikai par apelācijas sūdzību, ko iesniegusi *Facebook Belgium*.

Iesniedzējtiesai bija šaubas par VDAR paredzētā "vienas pieturas aģentūras" mehānisma [106] piemērošanas ietekmi uz DAI pilnvarām, un it īpaši radās jautājums, vai par faktiem, kas radušies pēc VDAR stāšanās spēkā, proti, pēc 2018. gada 25. maija, DAI var vērsties pret *Facebook Belgium*, jo kā attiecīgo datu pārzine ir identificēta *Facebook Ireland*. Proti, kopš šā datuma un it īpaši, piemērojot VDAR paredzēto "vienas pieturas aģentūras" principu, prasību atturēties no noteiktām darbībām esot tiesīgs celt tikai Īrijas Datu aizsardzības komisārs un tas esot darāms Īrijas tiesu kontrolē.

Šajā virspalātas sastāvā pasludinātajā spriedumā Tiesa precizē valsts uzraudzības iestāžu pilnvaras VDAR ietvaros. Tādējādi tā tostarp nospriež, ka ar šo regulu dalībvalsts uzraudzības iestādei, ievērojot vairākus nosacījumus, ir atļauts īstenot savas pilnvaras vērst šīs valsts tiesu iestāžu uzmanību uz jebkādiem iespējamiem VDAR pārkāpumiem

[105] Piemēram, pogas "patīk" vai "dalīties".

[106] VDAR 56. panta 1. punkts noteic: "Neskarot 55. pantu, galvenās uzņēmējdarbības vietas vai pārziņa vai apstrādātāja darbības vietas uzraudzības iestāde ir kompetenta rīkoties kā vadošā uzraudzības iestāde attiecībā uz minētā pārziņa vai apstrādātāja veiktu pārrobežu apstrādi."

un sākt tiesvedību saistībā ar pārrobežu datu apstrādi [107] arī tad, ja attiecībā uz šo apstrādi tā nav vadošā uzraudzības iestāde.

Pirmkārt, Tiesa precizē nosacījumus, ar kādiem valsts uzraudzības iestādei, kurai nav vadošās iestādes statusa saistībā ar pārrobežu datu apstrādi, ir jāīsteno savas pilnvaras vērst tiesu iestāžu uzmanību uz jebkādiem iespējamiem VDAR pārkāpumiem un vajadzības gadījumā sākt tiesvedību, lai nodrošinātu šīs regulas piemērošanu. Tādējādi, pirmām kārtām, ar VDAR šai uzraudzības iestādei ir jāpiešķir kompetence pieņemt lēmumu, ar kuru konstatē, ka ar šo apstrādi netiek ievēroti minētajā regulā paredzētie noteikumi, un, otrām kārtām, šīs pilnvaras ir jāīsteno, ievērojot attiecīgajā regulā paredzētās sadarbības un konsekvences procedūras [108].

Proti, attiecībā uz pārrobežu datu apstrādi VDAR ir paredzēts "vienas pieturas aģentūras" mehānisms [109], kas ir balstīts uz kompetenču sadalījumu starp "vadošo uzraudzības iestādi" un pārējām attiecīgajām valsts uzraudzības iestādēm. Šim mehānismam ir nepieciešama cieša, lojāla un efektīva sadarbība starp šīm iestādēm, lai nodrošinātu noteikumu par personas datu aizsardzību konsekventu un viendabīgu aizsardzību un tādējādi saglabātu tā lietderīgo iedarbību. Šajā ziņā vadošajai uzraudzības iestādei VDAR ir paredzēta galvenā kompetence pieņemt lēmumu, ar ko konstatē, ka pārrobežu apstrādē ir pārkāptas šīs regulas normas[110], kamēr pārējo valsts uzraudzības iestāžu kompetencei šāda lēmuma pieņemšanai – pat tikai pagaidu kārtā – ir izņēmuma raksturs [111]. Tomēr savu pilnvaru īstenošanā vadošā uzraudzības iestāde nevar atmest būtisko dialogu, kā arī lojālu un efektīvu sadarbību ar pārējām attiecīgajām uzraudzības iestādēm. Tādēļ šīs sadarbības ietvaros vadošā uzraudzības iestāde nevar neņemt vērā citu attiecīgo uzraudzības iestāžu viedokli un jebkurš būtisks un motivēts iebildums, ko izteikusi kāda no šīm iestādēm, vismaz uz laiku bloķē vadošās uzraudzības iestādes lēmuma projekta pieņemšanu.

Turklāt Tiesa precizē, ka apstāklis, ka dalībvalsts uzraudzības iestāde, kas nav vadošā uzraudzības iestāde attiecībā uz pārrobežu datu apstrādi, pilnvaras – vērst šīs dalībvalsts tiesu uzmanību uz jebkādu iespējamu VDAR pārkāpumu un sākt tiesvedību – var īstenot, tikai ievērojot lēmumu pieņemšanas pilnvaru sadali starp vadošo uzraudzības iestādi un pārējām uzraudzības iestādēm [112], atbilst Hartas 7., 8. un 47. pantam, kuros datu subjektam garantētas tiesības attiecīgi uz savu personas datu aizsardzību un tiesības uz efektīvu tiesību aizsardzību.

Otrkārt, Tiesa nospriež, ka datu pārrobežu apstrādes gadījumā dalībvalsts uzraudzības iestādes, kas nav vadošā uzraudzības iestāde, iespēja izmantot pilnvaras celt prasību

[107] VDAR 4. panta 23. punkta izpratnē.
[108] Paredzētas VDAR 56. un 60. pantā.
[109] VDAR 56. panta 1. punkts.
[110] VDAR 60. panta 7. punkts.
[111] VDAR 56. panta 2. punktā un 66. pantā ir paredzēti izņēmumi no vadošās uzraudzības iestādes lēmumu pieņemšanas kompetences principa.
[112] Tā ir paredzēta VDAR 55. un 56. pantā, lasot tos kopā ar 60. pantu.

tiesā [113] nav pakārtota priekšnosacījumam, ka personas datu pārrobežu apstrādes pārzinim vai to veicošajam apstrādātājam, pret kuru ir celta šī prasība, šīs dalībvalsts teritorijā ir jābūt galvenajai uzņēmējdarbības vietai vai kādam citam dibinājumam. Tomēr šo pilnvaru īstenošanai ir jāietilpst VDAR teritoriālās piemērošanas jomā [114], un tas nozīmē, ka personas datu pārrobežu apstrādes pārzinim vai to veicošajam apstrādātājam ir jābūt dibinājumam Savienības teritorijā.

Treškārt, Tiesa nosprież, ka datu pārrobežu apstrādes gadījumā tādas dalībvalsts uzraudzības iestādes, kas nav vadošā uzraudzības iestāde, pilnvaras vērst šīs valsts tiesu iestāžu uzmanību uz jebkuru iespējamu VDAR pārkāpumu un vajadzības gadījumā sākt tiesvedību, var tikt izmantotas gan pret pārziņa galveno uzņēmējdarbības vietu, kas atrodas šīs iestādes dalībvalstī, gan pret citu šā pārziņa dibinājumu, ja vien šīs prasības priekšmets ir datu apstrāde saistībā ar šā dibinājuma darbībām un šī iestāde ir kompetenta īstenot šīs pilnvaras.

Tomēr Tiesa precizē, ka šo pilnvaru īstenošanas priekšnoteikums ir VDAR piemērojamība. Šajā gadījumā, tā kā Beļģijā esošās *Facebook* grupas uzņēmējdarbības vietas darbības ir nesaraujami saistītas ar pamatlietā aplūkoto personas datu apstrādi, attiecībā uz kuru *Facebook Ireland* ir pārzinis Savienības teritorijā, šī apstrāde tiek veikta "saistībā ar darbībām, ko veic pārziņa [..] uzņēmējdarbības vietā", un tātad ietilpst VDAR piemērošanas jomā.

Ceturtkārt, Tiesa nosprież, ka, ja dalībvalsts uzraudzības iestāde, kas nav "vadošā uzraudzības iestāde", pirms VDAR stāšanās spēkā ir cēlusi prasību tiesā par personas datu pārrobežu apstrādi, šo prasību no Savienības tiesību viedokļa var turpināt uzturēt, pamatojoties uz Direktīvas 95/46 noteikumiem, kura joprojām ir piemērojama tās noteikumu pārkāpumiem, kas izdarīti līdz šīs direktīvas atcelšanas datumam. Turklāt šī iestāde var celt minēto prasību par pārkāpumiem, kas izdarīti pēc VDAR stāšanās spēkā, ja vien runa ir par kādu no situācijām, kurās ar šo regulu izņēmuma kārtā minētajai iestādei ir piešķirta kompetence pieņemt lēmumu, kurā konstatēts, ka ar attiecīgo datu apstrādi nav ievērotas šajā regulā ietvertās normas, un ja vien šī iestāde ievēro šajā regulā paredzētās sadarbības un konsekvences procedūras.

Visbeidzot, piektkārt, Tiesa atzīst, ka VDAR tiesību norma – saskaņā ar kuru katra dalībvalsts ar tiesību aktiem paredz, ka tās uzraudzības iestādei ir pilnvaras pievērst tiesu iestāžu uzmanību šīs regulas pārkāpumiem un vajadzības gadījumā sākt tiesvedību, – ir apveltīta ar tiešu iedarbību. Līdz ar to minētā iestāde var atsaukties uz šo tiesību normu, lai celtu vai uzturētu prasību pret privātpersonām, pat ja šī tiesību norma nav tikusi īpaši ieviesta attiecīgās dalībvalsts tiesību aktos.

[113] Atbilstoši VDAR 58. panta 5. punktam.

[114] VDAR 3. panta 1. punktā ir noteikts, ka šo regulu piemēro personas datu apstrādei "saistībā ar darbībām, ko veic pārziņa vai apstrādātāja uzņēmējdarbības vietā Savienībā, neatkarīgi no tā, vai apstrāde notiek vai nenotiek Savienībā".

2024. gada 16. janvāra spriedums (virspalāta) Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Šajā lietā (skat. arī II.1. sadaļu "Vispārējā tiesiskā regulējuma piemērošanas joma") Tiesa norāda, ka VDAR normas par valsts uzraudzības iestāžu kompetenci un tiesībām iesniegt sūdzību [115] neprasa pieņemt valsts piemērošanas pasākumus un ir pietiekami skaidras, precīzas un beznosacījuma, lai būtu apveltītas ar tiešu iedarbību. No tā izriet, ka, lai arī atstājot dalībvalstīm rīcības brīvību attiecībā uz izveidojamo uzraudzības iestāžu skaitu [116], VDAR tomēr noteic pilnvaru apjomu, ar kādām šīm iestādēm jābūt apveltītām, lai uzraudzītu VDAR piemērošanu. Tādējādi gadījumā, ja dalībvalsts izvēlas izveidot tikai vienu valsts uzraudzības iestādi, šai iestādei noteikti ir piešķirtas visas šajā regulā paredzētās pilnvaras. Jebkura citāda interpretācija apdraudētu šo normu lietderīgo iedarbību un draudētu vājināt lietderīgo iedarbību visām pārējām VDAR normām, uz kurām varētu attiekties sūdzība.

Attiecībā uz apstākli, ka valsts konstitucionāla ranga tiesību normas aizliedz izpildvarai pakļautajai uzraudzības iestādei uzraudzīt to, kā VDAR piemēro likumdošanas varai piederīgs orgāns, Tiesa uzsver, ka, tieši ievērojot dalībvalstu konstitucionālo iekārtu, VDAR ir vienīgi prasīts, lai tās izveidotu vismaz vienu uzraudzības iestādi, vienlaikus piedāvājot tām iespēju izveidot vairākas uzraudzības iestādes. Tādējādi VDAR katrai dalībvalstij ir atzīta rīcības brīvība, kas tai ļauj izveidot tik daudz uzraudzības iestāžu, cik tas var būt nepieciešams tostarp tālab, lai izpildītu prasības, kas saistītas ar tās konstitucionālo iekārtu.

Turklāt dalībvalsts atsaukšanās uz valsts tiesību normām nevar apdraudēt Savienības tiesību vienotību un efektivitāti. Proti, Savienības tiesību pārākuma principam piemītošās sekas ir saistošas visām dalībvalsts struktūrām, un valsts tiesību normas, tostarp konstitucionāla ranga, nevar tam radīt šķērsli.

Tādējādi situācijā, kad dalībvalsts ir izvēlējusies izveidot tikai vienu uzraudzības iestādi, tā nevar no šīs iestādes uzraudzības atbrīvot VDAR piemērošanas jomā ietilpstošu personas datu apstrādi, atsaucoties uz valsts tiesību normām, pat ja tām ir konstitucionāls rangs.

[115] Attiecīgi VDAR 55. panta 1. punkts un 77. panta 1. punkts.
[116] Saskaņā ar VDAR 51. panta 1. punktu.

4. Administratīvo naudas sodu piemērošanas nosacījumi

2023. gada 5. decembra spriedums (virspalāta) Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Šajā lietā (skat. arī II.3. sadaļu "Jēdziens "personas datu apstrāde"", II.5. sadaļu "Jēdziens "personas datu pārzinis"" un II.6. sadaļu "Jēdziens "kopīgs pārzinis"") Tiesa konstatē, ka saskaņā ar VDAR 83. pantu administratīvu naudas sodu pārzinim var piemērot tikai tad, ja ir pierādīts, ka tas šajā regulā ietvertos noteikumus ir pārkāpis tīši vai aiz neuzmanības [117].

Šajā ziņā Tiesa precizē, ka Savienības likumdevējs nav atstājis dalībvalstīm rīcības brīvību attiecībā uz pamatnosacījumiem, kas jāievēro uzraudzības iestādei, kad tā nolemj piemērot administratīvu naudas sodu pārzinim saskaņā ar šo tiesību normu. Tas, ka VDAR sniedz dalībvalstīm iespēju paredzēt izņēmumus attiecībā uz publiskām iestādēm un publiskām struktūrām, kuras darbojas to teritorijā [118], kā arī prasības procedūrai, kas uzraudzības iestādēm jāievēro, lai piemērotu administratīvu naudas sodu [119], nekādi nenozīmē, ka tās arī būtu pilnvarotas paredzēt šādus pamatnosacījumus.

Attiecībā uz šiem nosacījumiem Tiesa atzīmē, ka viens no VDAR uzskaitītajiem elementiem, uz kuru balstoties uzraudzības iestāde pārzinim piemēro administratīvu naudas sodu, ir tas, ka "pārkāpums izdarīts tīši vai neuzmanības dēļ" [120]. Savukārt nevienā no šiem elementiem vispār nav minēta iespēja saukt pie atbildības pārzini, ja tas nav rīkojies prettiesiski. Tādējādi tikai tie VDAR normu pārkāpumi, kurus pārzinis izdarījis tīši vai neuzmanības dēļ, var būt pamats, lai pārzinim piemērotu administratīvo naudas sodu atbilstoši šīs regulas 83. pantam.

Tiesa piebilst, ka šo interpretāciju apstiprina VDAR vispārējā sistēma un mērķis. Šajā kontekstā tā precizē – tas, ka saskaņā ar VDAR pastāv sankciju sistēma, kas ļauj piemērot administratīvu naudas sodu, ja to pamato katras lietas īpašie apstākļi, mudina pārziņus un apstrādātājus ievērot šo regulu un ar preventīvo iedarbību administratīvie naudas sodi palīdz stiprināt datu subjektu aizsardzību. Tomēr Savienības likumdevējs nav uzskatījis par nepieciešamu paredzēt administratīvu naudas sodu piemērošanu vainas neesamības gadījumā. Ņemot vērā, ka VDAR ir paredzēts gan līdzvērtīgs, gan viendabīgs aizsardzības līmenis un ka šajā nolūkā tā ir jāpiemēro saskanīgi visā Savienībā, ļaut dalībvalstīm paredzēt šādu sistēmu naudas soda piemērošanai būtu pretrunā šim mērķim.

---

[117] Pārkāpums paredzēts VDAR 83. panta 4.–6. punktā.

[118] VDAR 83. panta 7. punkts noteic, ka "[..] katra dalībvalsts var izstrādāt noteikumus par to, vai un līdz kādam apjomam administratīvos naudas sodus var piemērot publiskām iestādēm un struktūrām, kas veic uzņēmējdarbību minētajā dalībvalstī".

[119] Atbilstoši VDAR 83. panta 8. punktam, lasot to šīs regulas 129. apsvēruma gaismā.

[120] VDAR 83. panta 2. punkta b) apakšpunkts.

Turklāt Tiesa secina, ka šāds naudas sods var tikt piemērots pārzinim saistībā ar personas datu apstrādes darbībām, ko apstrādātājs ir veicis tā vārdā, izņemot gadījumus, kad saistībā ar šīm darbībām minētais apstrādātājs ir veicis apstrādi savām vajadzībām vai ir apstrādājis šos datus ar pārziņa noteikto apstrādes sistēmu vai kārtību nesavietojamā veidā vai tā, ka nevar pamatoti uzskatīt, ka šis pārzinis tam būtu piekritis. Šādā gadījumā apstrādātājs ir jāuzskata par pārzini attiecībā uz šādu apstrādi.

2023. gada 5. decembra spriedums (virspalāta) Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (turpmāk tekstā – "*DW*") ir nekustamā īpašuma sabiedrība, kurai netieši, ar kapitāldaļām dažādās sabiedrībās, pieder daudzas komercplatības un dzīvojamās platības. Savā komercdarbībā tā apstrādā šo platību nomnieku un īrnieku personas datus.

Pēc 2017. un 2019. gadā veiktām vairākām pārbaudēm *Berliner Beauftragte für den Datenschutz* (Berlīnes Datu uzraudzības iestāde, Vācija) konstatēja vairākus *DW* pieļautus VDAR pārkāpumus. Ar 2019. gada 30. oktobra lēmumu šī uzraudzības iestāde, pamatojoties uz minēto, piemēroja *DW* administratīvus naudas sodus.

DW par šo nolēmumu iesniedza sūdzību *Landgericht Berlin* (Berlīnes apgabaltiesa, Vācija), kura tiesvedību tālāk nevirzīja. Šī tiesa norādīja, ka atbilstoši Vācijas tiesiskajam regulējumam [121] administratīvu pārkāpumu varot konstatēt tikai attiecībā uz fizisku personu, nevis juridisku personu. Turklāt juridiskas personas atbildības iestāšanās gadījumā tai var tikt piedēvētas tikai tās struktūru locekļu vai pārstāvju darbības. *Staatsanwaltschaft Berlin* (Berlīnes prokuratūra, Vācija) šo lēmumu pārsūdzēja *Kammergericht Berlin* (Berlīnes Augstākā tiesa, Vācija). Šajā kontekstā šī tiesa vērsās Tiesā ar lūgumu sniegt prejudiciālu nolēmumu par VDAR interpretāciju.

Šajā spriedumā Tiesa virspalātas sastāvā lemj par administratīvā naudas soda piemērošanas nosacījumiem saskaņā ar VDAR. Pirmkārt, tā izvērtē, vai dalībvalstis var noteikt, ka administratīvais naudas sods juridiskai personai var tikt piemērots tikai tad, ja par šīs regulas pārkāpumu iepriekš tiek vainota identificēta fiziska persona. Otrkārt, tāpat kā spriedumā *Nacionalinis visuomenės sveikatos centras* (skat. iepriekš) tā izskata arī jautājumu par to, vai VDAR normu pārkāpumam, par kuru ir noteikts sods, ir jābūt izdarītam tīši vai aiz neuzmanības.

Attiecībā uz administratīva naudas soda piemērošanu juridiskai personai saskaņā ar VDAR Tiesa vispirms norāda, ka VDAR paredzētie principi, aizliegumi un pienākumi it īpaši attiecas uz "pārziņiem", kuru atbildība attiecas uz jebkādu personas datu apstrādi, ko tie veic paši vai kas tiek veikta viņu vārdā. Tieši šī atbildība VDAR normu pārkāpuma gadījumā ir pamats administratīva naudas soda piemērošanai pārzinim atbilstoši šīs

[121] 1968. gada 24. maija *Gesetz über Ordnungswidrigkeiten* (Administratīvo pārkāpumu likums; *BGBl*. 1968 I, 481. lpp.), redakcijā, kas izziņota 1987. gada 19. februārī (*BGBl*. 1987 I, 602. lpp.) un pielāgota ar 2020. gada 19. jūnija likumu (*BGBl*. 2020 I, 1350. lpp.).

regulas 83. pantam. Tomēr Savienības likumdevējs šādas atbildības noteikšanas nolūkos nav nošķīris fiziskas un juridiskas personas, jo šī atbildība ir pakļauta tikai nosacījumam, ka šīs personas atsevišķi vai kopā ar citām personām nosaka personas datu apstrādes nolūkus un līdzekļus [122]. Līdz ar to principā ikviena persona, kura atbilst šim nosacījumam, ir atbildīga par jebkādu VDAR pārkāpumu, ko tā izdarījusi pati vai kas izdarīts tās vārdā. Tas nozīmē, pirmkārt, ka juridiskas personas ir atbildīgas ne tikai par pārkāpumiem, ko izdarījuši to pārstāvji, vadītāji vai pārvaldītāji, bet arī jebkura cita persona, kura rīkojas šo juridisko personu komercdarbības ietvarā un to vārdā. Otrkārt, šādu pārkāpumu gadījumā ir jābūt iespējai VDAR paredzētos administratīvos naudas sodus piemērot tieši juridiskām personām, ja tās var kvalificēt kā pārziņus.

Turpinājumā Tiesa norāda, ka neviena VDAR tiesību norma neļauj uzskatīt, ka administratīva naudas soda piemērošana juridiskai personai kā pārzinim būtu pakļauta iepriekšējam konstatējumam, ka šo pārkāpumu ir izdarījusi identificēta fiziska persona. Turklāt Savienības likumdevējs šajā ziņā nav atstājis dalībvalstīm rīcības brīvību. Apstāklis, ka VDAR tām sniedz iespēju paredzēt prasības saistībā ar procedūru, kas uzraudzības iestādēm jāievēro, piemērojot administratīvu naudas sodu [123], nekādi nenozīmē, ka tām būtu arī tiesības paredzēt pamatnosacījumus papildus VDAR jau iekļautajiem.

Šajā kontekstā Tiesa precizē, ka atļaut dalībvalstīm vienpusēji un kā obligātu nosacījumu administratīvā naudas soda piemērošanai saskaņā ar VDAR 83. pantu pārzinim, kas ir juridiska persona, izvirzīt prasību, ka par attiecīgo pārkāpumu iepriekš ir tikusi vainota vai ir vainojama identificēta fiziska persona, būtu pretrunā VDAR mērķim. Turklāt šāda papildu prasība rezultātā varētu vājināt juridiskām personām kā pārziņiem piemēroto administratīvo naudas sodu iedarbīgumu un atturošo iedarbību.

Visbeidzot Tiesa uzsver, ka jēdziens "uzņēmums" LESD 101. un 102. panta izpratnē [124] neietekmē to, vai un kādos apstākļos saskaņā ar VDAR var tikt piemērots administratīvs naudas sods pārzinim, kas ir juridiska persona, un tam ir nozīme tikai šāda naudas soda apmēra noteikšanā.

Tādējādi Tiesa secina, ka VDAR [125] ir pretrunā tāds valsts tiesiskais regulējums, saskaņā ar kuru administratīvu naudas sodu juridiskai personai kā pārzinim par šīs regulas pārkāpumu [126] var piemērot tikai tad, ja atbildība par šo pārkāpumu iesākumā ir attiecināta uz identificētu fizisku personu.

Attiecībā uz jautājumu par to, vai dalībvalstis var paredzēt administratīvā naudas soda piemērošanu pat tad, ja pārkāpums, par kuru paredzēts sods, nav izdarīts tīši vai aiz neuzmanības, Tiesa vispirms atgādina, ka materiāltiesiskos nosacījumus, kas

[122] Atbilstoši VDAR 4. panta 7. punktam.
[123] Kā izriet no VDAR 58. panta 4. punkta un 83. panta 8. punkta, lasot tos šīs regulas 129. apsvēruma gaismā.
[124] Uz ko ir atsauce VDAR 150. apsvērumā.
[125] VDAR 58. panta 2. punkta i) apakšpunkts un 83. panta 1.–6. punkts.
[126] Kas paredzēts VDAR 83. panta 4.–6. punktā.

uzraudzības iestādei jāievēro, piemērojot šādu naudas sodu pārzinim, noteic vienīgi Savienības tiesības un ka dalībvalstīm šajā ziņā nav nekādas rīcības brīvības. Izmantojot tādu pašu argumentāciju, kāda piemērota iepriekš minētajā spriedumā *Nacionalinis visuomenės sveikatos centras*, Tiesa konstatē, ka saskaņā ar VDAR 83. pantu administratīvu naudas sodu var piemērot tikai tad, ja ir pierādīts, ka pārzinis, kas ir gan juridiska persona, gan uzņēmums šajā regulā ietvertos noteikumus ir pārkāpis tīši vai aiz neuzmanības.

5. Valsts uzraudzības iestāžu pilnvaru saikne ar citu valsts iestāžu pilnvarām

2023. gada 4. jūlija spriedums (virspalāta) Meta Platforms u.c. (Vispārīgie sociālā tīkla lietošanas noteikumi) (C-252/21, EU:C:2023:537)

Šajā lietā (skat. arī V.5. sadaļu "Personas datu apstrāde tiešsaistes sociālajos tīklos"), lemjot par konkurences iestādes kompetenci konstatēt personas datu apstrādes neatbilstību VDAR, Tiesa norāda, ka, ievērojot pienākumu lojāli sadarboties [127] ar datu aizsardzības uzraudzības iestādēm, šāda iestāde, pārbaudot uzņēmuma dominējošā stāvokļa ļaunprātīgu izmantošanu [128], var konstatēt, ka šā uzņēmuma vispārīgie lietošanas noteikumi personas datu apstrādes jomā un to īstenošana neatbilst šai regulai, ja tas ir nepieciešams, lai konstatētu šādas ļaunprātīgas izmantošanas esamību. Tomēr, ja konkurences iestāde atklāj VDAR pārkāpumu, konstatējot dominējošā stāvokļa ļaunprātīgu izmantošanu, tā neaizstāj uzraudzības iestādes.

Tādējādi, ņemot vērā lojālas sadarbības principu, ja konkurences iestādēm, īstenojot savas pilnvaras, ir jāpārbauda uzņēmuma rīcības atbilstība VDAR noteikumiem, tām ir godprātīgi jāapspriežas un jāsadarbojas ar attiecīgajām valsts uzraudzības iestādēm vai vadošo uzraudzības iestādi. Tādējādi visām šīm iestādēm ir jāievēro savas attiecīgās pilnvaras un kompetence, lai tiktu izpildīti no VDAR izrietošie pienākumi, sasniegti šīs regulas mērķi un saglabāta tās lietderīgā iedarbība. No tā izriet, ka tad, ja konkurences iestāde – veicot pārbaudi, lai konstatētu uzņēmuma dominējošā stāvokļa ļaunprātīgas izmantošanas esamību, – uzskata, ka ir jāpārbauda šā uzņēmuma rīcības atbilstība VDAR noteikumiem, šai iestādei ir jāpārliecinās, vai par šo vai līdzīgu rīcību jau nav pieņemts lēmums kompetentajā valsts uzraudzības iestādē vai vadošajā uzraudzības iestādē, vai arī Tiesā. Ja tas tā ir, konkurences iestāde nevar to neņemt vērā, tomēr no konkurences tiesību piemērošanas viedokļa tā var brīvi izdarīt savus secinājumus.

[127] Nostiprināts LES 4. panta 3. punktā.
[128] LESD 102. panta izpratnē.

Ja konkurences iestādei ir šaubas par kompetentās valsts uzraudzības iestādes vai vadošās uzraudzības iestādes veiktā novērtējuma tvērumu, ja attiecīgo vai līdzīgu rīcību vienlaikus pārbauda minētās iestādes vai ja – gadījumā, kad minētās iestādes nav veikušas izmeklēšanu, – tā uzskata, ka uzņēmuma rīcība neatbilst VDAR noteikumiem, tai ir jāapspriežas ar šīm iestādēm un jālūdz tās sadarboties, lai kliedētu savas šaubas vai noteiktu, vai ir lietderīgi pirms sava vērtējuma sagaidīt, kad lēmumu būs pieņēmusi attiecīgā uzraudzības iestāde. Ja šīs iestādes neiebilst vai saprātīgā termiņā nesniedz atbildi, valsts konkurences iestāde var turpināt izmeklēšanu.

EIROPAS SAVIENĪBAS
TIESA

Pētniecības un dokumentācijas direkcija

2024. gada jūlijs