



Temaatiline ülevaade

ISIKUANDMETE KAITSE

Õigus isikuandmete kaitsele on põhiõigus, mille tagamine on Euroopa Liidu oluline eesmärk.

See õigus on sätestatud Euroopa Liidu põhiõiguste hartas (edaspidi „harta“), mille artiklis 8 on ette nähtud, et:

„1. Igaühel on õigus oma isikuandmete kaitsele.

2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.

3. Nende sätete täitmist kontrollib sõltumatu asutus.“

Kõnealune põhiõigus on lisaks tihedalt seotud õigusega era- ja perekonnaelu austamisele, mille näeb ette harta artikkel 7.

Õigus isikuandmete kaitsele on ette nähtud ka Euroopa Liidu toimimise lepingu (ELTL) artikli 16 lõikes 1, mille eelkäija oli EÜ artikkel 286.

Mis puudutab teisest õigust, siis on Euroopa Ühendus alates 1990. aastate keskpaigast kehtestanud isikuandmete kaitse eesmärgil mitmesuguseid instrumente. Direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta¹, mis võeti vastu EÜ artikli 100A alusel, kujutas selles valdkonnas põhilist liidu õigusakti. Nimetatud direktiivis olid kehtestatud isikuandmete töötlemise seaduslikkust reguleerivad üldised tingimused ja andmesubjektide õigused ning seal oli nähtud muu hulgas ette sõltumatute järelevalveasutuste loomine liikmesriikides.

¹ Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT 1995, L 281, lk 31; ELT eriväljaanne 13/15, lk 355), 20. novembri konsolideeritud redaktsioon, mis tunnustati kehtetuks alates 25. maist 2018 (vt 5. joonealune märkus).

Direktiivi 95/46 täiendati seejärel direktiiviga 2002/58/EÜ², millega ühtlustati õigust eraelu puutumatusse kaitsele reguleerivad liikmesriikide õigusnormid eelkõige isikuandmete töötlemisel elektroonilise side sektoris³. Tuleb märkida, et liidu seadusandjal on kavas see direktiiv uuesti läbi vaadata. Sellega seoses esitas komisjon 10. jaanuaril 2017 ettepaneku asendada see direktiiv määrusega eraelu austamise ja elektroonilise side kohta⁴.

Mis puudutab vabadusel, turvalisusel ja õigusel rajanevat ala (varem ELL artiklid 30 ja 31), siis reguleeris raamotsus 2008/977/JSK⁵ kuni 2018. aasta maini kriminaalasjades tehtavas õigusalasises ja politseikoostöös käsitletavate isikuandmete kaitset.

Euroopa Liit töötas 2016. aastal selles valdkonnas välja uue üldise õigusliku raamistiku. Selleks võttis ta vastu määruse (EL) 2016/679⁶ isikuandmete kaitse kohta (edaspidi „isikuandmete kaitse üldmäärus“), millega tunnustati kehtetuks direktiiv 95/46 ja mida kohaldatakse alates 25. maist 2018, ning nende andmete kaitset kriminaalasjades käsitleva direktiivi (EL) 2016/680⁷, millega tunnustati kehtetuks raamotsus 2008/977/JSK ning mille liikmesriigid peavad üle võtma 6. maiks 2018.

Viimaseks, mis puudutab ELi institutsioonide ja asutuste poolset isikuandmete töötlemist, siis see oli algul reguleeritud määrusega (EÜ) nr 45/2001⁸. Just see määrus võimaldas 2004. aastal luua Euroopa andmekaitseinspektori ametikoha. 2018. aastal kehtestas Euroopa Liit selles valdkonnas uue õigusraamistiku, eeskätt võttes vastu määruse (EL) 2018/1725⁹, millega tunnustati kehtetuks määrus nr 45/2001 ja otsus nr^o1247/2002/EÜ¹⁰ ning mis on kohaldatav alates 11. detsembrist 2018. Kogu liitu hõlmava isikuandmete kaitset käsitleva sidusa lähenemisviisi huvides on selle uue määruse eesmärk ühtlustada andmekaitse norme võimalikult suures ulatuses isikuandmete kaitse üldmäärusega kehtestatud korraga.

² Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatusse kaitset elektroonilise side sektoris (eraelu puutumatus ja elektroonilist sidet käsitlev direktiiv) (EÜT 2002, L 201, lk 37; ELT eriväljaanne 13/29, lk 514), 19. detsembril 2009. aasta konsolideeritud redaktsioon.

³ Direktiivi 2002/58 muudeti Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiviga 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (ELT 2006, L 105, lk 54). Euroopa Kohus tunnistas selle direktiivi kehtetuks 8. aprillil 2014. aasta kohtuotsuses Digital Rights Ireland ja Seitlinger jt (C-293/12 ja C-594/12, [EU:C:2014:238](#)) põhjusel, et see riivas jämedalt õigust eraelu puutumatusse ja isikuandmete kaitsele (vt käesoleva dokumendi alajaotus I.1. „Liidu teisele õiguse kooskõla õigusega isikuandmete kaitsele“).

⁴ [Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnustatakse kehtetuks direktiiv 2002/58/EÜ \(privaatsust ja elektroonilist sidet käsitlev määrus\). COM/2017/010 \(final\) – 2017/03 \(COD\).](#)

⁵ Nõukogu 27. novembri 2008. aasta raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õiguslaselise koostöö raames töödeldavate isikuandmete kaitse kohta (ELT 2008, L 350, lk 60), mis tunnustati kehtetuks alates 6. maist 2018 (vt 6. joonealune märkus).

⁶ Euroopa Parlamendi ja nõukogu 27. aprillil 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnustamise kohta (ELT 2016, L 119, lk 1).

⁷ Euroopa Parlamendi ja nõukogu 27. aprillil 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnustatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT 2016, L 119, lk 89).

⁸ Euroopa Parlamendi ja nõukogu 18. detsembril 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT 2001, L 8, lk 1).

⁹ Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnustatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ.

¹⁰ Euroopa Parlamendi, nõukogu ja komisjoni 1. juuli 2002. aasta otsus nr 1247/2002/EÜ Euroopa andmekaitseinspektori ülesannete täitmist reguleerivate määruste ja üldtingimuste kohta (EÜT 2002, L 183, lk 1; ELT eriväljaanne 01/04, lk 43).

SISUKORD

I. ÕIGUS ISIKUANDMETE KAITSELE, NAGU SEE TULENEB EUROOPA LIIDU PÕHIÕIGUSTE HARTAST	4
1. Liidu teisese õiguse kooskõla õigusega isikuandmete kaitsele.....	4
2. Õiguse isikuandmete kaitsele tagamine liidu õiguse rakendamisel.....	7
II. ISIKUANDMETE TÖÖTLEMINE SELLES VALDKONNAS KEHTIVATE ÜLDNORMIDE KOHASELT ...	9
1. Isikuandmete töötlemine, mis on direktiivi 95/46 kohaldamisalast välja jäetud.....	9
2. Mõiste „isikuandmed“.....	11
3. Mõiste „isikuandmete töötlemine“.....	13
4. Mõiste „isikuandmete kataloog“.....	17
5. Mõiste „isikuandmete vastutav töötleja“.....	17
6. Isikuandmete töötlemise seaduslikkuse kriteeriumid.....	20
III. ISIKUANDMETE TÖÖTLEMINE DIREKTIIVI 2002/58 TÄHENDUSES	28
IV. ISIKUANDMETE EDASTAMINE KOLMANDATESSE RIIKIDESSE	34
V. ISIKUANDMETE KAITSE INTERNETIS	40
1. Õigus esitada isikuandmete töötlemisele vastuväiteid („õigus olla unustatud“).....	41
2. Isikuandmete töötlemine ja intellektuaalomandi õigused.....	42
3. Isikuandmetele suunavate linkide eemaldamine.....	46
4. Veebisaidi kasutaja nõusolek teabe salvestamiseks.....	49
VI. RIIGISESED JÄRELEVALVEASUTUSED	50
1. Sõltumatuse nõude ulatus.....	50
2. Kohaldatava õiguse ja pädeva järelevalveasutuse kindlaksmääramine.....	52
3. Riigisestse järelevalveasutuste pädevus.....	53
VII. EUROOPA ÕIGUSAKTIDE TERRITORIAALNE KOHALDAMINE	57
VIII. ÜLDSUSE ÕIGUS TUTVUDA EUROOPA LIIDU INSTITUTSIOONIDE DOKUMENTIDEGA JA ISIKUANDMETE KAITSE	58

I. Õigus isikuandmete kaitsele, nagu see tuleneb Euroopa Liidu põhiõiguste hartast

1. Liidu teise õiguse kooskõla õigusega isikuandmete kaitsele

[9. novembri 2010. aasta kohtuotsus \(suurkoda\) Volker und Markus Schecke ja Eifert \(C-92/09 ja C-93/09, EU:C:2010:662\)¹¹](#)

Selles kohtuasjas olid põhikohtuasjades kaebuse esitanud Hesseni liidumaa põllumajandustootjad, kes ei olnud rahul sellega, et nende kui Euroopa Põllumajanduse Tagatistfondist (EAGF) või Euroopa Maaelu Arengu Põllumajandusfondist (EAFRD) toetuse saajate kohta avaldati isikuandmed Bundesanstalt für Landwirtschaft und Ernährungi (Saksamaa Liitvabariigi põllumajandus- ja toiduamet) veebisaidil. Nimetatud põllumajandustootjad ei olnud sellise avaldamisega nõus, väites eelkõige, et seda ei õigusta ülekaalukas avalik huvi. Hesseni liidumaa väitel tulenes nende andmete avaldamine määrustest (EÜ) nr 1290/2005¹² ja nr 259/2008¹³, mis reguleerisid ühise põllumajanduspoliitika rahastamist ja kohustasid avaldama nende füüsiliste isikute andmed, kes saavad EAGFist ja EAFRDst toetust.

Niisuguses kontekstis esitas Verwaltungsgericht Wiesbaden (Wiesbadeni halduskohus, Saksamaa) Euroopa Kohtule mitu eelotsuse küsimust, mis käsitlevad seda, kas määruste nr 1290/2005 ja nr 259/2008 teatavad sätted, mis kohustavad sellise info eelkõige liikmesriigi asutuste veebisaitide kaudu avalikkusele kättesaadavaks tegema, on kehtivad.

Kaaludes hartas sätestatud õigust isikuandmete kaitsele ja Euroopa fondidest saadava toetuse läbipaistvuse kohustust, otsustas Euroopa Kohus, et internetisaidil toetusesaajate kohta nimeliste andmete ja toetusesummade avaldamine riivab üldiselt toetusesaajate õigust eraelu puutumatusse ja konkreetselt nende õigust isikuandmete kaitsele, sest kolmandatel isikutel on saidile vaba ligipääs (punktid 56–64).

Et niisugune riive oleks õigustatud, peab see olema ette nähtud seadusega, arvestama nimetatud õiguste põhisisu, olema proportsionaalsuse põhimõtet järgides vajalik ja vastama tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele, kusjuures neist õigustest ette nähtud erandid ja nende piirangud peavad piirduma vältimatult vajalikuga (punkt 65). Niisuguses kontekstis asus Euroopa Kohus seisukohale, et kuigi demokraatlikus ühiskonnas on maksumaksjatel õigus olla informeeritud avaliku sektori rahaliste vahendite kasutamisest, olid nõukogu ja komisjon siiski kohustatud tasakaalustatult kaaluma erinevaid asjas esinevaid huve, mis tähendab, et enne vaidlustatud sätete vastuvõtmist oleksid asjasse puutuvad institutsioonid pidanud kontrollima, kas igas liikmesriigis ühel konkreetsel veebisaidil isikuandmete avaldamine

¹¹ Seda kohtuotsust käsitleti 2010. aasta aastaaruandes, lk 11.

¹² Nõukogu 21. juuni 2005. aasta määrus (EÜ) nr 1290/2005 ühise põllumajanduspoliitika rahastamise kohta (ELT 2005, L 209, lk 1), mis tunnistati kehtetuks Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta määrusega (EL) nr 1306/2013 ühise põllumajanduspoliitika rahastamise, haldamise ja seire kohta (ELT 2013, L 347, lk 549).

¹³ Komisjoni 18. märtsi 2008. aasta määrus (EÜ) nr 259/2008, milles sätestatakse nõukogu määruse (EÜ) nr 1290/2005 kohaldamise üksikasjalikud eeskirjad seoses Euroopa Põllumajanduse Tagatistfondi (EAGF) ja Maaelu Arengu Euroopa Põllumajandusfondi (EAFRD) vahenditest toetuse saajaid hõlmava teabe avaldamisega (ELT 2008, L 76, lk 28), mis tunnistati kehtetuks komisjoni 6. augusti 2014. aasta rakendusmäärusega (EL) nr 908/2014, milles sätestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 1306/2013 rakenduseeskirjad seoses makse- ja muude asutustega, finantsjuhtimisega, raamatupidamisarvestuse kontrollimise ja heakskiitmisega, kontrollieeskirjadega, tagatistega ja läbipaistvusega (ELT 2014, L 255, lk 59).

ei lähe kaugemale sellest, mis on taotletavate õiguspäraste eesmärkide saavutamiseks vajalik (punktid 77, 79, 85 ja 86).

Nii tunnistas Euroopa Kohus kehtetuks määruse nr 1290/2005 teatavad sätted ja määruse nr 259/2008 tervikuna, kuna need näevad EAGFist ja EAFRDst toetust saanud füüsiliste isikute puhul ette iga toetusesaaja isikuandmete avaldamise, tegemata neil isikutel vahet asjasse puutuvate kriteeriumide alusel, nagu toetuse saamise ajavahemikud, toetuse sagedus või liik ja tähtsus (punkt 92 ja resolutsiooni punkt 1). Euroopa Kohus ei seadnud siiski kahtluse alla tagajärgi, mis kaasnesid kõnesolevat toetust saanute nimekirjade avaldamisega riigisiseste ametiasutuste poolt enne selle kohtuotsuse kuulutamise kuupäeva (punkt 94 ja resolutsiooni punkt 2).

[17. oktoobri 2013. aasta kohtuotsus Schwarz \(C-291/12, EU:C:2013:670\)](#)

Michael Schwarz taotles Stadt Bochumilt (Saksamaa) passi väljastamist, ent keeldus selleks sõrmejälgi andmast. Kuna Stadt Bochum jättis tema taotluse rahuldamata, esitas M. Schwarz Verwaltungsgericht Gelsenkirchenile (Gelsenkircheni halduskohus, Saksamaa) kaebuse, nõudes, et viimane kohustaks seda linna väljastama talle passi ilma sõrmejälgi võtmata. M. Schwarz väidab selles kohtus, et määrus (EÜ) nr 2252/2004¹⁴, mis kehtestas kohustuse võtta passi taotlejatelt sõrmejäljed, ei ole kehtiv muu hulgas seetõttu, et määrus eirab õigust isikuandmete kaitsele ja õigust eraelu puutumatusse.

Neil asjaoludel pöördus Verwaltungsgericht Gelsenkirchen eelotsusetaotlusega Euroopa Kohtu poole, paludes selgitada, kas see määrus on – eelkõige harta kontekstis – kehtiv, arvestades, et see kohustab passitaotlejat andma sõrmejälgi ja näeb ette nende säilitamise passis.

Euroopa Kohus vastas jaatavalt, otsustades, et ehkki sõrmejälgede võtmine ja säilitamine, mida reguleerib määruse nr 2252/2004 artikli 1 lõige 2, riivavad õigust eraelu puutumatusse ja õigust isikuandmete kaitsele, õigustab seda riivet eesmärk kaitsta passe nende kuritahtliku kasutamise eest.

Esiteks on niisugusel seaduses ette nähtud piirangul liidu poolt tunnustatud üldist huvi pakkuv eesmärk, sest sellega soovitakse eelkõige takistada isikute ebaseaduslikku sisenemist liidu territooriumile (punktid 35–38). Sõrmejälgede võtmine ja säilitamine on selle eesmärgi saavutamiseks sobivad. Ühelt poolt ei ole sõrmejälgede abil isiku identiteedi tuvastamise meetod küll täielikult usaldusväärne, ent see vähendab märkimisväärselt riski, et siseneda lubatakse isikutel, kes ei ole selleks õigustatud. Teiselt poolt ei tähenda passi omaniku sõrmejälgede ebapiisav kokkulangevus sellesse dokumenti sisestatud andmetega, et puudutatud isikul keelatakse automaatselt liidu territooriumile sisenemine, vaid selle ainus tagajärg on põhjalik kontroll, mille eesmärk on tuvastada vastava isiku isikusamasus lõplikult (punktid 42–45).

Mis puudutab sellise andmete töötlemise vajalikkust, siis ei ole Euroopa Kohtule esitatud andmeid niisuguste meetmete olemasolu kohta, mis oleksid piisavalt tõhusad, ent samal ajal riivaksid harta artiklites 7 ja 8 tunnustatud õigusi vähem kui sõrmejälgedel põhinev meetod

¹⁴ Nõukogu 13. detsembri 2004. aasta määrus (EÜ) nr 2252/2004 liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta (ELT 2004, L 385, lk 1), nii nagu seda on muudetud Euroopa Parlamendi ja nõukogu 6. mai 2009. aasta määrusega (EÜ) nr 444/2009 (ELT 2009, L 142, lk 1).

(punkt 53). Määruse nr 2252/2004 artikli 1 lõige 2 ei näe ette sõrmejälgede töötlemist, mis läheb kaugemale sellest, mis on vajalik taotletud eesmärgi saavutamiseks. Nimelt on määruses selgelt sätestatud, et sõrmejälgi võib kasutada ainult passi ehtsuse ja selle kasutaja isikusamasuse kontrollimiseks. Veelgi enam, määruse artikli 1 lõige 2 näeb ette kaitse riski vastu, et sõrmejälgi sisaldavaid andmeid võivad lugeda selleks mittevolitatud isikud, ja näeb ette sõrmejälgede säilitamise ainult passis, mis jääb üksnes selle omaniku käsutusse (punktid 54–57, 60 ja 63).

[8. aprilli 2014. aasta kohtuotsus \(suurkoda\) Digital Rights Ireland ja Seitlinger jt \(liidetud kohtuasjad C-293/12 ja C-594/12, EU:C:2014:238\)](#)¹⁵

Käesoleva kohtuotsuse ajendiks on nõuded hinnata andmete säilitamist käsitleva direktiivi 2006/24/EÜ kehtivust seoses põhiõigustega eraelu puutumatusel ja isikuandmete kaitsele, mis esitati Iirimaa ja Austria kohtutes algatatud riigisisestes kohtuvaidlustes. Kohtuasjas C-293/12 lahendas High Court (Iirimaa kõrge kohus) äriühingu Digital Rights ja Iirimaa ametiasutuste vahelist kohtuvaidlust, mis käsitles nende riigisiseste meetmete õiguspärasust, mis reguleerivad elektroonilise side kohta käivate andmete säilitamist. Kohtuasjas C-594/12 esitati Verfassungsgerichtshofile (Austria konstitutsioonikohus) mitu konstitutsiooniõiguse valdkonda kuuluvat kaebust, milles paluti tühistada riigisisene norm, millega direktiiv 2006/24 Austria õigusesse üle võeti.

Iiri ja Austria kohus palusid oma eelotsusetaotlustes, et Euroopa Kohus hindaks, kas direktiiv 2006/24 on harta artikleid 7, 8 ja 11 arvestades kehtiv. Konkreetsemalt küsisid need kohtud Euroopa Kohtult, kas üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujatele sellest direktiivist tulenev kohustus säilitada teatud aja jooksul isiku eraelu ja suhtlust käsitlevaid andmeid ja teha need pädevatele riigisisestele asutustele kättesaadavaks kujutab endast nende põhiõiguste põhjendamatut riivet. Asjasse puutuvad eelkõige andmed, mis on vajalikud sideallika ja side sihtpunkti seireks ja tuvastamiseks, side kuupäeva, aja ja kestuse ning sideliigi kindlaksmääramiseks, kasutaja sidevahendi ja mobiilsidevahendi asukoha kindlaksmääramiseks, ning andmed, mille hulka kuuluvad abonendi või registreeritud kasutaja nimi ja aadress, telefoninumbrid, millelt ja millele helistati, ning internetiteenuste puhul IP-aadress. Need andmed võimaldavad muu hulgas teada, millise isikuga ja millise sidevahendi kaudu abonent või registreeritud kasutaja suhtles, ning teha kindlaks side toimumise aja ja koha. Need andmed võimaldavad ka teada, kui sageli abonent või registreeritud kasutaja teatud isikutega mingil ajavahemikul suhtles.

Euroopa Kohus otsustas esmalt, et direktiivi 2006/24 sätetega teenusepakkujatele niisuguste kohustuste kehtestamine kujutab endast harta artiklites 7 ja 8 ette nähtud õiguse eraelu puutumatusel ja õiguse isikuandmete kaitsele eriti rasket riivet. Niisuguses kontekstis tõdes Euroopa Kohus, et tõepoolest võib riive olla õigustatud üldist huvi pakkuva eesmärgiga, nagu võitlusega organiseeritud kuritegevuse vastu. Euroopa Kohus märkis esiteks, et direktiiviga ette nähtud andmete säilitamine ei riiva õiguse eraelu puutumatusel ega isikuandmete kaitse põhiõiguse põhisisu, kuivõrd direktiiv ei luba elektroonilise side sisu kui sellisega tutvumist ning näeb ette, et elektrooniliste sideteenuste või sidevõrkude pakkujad peavad kinni pidama teatavatest andmekaitse ja andmeturbe põhimõtetest. Teiseks märkis Euroopa Kohus, et andmete säilitamine eesmärgiga teha need vajaduse korral pädevatele riigisisestele asutustele

¹⁵ Seda kohtuotsust käsitleti 2014. aasta aastaaruandes, lk 60.

kättesaadavaks tõepoolest vastab üldist huvi pakkuvale eesmärgile, aidates kaasa võitlusele raske kuritegevuse vastu avaliku julgeoleku tagamiseks (punktid 38–44).

Euroopa Kohus leidis siiski, et andmete säilitamist käsitlevat direktiivi vastu võttes ületas liidu seadusandja piire, mis tulenevad proportsionaalsuse põhimõttest. Seetõttu tunnistas ta direktiivi kehtetuks, sest leidis, et põhiõiguste ulatuslik ja väga raske riive, mis direktiiviga ette on nähtud, ei ole piisavalt täpselt piiritletud, mis võimaldaks tagada, et riive piirdub tõepoolest vaid vältimatult vajalikuga (punkt 65). Direktiiv 2006/24 oli nimelt üldisel viisil kohaldatav kõigi isikute ja kõigi elektroonilise side vahendite suhtes ning kõigi liiklusandmete suhtes, ilma ühegi eristuse, piirangu või erandita, mis oleks ette nähtud raskete kuritegude vastu võitlemise eesmärgil (punktid 57–59). Direktiiv ei näinud ette ühtegi objektiivset kriteeriumi, mis võimaldaks tagada, et pädevatel riigisestel asutustel on andmetele juurdepääs ja nad saavad hiljem andmeid kasutada üksnes selliste kuritegude ennetamise, avastamise või kohtus menetlemise eesmärgil, mida võib pidada piisavalt rasketeks kuritegudeks, et õigustada sellist riivet; ka ei sätestanud direktiiv materiaal- ega menetlusõiguslikke tingimusi sellise juurdepääsu või kasutamise suhtes (punktid 60–62). Mis viimaseks puudutab andmete säilitamistähtaega, siis nägi direktiiv ette vähemalt kuuekuulise tähtaja, ilma et andmeliikidel oleks tehtud mingit vahet selle järgi, milliseid isikuid need puudutavad või kui kasulikud võivad andmed taotletava eesmärgi seisukohalt olla (punktid 63 ja 64).

Mis lisaks puudutab harta artikli 8 lõikest 3 tulenevaid nõudeid, siis tõdes Euroopa Kohus, et direktiivis 2006/24 ei ole ette nähtud piisavaid garantiisid, mis võimaldaksid tagada andmete tõhusa kaitsmise kuritarvituste ohu eest ning ebaseadusliku juurdepääsu ja kasutamise eest, ning et samuti ei nõua direktiiv andmete säilitamist liidu territooriumil.

Järelikult ei taganud direktiiv täiel määral, et andmekaitse ja andmeturbe nõuete täitmist kontrollib sõltumatu asutus, nagu on hartas siiski selgelt ette nähtud (punktid 66–68).

2. Õiguse isikuandmete kaitsele tagamine liidu õiguse rakendamisel

[21. detsembri 2016. aasta kohtuotsus \(suurkoda\) Tele2 Sverige \(liidetud kohtuasjad C-203/15 ja C-698/15, EU:C:2016:970\)¹⁶](#)

Pärast seda, kui Euroopa Kohus oli teinud kohtuotsuse Digital Rights Ireland ja Seitlinger jt ning tunnistanud kehtetuks direktiivi 2006/24 (vt eespool), esitati Euroopa Kohtule lahendamiseks kaks kohtuasja, mis käsitlesid Rootsis ja Ühendkuningriigis elektroonilise side teenuse pakujate suhtes kehtestatud üldist kohustust säilitada sideandmeid, mille säilitamine oli ette nähtud kehtetuks tunnistatud direktiiviga.

Järgmisel päeval pärast kohtuotsuse Digital Rights Ireland ja Seitlinger jt kuulutamist teavitas telekommunikatsiooniettevõtja Tele2 Sverige Rootsi posti- ja telekommunikatsiooni järelevalveasutust oma otsusest lõpetada andmete säilitamine ning oma kavatsusest kustutada juba registreeritud andmed (kohtuasi C-203/15). Rootsi õiguses oli elektroonilise side teenuse pakujatele nimelt ette nähtud eranditeta kohustus süstemaatiliselt ja pidevalt säilitada kõiki oma abonentide ja registreeritud kasutajate liiklusandmeid ja asukohtaandmeid kõigi elektroonilise side vahendite osas. Kohtuasjas C-698/15 olid kolm isikut esitanud kaebuse

¹⁶ Seda kohtuotsust käsitleti 2016. aasta aastaaruandes, lk 62.

Ühendkuningriigi andmesäilituskorra kohta, mis võimaldas siseministril kohustada avalik-õiguslikke telekommunikatsiooniettevõtjaid säilitama kõiki sideandmeid maksimaalselt 12 kuu jooksul, välistades siiski sideseansi sisu säilitamise.

Euroopa Kohtu poole pöördusid Kammarrätten i Stockholm (Stockholmi apellatsiooniasstme halduskohus, Rootsi) ja Court of Appeal (England and Wales) (Civil Division) (apellatsioonikohus (Inglismaa ja Wales) (tsiviilkoda), Ühendkuningriik), paludes Euroopa Kohtul otsustada, kuidas tuleb tõlgendada nn eraelu puutumatus ja elektroonilise side direktiivi 2002/58 artikli 15 lõiget 1, mis võimaldab liikmesriikidel kehtestada teatavaid erandeid selles direktiivis sätestatud kohustusest tagada elektroonilise side ja sellega kaasnevate liiklusandmete konfidentsiaalsus.

Euroopa Kohus otsustas kõnealuses kohtuotsuses esmalt, et direktiivi 2002/58 artikli 15 lõikega 1 koostoimes harta artiklitega 7, 8, 11 ja artikli 52 lõikega 1 on vastuolus niisugused riigisisesed õigusnormid nagu Rootsi omad, milles on kuritegevuse vastu võitlemise eesmärgil ette nähtud kõiki elektroonilise side vahendeid puudutav kohustus säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed. Euroopa Kohtu hinnangul väljuvad õigusnormid vältimatult vajaliku piiridest ja demokraatlikus ühiskonnas ei saa neid lugeda põhjendatuks, nagu nõuab artikli 15 lõige 1, tõlgendatuna harta eespool viidatud artikleid arvestades (punktid 99–105, 107, 112 ja resolutsiooni punkt 1).

Sama sättega, tõlgendatuna koostoimes samade harta normidega, on vastuolus ka liikmesriigi õigusnormid, mis reguleerivad liiklusandmete ja asukohaandmete kaitset ja turvalisust ning eelkõige pädevate ametiasutuste juurdepääsu säilitatavatele andmetele, piiramata seda juurdepääsu kuritegevuse vastu võitlemise raames üksnes raske kuritegevuse vastu võitlemisega, nägemata ette, et andmetele juurdepääsu saamise eeltingimus on kohtu või sõltumatu haldusasutuse eelnev kontroll, ning nõudmata, et kõnealuseid andmeid säilitataks liidu territooriumil (punktid 118–122, 125 ja resolutsiooni punkt 2).

Euroopa Kohus asus aga seisukohale, et direktiivi 2002/58 artikli 15 lõikega 1 ei ole vastuolus õigusnormid, mis raske kuritegevuse vastu võitlemise eesmärgil võimaldavad niisuguste andmete eesmärgipärast ennetavat säilitamist, tingimusel et andmete säilitamine oleks säilitatavate andmete liigi, asjasse puutuvate sidevahendite ja isikute ning säilitamise kestuse osas piiratud vältimatult vajalikuga. Nimetatud nõuete täitmiseks peavad need liikmesriigi õigusnormid esiteks sätestama selged ja täpsed eeskirjad, mis võimaldaks tõhusalt kaitsta neid isikuandmeid kuritarvitamise ohu eest. Konkreetsemalt peavad need liikmesriigi õigusnormid ette nägema, millistel asjaoludel ja milliste tingimuste kohaselt võib andmete säilitamise meetme ennetavalt võtta, tagades seeläbi, et niisugune meede piirduks vältimatult vajalikuga. Mis teiseks puudutab sisulisi tingimusi, millele liikmesriigi õigusnormid peavad vastama, et tagada, et need piirduks vältimatult vajalikuga, siis peab andmete säilitamine siiski alati vastama objektiivsetele kriteeriumidele, mis loovad seose säilitatavate andmete ja taotletava eesmärgi vahel. Nimelt peavad need tingimused olema sellised, mis praktikas võimaldaksid meetme ulatust ja seeläbi ka puudutatud isikute ringi tõhusalt piirata. Mis puudutab niisugust piirangut, siis liikmesriigi õigusnormid peavad lähtuma objektiivsetest asjaoludest, mis võimaldavad meetme suunata isikute ringile, kellega seotud andmetest võib avalduda kas või kaudne seos raskete kuritegudega, või mis võimaldavad ühel või teisel viisil võidelda raske kuritegevusega või ära hoida suure ohu avalikule julgeolekule (punktid 108–111).

II. Isikuandmete töötlemine selles valdkonnas kehtivate üldnormide kohaselt

1. Isikuandmete töötlemine, mis on direktiivi 95/46 kohaldamisalast välja jäetud

[30. mai 2006. aasta kohtuotsus \(suurkoda\) parlament vs. nõukogu \(C-317/04 ja C-318/04, EU:C:2006:346\)](#)

Pärast 11. septembri 2001. aasta terrorirünnakuid olid Ameerika Ühendriigid võtnud vastu õigusnormid, mille kohaselt peavad lennuettevõtjad, kes korraldavad rahvusvahelist lennureisijatevedu Ameerika Ühendriikide territooriumile, läbi selle territooriumi või sealt välja, võimaldama Ameerika Ühendriikide ametiasutusele elektroonilise juurdepääsu nende broneerimis- ja väljumiskontrolli süsteemi ehk Passenger Name Recordsi (PNR) andmetele.

Komisjon leidis, et need sätted võivad minna vastuollu nii Euroopa kui ka liidu liikmesriikide isikuandmete kaitse alaste õigusnormidega ning alustas läbirääkimisi Ameerika Ühendriikide ametiasutustega. Läbirääkimiste tulemusel võttis komisjon 14. mail 2004 vastu otsuse 2004/535/EÜ¹⁷, milles tõdes, et Ameerika Ühendriikide Tolli- ja Piirivalveamet (United States Bureau of Customs and Border Protection, edaspidi „CBP“) tagab Euroopa Ühendusest edastatud PNR-andmete piisava kaitsetaseme (edaspidi „piisava kaitse otsus“). Seejärel võttis nõukogu 17. mail 2004 vastu otsuse 2004/496/EÜ¹⁸, millega kiideti heaks Euroopa Ühenduse ja Ameerika Ühendriikide vahelise lepingu sõlmimine ühenduse liikmesriikide territooriumil asutatud lennuettevõtjate poolt PNR-andmete töötlemise ja edastamise kohta CBP-le.

Euroopa Parlament palus Euroopa Kohtul kaks eespool nimetatud otsust tühistada, väites eelkõige, et piisava kaitse otsus võeti vastu *ultra vires*, et EÜ artikkel 95 (nüüd ELTL artikkel 114) ei olnud sobiv õiguslik alus, et lepingu sõlmimist heaks kiita, ja et nii ühel kui teisel juhul oli rikutud põhiõigusi.

Piisava kaitse otsusega seoses analüüsis Euroopa Kohus esmalt, kas komisjon võis oma otsuse vastuvõtmiseks õiguspäraselt tugineda direktiivile 95/46. Niisuguses kontekstis asus Euroopa Kohus seisukohale, et piisava kaitse otsusest tulenevalt kujutab PNR-andmete edastamine CBP-le endast töötlemist, mille ese on avalik julgeolek ja riigi toimingud karistusõiguse valdkonnas. Euroopa Kohus leidis, et kuigi esialgu kogusid lennuettevõtjad PNR-andmeid liidu õiguse valdkonda kuuluva tegevuse ehk teenuse tarbimiseks õigust andva lennukipileti müügi käigus, on piisava kaitse otsuses arvestatud andmete töötlemise iseloom hoopis midagi muud. Nimelt ei puuduta kõnealune otsus mitte teenuse osutamiseks vajalikku andmetöötlust, vaid andmetöötlust, mida peetakse vajalikuks, et tagada avalik julgeolek ja õiguskaitse (punktid 56 ja 57).

¹⁷ Komisjoni 14. mai 2004. aasta otsus 2004/535/EÜ Ameerika Ühendriikide Tolli- ja Piirivalveametile edastatavates reisijaregistris sisalduvate lennureisijate isikuandmete piisava kaitse kohta (ELT 2004, L 235, lk 11).

¹⁸ Nõukogu 17. mai 2004. aasta otsus 2004/496/EÜ, mis käsitleb Euroopa Ühenduse ja Ameerika Ühendriikide vahelise lepingu sõlmimist lennuettevõtjate poolt reisijate isikuandmete töötlemise ja edastamise kohta Ameerika Ühendriikide Sisejulgeolekuministeeriumi Tolli ja Piirivalvebüroole (ELT 2004, L 183, lk 83; parandus ELT 2005, L 255, lk 168).

Euroopa Kohus otsustas, et kuna eraõiguslikud ettevõtjad kogusid PNR-andmeid kommertseesmärgil ning just nemad korraldasid nende edastamist kolmandasse riiki, siis ei kuulu kõnealune edastamine viidatud sätte kohaldamisalasse. Edastamine toimus sellises ametivõimude loodud raamistikus, mille eesmärk oli tagada avalik julgeolek. Sellest järeldas Euroopa Kohus, et piisava kaitse otsus ei kuulu direktiivi kohaldamisalasse, sest see otsus puudutab isikuandmete töötlemist, mis on direktiivi kohaldamisalast välja jäetud. Euroopa Kohus tühistas sellest lähtudes piisava kaitse otsuse (punktid 58 ja 59).

Mis puudutab nõukogu otsust, siis tuvastas Euroopa Kohus, et EÜ artikkel 95 koostoimes direktiivi 95/46 artikliga 25 ei anna ühendusele pädevust sõlmida Ameerika Ühendriikidega kõnealune leping. Leping käsitleb sama andmeedastust, mis piisava kaitse otsuski, seega sellist andmetöötlust, mis ei kuulu direktiivi kohaldamisalasse. Sellest lähtudes tühistas Euroopa Kohus otsuse, millega nõukogu oli lepingu sõlmimise heaks kiitnud (punktid 67–69).

[11. detsembri 2014. aasta kohtuotsus Ryneš \(C-212/13, EU:C:2014:2428\)](#)

Korduvate rünnakute tõttu paigaldas F. Ryneš oma maja külge turvakaamera. Pärast järgmist tema maja suhtes toime pandud rünnakut võimaldasid kaamera salvestised tuvastada kaks kahtlusalust, kelle suhtes alustati kriminaalmenetlust. Üks kahest kahtlusalusest vaidlustas turvakaamera abil salvestatud andmete töötlemise seaduslikkuse Tšehhi isikuandmete kaitse ametis, kes tuvastas, et F. Ryneš oli rikkunud isikuandmete kaitse eeskirju ning määras viimasele trahvi.

Nejvyšší správní soud (Tšehhi kõrgeim halduskohus), kes lahendas F. Ryneši kassatsioonkaebust Městský soud v Praze (Praha linnakohus, Tšehhi Vabariik) otsuse peale, millega oli jäetud isikuandmete kaitse ameti otsus muutmata, palus Euroopa Kohtul selgitada, kas salvestised, mille F. Ryneš oli teinud oma elu, tervise ja vara kaitseks, kujutasid endast isikuandmete töötlemist, mis ei olnud hõlmatud direktiiviga 95/46, sest need oli teinud füüsiline isik üksnes isiklikel või kodustel eesmärkidel selle direktiivi artikli 3 lõike 2 teise taande tähenduses.

Euroopa Kohus otsustas, et füüsilise isiku poolt tema perekonna eluasemeks oleva maja külge omanike vara, tervise ja elu kaitseks paigaldatud ja isikutest pidevsalvestusseadmesse ehk kõvakettale videosalvestust tegeva kaamerasüsteemi kasutamine, kui selline süsteem jälgib ka avalikku ruumi, ei ole isikuandmete töötlemine üksnes isiklikel või kodustel eesmärkidel (punkt 35 ja resolutsioon).

Sellega seoses tuletas Euroopa Kohus meelde, et harta artikliga 7 tagatud põhiõiguse eraelu puutumatusale kaitse nõuab, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda vältimatult vajalikuga. Kuivõrd direktiivi 95/46 sätteid tuleb osas, milles need reguleerivad põhivabadusi ja eriti õigust eraelu puutumatusale riivata võivad isikuandmete töötlemist, tingimata tõlgendada hartas sätestatud põhiõigusi arvestades, tuleb direktiivi artikli 3 lõike 2 teises taandes ette nähtud erandit tõlgendada kitsalt (punktid 27–29). Selle sätte sõnastus ise arvab „üksnes“ isiklikel või kodustel eesmärkidel toimuva andmete töötlemise direktiivi 95/46 kohaldamisalast välja. Ent osas, milles niisugune videovalve kas või osaliselt ulatub avalikku ruumi ja on seetõttu suunatud selle vahendi abil andmete töötleva isiklikust sfäärist väljapoole, ei saa seda pidada tegevuseks, millega tegeldakse üksnes „isiklikel või kodustel“ eesmärkidel nimetatud sätte tähenduses (punktid 30, 31 ja 33).

2. Mõiste „isikuandmed“

[19. oktoobri 2016. aasta kohtuotsus Breyer \(C-582/14, EU:C:2016:779\)¹⁹](#)

Patrick Breyer esitas Saksa tsiviilkohtutele kaebuse, et Saksamaa Liitvabariigil keelataks kas otse või kolmandate isikute vahendusel salvestada elektroonilisi andmeid, mis edastati pärast Saksamaa föderaalasutuste veebisaitide iga külastamist. Rünnete ärahoidmiseks ja „ründajate“ kriminaalvastutusele võtmise võimaldamiseks salvestasid Saksamaa föderaalasutuste elektrooniliste teabe- ja sideteenuste pakkujad andmeid, mille hulka kuulus „dünaamiline“ IP-aadress ehk IP-aadress, mis iga uue interneti mineku korral muutub, ning saidi külastamise kuupäev ja kellaaeg. Erinevalt staatilistest IP-aadressidest ei võimaldanud dünaamilised IP-aadressid üldsusele kättesaadavate failide abil *a priori* ühendada kindlat arvutit ja füüsilist võrguühendust, mida võrguühenduse pakkuja kasutas. Salvestatud andmed ei andnud elektrooniliste teabe- ja sideteenuste pakkujale iseenesest võimalust kasutajat tuvastada. Seevastu olid internetiühenduse pakkujal täiendavad andmed, mis ühendatuna selle IP-aadressiga oleksid võimaldanud selle kasutaja tuvastada.

Niisuguses kontekstis palus Bundesgerichtshof (Saksamaa kõrgeim üldkohus), kellele oli esitatud kassatsioonkaebus, Euroopa Kohtul selgitada, kas IP-aadress, mida elektrooniliste teabe- ja sideteenuste pakkuja oma veebisaidi külastuste kohta salvestab, kujutab endast teenusepakkuja jaoks isikuandmeid.

Euroopa Kohus märkis esiteks, et selleks, et andmeid saaks kvalifitseerida direktiivi 95/46 artikli 2 punkti a tähenduses „isikuandmeteks“, ei ole nõutud, et kõik isikut tuvastada võimaldavad andmed oleksid ühe isiku valduses. Asjaolu, et veebisaidi kasutaja tuvastamiseks vajalikud täiendavad andmed ei ole mitte elektrooniliste teabe- ja sideteenuste pakkuja valduses, vaid selle kasutaja internetiühenduse pakkuja valduses, ei näi seega välistavat, et elektrooniliste teabe- ja sideteenuste pakkuja poolt salvestatud dünaamilised IP-aadressid on selle teenusepakkuja jaoks isikuandmed direktiivi 95/46 artikli 2 punkti a tähenduses (punktid 43 ja 44).

Sellest tulenevalt otsustas Euroopa Kohus, et dünaamiline IP-aadress, mille elektrooniliste teabe- ja sideteenuste pakkuja salvestab hetkel, kui isik külastab veebisaiti, mille see teenusepakkuja teeb üldsusele kättesaadavaks, kujutab selle teenusepakkuja suhtes direktiivi 95/46 artikli 2 punkti a tähenduses isikuandmeid, kui tal on seaduslikud vahendid, mis võimaldavad andmesubjekti tuvastada tänu andmesubjekti puudutavale täiendavale teabele, mis on selle isiku internetiühenduse pakkuja valduses (punkt 49 ja resolutsiooni punkt 1).

[20. detsembri 2017. aasta kohtuotsus Nowak \(C-434/16, ECLI:EU:C:2017:994\)](#)

Raamatupidamise praktikant Peter Nowak kukkus läbi lirimaa raamatupidamiskspertide instituudi korraldatud eksamil. Ta esitas andmekaitseaduse artikli 4 alusel taotluse tutvuda kõigi teda puudutavate isikuandmetega, mis olid raamatupidamiskspertide instituudi käes. Raamatupidamiskspertide instituut edastas P. Nowakile teatavad dokumendid, aga keeldus edastamast tema eksamitöö koopiit, väites, et see ei sisalda andmekaitseaduse mõttes P. Nowakit puudutavaid isikuandmeid.

¹⁹ Seda kohtuotsust käsitleti 2016. aasta aastaaruandes, lk 61.

Kuivõrd andmekaitsevolinik jättis samal põhjendusel isikuandmetega tutvumise taotluse rahuldamata, pöördus P. Nowak liikmesriigi kohtute poole. Supreme Court (Iirimaa kõrgeim kohus), kes lahendas P. Nowaki edasikaebust, pöördus Euroopa Kohtu poole küsimusega, kas direktiivi 95/46 artikli 2 punkti a tuleb tõlgendada nii, et niisugustel asjaoludel nagu põhikohtuasjas kujutavad eksaminandi poolt kutsealasel eksamil antud kirjalikud vastused ja võimalikud märkused, mille eksamineerija on neile lisanud, endast selle sätte mõttes eksaminandi isikuandmeid.

Esiteks märkis Euroopa Kohus, et selleks, et andmeid saaks kvalifitseerida „isikuandmeteks“ direktiivi 95/46 artikli 2 punkti a tähenduses, ei ole nõutud, et kõik andmesubjekti tuvastada võimaldavad andmed oleksid ühe isiku valduses. Lisaks, olukorras, kus eksamineerijale ei ole eksaminandi isik tema eksamitöö vastuste hindamise ajal teada, valdab eksamit korraldav üksus, praegusel juhtumil raamatupidamiskspertide instituut, siiski vajalikku infot, mis võimaldab tal raskusteta ja kahtlusteta eksaminandi tuvastada, lähtudes tema eksamitööle või selle pealdislehele kantud identifitseerimisnumbrist, ja seega teada saada, et see oli just see eksaminand, kes vastavad vastused andis.

Teiseks tõdes Euroopa Kohus, et kirjalikud vastused, mille eksaminand kutsealasel eksamil annab, kujutavad endast eksaminandi isikut puudutavat teavet. Vastuste sisu peegeldab eksaminandi teadmiste ja oskuste taset konkreetses valdkonnas ning vajaduse korral ka tema arutlusoskusi, analüüsi- ja kriitilise mõtlemise võimet. Lisaks on nende vastuste kogumise eesmärk hinnata eksaminandi kutsealaseid võimeid ja tema võimekust vastaval alal tegutseda. Eelkõige eksaminandi eksamil õnnestumist või ebaõnnestumist kajastava teabe kasutamine võib avaldada mõju eksaminandi õigustele ja huvidele, sest see võib otsustada või mõjutada näiteks isiku võimalust vastaval kutsealal tegutseda asuda või saada taotletud ametikoht. Tõdemus, et kirjalikud vastused, mille eksaminand kutsealasel eksamil annab, kujutavad endast tulenevalt nende sisust, eesmärgist ja toimest eksaminandi puudutavat teavet, kehtib muu hulgas samuti juhtumil, kui tegemist on avatud materjalidega eksamiga (punktid 31 ja 36–40).

Kolmandaks, mis puudutab eksamineerija märkusi eksaminandi vastuste kohta, siis leidis Euroopa Kohus, et need kujutavad endast, nagu eksaminandi poolt eksami kestel antud vastusedki, teavet, mis puudutab vastavat eksaminandi, sest need märkused peegeldavad eksamineerija arvamust või hinnangut eksaminandi individuaalsele sooritusele eksamil ja eelkõige tema teadmistele ja oskustele asjasse puutuvast valdkonnas. Nende märkuste eesmärk ongi nimelt dokumenteerida eksamineerija hinnang eksaminandi sooritusele ja need võivad avaldada eksaminandile mõju (punktid 42 ja 43).

Neljandaks otsustas Euroopa Kohus, et eksaminandi kirjalikke vastuseid kutsealasel eksamil ja eksamineerija võimalikke märkusi nende kohta võidakse direktiivi 95/46 artikli 6 lõike 1 punktide d ja e mõttes eriti täpsuse ja säilitamisvajaduse seisukohast kontrollida ning et neid võidakse direktiivi artikli 12 punkti b alusel parandada või kustutada. Asjaolu, et eksaminandile antakse direktiivi artikli 12 punkti a alusel õigus vastuste ja märkustega tutvuda, on kantud direktiivi eesmärgist tagada, et eksaminandi õigus eraelu puutumatusele on teda puudutavaid andmeid käsitlevas osas kaitstud ja seda sõltumata küsimusest, kas eksaminandil on selline andmetega tutvumise õigus ka vastavalt eksamimenetluse suhtes kohaldatavale riigisisesele õigusele. Euroopa Kohus rõhutas siiski, et direktiivi 95/46 artikli 12 punktide a ja b tulenevad õigused andmetega tutvuda ja neid parandada ei laiene eksamiküsimustele, sest need ei kujuta sellisena endast eksaminandi isikuandmeid (vt punktid 56 ja 58).

Neid asjaolusid arvestades otsustas Euroopa Kohus, et niisugustel asjaoludel nagu põhikohtuasjas kujutavad eksaminandi poolt kutsealasel eksamil antud kirjalikud vastused ja võimalikud märkused, mille eksamineerija on neile lisanud, endast direktiivi 95/46 artikli 2 punkti a mõttes isikuandmeid (vt punkt 62 ja resolutsioon).

3. Mõiste „isikuandmete töötlemine“

[6. novembri 2003. aasta kohtuotsus \(suurkoda\) Lindqvist \(C-101/01, EU:C:2003:596\)](#)

Rootsi luteri kiriku koguduse vabatahtlik Bodil Lindqvist tegi oma personaalarvutiga veebilehed, kus ta avaldas isikuandmed mitme isiku kohta, kes töötasid nagu temagi vabatahtlikena selle koguduse juures. B. Lindqvistile määrati trahv, sest ta tegeles isikuandmete automatiseeritud töötlemisega sellest eelnevalt Rootsi Datainspektionile (elektroonilisel teel edastatavate andmete kaitse üle järelevalvet tegev ametiasutus) kirjalikult teatamata, edastas ilma loata töödeldud isikuandmeid kolmandatesse riikidesse ja töötles delikaatseid isikuandmeid.

B. Lindqvist kaebas selle otsuse edasi Göta hovrätti (Göta apellatsioonikohus, Rootsi), kes omakorda esitas Euroopa Kohtule eelotsusetaotluse, et viimane selgitaks eelkõige, kas B. Lindqvist tegeles „isikuandmete täielikult või osaliselt automatiseeritud töötlemisega“ direktiivi 95/46 tähenduses.

Euroopa Kohus tõdes, et toiming, mis seisneb veebilehel erinevatele isikutele osutamises ja nende isiku äranäitamises kas nime või muude vahendite, näiteks telefoninumbri või nende töötingimusi ja vaba aja harrastusi puudutava teabe alusel, on „isikuandmete täielikult või osaliselt automatiseeritud töötlemine“ kõnealuse direktiivi tähenduses (punkt 27 ja resolutsiooni punkt 1). Isikuandmete selline töötlemine vabatahtliku või usulise tegevuse huvides ei kuulu ühegi selles direktiivis sätestatud erandi alla, sest see ei kuulu avaliku julgeoleku kategooriasse kuuluvate tegevuste hulka ega ka üksnes isiklikel või kodustel eesmärkidel toimuvate tegevuste hulka, mis jäävad väljapoole direktiivi kohaldamisala (punktid 38, 43–48 ja resolutsiooni punkt 2).

[13. mai 2014. aasta kohtuotsus \(suurkoda\) Google Spain ja Google \(C-131/12, EU:C:2014:317\)](#)

Hispaania kodanik esitas 2010. aastal Agencia Española de Protección de Datosile (Hispaania andmekaitseamet) kaebuse laia levikuga Hispaania päevalehe Vanguardia Ediciones SLi toimetuse ja Google Spaini ning Google'i peale. See isik väitis, et kui internetikasutaja sisestab Google'i otsingumootoris tema nime, kuvatakse otsingutulemustes lingid kahele La Vanguardia ajalehe 1998. aasta leheküljele, kus on avaldatud teade tema võlgade tõttu arestitud kinnisvara enampakkumise kohta. Kaebaja nõudis selles kaebuses esiteks, et La Vanguardiat kohustataks need leheküljed eemaldama või neid muutma või kasutama otsingumootorite võimaldatavaid vahendeid tema isikuandmete kaitseks. Teiseks nõudis ta, et äriühingut Google Spain või Google kohustataks eemaldama või peitma tema isikuandmed nii, et need ei ilmuks enam otsingutulemustes ega annaks linke La Vanguardia ajalehele.

Hispaania andmekaitseamet jättis La Vanguardia peale esitatud kaebuse rahuldamata, pidades teabe avaldamist õiguspäraseks, ent rahuldab kaebuse äriühinguid Google Spain ja Google puudutavas osas ja kohustas neid kaht äriühingut eemaldama andmed otsinguindeksist ja muutma edasise tutvumise kõnealuste andmetega võimatuks. Nimetatud äriühingud esitasid

selle otsuse peale eraldi kaebused Audiencia Nacionalile (üleriigiline kohus, Hispaania) nõudega, et Hispaania andmekaitseameti otsus tühistataks. Audiencia Nacional esitas Euroopa Kohtule terve rea eelotsuse küsimusi.

Sellega seoses avanes Euroopa Kohtul võimalus täpsustada direktiivi 95/46 kontekstis mõistet „isikuandmete töötlemine“ internetis.

Euroopa Kohus otsustas, et otsingumootori tegevust, mis seisneb kolmandate isikute poolt internetis avaldatud või sinna lisatud teabe leidmises, automaatses indekseerimises, ajutises säilitamises ja lõpuks internetikasutajatele kättesaadavaks tegemises teatavas eelistusjärjekorras, tuleb pidada „isikuandmete töötlemiseks“, kui see teave sisaldab isikuandmeid (resolutsiooni punkt 1). Euroopa Kohus tuletas lisaks meelde, et direktiivis loetletud toiminguid tuleb pidada isikuandmete töötlemiseks ka juhul, kui need puudutavad üksnes teavet, mis on meedias juba avaldatud. Kui direktiivi kohaldamisel tehtaks niisugusel juhtumil üldine erand, kaotaks direktiiv suuresti oma mõtte (punktid 29 ja 30).

[10. juuli 2018. aasta kohtuotsus \(suurkoda\) Jehovahi tunnistajad \(C-25/17, ECLI:EU:C:2018:551\)²⁰](#)

Soome andmekaitsevolinik tegi otsuse, millega keelati Jehoova tunnistajate kogukonnal tema liikmete ükselt uksele tehtava kuulutustöö käigus isikuandmeid koguda või töödelda viisil, mis ei vasta isikuandmete töötlemist reguleerivates Soome õigusnormides sätestatud tingimustele. Selle kogukonna liikmed teevad ükselt uksele toimuva kuulutustöö käigus märkmeid kohtumiste kohta inimestega, keda nad ise ega ka kogukond ei tunne. Andmeid kogutakse mälu värskendamiseks ja selleks, et neid saaks kasutada võimaliku hilisema külastuse tarbeks, ilma et andmesubjektid oleksid andmete kogumiseks nõusoleku andnud või et neid oleks sellest teavitatud. Jehoova tunnistajate kogukond on märkmete tegemise kohta andnud oma liikmetele juhised, mis sisalduvad vähemalt ühes kogukonna brošüüridest, mis on pühendatud kuulutustööle.

Euroopa Kohus otsustas, et usukogukonna liikmete poolt isikuandmete kogumine ükselt uksele tehtava kuulutustöö käigus ja nende andmete hilisem töötlemine ei kuulu erandite alla, mis on väljaspool direktiivi 95/46 kohaldamisala, kuna need ei kujuta endast ei isikuandmete töötlemist direktiivi artikli 3 lõike 2 esimeses taandes nimetatud tegevuse käigus ega isikuandmete töötlemist, millega tegelevad füüsilised isikud üksnes isiklikel või kodustel eesmärkidel direktiivi artikli 3 lõike 2 teise taande tähenduses (punkt 51 ja resolutsiooni punkt 1).

[14. veebruari 2019. aasta kohtuotsus Buivids \(C-345/17, EU:C:2019:122\)](#)

Kõnealusel kohtuasjas käsitles Euroopa Kohus esiteks direktiivi 95/46 kohaldamisala ja teiseks selle direktiivi artiklis 9 sisalduvat mõistet „isikuandmete töötlemine ainult ajakirjanduse jaoks“.

Selle kohtuotsuse taustaks on Läti kõrgeima kohtu esitatud eelotsusetaotlus põhikohtuasjas kassaator S. Buividsi (edaspidi „kassaator“) ja Läti andmekaitseinspeksiooni vahelises vaidluses, mille aluseks on nõue tunnistada õigusvastaseks andmekaitseinspeksiooni otsus, milles leitakse, et S. Buivids rikkus liikmesriigi õigusnorme isikuandmete kaitse vallas, avaldades veebisaidil tema

²⁰ Seda kohtuotsust käsitleti 2018. aasta aastaaruandes, lk 87 ja 88.

enda filmitud video sellest, kuidas ta andis tema vastu algatatud väärteomenetluses Läti politseijaoskonna ruumides ütlusi. Kui esimese ja teise astme kohus olid tema vastava kaebuse rahuldamata jätnud, esitas kassaator kassatsioonkaebuse riigi kõrgeimale kohtule. S. Buivids tugines selles kohtus oma sõnavabadusele, väites, et kõnealusel videos on näha riigi politseiametnike ehk avaliku elu tegelasi avalikus kohas ja seetõttu ei kuulu need isikud isikuandmete kaitse seaduse sätete kohaldamisalasse.

Mis esimesena puudutab direktiivi 95/46 kohaldamisala, siis märkis Euroopa Kohus, et esiteks kujutavad kõnealusel videos salvestatud kaadrid politseiametnikest endast isikuandmeid ning et teiseks on kassaatori kasutatud kaamera mällu neist isikutest video salvestamise puhul tegemist isikuandmete töötlemisega. Euroopa Kohus lisas, et see, kui internetis asuval videosaidil, mis võimaldab kasutajatel videoid vaadata ja jagada, avaldatakse selline video, milles on näha isikuandmed, kujutab endast nende andmete täielikult või osaliselt automatiseeritud töötlemist. Lisaks toonitas Euroopa Kohus, et sellise video salvestamine ja avaldamine ei kuulu erandite alla, mis on väljaspool direktiivi 95/46 kohaldamisala ja mis puudutavad eelkõige isikuandmete töötlemist selle direktiivi kohaldamisalasse mittekuuluvate tegevuste käigus ja isikuandmete töötlemist, millega tegelevad füüsilised isikud üksnes isiklikel või kodustel eesmärkidel. Sellest tulenevalt järeldas Euroopa Kohus, et selle direktiivi kohaldamisalasse kuulub politseijaoskonnas ütluste andmise käigus politseiametnikest videosalvestise tegemine ja selliselt salvestatud video avaldamine videosaidil, mis võimaldab kasutajatel videoid avaldada, vaadata ja jagada (punktid 31, 32, 35, 39, 42, 43 ja resolutsiooni punkt 1).

Mis teisena puudutab mõiste „isikuandmete töötlemine ainult ajakirjanduse jaoks“ ulatust, siis tuletas Euroopa Kohus esmalt meelde, et lähtudes mõiste „ajakirjandus“ laiast tõlgendusest, kohaldatakse direktiivi 95/46 artiklis 9 ette nähtud erandeid ja kõrvalekaldeid kõikide ajakirjandusega tegelevate isikute suhtes. Nii otsustas Euroopa Kohus, et asjaolu, et kassaator ei ole kutseline ajakirjanik, ei välista võimalust, et kõnealusel video salvestamine ja selle edastamine on võimalik kvalifitseerida kui „isikuandmete töötlemine ainult ajakirjanduse jaoks“. Lisaks rõhutas Euroopa Kohus, et direktiivi 95/46 artiklis 9 ette nähtud erandeid ja kõrvalekaldeid tohib kohaldada ainult niivõrd, kui on vajalik selleks, et omavahel tasakaalustada kaks põhiõigust ehk õigus eraelu puutumatus kaitsele ja sõnavabadus. Euroopa Kohus täpsustas selle kohta, et ei ole välistatud, et kõnealusel video salvestamine ja avaldamine, mis toimus ilma videosalvestises kujutatud politseiametnike salvestamisest ja salvestamise eesmärkidest teavitamata, riivab nende andmesubjektide põhiõigust eraelu puutumatus austamisele. Euroopa Kohus järeldas siiski, et videosalvestise tegemine ja selliselt salvestatud video avaldamine videosaidil võivad endast kujutada isikuandmete töötlemist ainult ajakirjanduse jaoks selle sätte tähenduses, juhul kui sellest videost ilmneb, et salvestamise ja avaldamise ainus eesmärk oli teabe, arvamuste või mõtete üldsusele avalikustamine – seda peab kontrollima eelotsusetaotluse esitanud kohus (punktid 51, 52, 55, 63, 67 ja resolutsiooni punkt 2).

[22. juuni 2021. aasta kohtuotsus \(suurkoda\) Latvijas Republikas Saeima \(karistuspunktid\) \(C-439/19, EU:C:2021:504\)](#)

B on füüsiline isik, kellele on ühe või mitme liiklusrikkumise eest määratud karistuspunkte. Ceļu satiksmes drošības direkcija (Läti liiklusohutusamet) (edaspidi „CSDD“) kandis need karistuspunktid riiklikku sõiduki- ja sõidukijuhtide registrisse.

Läti liiklusõigusnormide²¹ kohaselt on sellesse registrisse kantud teave sõidukijuhtidele määratud karistuspunktide kohta üldsusele kättesaadav ning selle teabe edastab CSDD igale isikule, kes seda taotleb, ilma et viimane oleks teabe saamiseks põhjendanud erihuvi, sealhulgas ettevõtjatele taaskasutamise eesmärgil. Paludes selgitada, kas need õigusnormid on õiguspärased, esitas B Latvijas Republikas Satversmes tiesale (Läti konstitutsioonikohus) põhiseaduslikkuse järelevalve taotluse, selleks et viimane kontrolliks, kas need normid on kooskõlas õigusega eraelu puutumatusel.

Konstitutsioonikohus leidis, et kõnealust konstitutsiooniõigust hinnates peab ta arvesse võtma ka isikuandmete kaitse üldmäärust. Seega palus ta Euroopa Kohtul selgitada isikuandmete kaitse üldmääruse erinevate sätet kehtivust, selleks et teha kindlaks, kas Läti liiklusõigusnormid on selle määrusega kooskõlas.

Suurkoja otsuses tõdes Euroopa Kohus, et karistuspunkte puudutavate isikuandmete töötlemine kujutab endast „süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemist“²², milleks nähakse isikuandmete kaitse üldmäärusega ette tugevam kaitse nende andmete erilise tundlikkuse tõttu (punktid 10, 46, 74, 94 ja resolutsiooni punkt 1).

Selle käigus märkis ta kõigepealt, et teave karistuspunktide kohta on isikuandmed ning et nende andmete CSDD poolt kolmandatele isikutele edastamine kujutab endast töötlemist, mis kuulub isikuandmete kaitse üldmääruse esemelisse kohaldamisalasse. Nimetatud kohaldamisala on nimelt väga lai ning see töötlemine ei kuulu erandite hulka määruse kohaldamisest (punktid 60, 61 ja 72).

Seega ei hõlma esiteks seda töötlemist erand, mille kohaselt isikuandmete kaitse üldmäärust ei kohaldata, kui töötlemine toimub tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse²³. Seda erandit tuleb lugeda selliseks, et selle ainus eesmärk on välistada määruse kohaldamisalast isikuandmete töötlemine, mida riigiasutused teevad tegevuse raames, mille eesmärk on säilitada riigi julgeolek, või tegevuse raames, mis võidakse liigitada samasse kategooriasse. Niisugune tegevus hõlmab eelkõige seda, mille eesmärk on kaitsta riigi põhifunktsioone ja ühiskonna põhihuvisid. Liiklusohutusega seotud tegevus ei teeni aga seda eesmärki ning järelikult ei saa seda liigitada nende tegevuste kategooriasse, mille eesmärk on kaitsta riigi julgeolekut (punktid 62 ja 66–68).

Teiseks ei ole karistuspunkte puudutavate isikuandmete edastamine enam töötlemine, mille suhtes kehtiks erand, mis näeb ette, et isikuandmete kaitse üldmäärust ei kohaldata, kui isikuandmeid töötlevad karistusõiguse valdkonnas pädevad asutused²⁴. Euroopa Kohus tuvastas sellega seoses, et andmete edastamisel ei saa CSDDd lugeda niisuguseks „pädevaks asutuseks“²⁵ (punktid 69–71).

²¹ 1. oktoobri 1997. aasta liiklusseaduse (Ceļu satiksmes liikums, Latvijas Vēstnesis, 1997, nr 274/276) artikli 14¹ lõige 2.

²² Isikuandmete kaitse üldmääruse artikkel 10.

²³ Isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkt a.

²⁴ Isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkt d.

²⁵ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT 2016, L 119, lk 89), artikli 3 lõige 7.

Selleks et kindlaks teha, kas selliste liiklusrikkumisi puudutavate isikuandmetega tutvumine nagu karistuspunktid kujutab endast „süütegusid“²⁶ puudutavate isikuandmete töötlemist, millel on tugevam kaitse, tuvastas Euroopa Kohus, tuginedes eelkõige isikuandmete kaitse üldmääruse kujunemisloole, et see mõiste viitab üksnes süütegudele. Siiski ei ole asjaolu, et liiklusrikkumised on Läti õigussüsteemis kvalifitseeritud haldusõigusrikkumisteks, määrava tähtsusega selle hindamisel, kas need rikkumised kuuluvad mõiste „süütegu“ alla, kuna tegemist on liidu õiguse autonoomse mõistega, mida kogu liidus tuleb tõlgendada autonoomselt ja ühetaoliselt. Seega pärast seda, kui Euroopa Kohus meenutas rikkumise karistusõigusliku laadi hindamise kolme asjakohast kriteeriumi, nimelt rikkumise õiguslik kvalifikatsioon riigisiseses õiguses, rikkumise laad ja asjaomast isikut ähvardava sanktsiooni rangusaste, otsustas Euroopa Kohus, et kõnealused liiklusrikkumised kuuluvad isikuandmete kaitse üldmääruse tähenduses mõiste „süüteod“ alla. Kahe esimese kriteeriumi osas tuvastas Euroopa Kohus, et isegi kui riigisiseses õiguses ei kvalifitseerita rikkumisi „kuritegudeks“, võib niisugune olemus tuleneda rikkumise laadist, eelkõige selle karistavast eesmärgist, mis on karistusel, mille rikkumine võib endaga kaasa tuua. Käesolevas asjas on aga liiklusrikkumiste eest karistuspunktide määramisel nagu muudel karistustel, mille võib nende rikkumiste toimepanemine kaasa tuua, muu hulgas selline karistav eesmärk. Kolmanda kriteeriumi osas märkis Euroopa Kohus, et ainult teatud rangusastmega liiklusrikkumiste eest määratakse karistuspunkte ja et seega võivad sellised rikkumised tuua kaasa teatava rangusega sanktsioonid. Lisaks lisandub karistuspunktide määramine üldjuhul kohaldatavale sanktsioonile ning nende punktide kumuleerimine toob kaasa õiguslikud tagajärjed, milleks võib olla isegi juhtimiskeeld (punktid 77, 80, 85, 87–90 ja 93).

4. Mõiste „isikuandmete kataloog“

[10. juuli 2018. aasta kohtuotsus \(suurkoda\) Jehovahi tõdustajate \(C-25/17, ECLI:EU:C:2018:551\)](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete töötlemine““) täpsustas Euroopa Kohus ka direktiivi 95/46 artikli 2 punktis c kasutatud mõistet „kataloog“.

Euroopa Kohus tõdes, et see direktiiv on isikuandmete automatiseerimata töötlemise suhtes kohaldatav vaid siis, kui töödeldavad andmed sisalduvad kataloogis või kui nad hiljem kantakse sellisesse kataloogi, ning otsustas, et mõiste „kataloog“ hõlmab selliste isikuandmete kogumit, mis on kogutud ükselt uksele tehtava kuulutustöö käigus ning mis sisaldab nimesid ja aadresse ning muid andmeid külastatud isikute kohta, kui need andmed on korrastatud konkreetsete kriteeriumide põhjal, mis praktikas võimaldavad neid hilisema kasutamise eesmärgil hõlpsalt üles leida. Selleks et niisugune kogum kuuluks selle mõiste alla, ei ole vaja, et see hõlmaks kartoteeki, spetsiifilisi loetelusid või muid otsingusüsteeme (punkt 62 ja resolutsiooni punkt 2).

5. Mõiste „isikuandmete vastutav töötaja“

[10. juuli 2018. aasta kohtuotsus \(suurkoda\) Jehovahi tõdustajate \(C-25/17, ECLI:EU:C:2018:551\)](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete töötlemine““ ja alajaotus II.4. „Mõiste „isikuandmete kataloog““) võttis Euroopa Kohus seisukoha usukogukonna vastutuse

²⁶ Isikuandmete kaitse üldmääruse artikkel 10.

kohta isikuandmete töötlemise eest, millega tema liikmed tegelevad ükselt uksele tehtava kuulutustöö käigus, mida kogukond korraldab, koordineerib ja julgustab.

Euroopa Kohus otsustas, et igaühe kohustust järgida isikuandmete kaitset reguleerivaid liidu õigusnorme ei saa pidada sekkumiseks usukogukondade korralduslikku autonoomiasse. Sellega seoses otsustas Euroopa Kohus, et direktiivi 95/46 artikli 2 punkti d koostoimes põhiõiguste harta artikli 10 lõikega 1 tuleb tõlgendada nii, et see võimaldab pidada usukogukonda selle kuulutustööd tegevate liikmetega kaasvastutavaks isikuandmete töötlemise eest, millega viimased tegelevad ükselt uksele tehtava kuulutustöö käigus, mida kogukond korraldab, koordineerib ja julgustab, ilma et selleks oleks vaja, et kogukonnal oleks andmete juurdepääs või et oleks tuvastatud, et ta on oma liikmetele andnud kirjalikke juhiseid või korraldusi andmete töötlemise kohta (punktid 74, 75 ja resolutsiooni punkt 3).

[5. juuni 2018. aasta kohtuotsus \(suurkoda\) Wirtschaftsakademie Schleswig Holstein \(C-210/16, ECLI:EU:C:2018:388\)²⁷](#)

Saksamaa andmekaitseasutus kui järelevalveasutus direktiivi 95/46 artikli 28 mõttes oli teinud Saksamaa äriühingule, kes on spetsialiseerunud haridusvaldkonnale ja pakub koolitusteenuseid fännilehe kaudu, mida majutatakse suhtlusvõrgustiku Facebook veebisaidil, korralduse see fännileht inaktiveerida. Nimelt ei olnud selle asutuse sõnul ei see äriühing ega Facebook teavitanud fännilehe külastajaid, et viimane kogub küpsiste abil nende isikuandmeid ja seejärel töötlevad nimetatud äriühing ja Facebook neid andmeid.

Niisuguses kontekstis täpsustas Euroopa Kohus mõistet isikuandmete „vastutav töötleja“. Euroopa Kohus asus seisukohale, et selline Facebookis majutatava fännilehe haldaja nagu põhikohtuasjas kõne all olev äriühing osaleb seeläbi, et ta seadistab fännilehe lähtuvalt oma sihtrühmast ja oma tegevuse juhtimise või müügiedenduse eesmärkidest, oma fännilehe külastajate isikuandmete töötlemise eesmärkide ja vahendite kindlaksmääramises. Seetõttu tuleb see haldaja Euroopa Kohtu hinnangul lugeda koos Facebook Irelandiga (USA äriühingu Facebook liidus asuv tütarettevõtja) selle töötlemise eest liidus vastutavaks direktiivi 95/46 artikli 2 punkti d tähenduses (punkt 39).

[29. juuli 2019. aasta kohtuotsus Fashion ID \(C-40/17, EU:C:2019:629\)](#)

Selles kohtuotsuses avanes Euroopa Kohtul võimalus arendada mõistet „vastutav töötleja“ edasi seoses „tarkvara seadistuse“ lisamisega veebisaidile.

Vaidluse all oleval juhtumil lisas internetis moerõivaid müüv Saksamaa ettevõtja Fashion ID oma veebisaidile sotsiaalvõrgustiku Facebook sotsiaalmoduli „meeldib“. Selle nupu lisamine näib olevat kaasa toonud selle, et kui külastaja külastab Fashion ID veebisaiti, edastatakse selle külastaja isikuandmed Facebook Irelandile. Teabe edastamine toimub ilma, et külastaja oleks sellest teadlik, ja sõltumata asjaolust, kas ta on sotsiaalvõrgustiku Facebook liige või kas ta on Facebooki „meeldib“-nupule klõpsanud.

Verbraucherzentrale NRW, mis on tarbijate huve kaitsev Saksa mittetulundusühing, heidab Fashion ID-le ette, et ta edastas oma veebisaidi külastajate isikuandmed Facebook Irelandile

²⁷ Seda kohtuotsust käsitleti 2018. aasta aastaaruandes, lk 86 ja 87.

esiteks ilma nende nõusolekuta ja teiseks rikkudes teavitamiskohustusi, mis on ette nähtud isikuandmete kaitset reguleerivates sätetes. Kohtuasja lahendav Oberlandesgericht Düsseldorf (liidumaa kõrgeim üldkohus Düsseldorfis, Saksamaa) palus Euroopa Kohtul tõlgendada mitut direktiivi 95/46 sätet.

Euroopa Kohus tõdes esmalt, et niisugust veebisaidi haldajat nagu Fashion ID saab käsitada vastutava töötlejana direktiivi 95/46 artikli 2 punkti d tähenduses. See vastutus piirdub siiski isikuandmete töötlemise toiminguga või toimingute kogumiga, mille eesmärgid ja vahendid ta realselt kindlaks määrab, ehk asjaomaste andmete kogumise ja üleandmisega. Seevastu on Euroopa Kohtu hinnangul esmapilgul välistatud, et Fashion ID määrab kindlaks eesmärgid ja vahendid, mis on isikuandmete töötlemise hilisematel toimingutel, mida teeb Facebook Ireland pärast andmete talle edastamist, mistõttu ei saa Fashion ID-d pidada artikli 2 punkti d tähenduses nende toimingute eest vastutavaks (punktid 76, 85 ja resolutsiooni punkt 2).

Lisaks rõhutas Euroopa Kohus, et on vaja, et veebilehe haldajal ja niisugusel sotsiaalmodule pakkujal nagu Facebook Ireland oleks mõlemal töötlemistoimingute tegemise vastu direktiivi 95/46 artikli 7 punkti f tähenduses õigustatud huvi, selleks et need toimingud oleksid nende puhul põhjendatud (punkt 97 ja resolutsiooni punkt 3).

Viimaseks täpsustas Euroopa Kohus, et direktiivi 95/46 artikli 2 punkti h ja artikli 7 punkti a kohase andmesubjekti nõusoleku peab veebisaidi haldaja saama üksnes seoses isikuandmete töötlemise toimingutega, mille eesmärgid ja vahendid haldaja kindlaks määrab. Niisuguses olukorras lasub artiklis 10 ette nähtud teavitamiskohustus samuti haldajal, kuid teave, mida ta peab andmesubjektile andma, peab siiski puudutama üksnes seda isikuandmete töötlemise toimingut või toimingute kogumit, mille eesmärgid ja vahendid ta kindlaks määrab (punkt 106 ja resolutsiooni punkt 4).

[9. juuli 2020. aasta kohtuotsus Land Hessen C-272/19, EU:C:2020:535](#)

Kodanik, kes oli esitanud petitsiooni Hesseni liidumaa (Saksamaa) parlamendi petitsioonikomisjonile, taotles sellelt komisjonilt võimalust tutvuda teda puudutavate isikuandmetega, mida komisjon oli tema petitsiooni menetlemise käigus töödeldud. Ta tugines oma taotluses isikuandmete kaitse üldmäärusele, mis näeb ette andmesubjekti õiguse sellele, et vastutav töötleja võimaldab tal tutvuda teda puudutavate isikuandmetega.

Hesseni liidumaa parlamendi president jättis selle taotluse rahuldamata põhjusel, et petitsioonimenetlus kujutab endast parlamentaarset ülesannet ning parlamendi suhtes ei kuulu isikuandmete kaitse üldmäärus kohaldamisele.

Verwaltungsgericht Wiesbaden (Wiesbadeni halduskohus, Saksamaa), kellele kõnealune kodanik esitas kaebuse, leidis, et Saksa õigus ei anna mingit õigust tutvuda isikuandmetega niisuguse petitsiooni raames, nagu oli kõne all põhikohtuasjas. Kuivõrd aga Verwaltungsgericht Wiesbaden (Wiesbadeni halduskohus) arvas, et selline tutvumise õigus võib tuleneda isikuandmete kaitse üldmäärusest, pöördus ta selle kohta selgituse saamiseks Euroopa Kohtu poole. Lisaks kahtles Verwaltungsgericht Wiesbaden (Wiesbadeni halduskohus) oma sõltumatuses ja staatuses olla see kohus, kes võib esitada Euroopa Kohtule eelotsuse küsimusi, mistõttu esitas ta Euroopa Kohtule ka selle kohta küsimuse.

Euroopa Kohus vastas oma otsuses, et kui liikmesriigi liidumaa parlamendi petitsioonikomisjon määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid, tuleb seda komisjoni pidada „vastutavaks töötlejaks“ isikuandmete kaitse üldmääruse tähenduses²⁸. Isikuandmete töötlemine sellise komisjoni poolt kuulub seega selle määruse, eelkõige selle sätte kohaldamisalasse, mis annab andmesubjektidele õiguse tutvuda neid puudutavate isikuandmetega²⁹.

Euroopa Kohus leidis muu hulgas, et Hesseni liidumaa parlamendi petitsioonikomisjoni tegevus ei kuulu isikuandmete kaitse üldmääruses ette nähtud erandi alla. Ta küll mõõnis, et selline tegevus on avalik tegevus ja liidumaa enda tegevus, sest komisjon aitab kaudselt kaasa parlamendi tegevusele, kuid märkis, et see tegevus on ühtlasi nii poliitiline kui ka haldusalane. Pealegi ei nähtu Euroopa Kohtu käsutuses olevast toimikust, et see tegevus vastaks käesoleval juhul mõnele isikuandmete kaitse üldmääruses ette nähtud erandile (punktid 71–74 ja resolutsioon).

6. Isikuandmete töötlemise seaduslikkuse kriteeriumid

[16. detsembri 2008. aasta kohtuotsus \(suurkoda\) Huber \(C-524/06, EU:C:2008:724\)](#)³⁰

Saksamaa Liitvabariigi migratsiooni- ja pagulasamet (Bundesamt für Migration und Flüchtlinge, Saksamaa) haldas tsentraliseeritud välismaalaste registrit, kuhu olid koondatud teatavad isikuandmed välismaalaste kohta, kes elavad Saksamaa territooriumil rohkem kui kolmekuulise ajavahemiku jooksul. Keskregistrit kasutati statistika eesmärgil ning seda kasutasid ka julgeolekuasutused ja politsei, samuti kohtud oma volituste kasutamisel kuritegelike või avalikku julgeolekut ohustavate tegude vastu võitlemisel ja nende uurimisel.

Austria kodanik Heinz Huber asus 1996. aastal elama Saksamaale, et pidada seal füüsilisest isikust ettevõtjana kindlustusagendi ametit. Leides, et teda on tema kohta keskregistris sisalduvate andmete töötlemisega diskrimineeritud, iseäranis kuna Saksa kodanike kohta sellist registrit ei peeta, taotles H. Huber nende andmete kustutamist.

Niisuguses kontekstis palus Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Põhja-Rein-Vestfaali liidumaa kõrgeim halduskohus, Saksamaa), kelle poole vaidluse lahendamiseks pöörduti, Euroopa Kohtul selgitada, kas kirjeldatud registris toimuv isikuandmete töötlemine on liidu õigusega kooskõlas.

Euroopa Kohus tuletas esmalt meelde, et liidu kodaniku õigus elada liikmesriigis, mille kodanik ta ei ole, ei ole tingimusteta, vaid võib olla allutatud piirangutele. Sellise registri kasutamine elamisõigust käsitlevate õigusnormide kohaldamise eest vastutava ametiasutuse abistamiseks on põhimõtteliselt õiguspärane ning selle olemust arvestades kooskõlas EÜ artikli 12 lõikes 1 (nüüd ETL artikli 18 esimene lõik) toodud kodakondsuse alusel diskrimineerimise keeluga. Sellisesse registrisse ei või aga olla kantud muud teavet peale selle, mis on nimetatud eesmärgi saavutamiseks isikuandmete kaitse direktiivi tähenduses vajalik (punktid 54, 58 ja 59).

²⁸ Isikuandmete kaitse üldmääruse artikli 4 punkt 7.

²⁹ Isikuandmete kaitse üldmääruse artikkel 15.

³⁰ Seda kohtuotsust käsitleti 2008. aasta aastaaruandes, lk 45.

Mis puudutab direktiivi 95/46 artikli 7 punktis e sisalduvat töötlemise vajalikkuse mõistet, siis tuletas Euroopa Kohus esmalt meelde, et tegemist on liidu õiguse autonoomse mõistega, mida tuleb tõlgendada nii, et see oleks täielikult kooskõlas direktiivi 95/46 eesmärgiga, mis on määratletud selle direktiivi artikli 1 lõikes 1. Seejärel tõdes Euroopa Kohus, et isikuandmete töötlemise süsteem on liidu õigusega kooskõlas, kui see sisaldab üksnes neid andmeid, mis on vajalikud selleks, et asjaomased ametiasutused saaksid neid õigusnorme kohaldada, ja kui selle tsentraliseeritus võimaldab neid õigusnorme tõhusamalt kohaldada elamisõiguse suhtes, mis on liidu kodanikel, kes ei ole kõnealuse liikmesriigi kodanikud.

Igal juhul ei saa direktiivi 95/46 artikli 7 punkti e tähenduses vajalikuks pidada sellises registris nimeliste isikuandmete säilitamist ja töötlemist statistika eesmärgil (punktid 52, 66 ja 68).

Seoses registris sisalduvate andmete kasutamisega kuritegevusvastases võitluses märkis Euroopa Kohus, et niisuguse võitluse eesmärk on toimepandud kuritegude ja muude õigusrikkumiste lahendamine, sõltumata nende toimepanijate kodakondsusest. Sellest tulenevalt ei saa liikmesriigi jaoks kuritegevusvastase võitluse seisukohast olla tema kodanike olukord erinev tema territooriumil elavate välismaalastest liidu kodanike olukorrast. Seega on tema kodanike ja nende liidu kodanike erinev kohtlemine, mida tekitab kuritegevusvastase võitluse eesmärgil üksnes nende liidu kodanike isikuandmete süstemaatiline töötlemine, kes ei ole asjaomase liikmesriigi kodanikud, EÜ artikli 12 lõikega 1 keelatud diskrimineerimine (punktid 78–80).

[24. novembri 2011. aasta kohtuotsus ASNEF ja FECEMD \(C-468/10 ja C-469/10, EU:C:2011:777\)](#)

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ühelt poolt ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) teiselt poolt esitasid Tribunal Supremo (Hispaania kõrgeim kohus) kaebuse, vaidlustamaks rida artikleid kuninga dekreedis 1720/2007, millega rakendati direktiivi 95/46 üle võtnud konstitutsioonilist seadust 15/1999.

ASNEF ja FECEMD leidsid eelkõige, et Hispaania õiguses lisatakse andmete ilma andmesubjekti nõusolekuta töötlemise eeltingimusena lisanõue, mida direktiivis 95/46 ei ole, nimelt et andmed peavad olema „avalikkusele kättesaadavas allikas“, mis on loetletud konstitutsioonilise seaduse 15/1999 artikli 3 punktis j. Nad väitsid, et nimetatud seadus ja kuninga dekreet 1720/2007 piiravad direktiivi 95/46 artikli 7 punkti f ulatust. Selle punkti kohaselt eeldab isikuandmete töötlemine andmesubjekti nõusolekuta, et vastutav töötleja või andmeid saav kolmas isik või kolmandad isikud tegutsevad õigustatud huvides.

Sellega seoses märkis Euroopa Kohus esmalt, et direktiivi 95/46 artikkel 7 näeb ette ammendava ja piirava loetelu juhtudest, millal ilma andmesubjekti nõusolekuta isikuandmete töötlemist võib pidada seaduslikuks. Liikmesriigid ei saa seega direktiivi artikli 5 alusel lisada muid isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume nendele, mis on juba ette nähtud direktiivi artiklis 7, ega muuta täiendavaid nõudeid kehtestades nende kriteeriumide ulatust, mis on ette nähtud kõnealuses artiklis 7. Direktiivi artikkel 5 lubab liikmesriikidel üksnes selle direktiivi II peatüki sätetega – ja järelikult sama direktiivi artikliga 7 – lubatud ulatuses määrata täpsemalt kindlaks tingimused, millal isikuandmete töötlemine on seaduslik (punktid 30, 32 ja 33).

Täpsemalt, et läbi viia selles asjas vastanduvate õiguste ja huvide vajalik kaalumine, mida nõuab direktiivi 95/46 artikli 7 punkt f, võivad liikmesriigid kehtestada suuniseid. Samuti võivad nad võtta arvesse asjaolu, et nimetatud töötlemisega põhjustatud andmesubjekti põhiõiguste riive raskus võib varieeruda sõltuvalt sellest, kas kõnesolevad andmed sisalduvad juba avalikkusele kättesaadavates allikates või mitte (punktid 44 ja 46).

Euroopa Kohus leidis aga siiski, et kui riigisisemed õigusnormid välistavad teatavate isikuandmete kategooriate osas nende töötlemise võimaluse, nähes nende kategooriate suhtes lõplikult ette vastanduvate õiguste ja huvide kaalumise tulemuse, ilma et oleks lubatud konkreetse juhtumi erelistest asjaoludest lähtuv teistsugune tulemus, ei ole enam tegemist täpsustamisega direktiivi 95/46 artikli 5 tähenduses. Eelnevast tulenevalt järeltas Euroopa Kohus, et direktiivi 95/46 artikli 7 punktiga f on vastuolus, kui liikmesriik välistab kategooriliselt ja üldiselt teatud isikuandmete kategooriate töötlemise, ilma et oleks lubatud kaaluda konkreetset juhtumil vastanduvaid õigusi ja huve (punktid 47 ja 48).

[19. oktoobri 2016. aasta kohtuotsus Breyer \(C-582/14, EU:C:2016:779\)](#)

Kõnealusel kohtuotsuses (vt ka alajaotus II.2. „Mõiste „isikuandmed““) tegi Euroopa Kohus muu hulgas otsuse selle kohta, kas direktiivi 95/46 artikli 7 punktiga f on vastuolus riigisisene säte, mille kohaselt võib elektrooniliste teabe- ja sideteenuste osutaja koguda ja kasutada kasutaja isikuandmeid ilma tema nõusolekuta üksnes juhul, kui see on vajalik kasutaja poolt elektrooniliste teabe- ja sideteenuste konkreetse kasutuselevõtu võimaldamiseks ja arve esitamiseks, ning mille kohaselt ei saa elektrooniliste teabe- ja sideteenuste üldise toimimise tagamise eesmärk õigustada andmete kasutamist pärast vastava side toimumist.

Euroopa Kohus otsustas, et kõne all olevad liikmesriigi õigusnormid on vastuolus direktiivi 95/46 artikli 7 punktiga f. Nimelt on isikuandmete töötlemine selle sätte mõttes seaduslik üksnes juhul, kui see on vastutava andmetöötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud eesmärgi saavutamiseks vajalik, tingimusel et ei prevaleeri puudutatud isiku huvi või tema põhiõigused ja -vabadused. Käesolevas kohtuasjas välistasid Saksamaa õigusnormid aga kategooriliselt ja üldiselt teatud isikuandmete kategooriate töötlemise, ilma et oleks lubatud kaaluda konkreetset juhtumil vastanduvaid õigusi ja huve. Seega piirasid need ebaseaduslikult direktiivi 95/46 artikli 7 punktis f sätestatud põhimõtte ulatust, välistades selle, et elektrooniliste teabe- ja sideteenuste üldise toimimise tagamise eesmärki võidaks kaaluda kasutajate huvi või põhiõiguste ja -vabadustega (punktid 62–64 ja resolutsiooni punkt 2).

[4. mai 2017. aasta kohtuotsus Rīgas satiksme \(C-13/16, EU:C:2017:336\)](#)

See kohtuasi käsitles kohtuvaidlust Riia politsei ameti ja Rīgas satiksme (Riia linna trollibussiteenust osutav äriühing) vahel liiklusõnnetuse tekitaja isikuandmete avalikustamise taotluse üle. Liiklusõnnetuse toimumise ajal oli üks taksojuht jätnud oma sõiduki teeveerele seisma. Just siis, kui Rīgas satiksme troll taksost mööda sõitis, avas takso tagaistmel istuv klient sõiduki ukse, mis trollikeret riivas ning seda kahjustas. Hagi esitamiseks pöördus Rīgas satiksme muu hulgas politsei ameti poole, paludes teavet õnnetuse põhjustanud isiku kohta. Politsei amet keeldus avalikustamast takso kliendi isikukoodi ja elukohta ning dokumente liiklusõnnetuses osalenute selgitustega, põhjendades keeldumist sellega, et karistuse määramisega päädiva väärtemenetlusega seotud teavet saab anda üksnes menetlusosalistele, ning viidates

isikukoodi ja aadressi puudutavas tõigale, et isikuandmete kaitse seadus keelab eraõiguslike isikute kohta niisuguse info avaldamise.

Neil asjaoludel otsustas Augstākās tiesas Administratīvo lietu departaments (Lāti kõrgeima kohtu halduskolleeģium) esitada Euroopa Kohtule küsimuse, kas direktiivi 95/46 artikli 7 punkt f näeb ette kohustuse avalikustada kolmandale isikule isikuandmeid, mis võimaldavad kolmandal isikul esitada tsiviilkohtusse nõude andmekaitsesubjekti tekitatud kahju hüvitamiseks, ja kas asjaolu, et see isik on alaealine, võib mõjutada kõnealuse sätte tõlgendust.

Euroopa Kohus otsustas, et direktiivi 95/46 artikli 7 punkti f tuleb tõlgendada nii, et selles ei ole kehtestatud kohustust avalikustada kolmandale isikule isikuandmeid, mis võimaldavad kolmandal isikul esitada tsiviilkohtusse nõude kahju hüvitamiseks, mille tekitab andmekaitsesubjekt. Direktiivi artikli 7 punktiga f ei ole siiski vastuolus, kui andmed avalikustatakse riigisisese õiguse alusel ja järgides kõnealuses sättes ette nähtud tingimusi (punktid 27, 34 ja resolutsioon).

Selles kontekstis märkis Euroopa Kohus, et kui liikmesriigi kohtu tehtavast kontrollist ei tulene teisiti, ei näi niisugustel tingimustel, nagu on kõne all käesolevas kohtuasjas, olevat põhjendatud keelduda seetõttu, et kahju tekitaja on alaealine, kannatanule selliste isikuandmete avalikustamisest, mis võimaldavad esitada kahju hüvitamise nõude kahju tekitaja vastu või vajaduse korral vanemlikku vastutust omavate isikute vastu (punkt 33).

[27. septembri 2017. aasta kohtuotsus Puškár \(C-73/16, EU:C:2017:725\)](#)

Põhikohtuasjas esitas Peter Puškár kaebuse Najvyšší súd Slovenskej republiky (Slovaki Vabariigi kõrgeim kohus), paludes, et nimetatud kohus kohustaks Finančné riaditeľstvo'd (finantsamet) ja selle alla kuuluvaid maksuasutusi ning Kriminálny úrad finančnej správyd (finantskuritegude vastase võitluse büroo) mitte kandma tema nime registrisse, millesse on kantud isikud, keda finantsamet peab variisikuteks, ja mille finantsamet on koostanud maksude kogumise raames ning mida ajakohastavad finantsamet ja finantskuritegude vastase võitluse büroo (edaspidi „vaidlusalune register“). Lisaks palus kaebaja kustutada kõik teda puudutavad kanded neist registritest ja finantshalduse infosüsteemist.

Neil asjaoludel pöördus Najvyšší súd Slovenskej republiky (Slovaki Vabariigi kõrgeim kohus) Euroopa Kohtu poole muu hulgas küsimusega, kas harta artiklis 7 ette nähtud õigust era- ja perekonnaelu, kodu ja sõnumite puutumatuselle ning harta artiklis 8 ette nähtud õigust isikuandmete kaitsele võib tõlgendada nii, et liikmesriik ei või ilma andmesubjekti nõusolekuta luua isikuandmete registreid maksude kogumise eesmärgil, ehk teisisõnu, kas isikuandmete kogumine, mida viib läbi haldusorgan maksupettustega võitlemiseks, kätkeb endas riski.

Euroopa Kohus otsustas, et direktiivi 95/46 artikli 7 punktiga e ei ole vastuolus, kui liikmesriigi ametiasutused töötlevad isikuandmeid maksude kogumise ja maksupettustega võitlemise eesmärgil nii, nagu seda on tehtud sellise isikute registri koostamisega, nagu on kõne all põhikohtuasjas, ilma et neil oleks selleks andmesubjektide nõusolek, tingimusel, et esiteks on neile asutustele pandud liikmesriigi õigusaktidega üldiste huvidega seotud ülesannete täitmine selle sätte tähenduses, selle registri koostamine ja sellesse andmesubjektide nimede kandmine on tegelikult sobiv ja vajalik taotletavate eesmärkide saavutamiseks ning on piisav alus eeldada, et andmesubjektid on selles registris põhjendatult, ning et teiseks on täidetud kõik

direktiivis 95/46 ette nähtud sellise isikuandmete töötlemise seaduslikkuse tingimused (punkt 117 ja resolutsiooni punkt 3).

Euroopa Kohus märkis selle kohta, et eelotsusetaotluse esitanud kohus peab kontrollima, kas vaidlusaluse registri koostamine on vajalik põhikohtuasjas kõne all olevate üldiste huvidega seotud ülesannete täitmiseks, arvestades eelkõige vaidlusaluse registri koostamise täpset eesmärki, registris olevatele isikutele kaasnevaid õiguslikke tagajärgi ja seda, kas register on avalik või mitte. Lisaks, mis puudutab proportsionaalsuse põhimõtet, siis peab liikmesriigi kohus kontrollima, kas vaidlusaluse registri koostamine ja sellesse andmesubjektide nimede kandmine on sobivad meetmed nendega taotletud eesmärkide saavutamiseks ning kas nende eesmärkide saavutamiseks ei ole muid, vähem piiravaid meetmeid (punktid 111, 112 ja 113).

Euroopa Kohus tõdes ka, et vaidlusalusesse registrisse kandmine võib sellesse kantud isiku teatavaid õigusi kahjustada. Registrisse kandmine võib nimelt kahjustada tema mainet ja mõjutada tema suhteid maksuasutustega. Registrisse kandmine võib ka mõjutada kõnealuse isiku süütuse presumptsiooni, mis on sätestatud harta artikli 48 lõikes 1, ning samuti vaidlusalusesse registrisse kantud füüsiliste isikutega seostatud juriidiliste isikute ettevõtlusvabadust, mis on sätestatud harta artiklis 16. Niisugune sekkumine võib olla sobiv ainult juhul, kui on piisavalt alust kahtluseks, et andmesubjekt tegutseb temaga seostatud juriidiliste isikute juhtkonnas fiktiivselt ning kahjustab sellega maksude kogumist ja maksupettustega võitlemist (punkt 114).

Lisaks leidis Euroopa Kohus, et kui esinevad põhjused piirata direktiivi 95/46 artikli 13 alusel selle direktiivi artiklis 6 ja artiklites 10–12 ette nähtud teatavaid õigusi, nagu andmesubjekti õigus teabele, siis peab selline piirang olema vajalik, et kaitsta mõnd artikli 13 lõikes 1 nimetatud huvi, nagu muu hulgas olulised majanduslikud ja rahanduslikud huvid maksude valdkonnas, ning see piirang peab põhinema seadusandlikel aktidel (punkt 116).

[11. novembri 2020. aasta kohtuotsus Orange Romania \(C-61/19, EU:C:2020:901\)](#)

Orange România SA osutab Rumeenia turul mobiilsideteenuseid. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Rumeenia isikuandmete töötlemise riiklik järelevalveasutus) määras 28. märtsil 2018 Orange Româniele trahvi põhjusel, et viimane kogus ja säilitas ilma oma klientide otsese nõusolekuta koopiaid nende isikut tõendavatest dokumentidest.

ANSPDCP märkis, et Orange România sõlmis ajavahemikul 1.–26. märtsini 2018 mobiilsideteenuste osutamiseks lepinguid, mis sisaldavad tingimust, et kliente on teavitatud sellest, et nende isikut tõendavate dokumentide koopiaid kogutakse ja säilitatakse isiku tuvastamise eesmärgil, ning nad on andnud selleks oma nõusoleku. Seda tingimust puudutava lahtri märgistas vastutav isikuandmete töötleja enne lepingu allkirjastamist.

Selles kontekstis palus Tribunalul București (Bukaresti esimese astme kohus, Rumeenia) Euroopa Kohtul täpsustada tingimusi, millal võib klientide nõusolekut isikuandmete töötlemiseks pidada nõuetekohaseks.

Euroopa Kohus märkis kõigepealt, et liidu õiguses³¹ on ette nähtud loetelu juhtudest, mil isikuandmete töötlemist saab pidada seaduslikuks. Eelkõige peab andmesubjekti nõusolek olema vabatahtlik, konkreetne, teadlik ja ühemõtteline³². Niisiis ei ole nõusolek nõuetekohaselt antud vaikimise, eelnevalt märgistatud lahtrite või tegevusetuse korral (punktid 34, 36, 37 ja 39).

Lisaks, kui andmesubjekti nõusolek on antud kirjaliku kinnitusena, mis puudutab ka muid küsimusi, siis peab selline kinnitus olema esitatud arusaadaval ja lihtsasti kättesaadaval kujul ning olema selgelt ja lihtsalt sõnastatud. Selleks, et tagada andmesubjektile tegelik valikuvabadus, ei tohi lepingutingimused andmesubjekti eksitada selles, kas tal on võimalik sõlmida leping ka juhul, kui ta keeldub nõustumast teda puudutavate andmete töötlemisega (punktid 34, 36, 37, 39 ja 41).

Euroopa Kohus täpsustas, et kuivõrd Orange România on isikuandmete vastutav töötleja, siis peab ta olema võimeline tõendama, et nende andmete töötlemine on seaduslik, ja seega, et tema kliendid on konkreetset juhul andnud nõuetekohase nõusoleku. Kuna aga tundub, et asjaomased kliendid ei täitnud nende isikut tõendavate dokumentide koopiade kogumise ja säilitamise tingimust puudutavat märkeruutu ise, ei saa üksnes selle põhjal, et see ruut on täidetud, lugeda tõendatuks, et need kliendid avaldasid tõesti selleks nõusolekut. Liikmesriigi kohus peab selles küsimuses tegema vajaliku kontrolli (punktid 42 ja 46).

Ühtlasi peab liikmesriigi kohus muu hulgas hindama, kas asjaomased lepingutingimused võisid kõnealuseid kliente eksitada seoses võimalusega sõlmida leping olenemata keeldumisest nõustuda tema kohta käivate andmete töötlemisega, kuivõrd selle kohta puudusid täpsustused. Lisaks täheldas Euroopa Kohus, et juhul, kui klient keeldus oma isikuandmete töötlemisele nõusoleku andmisest, nõudis Orange România, et asjaomane klient kinnitaks kirjalikult, et ta ei nõustu oma isikut tõendava dokumendi koopia kogumise ega säilitamisega. Euroopa Kohus leidis, et selline täiendav nõue võib sobimatult mõjutada valikuvabadust olla sellise kogumise ja säilitamise vastu. Igal juhul peab see äriühing tõendama, et tema kliendid on aktiivse tegevusega väljendanud oma nõusolekut nende kohta käivate isikuandmete töötlemisega, ja see äriühing ei saa nõuda, et nad väljendaks oma keeldumist aktiivselt (punktid 49–51).

Seega järeltas Euroopa Kohus, et telekommunikatsiooniteenuste osutamise lepinguga, milles on tingimus, mille kohaselt andmesubjekti on teavitatud ja ta on nõustunud, et tema isikut tõendava dokumendi koopia kogutakse ja säilitatakse isiku tuvastamise eesmärgil, ei saa tõendada, et see isik on andnud selleks kogumiseks ja säilitamiseks nõuetekohase nõusoleku, kui vastutav töötleja on sellele tingimusele viitava märkeruudu täitnud enne lepingu allkirjastamist või kui lepingu tingimused võivad andmesubjekti eksitada selles, kas tal on võimalik sõlmida leping ka juhul, kui ta keeldub nõustumast teda puudutavate andmete töötlemisega, või kui vastutav töötleja on sobimatult mõjutanud valikuvabadust olla sellise kogumise ja säilitamise vastu, nõudes, et andmesubjekt, kes keeldub selleks töötlemiseks nõusolekut andmast, täidaks keeldumise dokumenteerimiseks täiendava formulari (punkt 52 ja resolutsioon).

³¹ Direktiivi 95/46 artikkel 7 ja isikuandmete kaitse üldmääruse artikkel 6.

³² Direktiivi 95/46 artikli 2 punkt h ja isikuandmete kaitse üldmääruse artikli 4 punkt 11.

[12. mai 2021. aasta kohtuotsus \(suurkoda\) Bundesrepublik Deutschland \(Interpoli tagaotsimisteade\) \(C-505/19, EU:C:2021:376\)](#)

Rahvusvaheline Kriminaalpolitsei Organisatsioon (edaspidi „Interpol“) avaldas 2012. aastal Ameerika Ühendriikide taotlusel ja selle riigi asutuste välja antud vahistamismääruse alusel Saksa kodaniku WSi tagaotsimisteate tema võimaliku väljaandmise eesmärgil. Kui tuvastatakse, et tagaotsimisteates nimetatud isik asub Interpoli liikmesriigis, peab see riik üldjuhul selle isiku esialgselt vahi alla võtma või jälgima või piirama tema liikumist.

Kuid juba enne tagaotsimisteate avaldamist oli WSi suhtes algatatud Saksamaal uurimismenetlus, mis eelotsusetaotluse esitanud kohtu sõnul puudutas samu tegusid, mis olid tagaotsimisteate aluseks. See menetlus lõpetati 2010. aastal pärast seda, kui WS oli Saksa karistusõiguses ette nähtud spetsiaalse kokkuleppemenetluse kohaselt tasunud rahasumma. Seejärel teatas Bundeskriminalamt (Saksamaa föderaalne kriminaalpolitseiamet) Interpolile, et ta leiab, et nimetatud varasema menetluse tõttu on käsitletavas asjas kohaldatav *ne bis in idem*'i põhimõte. Selle põhimõttega, mis on tagatud nii Schengeni lepingu rakendamise konventsiooni³³ artiklis 54 kui ka harta artiklis 50, on eelkõige keelatud võtta isikut, kelle kohta on tehtud lõplik otsus, sama süüteo eest uuesti vastutusele.

WS esitas 2017. aastal Verwaltungsgericht Wiesbadenile (Wiesbadeni halduskohus, Saksamaa) Saksamaa Liitvabariigi vastu kaebuse, milles palus kohtul kohustada seda riiki võtma vajalikud meetmed kõnealuse tagaotsimisteate kõrvaldamiseks. WS väitis sellega seoses, et lisaks *ne bis in idem*'i põhimõtte rikkumisele rikutakse tema õigust vabale liikumisele, mis on tagatud ELTL artiklis 21, kuna tal ei ole võimalik reisida Schengeni lepingu osalisriigis või liikmesriigis, ilma et teda ähvardaks vahi alla võtmise oht. Ta leidis samuti, et nende rikkumiste tagajärjel on tagaotsimisteates tema kohta sisalduvate isikuandmete töötlemine vastuolus direktiiviga 2016/680, mis käsitleb isikuandmete töötlemist kriminaalasjades³⁴.

Sellises olukorras otsustas Verwaltungsgericht Wiesbaden küsida Euroopa Kohtult, kas *ne bis in idem*'i põhimõte on kohaldatav, ja täpsemalt, kas on võimalik võtta esialgselt vahi alla tagaotsimisteates nimetatud isik, kes on sellises olukorras nagu käsitletav olukord. Lisaks soovis see kohus teada, et juhul kui see põhimõte on kohaldatav, siis millised on tagajärjed tagaotsimisteates sisalduvate isikuandmete töötlemisele liikmesriikide poolt.

Euroopa Kohus otsustas suurkoja otsuses, et direktiivi 2016/680 sätteid tuleb lähtuvalt Schengeni konventsiooni artiklist 54 ja harta artiklist 50 tõlgendada nii, et nendega ei ole vastuolus Interpoli välja antud tagaotsimisteates sisalduvate isikuandmete töötlemine seni, kuni sellise lõpliku kohtuotsusega ei ole tuvastatud, et tagaotsimisteate aluseks olevate tegude suhtes on kohaldatav *ne bis in idem*'i põhimõte, tingimusel et isikuandmete selline töötlemine vastab nimetatud direktiivis sätestatud tingimustele (punkt 121 ja resolutsiooni punkt 2).

³³ Konventsioon, millega rakendatakse 14. juuni 1985. aasta Schengeni lepingut Beneluxi Majandusliidu riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vahel nende ühispiiril kontrolli järkjärgulise kaotamise kohta (EÜT 2000, L 239, lk 19; ELT eriväljaanne 19/02, lk 9) (edaspidi „Schengeni konventsioon“).

³⁴ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT 2016, L 119, lk 89).

Mis puudutab Interpoli tagaotsimisteates sisalduvate isikuandmete küsimust, siis märkis Euroopa Kohus, et isikuandmete suhtes tehtav mis tahes toiming, näiteks isikuandmete salvestamine liikmesriigi andmebaasidesse, kujutab endast direktiivi 2016/680³⁵ kohaldamisalasse kuuluvat isikuandmete töötlemist. Lisaks leidis ta ühelt poolt, et isikuandmete niisugusel töötlemisel on õiguspärane eesmärk, ning teiselt poolt, et seda ei saa pidada ebaseaduslikuks üksnes seetõttu, et *ne bis in idem*'i põhimõte võib olla kohaldatav tegude suhtes, millel tagaotsimisteade põhineb³⁶. Pealegi võib isikuandmete niisugune töötlemine liikmesriikide poolt osutada vajalikuks just nimelt selleks, et kontrollida, kas see põhimõte on kohaldatav (punktid 111, 114, 116, 117 ja 119).

Neil asjaoludel otsustas Euroopa Kohus samuti, et direktiiviga 2016/680, tõlgendatuna lähtuvalt Schengeni konventsiooni artiklist 54 ja harta artiklist 50, ei ole vastuolus tagaotsimisteates sisalduvate isikuandmete töötlemine seni, kuni lõpliku kohtuotsusega ei ole tuvastatud, et konkreetsel juhul on kohaldatav *ne bis in idem*'i põhimõte. Isikuandmete selline töötlemine peab siiski vastama nimetatud direktiivis sätestatud tingimustele. Eelnevat silmas pidades peab see olema vajalik liikmesriigi pädeva asutuse ülesande täitmiseks süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise eesmärgil³⁷ (punkt 121 ja resolutsiooni punkt 2).

Seevastu juhul, kui *ne bis in idem*'i põhimõte on kohaldatav, ei ole Interpoli tagaotsimisteates sisalduvate isikuandmete salvestamine liikmesriikide andmebaasidesse enam vajalik, kuna asjaomast isikut ei saa tagaotsimisteatega hõlmatud tegude eest enam kriminaalvastutusele võtta ja seega samade tegude eest vahi alla võtta. Järelikult peab asjaomasel isikul olema võimalik nõuda, et need andmed kustutataks. Kui andmeid siiski ei kustutata, peab nende juurde olema lisatud mäрге, et *ne bis in idem*'i põhimõtte tõttu ei saa asjaomast isikut samade tegude eest liikmesriigis või osalisriigis enam vastutusele võtta (punkt 120).

[22. juuni 2021. aasta kohtuotsus \(suurkoda\) Latvijas Republikas Saeima \(karistuspunktid\) \(C-439/19, EU:C:2021:504\)](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete töötlemine““) otsustas Euroopa Kohus, et isikuandmete kaitse üldmäärusega on vastuolus õigusnormid, millega kohustatakse Ceļu satiksmes drošības direkcijai (Läti liiklusohutusamet) (edaspidi „CSDD“) tegema üldsusele kättesaadavaks andmed karistuspunktide kohta, mis sõidukijuhtidele on määratud liiklusrikkumiste eest, ilma et isik, kes seda taotleb, peaks tõendama erilist huvi nende andmete saamiseks. Ta tõdes, et tõendatud ei ole Läti valitsuse viidatud vajadus edastada liiklusrikkumiste eest määratud karistuspunkte puudutavaid isikuandmeid eelkõige liiklusohutuse parandamiseks. Lisaks leidis Euroopa Kohus, et ei üldsuse huvi tutvuda ametlike dokumentidega ega ka õigus teabevabadusele ei õigusta selliseid õigusnorme (punktid 113, 120–122 ja resolutsiooni punkt 2).

Selles kontekstis toonitas Euroopa Kohus, et Läti õigusnormides viidatud liiklusohutuse parandamine kujutab endast üldise huvi eesmärki, mida liit tunnustab, ning et seega on

³⁵ Vt direktiivi 2016/680 artikli 2 lõige 1 ja artikli 3 punkt 2.

³⁶ Vt direktiivi 2016/680 artikli 4 lõike 1 punkt b ja artikli 8 lõige 1.

³⁷ Vt direktiivi 2016/680 artikli 1 lõige 1 ja artikli 8 lõige 1.

liikmesriikidel õigus kvalifitseerida liiklusohutus „avalikes huvides olevaks ülesandeks“³⁸. Siiski ei ole tõendatud, et Läti süsteem karistuspunkte puudutavate isikuandmete edastamise kohta oleks kõnealuse eesmärgi saavutamiseks vajalik. Esiteks on Läti seadusandjal hulk õiguskaitsevahendeid, mis oleksid viimasel võimaldanud saavutada see eesmärk muude vahenditega, mis on asjaomaste isikute põhiõigusi vähem piiravad. Teiseks tuleb arvesse võtta karistuspunkte puudutavate andmete tundlikkust ja asjaolu, et nende andmete üldsusele edastamine võib kujutada endast õiguse eraelu puutumatusel ja isikuandmete kaitsele tõsist riivet, kuna see võib põhjustada ühiskonna hukkamõistu ja tuua kaasa andmesubjekti stigmatiseerimise (punktid 109–113).

Lisaks tõdes Euroopa Kohus, et võttes arvesse nende andmete tundlikkust ja mõlemasse põhiõigusesse sekkumise tõsidust, kaaluvad need õigused üles nii avaliku huvi tutvuda ametlike dokumentidega, nagu riiklik sõiduki- ja sõidukijuhtide register, kui ka õiguse teabevabadusele (punktid 120 ja 121).

Peale selle otsustas Euroopa Kohus identsetel põhjendustel, et isikuandmete kaitse üldmäärusega on samuti vastuolus Läti õigusnormid, kuna need lubavad CSDD-l edastada andmed karistuspunktide kohta, mis on sõidukijuhtidele määratud liiklusrikkumiste eest, ettevõtjatele selleks, et viimased saaksid neid taaskasutada ja üldsusele edastada (punkt 126 ja resolutsiooni punkt 3).

Lõpuks täpsustas Euroopa Kohus, et liidu õiguse esimuse põhimõttega on vastuolus, kui eelotsusetaotluse esitanud kohus, kellele on esitatud kaebus nende Läti õigusnormide peale, mille Euroopa Kohus on tunnistanud liidu õigusega vastuolus olevaks, otsustab säilitada nende õigusnormide õiguslikud tagajärjed kuni ajani, mil ta teeb oma lõpliku kohtuotsuse (punkt 137 ja resolutsiooni punkt 4).

III. Isikuandmete töötlemine direktiivi 2002/58 tähenduses

[2. oktoobri 2018. aasta kohtuotsus \(suurkoda\) Ministerio Fiscal \(C-207/16, ECLI:EU:C:2018:788\)](#)³⁹

Käesolevas kohtuasjas oli kõne all rahakoti ja mobiiltelefoni röövi üle käiva eeluurimise raames esitatud taotlus, mille Hispaania eeluurimiskohus jättis rahuldamata. Täpsemalt esitas kriminaalpolitsei eeluurimiskohtule taotluse, paludes võimaldada juurdepääs niisuguste telefoninumbrite kasutajate tuvastamist võimaldavatele andmetele, mis aktiveeriti varastatud mobiiltelefonis 12 päevase ajavahemiku jooksul röövi toimumisest. Keeldumist põhjendati sellega, et eeluurimise alustamise põhjustanud faktilised asjaolud ei vasta „raske“ rikkumise koosseisule – mis on Hispaania õiguse järgi rikkumine, mida karistatakse pikema kui viieaastase vanglakaristusega – ja et kasutajate tuvastamist võimaldavate andmetega tutvumist tohib võimaldada ainult sellist tüüpi rikkumise korral.

Euroopa Kohus tuletas meelde, et avaliku võimu esindaja juurdepääs elektroonilise side teenuste osutajate säilitatavatele isikuandmetele eeluurimismenetluse käigus kuulub

³⁸ Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e kohaselt on isikuandmete töötlemine õiguspärane, kui see on „vajalik avalikes huvides oleva ülesande täitmiseks [...]“.

³⁹ Seda kohtuotsust käsitleti 2018. aasta aastaaruandes, lk 88 ja 89.

direktiivi 2002/58 kohaldamisalasse. Kohus otsustas seejärel, et juurdepääs andmetele, milleks on perekonnanimi, eesnimi ja vajaduse korral ka aadress, millega saab tuvastada nende SIM-kaartide omanikke, mis avati varastatud mobiiltelefonis, kujutab endast nimetatud isikutele hartas tagatud põhiõiguste eraelu austamisele ja isikuandmete kaitsele riivet isegi juhul, kui ei esine asjaolusid, mis võimaldaksid kvalifitseerida sellise riive „raskeks“. Seejuures ei oma tähtsust tõik, kas asjasse puutuvad eraelulised andmed on delikaatsed või mitte või kas puudutatud isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi või mitte. Euroopa Kohus toonitas siiski, et see riive ei ole aga nii raske, et sellist juurdepääsu tuleks kuritegude ennetamisel, uurimisel, avastamisel ja menetlemisel piirata võitlusega raske kuritegevuse vastu. Nimelt, kuigi direktiivis 2002/58 on ammendavalt loetletud eesmärgid, millega saab põhjendada riigisiseseid õigusnorme, mis reguleerivad avaliku võimu juurdepääsu asjasse puutuvatele andmetele ja näevad seega ette erandi elektroonilise side konfidentsiaalsuse põhimõttest, ning kuivõrd juurdepääs tohib toimuda ainult tõepoolest neil ja rangelt neil eesmärkidel, siis märkis Euroopa Kohus, et mis puudutab kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärki, siis direktiivi 2002/58 sõnastus ei piira seda eesmärki võitlusega üksnes raskete kuritegude vastu, vaid peab silmas „kuritegusid“ üldiselt (punktid 38, 42, 59–63 ja resolutsioon).

Selles kontekstis täpsustas Euroopa Kohus, et kuigi ta otsustas kohtuotsuses Tele2 Sverige ja Watson jt⁴⁰, et kuritegude ennetamise, uurimise, avastamise ja menetlemise puhul saab avalikule võimule juurdepääsu andmist elektroonilise side teenuste osutajate säilitatavatele isikuandmetele – mis koosvõetuna võimaldavad teha täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse – põhjendada ainult võitlusega raske kuritegevuse vastu, oli selline tõlgendus põhjendatud asjaoluga, et sellist juurdepääsu reguleerivate õigusnormidega taotletav eesmärk peab olema proportsioonis selle tegevusega kaasneva põhiõiguste riive raskusega. Nimelt saab proportsionaalsuse põhimõtte järgi põhjendada rasket riivet kuritegude ennetamisel, uurimisel, avastamisel ja menetlemisel üksnes võitlusega sellise kuritegevuse vastu, mida tuleb samuti pidada „raskeks“. Kui aga sellise juurdepääsuga kaasnev riive ei ole raske, võib juurdepääsu põhjendada ka üldiselt „kuritegude“ ennetamise, uurimise, avastamise ja menetlemise eesmärgiga (punktid 54–57).

Kõnesoleval juhtumil asus Euroopa Kohus seisukohale, et juurdepääsu ainult nendele andmetele, mille suhtes esitati vaidlusalune taotlus, ei saa pidada nende isikute põhiõiguste „raskeks“ riiveks, kelle andmetele juurdepääsu sooviti, sest need andmed ei võimalda teha täpseid järeldusi selliste isikute eraelu kohta. Euroopa Kohus järeldas sellest, et nendele andmetele juurdepääsuga kaasnevat riivet saab seega põhjendada üldiselt „kuritegude“ ennetamise, uurimise, avastamise ja menetlemise eesmärgiga, ilma et oleks vaja neid kuritegusid kvalifitseerida „raskeks“ (punktid 61 ja 62).

[6. oktoobri 2020. aasta kohtuotsused \(suurkoda\) Privacy International \(C-623/17, EU:C:2020:790\) ja La Quadrature du Net jt \(C-511/18, C-512/18 ja C-520/18, EU:C:2020:791\)](#)⁴¹

Kohtupraktika, mis käsitleb isikuandmete säilitamist ja nendele andmetele juurdepääsu elektroonilise side valdkonnas, ning eelkõige kohtuotsus Tele2 Sverige ja Watson jt, milles Euroopa Kohus leidis eelkõige, et liikmesriigid ei või panna elektroonilise side teenuste osutajatele liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise kohustust, on

⁴⁰ Euroopa Kohtu 21. detsembri 2016. aasta kohtuotsus Tele2 Sverige ja Watson jt (C-203/15 ja C-698/15, [EU:C:2016:970](#)).

⁴¹ Neid kohtuotsuseid käsitleti 2020. aasta aastaaruandes, lk 29–32.

tekitanud muret mõnes liikmesriigis, kes kardavad, et neilt on võetud vahend, mida nad peavad riigi julgeoleku kaitsmisel ja kuritegevuse vastu võitlemisel vajalikuks.

Selline on sisuline taust, mille põhjal Investigatory Powers Tribunalis (ametiasutuste järelevalve kohta esitatud kaebusi lahendav kohus, Ühendkuningriik) (Privacy International, C-623/17), Conseil d'État's (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) (La Quadrature du Net jt, liidetud kohtuasjad C-511/18 ja C-512/18) ja Cour constitutionnelle'is (Belgia konstitutsioonikohus) (Ordre des barreaux francophones et germanophone jt, C-520/18) algatati kohtuasjad, mis puudutavad nende õigusaktide õiguspärasust, mille teatud liikmesriigid on nendes valdkondades vastu võtnud ja millega eelkõige pannakse elektroonilise side teenuste osutajatele kohustus kasutajate liiklus- ja asukohaandmeid avaliku võimu asutusele edastada või selliseid andmeid üldiselt ja vahet tegemata säilitada.

Kahes 6. oktoobril 2020 kuulutatud suurkoja otsuses leiab Euroopa Kohus kõigepealt, et riigisisised õigusnormid, millega on elektroonilise side teenuste osutajatele kehtestatud riigi julgeoleku kaitsmise ja kuritegevuse vastu võitlemise eesmärgil kohustus säilitada liiklus- ja asukohaandmeid ja edastada neid sel eesmärgil julgeoleku- ja luureteenistustele, kuuluvad direktiivi 2002/58 kohaldamisalasse (kohtuotsuse Privacy International punkt 49 ja resolutsiooni punkt 1 ning kohtuotsuse La Quadrature du Net jt punkt 104).

Järgmiseks märkis Euroopa Kohus, et direktiiv 2002/58⁴² ei võimalda seda, et erand põhimõttelisest kohustusest tagada elektroonilise side ja sellega seotud andmete konfidentsiaalsus ning keelust neid andmeid salvestada muutuks reeglisk. See tähendab, et see direktiiv lubab liikmesriikidel võtta seadusandlikke meetmeid, mis piiravad direktiivis ette nähtud õigusi ja kohustusi ning eelkõige kohustust tagada side ja liiklusandmete konfidentsiaalsus⁴³ ka riigi julgeoleku kaitsmise eesmärgil ainult juhul, kui see on kooskõlas liidu õiguse üldpõhimõtetega, mille hulka kuulub proportsionaalsuse põhimõte, ja hartaga tagatud põhiõigustega⁴⁴ (kohtuotsuse Privacy International punktid 59 ja 60 ning kohtuotsuse La Quadrature du Net jt punkt 111 ja 113).

Selle raames leidis Euroopa Kohus esiteks kohtuasjas Privacy International, et direktiiviga 2002/58, tõlgendatuna harta alusel, on vastuolus liikmesriigi õigusnormid, mis panevad elektroonilise side teenuste osutajatele riigi julgeoleku kaitsmise eesmärgil kohustuse edastada julgeoleku- ja luureteenistustele üldiselt ja vahet tegemata liiklus- ja asukohaandmeid. Teiseks leidis Euroopa Kohus liidetud kohtuasjades La Quadrature du Net jt ning kohtuasjas Ordre des barreaux francophones et germanophone jt, et sama direktiiviga on vastuolus seadusandlikud meetmed, millega pannakse elektroonilise side teenuste osutajatele ennetava meetmena liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise kohustus.

Selliste andmete edastamise ning üldise ja vahet tegemata säilitamise kohustused kujutavad endast nimelt hartaga tagatud põhiõiguste eriti raskeid riiveid, ilma et andmesubjektide käitumisel oleks seos kõnealuste õigusnormidega taotletava eesmärgiga. Euroopa Kohus andis analoogilise tõlgenduse isikuandmete kaitse üldmääruse artikli 23 lõikele 1, leides, et seda tuleb lähtuvalt hartast tõlgendada nii, et sellega on vastuolus riigisisised õigusnormid, millega

⁴² Direktiivi 2002/58 artikli 15 lõiked 1 ja 3.

⁴³ Direktiivi 2002/58 artikli 5 lõige 1.

⁴⁴ Eelkõige harta artiklid 7, 8, 11 ja artikli 52 lõige 1.

pannakse üldkasutatavate veebipõhiste sideteenuste ja veebimajutusteenuste osutajatele kohustus üldiselt ja vahet tegemata säilitada nende teenustega seotud isikuandmeid (kohtuotsuse Privacy International punktid 71, 82 ja resolutsiooni punkt 2 ning kohtuotsuse La Quadrature du Net jt punktid 146, 168, 174, 177, 212 ja resolutsiooni punktid 1 ja 3).

Seevastu leidis Euroopa Kohus, et olukordades, kus liikmesriik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks ja vahetuks või ettearvatavaks, ei ole direktiiviga 2002/58, tõlgendatuna lähtuvalt hartast, vastuolus see, kui elektroonilise side teenuste osutajatele pannakse kohustus liiklus- ja asukohaandmeid üldiselt ja vahet tegemata säilitada. Euroopa Kohus täpsustas sellega seoses, et otsus, millega selline ettekirjutus tehakse, peab olema ajaliselt piiratud tingimata vajalikuga ning seda peab tõhusalt kontrollima kas kohus või sõltumatu haldusasutus – kelle otsus on siduv –, selleks et teha kindlaks, kas esineb mõni selline olukord ning kas on järgitud ette nähtud tingimusi ja tagatisi. Samadel tingimustel ei ole selle direktiiviga vastuolus ka elektroonilise side vahendite kõigi kasutajate andmete, eelkõige liiklus- ja asukohaandmete automatiseeritud analüüsimine (kohtuotsuse La Quadrature du Net jt punktid 137–139, 177–179 ning resolutsiooni punktid 1 ja 2).

Euroopa Kohus lisas, et direktiiviga 2002/58, tõlgendatuna lähtuvalt hartast, ei ole vastuolus seadusandlikud meetmed, mis võimaldavad liiklus- ja asukohaandmeid eesmärgipäraselt säilitada ajavahemikuks, mis on piiratud tingimata vajalikuga, kui see on objektiivsete ja mittediskrimineerivate asjaolude alusel piiritletud vastavalt andmesubjektide kategooriatele või geograafilise kriteeriumi põhjal. Samuti ei ole selle direktiiviga vastuolus seadusandlikud meetmed, mis näevad ette side lähtepunktile omistatud IP-aadresside üldise ja vahet tegemata säilitamise, kui see on ajaliselt piiratud tingimata vajalikuga, või elektroonilise side vahendite kasutajate identiteediga seotud andmete üldise ja vahet tegemata säilitamise, kusjuures viimati nimetatud juhul ei ole liikmesriikidel vaja säilitusaega piirata. Selle direktiiviga ei ole vastuolus ka seadusandlik meede, mis võimaldab elektroonilise side teenuste osutajate valduses olevate andmete kiirsäilitust, juhul kui esinevad olukorrad, kus andmeid on vaja säilitada seaduses sätestatud tähtaegadest pikemaks ajaks, et selgitada välja raskete kuritegude toimepanemine või riigi julgeoleku kahjustamine, kui selliseid kuritegusid või kahjustamisi on juba tuvastatud või kui nende olemasolu võib mõistlikult kahtlustada (kohtuotsuse La Quadrature du Net jt punktid 161, 163, 168 ja resolutsiooni punkt 1).

Peale selle otsustas Euroopa Kohus, et direktiiviga 2002/58, tõlgendatuna lähtuvalt hartast, ei ole vastuolus riigisisese õigusnormid, millega pannakse elektroonilise side teenuste osutajatele kohustus liiklus- ja asukohaandmeid reaajas koguda, kui see on piiratud isikutega, kelle puhul on mõjuv põhjus kahtlustada, et nad on ühel või teisel viisil seotud terrorismiga, ning kui seda kontrollib enne kas kohus või sõltumatu haldusasutus – kelle otsus on siduv –, selleks et tagada, et andmete reaajas kogumiseks antakse luba üksnes tingimata vajaliku piires. Kiireloomulisel juhul peab kontroll toimuma lühikese aja jooksul (kohtuotsuse La Quadrature du Net jt punkt 192 ja resolutsiooni punkt 2).

Viimaks käsitles Euroopa Kohus liidu õigusega vastuolus olevaks tunnistatud riigisiseste õigusnormide toime säilitamist teatavaks ajaks. Ta otsustas, et liikmesriigi kohus ei või kohaldada riigisisest õigusnormi, mis annab talle õiguse ajaliselt piirata tagajärgi, mis kaasnevad sellega, kui ta tühistab riigisisese õigusakti, millega on elektroonilise side teenuste osutajatele kehtestatud liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise kohustus, mis on tunnistatud vastuolus olevaks direktiiviga 2002/58, tõlgendatuna lähtuvalt hartast.

Liikmesriigi kohtule tarviliku vastuse andmiseks tuletas Euroopa Kohus samas meelde, et kehtiva liidu õiguse kohaselt võib üldjuhul üksnes riigisiseses õiguses kindlaks määrata reeglid, mis puudutavad rasketes kuritegudes kahtlustatavate isikute suhtes alustatud kriminaalmenetluses sellise teabe ja selliste tõendite lubatavust ja hindamist, mis on saadud andmete liidu õigusega vastuolus oleva säilitamise teel. Euroopa Kohus täpsustas siiski, et direktiiv 2002/58, tõlgendatuna lähtuvalt tõhususe põhimõttest, kohustab liikmesriigi kriminaalkohut jätma kriminaalmenetluses arvesse võtmata tõendid, mis on saadud liiklus- ja asukohaandmete liidu õigusega vastuolus oleva üldise ja vahet tegemata säilitamise teel, kui kuritegudes kahtlustatavatel ei ole võimalik nende tõendite suhtes tõhusalt seisukohta võtta (kohtuotsuse La Quadrature du Net jt punktid 222 ja 228 ning resolutsiooni punkt 4).

[2. märtsi 2021. aasta kohtuotsus \(suurkoda\) Prokuratuur \(tingimused elektroonilise side andmete juurdepääsuks\) \(C-746/18, EU:C:2021:152\)](#)

Eestis alustati H. K. suhtes kriminaalmenetlust, milles teda süüdistati vargustes, kolmandale isikule kuuluva pangakaardi kasutamises ja vägivaldas õigusemõistmises osalejate vastu. Esimese astme kohtu otsusega mõisteti H. K-le nende süütegude eest kaheaastane vangistus. Apellatsiooniasemes jäeti see otsus muutmata. Protokollid, millele nende süütegude tuvastamisel tugineti, olid koostatud eelkõige nende isikuandmete alusel, mis olid loodud elektroonilise side teenuste osutamise käigus. Riigikohtul (Eesti), kellele H. K. esitas kassatsioonkaebuse, tekkis kahtlus, kas tingimused, millistel uurimisasutus sai nendele andmetele juurdepääsu, on liidu õigusega⁴⁵ kooskõlas.

Need kahtlused puudutasid esiteks küsimust, kas ajavahemik, mille kohta on uurimisasutusel olnud andmete juurdepääs, on oluline asjaolu, mis võimaldab hinnata selle riive raskust, mida see juurdepääs endast asjaomaste isikute põhiõigustele kujutab. Seega, kui see ajavahemik on väga lühike või kogutud andmete hulk on väga väike, tekkis eelotsusetaotluse esitanud kohtul küsimus, kas üldine kuritegevusega võitlemise eesmärk ja mitte ainult võitlus raskete kuritegude vastu võib sellist riivet õigustada. Teiseks kahtles eelotsusetaotluse esitanud kohus selles, kas Eesti prokuratuuri võib talle riigisisese õigusega usaldatud erinevaid ülesandeid arvestades pidada kohtuotsuse Tele2 Sverige ja Watson jt⁴⁶ tähenduses sõltumatuks haldusasutuseks, kes võib anda uurimisasutusele kõnealustele andmetele juurdepääsu loa.

Euroopa Kohus otsustas suurkojas tehtud otsuses, et direktiiviga 2002/58, tõlgendatuna koostoimes hartaga, on vastuolus riigisisese õigusnormid, mis võimaldavad ametiasutustele kuritegude ennetamise, uurimise, avastamise ja kohtus menetlemise eesmärgil juurdepääsu liiklus- või asukohaandmetele, millest võib saada teavet elektroonilise sidevahendi kasutaja sideseansside või tema kasutatavate lõppseadmete asukoha kohta ja teha tema eraelu kohta täpseid järeldusi, ilma et see juurdepääs piirduks menetlustega, mille eesmärk on võitlus raske kuritegevuse vastu või avalikku julgeolekut ähvardava suure ohu ärahoidmine. Euroopa Kohtu hinnangul ei oma sealjuures tähtsust, millise ajavahemiku kohta on andmete juurdepääsu taotletud, ega selle ajavahemiku kohta kättesaadavate andmete hulk või liik. Lisaks leidis Euroopa Kohus, et selle direktiiviga, tõlgendatuna koostoimes hartaga, on vastuolus riigisisese õigusnormid, mis annavad prokuratuurile pädevuse anda ametiasutusele kriminaaluurimise

⁴⁵ Täpsemalt direktiivi 2002/58 artikli 15 lõige 1 koostoimes harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1.

⁴⁶ 21. detsembri 2016. aasta kohtuotsus Tele2 Sverige ja Watson jt (C-203/15 ja C-698/15, EU:C:2016:970, punkt 120).

läbiviimiseks liiklus- ja asukohaandmetele juurdepääsu luba (punktid 45, 59 ja resolutsiooni punktid 1 ja 2).

Mis puudutab kõnealuste õigusnormidega taotletud kuritegude ennetamise, uurimise, avastamise ja kohtus menetlemise eesmärki, siis leidis Euroopa Kohus proportsionaalsuse põhimõtte kohaselt, et ainult võitlus raskete kuritegude vastu ja avalikku julgeolekut ähvardava suure ohu ärahoidmine saavad õigustada ametiasutuste juurdepääsu liiklus- või asukohaandmete kogumile, millest võib teha asjaomaste isikute eraelu kohta täpseid järeldusi, ilma et selline juurdepääs võiks tulenevalt muudest asjaoludest, mis on seotud juurdepääsu taotluse proportsionaalsusega, nagu see ajavahemik, mille ulatuses on andmetele juurdepääsu taotletud, olla põhjendatud üldise kuritegude ennetamise, uurimise, avastamise ja kohtus menetlemise eesmärgiga (punktid 33 ja 35).

Mis puudutab prokuratuuri pädevust anda ametiasutusele kriminaaluurimise läbiviimiseks liiklus- ja asukohaandmetele juurdepääsu luba, siis tuletas Euroopa Kohus meelde, et liikmesriigi õiguses tuleb kindlaks määrata tingimused, mille kohaselt peavad elektroonilise side teenuste osutajad andma riigi pädevatele asutustele juurdepääsu nende käsutuses olevatele andmetele. Proportsionaalsuse nõude järgimiseks peavad sellistes õigusnormides siiski olema ette nähtud selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, millest tulenevalt on isikutel, kelle isikuandmetega on tegu, piisavad tagatised, mis võimaldavad neid andmeid kuritarvitamise ohu eest tõhusalt kaitsta. Need õigusnormid peavad olema riigisisises õiguses õiguslikult siduvad ja nendes peab olema märgitud, millistel asjaoludel ja tingimustel võib selliste andmete töötlemist ette nägeva meetme võtta, tagades seeläbi, et riive piirdub sellega, mis on rangelt vajalik (punkt 48).

Selleks et tegelikkuses oleks tagatud nende tingimuste täielik järgimine, on Euroopa Kohtu hinnangul esmatähtis, et riigi pädevate asutuste juurdepääs säilitatud andmetele oleks allutatud kohtu või sõltumatu haldusasutuse tehtavale eelnevale kontrollile ja et see kohus või haldusasutus teeks oma otsuse juurdepääsu taotleva asutuse põhjendatud taotluse alusel, mis on ennekõike esitatud kuriteo ennetamise, avastamise või kohtus menetlemise raames. Nõuetekohaselt põhjendatud kiireloomulisel juhul peab kontroll toimuma lühikese aja jooksul (punkt 51).

Sellega seoses täpsustas Euroopa Kohus, et eelnev kontroll nõuab muu hulgas, et kohtul või asutusel, kelle ülesanne on seda kontrolli teha, oleksid kõik volitused ja kõik vajalikud tagatised, et tagada erinevate asjaomaste huvide ja õiguste ühitamine. Mis puudutab konkreetsemalt kriminaaluurimist, siis eeldab selline kontroll, et see kohus või asutus suudaks tagada õiglase tasakaalu ühelt poolt kuritegevusvastase võitluse raames uurimise vajadustega seotud huvide ning teiselt poolt selliste isikute põhiõiguste vahel eraelu puutumatusel ja isikuandmete kaitsele, kelle andmetele juurdepääsu taotletakse. Kui seda kontrolli ei tee kohus, vaid sõltumatu haldusasutus, peab sellel asutusel olema staatus, mis võimaldab tal tegutseda oma ülesannete täitmisel objektiivselt ja erapooletult ning selleks peab ta olema kaitstud igasuguse välise mõju eest (punktid 52 ja 53).

Euroopa Kohtu sõnul tuleneb sellest, et sõltumatuse nõue, millele peab vastama eelnevat kontrolli tegev asutus, eeldab, et see asutus oleks andmetele juurdepääsu taotleva asutuse suhtes kolmas isik, mistõttu esimene saaks teha kontrolli objektiivselt ja erapooletult, olles kaitstud igasuguse välise mõju eest. Täpsemalt eeldab sõltumatuse nõue kriminaalõiguse

valdkonnas, et sellise eelneva kontrolli eest vastutav asutus ei oleks esiteks seotud kõnealuse kriminaaluurimisega ja et teiseks oleks tal kriminaalmenetluse poolte suhtes neutraalne positsioon. See ei ole aga nii prokuratuuri puhul, kes – nagu Eesti prokuratuur – juhib uurimismenetlust ja esindab vajaduse korral riiklikku süüdistust. Sellest järeldeb, et prokuratuur ei saa teha eespool nimetatud eelnevat kontrolli (punktid 54, 55 ja 57).

IV. Isikuandmete edastamine kolmandatesse riikidesse

[6. novembri 2003. aasta kohtuotsus \(suurkoda\) Lindqvist \(C-101/01, EU:C:2003:596\)⁴⁷](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete töötlemine““) palus eelotsusetaotluse esitanud kohus eelkõige selgitada, kas Bodil Lindqvist tegeles kõnealuse direktiivi mõttes isikuandmete edastamisega kolmandasse riiki.

Euroopa Kohus otsustas, et „andmete edastamist kolmandatesse riikidesse“ direktiivi 95/46 artikli 25 tähenduses ei ole toimunud, kui liikmesriigis asuv isik sisestab isikuandmed veebilehele, mis on salvestatud samas riigis või teises liikmesriigis asuva füüsilise või juriidilise isiku serveris, kus asub selle veebileheta tutvumist võimaldav veebisait, nii et need andmed muutuvad kättesaadavaks igapähele, kes kasutab interneti, kaasa arvatud kolmandates riikides asuvad isikud (punkt 71 ja resolutsiooni punkt 4).

Arvestades sellega seoses esiteks interneti arengutaset direktiivi 95/46 väljatöötamise ajal ja teiseks seda, et IV peatükis, kuhu kuulub artikkel 25 – mille eesmärk on tagada liikmesriikidepoolne kontroll isikuandmete edastamisel kolmandatesse riikidesse ning keelata isikuandmete edastamine kolmandasse riiki, kui kaitse tase selles kolmandas riigis ei ole piisav –, puuduvad interneti kasutamisele kohaldatavad sätted, ei saa eeldada, et ühenduse seadusandja soovis mõistega „andmete edastamine kolmandatesse riikidesse“ tulevikus hõlmata andmete niisugust sisestamist veebilehele, isegi kui andmed muutuvad seeläbi kättesaadavaks kolmandates riikides isikutele, kellel on nendega tutvumiseks vajalikud tehnilised vahendid (punktid 63, 64 ja 68).

[6. oktoobri 2015. aasta kohtuotsus \(suurkoda\) Schrems \(C-362/14, EU:C:2015:650\)⁴⁸](#)

Austria kodanik Maximilian Schrems, kes on sotsiaalvõrgustiku Facebook kasutaja, esitas Data Protection Commissionerile (Iirimaa andmekaitsevolinik) kaebuse, sest Facebook Ireland edastas oma kasutajate isikuandmeid Ameerika Ühendriikidesse ning säilitas neid selles riigis asuvates serverites, kus neid andmeid ka töödeldi. M. Schrems väitis, et Ameerika Ühendriikides kehtiv õigus ja valitsev praktika ei taga sellesse riiki edastatud isikuandmete piisavat kaitset ametiasutustepoolse jälgimise eest. Andmekaitsevolinik keeldus seda kaebust käsitlemast

⁴⁷ Seda kohtuotsust käsitleti 2003. aasta aastaaruandes, lk 67.

⁴⁸ Seda kohtuotsust käsitleti 2015. aasta aastaaruandes, lk 53.

eelkõige põhjusel, et komisjon oli oma otsuses 2000/520/EÜ⁴⁹ leidnud, et Ameerika Ühendriigid tagavad edastatud isikuandmete piisava kaitsetaseme nn Safe Harbouri⁵⁰ programmi raames.

Niisuguses kontekstis pöördus High Court (Iirimaa kõrge kohus) Euroopa Kohtu poole, paludes tõlgendada direktiivi 95/46/EÜ artikli 25 lõiget 6, mille järgi komisjon võib tuvastada, et kolmandas riigis on tagatud edastatud andmete kaitse piisav tase. See kohus palus ka sisuliselt hinnata, kas komisjoni otsus 2000/520, mille viimane võttis vastu direktiivi 95/46 artikli 25 lõike 6 alusel, on kehtiv.

Euroopa Kohus tunnistas komisjoni otsuse tervikuna kehtetuks, rõhutades esmalt, et niisuguse otsuse vastuvõtmiseks oleks komisjon pidanud jõudma nõuetekohaselt põhjendatud järeldusele, et asjasse puutuv kolmandas riigis on tegelikult tagatud põhiõiguste kaitse tase, mis on sisuliselt samaväärne liidu õiguskorras tagatuga. Komisjon ei jõudnud otsuses 2000/520 aga niisugusele järeldusele ja seega eirab otsuse artikkel 1 nõudeid, mis on ette nähtud direktiivi 95/46 artikli 25 lõikes 6 koostoimes hartaga, mistõttu on kõnealune otsus kehtetu. Safe Harbouri programmi põhimõtted on nimelt kohaldatavad ainult Ameerika Ühendriikide organisatsioonidele, kes on kinnituse andnud ja saavad isikuandmeid liidust, ilma et oleks nõutav, et Ameerika Ühendriikide ametiasutused oleksid kohustatud neid põhimõtteid järgima. Pealegi muudab otsus 2000/520/EÜ võimalikuks sekkumised nende isikute põhiõigustesse, kelle isikuandmed on edastatud või võidakse edastada liidust Ameerika Ühendriikidesse, sisaldamata järeldusi selle kohta, et Ameerika Ühendriikides kehtiks riigi tasandil õigusnormid, mille eesmärk oleks piirata võimalikke põhiõiguste riiveid, ja et sedalaadi sekkumiste vastu oleks olemas tõhus õiguslik kaitse (punktid 82, 87–89, 96–98 ja resolutsiooni punkt 2).

Lisaks tunnistas Euroopa Kohus otsuse 2000/520 artikli 3 kehtetuks, sest see jätab liikmesriigi järelevalveasutused ilma pädevusest, mis neil on tulenevalt direktiivi 95/46 artiklist 28, juhul kui isik toob esile asjaolud, mis võivad seada kahtluse alla selle, kas üksikisikute eraelu puutumatus ning põhiõiguste ja -vabaduste kaitsega on kooskõlas komisjoni otsus, milles on tuvastatud, et kolmas riik tagab kaitse piisava taseme (punktid 102–104). Euroopa Kohus otsustas, et otsuse 2000/520 artiklite 1 ja 3 kehtetus mõjutab kogu otsuse kehtivust (punktid 105 ja 106).

Mis puudutab võimatust niisugust riivet õigustada, siis märkis Euroopa Kohus esmalt, et liidu õigusakt, millega kaasneb sekkumine harta artiklitega 7 ja 8 tagatud põhiõigustesse, peab sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, mistõttu isikutel, kelle isikuandmed on asjasse puutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Niisuguste tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult (punkt 91).

Lisaks ja eelkõige nõuab eraelu puutumatus põhiõiguse kaitsmine liidu tasandil, et isikuandmete kaitse erandid ja piirangud piirduksid vältimatult vajalikuga (punkt 92). Vältimatult vajalikuga ei piirdu õigusakt, mis annab üldise loa säilitada kõikide selliste isikute kõik

⁴⁹ Komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium (EÜT 2000, L 215, lk 7; ELT eriväljaanne 16/01, lk 119).

⁵⁰ Safe Harbouri programm hõlmab tervet rida isikuandmete kaitse põhimõtteid, mille järgimise kohustuse võivad Ameerika Ühendriikide asutused endale vabatahtlikult võtta.

isikuandmed, kelle andmed on edastatud liidust, ilma et olenevalt taotletavast eesmärgist esineks eristamist, piiranguid või erandeid ning ilma et oleks ette nähtud objektiivset kriteeriumi, mis võimaldaks piiritleda ametiasutuste juurdepääsu andmetele ja nende hilisemat kasutamist konkreetsetel rangelt piiritletud eesmärkidel, millega nii andmete tutvumise kui ka kasutamisega kaasnev sekkumine võib olla põhjendatud (punkt 93). Täpsemalt tuleb õigusakti, mis võimaldab ametiasutustel elektroonilise side sisuga üldiselt tutvuda, pidada eraelu puutumatusse põhiõiguse põhisisu kahjustavaks. Samuti ei järgi õigusakt, milles ei ole andmesubjektile ette nähtud mingit võimalust kasutada õiguskaitselahendusi, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada, harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu (punktid 94 ja 95).

[26. juuli 2017. aasta arvamus 1/15 \(ELi ja Kanada vaheline PNR-leping\) \(suurkoda\) \(EU:C:2017:592\)](#)

Euroopa Kohus võttis 26. juulil 2017 esimest korda seisukoha rahvusvahelise lepingu projekti kooskõla kohta Euroopa Liidu põhiõiguste hartaga ja eelkõige sätetega, mis käsitlevad eraelu puutumatus ja isikuandmete kaitset.

Euroopa Liit ja Kanada saavutasid kokkuleppe broneeringuinfo edastamise ja töötlemise kohta (PNR-leping). Vastav leping allkirjastati 2014. aastal. Euroopa Liidu Nõukogu palus Euroopa Parlamendil lepingu heaks kiita, kuid viimane pöördus Euroopa Kohtu poole, et saada teada, kas kavandatud leping on liidu õigusega kooskõlas.

Kavandatud leping võimaldab Kanada ametiasutusele süstemaatiliselt ja pidevalt edastada kõikide lennureisijate broneeringuinfot, seda kasutada ja säilitada ning vajaduse korral edastada muudele ametiasutustele ja muudele kolmandatele riikidele, et võidelda terrorismi ja raskete rahvusvaheliste kuritegude vastu. Selleks on lepingus ette nähtud muu hulgas andmete säilitamine viie aasta jooksul ja see kehtestab erinõudeid broneeringuinfo turvalisuse ja tervikluse suhtes, näiteks delikaatsete andmete kohese peitmise kohustuse, nähes ette ka õiguse andmetega tutvuda, neid parandada ja kustutada ning võimaluse esitada vaideid või kaebusi.

Kavandatavas lepingus silmas peetud broneeringuinfo hõlmab muu hulgas lisaks lennureisija või lennureisijate nimele broneerimiseks vajalikku teavet, nagu kavandatud reisi kuupäevad ja reisiteekond; piletitega seotud teavet; teavet sama broneerimisnumbri all registreeritud isikute rühmade kohta; teavet maksevahendite või arve kohta; pagasiandmeid ning üldmärkusi reisijate kohta.

Euroopa Kohus asus antud arvamusel seisukohale, et PNR-lepingut ei saa olemasolevas vormis sõlmida, sest mitu selle lepingu sätet ei ole kooskõlas liidus kaitstavate põhiõigustega.

Euroopa Kohus tõdes esiteks, et nii broneeringuinfo edastamine liidust Kanada pädevale asutusele kui ka tingimuste raamistik, milles liit ja Kanada on kokku leppinud seoses info säilitamise, kasutamise ning võimaliku hilisema edastamisega teistele Kanada ametiasutustele, Europolile, Eurojustile, liikmesriikide õigus- või politseiasutustele või ka kolmandate riikide ametiasutustele, kujutavad endast harta artikliga 7 tagatud õiguse riiveid. Need toimingud riivavad ka harta artikliga 8 tagatud isikuandmete kaitse põhiõigust, kuna nende näol on tegemist isikuandmete töötlemisega (punktid 125 ja 126).

Euroopa Kohus toonitas samuti, et isegi kui teatud broneeringuinfo eraldi võetuna ei näi andvat olulist teavet andmesubjektide eraelu kohta, on selle info põhjal tervikuna siiski võimalik teada saada muu hulgas täielik reisiteekond, reisiharjumused, kahe või enama isiku vahelised suhted ning teave lennureisijate rahalise olukorra, toitumisharjumuste või tervisliku seisundi kohta ning neist võib isegi ilmneda reisijate delikaatseid andmeid, mis on määratletud kavandatava lepingu artikli 2 punktis e (andmed, mis paljastavad rassilise või etnilise päritolu, poliitilised vaated, usulised veendumused jne) (punkt 128).

Euroopa Kohus leidis, et kuigi riived võivad olla põhjendatud liidu üldist huvi pakkuva eesmärgiga (avaliku julgeoleku tagamine terroriaktide ja raskete rahvusvaheliste kuritegude vastu võitlemise raames), ei piirdu suur hulk selle lepingu sätetest vältimatult vajalikuga ega näe ette selgeid ja täpseid norme.

Täpsemalt märkis Euroopa Kohus, et arvestades ohtu, et andmete töötlemine võib toimuda vastuolus diskrimineerimiskeelu põhimõttega, nõuab delikaatsete andmete Kanadasse edastamine täpset ja eriti kindlat põhjendust, mis lähtub muudest põhjendustest kui avaliku julgeoleku kaitse terrorismi ja raskete rahvusvaheliste kuritegude eest. Kõnesoleval juhul niisugune põhjendus aga puudub. Euroopa Kohus järeltas, et delikaatsete andmete Kanadasse edastamist ja nende seal töötlemist ja säilitamist käsitlevad lepingusätted on põhiõigustega vastuolus (punktid 165 ja 232).

Teiseks leidis Euroopa Kohus, et kõigi lennureisijate broneeringuinfo säilitamine ja kasutamine pärast nende reisijate Kanadast lahkumist, mida kavandatav leping võimaldab, ei piirdu vältimatult vajalikuga. Mis puudutab lennureisijaid, kelle puhul terrorismi ja raskete rahvusvaheliste kuritegude ohtu ei tuvastatud nende Kanadasse saabumisest kuni sellest riigist lahkumiseni, siis ei näi nende broneeringuinfo ja kavandatava lepinguga taotletava eesmärgi vahel pärast nende lahkumist esinevat isegi mitte kaudset seost, mis põhjendaks selle info säilitamist. Kui aga konkreetsetel juhtudel on tuvastatud objektiivsed asjaolud, mis võimaldavad asuda seisukohale, et teatud lennureisijad võivad isegi pärast Kanadast lahkumist kujutada endast ohtu seoses terrorismi ja raskete rahvusvaheliste kuritegude vastu võitlemisega, on nende broneeringuinfo talletamine lubatav ka isegi viie aasta jooksul pärast nende viibimist kõnealusel riigis (punktid 205–207 ja 209).

Kolmandaks tõdes Euroopa Kohus, et Euroopa Liidu põhiõiguste harta artikliga 7 tagatud põhiõigus eraelu puutumatus eeldab, et andmesubjekt saab veenduda, et tema isikuandmeid töödeldakse õigesti ja seaduslikult. Vajaliku kontrolli tegemiseks peab sellel isikul olema õigus tutvuda teda käsitlevate andmetega, mida töödeldakse.

Sellega seoses rõhutas Euroopa Kohus, et kavandatava lepingu raames on oluline, et lennureisijaid teavitataks nende broneeringuinfo asjasse puutuvasse kolmandasse riiki edastamisest ja kasutamisest kohe, kui teavitamine ei saa enam kahjustada kavandatavas lepingus nimetatud ametiasutuste läbiviidavat uurimist. Niisugune teavitamine on vajalik nimelt selleks, et lennureisijad saaksid teostada oma õigust nõuda, et neil võimaldataks tutvuda neid käsitleva broneeringuinfo ja vajaduse korral seda infot parandataks, ning kasutada harta artikli 47 esimese lõigu alusel tõhusat õiguskaitsevahendit kohtus.

Olukordades, milles esinevad objektiivsed asjaolud, mis õigustavad broneeringuinfo kasutamist terrorismi ja raskete rahvusvaheliste kuritegude vastu võitlemiseks, ja mis tingivad vajaduse

kohtu või sõltumatu haldusasutuse eelneva loa järele, osutub seega vajalikuks lennureisijate isiklik teavitamine. Sama kehtib juhul, kui lennureisijate broneeringuinfot edastatakse teistele ametiasutustele või eraõiguslikele isikutele. Teavitamine tohib siiski toimuda alles siis, kui see ei saa enam kahjustada kavandatavas lepingus nimetatud ametiasutuste läbiviidavat uurimist (punktid 219, 220, 223 ja 224).

[16. juuli 2020. aasta kohtuotsus \(suurkoda\) Facebook Ireland ja Schrems \(C-311/18, ECLI:EU:C:2020:559\)⁵¹](#)

Isikuandmete kaitse üldmääruses on sätestatud, et isikuandmete edastamine kolmandatesse riikidesse võib toimuda ainult juhul, kui kõnealune kolmas riik tagab andmekaitse piisava taseme. Selle määruse kohaselt võib komisjon tuvastada, et kolmas riik tagab kaitse piisava taseme oma riigisisese õigusega või endale võetud rahvusvaheliste kohustustega⁵². Kaitse piisavuse otsuse puudumise korral võib niisugune edastamine toimuda üksnes siis, kui isikuandmete eksportija, kelle asukoht on liidus, näeb ette asjakohased kaitsemeetmed, mis võivad tuleneda eelkõige asjakohastest andmekaitse tüüptingimustest, mille on kehtestanud komisjon, ja kui andmesubjektide õigused on kohtulikult kaitstavad ja neil on olemas tõhusad õiguskaitsevahendid⁵³. Lisaks on üldmääruses täpselt ette nähtud tingimused, millel niisugune edastamine võib kaitse piisavuse otsuse või asjakohaste kaitsemeetmete puudumise korral toimuda⁵⁴.

Austria kodanik Maximilian Schrems on Facebooki kasutaja alates 2008. aastast. Nagu ka teiste liidus elavate kasutajate puhul edastab Facebook Ireland M. Schremsi isikuandmed kas täielikult või osaliselt Facebook Inc-i serveritesse, mis asuvad Ameerika Ühendriikide territooriumil, ja neid töödeldakse seal. M. Schrems esitas liri andmekaitsevolinikule kaebuse, milles ta sisuliselt palus, et viimane keelaks niisuguse edastamise. Ta väitis, et Ameerika Ühendriikides kehtiv õigus ja valitsev praktika ei taga sellesse riiki edastatavate isikuandmete piisavat kaitset sealsete avaliku võimu asutuste jälgimise eest. See kaebus jäeti rahuldamata eelkõige põhjendusega, et komisjon oli otsuses 2000/520⁵⁵ tõdenud, et Ameerika Ühendriigid tagavad kaitse piisava taseme. Euroopa Kohus tunnistas 6. oktoobri 2015. aasta otsusega, vastates High Courti (kõrge kohus, Iirimaa) eelotsusetaotlusele, selle otsuse kehtetuks (edaspidi „kohtuotsus Schrems I“)⁵⁶ (punktid 52 ja 53).

Pärast kohtuotsust Schrems I ja seejärel M. Schremsi kaebuse rahuldamata jätmise otsuse tühistamist liri kohtu poolt, palus liri andmekaitsevolinik M. Schremsil sõnastada oma kaebus ümber, arvestades, et Euroopa Kohus oli otsuse 2000/520 tühistanud. Ümbersõnastatud kaebuses jäi M. Schrems oma seisukoha juurde, et Ameerika Ühendriigid ei paku sinna edastatud andmete osas piisavat kaitset. M. Schrems palus peatada või keelata tulevikus tema isikuandmete edastamine liidust Ameerika Ühendriikidesse – edastamine, mida Facebook Ireland viib nüüdseks läbi otsuse 2010/87/EL⁵⁷ lisas olevate andmekaitse tüüptingimuste alusel.

⁵¹ Seda kohtuotsust käsitleti 2020. aasta aastaaruandes, lk-d 26–29.

⁵² Isikuandmete kaitse üldmääruse artikkel 45.

⁵³ Isikuandmete kaitse üldmääruse artikli 46 lõige 1 ja lõike 2 punkt c.

⁵⁴ Isikuandmete kaitse üldmääruse artikkel 49.

⁵⁵ Komisjoni 26. juuli 2000. aasta otsus vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium (EÜT 2000, L 215, lk 7; ELT eriväljaanne 16/01, lk 119).

⁵⁶ Euroopa Kohtu 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, [EU:C:2015:650](#) (vt ka pressiteade [nr 117/15](#)).

⁵⁷ Komisjoni 5. veebruari 2010. aasta otsus kolmandates riikides asuvatele volitatud töötlejatele isikuandmete edastamise lepingu tüüptingimuste kohta direktiivi 95/46/EÜ alusel (ELT 2010, L 39, lk 5), muudetud komisjoni 16. detsembri 2016. aasta rakendusotsusega (EL) 2016/2297 (ELT 2016, L 344, lk 100).

Kuna liri andmekaitsevoliniku hinnangul sõltus M. Schremsi kaebuse menetlemine eelkõige otsuse 2010/87 kehtivusest, pöördus liri andmekaitsevolinik High Courti poole, et viimane esitaks eelotsusetaotluse Euroopa Kohtule. Pärast selle menetluse algust võttis komisjon vastu otsuse (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield⁵⁸ (punktid 54, 55 ja 57).

Eelotsusetaotluse esitanud kohus esitab oma taotluses Euroopa Kohtule küsimuse üldmääruse kohaldatavuse kohta isikuandmete edastamise suhtes vastavalt otsuses 2010/87 ette nähtud kaitse tüüptingimustele; selle määrusega nõutud kaitsetaseme kohta niisuguse edastamise käigus ja järelevalveasutustel sellises kontekstis lasuvate kohustuste kohta. Lisaks tõstatab High Court küsimuse nii otsuse 2010/87 kui ka otsuse 2016/1250 kehtivusest.

Euroopa Kohus tõdes, et otsuse 2010/87 analüüsimisel Euroopa Liidu põhiõiguste harta (edaspidi „harta“) alusel ei ilmnenud asjaolusid, mis mõjutaksid selle otsuse kehtivust. Otsuse 2016/1250 tunnistas Euroopa Kohus seevastu kehtetuks (resolutsiooni punktid 4 ja 5).

Esmalt märkis Euroopa Kohus, et liidu õigus ja eelkõige üldmäärus on kohaldatavad olukorras, kus liikmesriigis asuv äriühing edastab äriisel eesmärgil isikuandmeid kolmandas riigis asuval teisele äriühingule, olenemata asjaolust, et edastamise käigus või järel võivad kõnealuseid andmeid töödelda asjaomase kolmanda riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeolekuga seotud eesmärkidel. Euroopa Kohus täpsustas, et selline edastamine ei tohiks isikuandmete kaitse üldmääruse kohaldamisalast välja jääda põhjusel, et kolmanda riigi ametiasutused andmeid selliselt töötlevad (punktid 86, 88, 89 ja resolutsiooni punkt 1).

Edastamise raames nõutud kaitsetasemega seoses otsustas Euroopa Kohus, et üldmääruse sätetes ette nähtud sellekohaseid nõudeid, mis puudutavad asjakohaseid kaitsemeetmeid, kohtulikult kaitstavaid õigusi ja tõhusaid õiguskaitsevahendeid, tuleb tõlgendada nii, et andmesubjektidele, kelle isikuandmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel, tuleb tagada õiguste kaitse, mille tase on sisuliselt samaväärne sellega, mis on liidus tagatud vastavalt üldmäärusele, tõlgendatuna lähtuvalt hartast. Euroopa Kohus täpsustas niisuguses kontekstis, et selleks et hinnata sellise edastamise korral tagatud kaitse taset, tuleb arvesse võtta nii liidus asuva andmete eksportija ja kolmandas riigis asuva isikuandmete vastuvõtja vahel kokku lepitud lepingutingimusi kui ka – osas, mis puudutab selle riigi ametiasutuste võimalust nõnda edastatavatele isikuandmetele juurde pääseda – kolmanda riigi õigussüsteemiga seotud asjakohast teavet (punkt 105 ja resolutsiooni punkt 2).

Seoses järelevalveasutustel niisuguse edastamise kontekstis lasuvate kohustustega otsustas Euroopa Kohus, et kui puudub Euroopa Komisjoni vastu võetud kehtiv kaitse piisavuse otsus, peab pädev järelevalveasutus muu hulgas peatama või keelama andmete edastamise kolmandasse riiki, kui ta kõiki edastamise asjaolusid arvestades leiab, et selles kolmandas riigis andmete edastamise tüüptingimusi ei järgita või ei saa järgida ja et liidu õiguse järgi nõutavat edastatavate andmete kaitset ei ole võimalik tagada muude meetmete abil ning liidus asuv vastutav töötaja või tema volitatud töötaja ei ole ise andmete edastamist peatanud või lõpetanud (punkt 121 ja resolutsiooni punkt 3).

Seejärel käsitles Euroopa Kohus otsuse 2010/87 kehtivust. Euroopa Kohtu hinnangul ei saa

⁵⁸ Komisjoni 12. juuli 2016. aasta rakendusotsus isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT 2016, L 207, lk 1).

üksnes asjaolu, et komisjoni otsuses sisalduvad andmekaitse tüüptingimused ei ole oma lepingulise laadi tõttu siduvad sellise kolmanda riigi ametisutustele, kuhu isikuandmeid võidakse edastada, mõjutada selle otsuse kehtivust. Euroopa Kohus täpsustas, et küll aga sõltub selle otsuse kehtivus küsimusest, kas see otsus sisaldab tõhusaid mehhanisme, mis praktikas võimaldavad tagada, et järgitakse liidu õigusega nõutava kaitse taset ja et selliste tingimuste alusel toimuv isikuandmete edastamine peatatakse või keelatakse juhul, kui neid tingimusi rikutakse või kui neid ei ole võimalik täita. Euroopa Kohus tõdes, et otsusega 2010/87 sätestatakse sellised mehhanismid. Ta toonitas sellega seoses muu hulgas, et selle otsusega kehtestatakse andmete eksportijale ja andmete vastuvõtjale kohustus enne kontrollida, kas asjaomasel kolmandas riigis on tagatud liidu õigusega nõutav kaitsetase ning juhul, kui andmete vastuvõtjal võib osutuda võimatuks neid tüüptingimusi täita, kohustus sellest teatada vastutavale töötlejale, kelle ülesanne on seepeale andmete edastamine peatada ja/või vastuvõtjaga sõlmitud leping üles öelda (punktid 132, 136, 137, 142, 148 ja resolutsiooni punkt 4).

Viimaks analüüsis Euroopa Kohus ka otsuse 2016/1250 kehtivust üldmäärusest tulenevate nõuete kontekstis, arvestades harta sätteid, mis tagavad õiguse era- ja perekonnaelu austamisele, isikuandmete kaitse ja õiguse tõhusale õiguskaitsevahendile. Euroopa Kohus tõdes selle kohta, et nimetatud otsuses on sama moodi nagu otsuses 2000/520 ette nähtud riikliku julgeoleku, avaliku huvi või USA õigusnormide järgimise vajaduste esimus kõnealuste põhimõtete ees, muutes võimalikuks nende isikute põhiõiguste riived, kelle andmed kõnealusesse kolmandasse riiki edastatakse. Euroopa Kohtu hinnangul ei ole isikuandmete kaitse piirangud, mis tulenevad USA riigisisestest õigusnormidest, mis reguleerivad USA avaliku võimu asutuste õigust pääseda juurde liidust USAsse edastatavatele isikuandmetele ja neid andmeid kasutada, ning millele komisjon otsuses 2016/1250 hinnangu andis, piiritletud viisil, mis vastaks liidu õiguses proportsionaalsuse põhimõttest tulenevatele nõuetele, mistõttu ei saa asuda seisukohale, et nendel sätetel põhinevad jälgimisprogrammid piirduvad rangelt vajalikuga. Euroopa Kohus tõdes selles otsuses sisalduvatele tõdemustele tuginedes, et teatavate jälgimisprogrammide osas ei saa neist normidest mingil viisil tuletada piiranguid selles ette nähtud volitusele programme rakendada, nagu ka mitte kaitsemeetmeid USA-välisele isikutele, kes on nende programmide potentsiaalseks sihtmärgiks. Euroopa Kohus lisas, et kuigi samad normid näevad ette nõuded, mida USA ametiasutused peavad asjasse puutuvate jälgimisprogrammide rakendamisel järgima, ei anna need normid andmesubjektidele õigusi, millele saaks USA ametiasutuste vastu kohtus tugineda (punktid 164, 165, 180–182, 184 ja 185).

Seoses kohtuliku kaitse nõudega otsustas Euroopa Kohus, et vastupidi sellele, mida komisjon leidis otsuses 2016/1250, ei anna selles otsuses käsitletud ombudsmani mehhanism andmesubjektidele õiguskaitsevahendit sellises organis, kes pakub liidu õiguses ette nähtutega sisuliselt samaväärseid kaitsemeetmeid, mis tagaks nii mehhanismi järgi ette nähtud ombudsmani sõltumatuse kui ka niisuguste normide olemasolu, mis volitavad nimetatud ombudsmani võtma vastu otsuseid, mis on USA luureametkondadele siduvad. Neil põhjustel tunnistas Euroopa Kohus otsuse 2016/1250 kehtetuks (punktid 195–197, 201 ja resolutsiooni punkt 5).

V. Isikuandmete kaitse internetis

1. Õigus esitada isikuandmete töötlemisele vastuväiteid („õigus olla unustatud“)

[13. mai 2014. aasta kohtuotsus \(suurkoda\) Google Spain ja Google \(C-131/12, EU:C:2014:317\)](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete kaitse““) täpsustas Euroopa Kohus seda, millise ulatusega on direktiivis 95/46/EÜ ette nähtud õigus andmetega tutvuda ja õigus esitada vastuväiteid isikuandmete töötlemisele internetis.

Internetis toimiva otsingumootori haldaja vastutuse ulatuse üle otsustades asus Euroopa Kohus sisuliselt seisukohale, et selleks, et direktiivi 95/46 artikli 12 punktis b ja artikli 14 esimese lõigu punktis a ette nähtud õigus andmetega tutvuda ja õigus esitada vastuväiteid oleks tagatud, on otsingumootori haldaja, kui neis artiklites sätestatud tingimused on täidetud, teatud tingimustel kohustatud kõrvaldama isiku nime põhjal tehtud otsingu järel kuvatavast tulemuste loetelust lingid veebilehtedele, mille on avaldanud kolmandad isikud ja mis sisaldavad teavet selle isiku kohta. Euroopa Kohus täpsustas, et selline kohustus võib esineda ka juhul, kui seda nime või teavet ei ole varem või samal ajal neilt veebilehtedelt kustutatud, isegi kui selle nime või teabe avaldamine neil veebilehtedel on seaduslik (punkt 88 ja resolutsiooni punkt 3).

Käsitledes küsimust, kas direktiiv võimaldab andmesubjektil nõuda, et niisugusest tulemuste loetelust kõrvaldataks lingid veebilehtedele, sest ta soovib, et tema kohta seal sisalduv teave teatud aja möödudes „unustataks“, siis märkis Euroopa Kohus esmalt, et isegi alguses seaduslik täpsete andmete töötlemine võib aja möödudes sattuda direktiiviga vastuollu, kui neid andmeid ei ole enam vaja eesmärkidel, milleks neid koguti või töödeldi. Nii on see eelkõige juhul, kui need andmed ei ole adekvaatsed, ei ole või enam ei ole asjakohased või kui andmed on neid eesmärke ja möödunud aega arvestades liiased (punkt 93). Järelikult juhul, kui andmesubjekti avalduse kohta tõdetakse, et linkide lisamine loetellu on praeguses olukorras direktiiviga vastuolus, tuleb see teave ja vastavad lingid kustutada (punkt 94). Selleks, et tunnustada andmesubjekti õigust nõuda, et tema isiku kohta käiv teave ei oleks käesoleval ajal enam tema nimega seostatav tulemuste loetelu kaudu, ei ole niisuguses kontekstis vajalik, et kõnesoleva teabe lisamine tulemuste loetellu tekitaks andmesubjektile kahju (punkt 96 ja resolutsiooni punkt 4).

Lõpuks täpsustas Euroopa Kohus, et kuna andmesubjekt võib harta artiklitest 7 ja 8 tulenevaid õigusi arvesse võttes nõuda, et kõnesolevat teavet ei tehtaks enam laiale üldsusele kättesaadavaks selle teabe lisamisega tulemuste loetellu, siis kaaluvad need õigused üldjuhul üles mitte üksnes otsingumootori haldaja majandushuvi, vaid ka üldsuse huvi vastava isiku nime põhjal tehtud otsinguga seda teavet leida. See ei kehti aga juhul, kui konkreetsetel põhjustel, näiteks isiku rolli tõttu avalikus elus, õigustab tema põhiõiguste riivet ülekaalukas avalik huvi pääseda niisuguse loetellu lisamisega kõnesolevale teabele ligi (punkt 97 ja resolutsiooni punkt 4).

2. Isikuandmete töötlemine ja intellektuaalomandi õigused

[29. jaanuari 2008. aasta kohtuotsus \(suurkoda\) Promusicae \(C-275/06, EU:C:2008:54\)](#)⁵⁹

Promusicae, helisalvestiste ja audiovisuaalsete salvestiste produtsente ja väljaandjaid ühendav Hispaania mittetulundusühing, pöördus Hispaania kohtute poole, et viimased kohustaksid Telefónica de España SAUd (äriühing, kelle tegevuse hulka kuulub muu hulgas internetiühenduse teenuste pakkumine), et see äriühing avaldaks teatavate isikute nimed ja füüsilised aadressid, kellele Telefónica osutab internetiühenduse teenust ja kelle „IP-aadress“ ning ühenduse kuupäev ja kellaaeg olid teada. Promusicae väidete kohaselt kasutasid kõnealused isikud failivahetusprogrammi (nn *peer-to-peer*-programm või „P2P“) (läbipaistev, sõltumatu, detsentraliseeritud ning kõrgetasemelise otsingu- ja allalaadimisfunktsiooniga varustatud võrdõigusvõrk) ja võimaldasid oma personaalarvuti ühiskasutatavate failide kaudu juurdepääsu fonogrammidele, mille varalised kasutusõigused kuulusid Promusicae liikmetele. Mittetulundusühing taotles talle eespool mainitud teabe edastamist, et ta saaks asjaomaste isikute vastu algatada tsiviilmenetluse.

Neil asjaoludel palus Juzgado de lo Mercantil no 5 de Madrid (Madridi 5. kaubanduskohus, Hispaania) Euroopa Kohtul selgitada, kas Euroopa õigusnormidest tulenevalt peavad liikmesriigid kehtestama kohustuse edastada tsiviilmenetluse raames autoriõiguse tõhusa kaitse tagamiseks isikuandmeid.

Euroopa Kohtu sõnul tõstatas käesolev eelotsusetaotlus küsimuse, kuidas saavutada vajalik kooskõla nõuete vahel, mis puudutavad selliste erinevate põhiõiguste kaitset nagu ühelt poolt õigus eraelu puutumatusele ja teiselt poolt õigus omandiõiguse kaitsele ning õigus tõhusale õiguskaitsevahendile.

Euroopa Kohus järeldas, et direktiivid 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta), 2001/29/EÜ⁶⁰ autoriõiguse ja sellega kaasnevate õiguste teatavate aspektide ühtlustamise kohta infoühiskonnas, 2004/48/EÜ⁶¹ intellektuaalomandi õiguste jõustamise kohta ja 2002/58⁶², milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), ei nõua, et liikmesriigid kehtestaksid põhikohtuasjaga sarnases olukorras kohustuse edastada tsiviilmenetluse raames autoriõiguse tõhusa kaitse tagamiseks isikuandmeid. Liidu õiguse kohaselt peavad liikmesriigid siiski nende direktiivide ülevõtmisel jälgima, et nad tugineksid asjaomaste direktiivide sellisele tõlgendusele, mis võimaldab tagada tasakaalu erinevate ühenduse õiguskorras kaitstud põhiõiguste vahel. Liikmesriikide ametiasutused ja kohtud ei pea nende direktiivide ülevõtmismeetmete rakendamisel mitte ainult tõlgendama oma riigisisest õigust kooskõlas asjaomaste direktiividega, vaid nad peavad ka jälgima, et nad ei tugineks asjaomaste direktiivide sellisele tõlgendusele, mis on vastuolus viidatud põhiõigustega või

⁵⁹ Seda kohtuotsust käsitleti 2008. aasta aastaaruandes, lk 46.

⁶⁰ Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT 2000, L 178, lk 1; ELT eriväljaanne 13/25, lk 399).

⁶¹ Euroopa Parlamendi ja nõukogu 22. mai 2001. aasta direktiiv 2001/29/EÜ autoriõiguse ja sellega kaasnevate õiguste teatavate aspektide ühtlustamise kohta infoühiskonnas (EÜT 2001, L 167, lk 10; ELT eriväljaanne 17/01, lk 230).

⁶² Euroopa Parlamendi ja nõukogu 29. aprilli 2004. aasta direktiiv 2004/48/EÜ intellektuaalomandi õiguste jõustamise kohta (ELT 2004, L 157, lk 45; parandus ELT L 195, lk 16, ei kehti eestikeelse teksti kohta; ELT eriväljaanne 17/02, lk 32).

muude ühenduse õiguse üldpõhimõtetega, näiteks proportsionaalsuse põhimõttega (punkt 70 ja resolutsioon).

[24. novembri 2011. aasta kohtuotsus Scarlet Extended \(C-70/10, EU:C:2011:771\)](#)⁶³

Muusikateoste autoreid, heliloojaid ja kirjastajaid esindav Belgia organisatsioon SCRL (SABAM) tuvastas, et võrdõigusvõrgu abil laadivad internetiühenduse pakkuja Scarlet Extended SA (edaspidi „Scarlet“) teenust kasutavad internetikasutajad internetist ilma loata ja autoritasu maksmata alla SABAMi kataloogi kuuluvaid teoseid. SABAM pöördus riigisisese kohtusse ja saavutas esimeses kohtuastmes selle, et kohus tegi Scarletile ettekirjutuse lõpetada autoriõiguste rikkumised, muutes oma klientidele võimatuks võrdõigusvõrgu tarkvara abil mis tahes moel saata või vastu võtta SABAMi kataloogi kuuluvaid muusikateost sisaldavaid faile.

Scarlet pöördus cour d'appel de Bruxelles'i (Brüsseli apellatsioonikohus, Belgia), kes peatas kohtuasjas menetluse, paludes Euroopa Kohtul eelotsusemenetluses selgitada, kas niisugune ettekirjutus on liidu õigusega kooskõlas.

Euroopa Kohus otsustas, et direktiive 95/46, 2000/31, 2001/29, 2002/58 ja 2004/48 koosmõjus ning arvestades kohaldatavatest põhiõigustest tulenevaid nõudeid tuleb tõlgendada nii, et nendega on vastuolus Scarletile adresseeritud kohtu ettekirjutus rakendada sellist filtreerimissüsteemi, mis filtreerib kogu tema teenuse raames ja eelkõige võrdõigusvõrgu tarkvara abil toimuva elektroonilise side; mida kohaldatakse vahet tegemata kõigile tema klientidele; mis on ennetav; mida rakendatakse ainult tema kulul ja mis ei ole ajaliselt piiratud ning mis on selleks, et blokeerida autoriõigust rikkuvate failide edastamine, võimeline tuvastama selle teenusepakkuja võrgus selliste failide vahetuse, mis sisaldavad muusika-, kinematograafilisi või audiovisuaalteoseid, mille intellektuaalomandi õigusi ettekirjutuse nõude esitaja väidab omavat (punkt 54 ja resolutsioon).

Euroopa Kohtu hinnangul ei ole niisugune ettekirjutus kooskõlas direktiivi 2000/31 artikli 15 lõikes 1 sätestatud keeluga kehtestada internetiühenduse pakkujale üldine jälgimiskohustus ega nõudega tagada õiglane tasakaal ühelt poolt intellektuaalomandi õiguse ja teiselt poolt ettevõtlusvabaduse, isikuandmete kaitse õiguse ja õiguse saada ja edastada teavet vahel (punktid 40 ja 49).

Niisuguses kontekstis märkis Euroopa Kohus esiteks, et kohtu ettekirjutus rakendada vaidluselust filtreerimissüsteemi tähendab, et kogu edastatavat sisu tuleb analüüsida süstemaatiliselt ning koguda ja identifitseerida tuleb selles võrgus toimuva õigusvastase sisu edastuse allikaks olevate kasutajate IP-aadressid, mis on kaitstud isikuandmed, sest nende identifitseerimine võimaldab selliste kasutajate täpse tuvastamise (punkt 51). Teiseks on oht, et selline kohtu ettekirjutus rikub teabevabadust, kuna on tõenäoline, et see süsteem ei erista piisaval määral õigusvastast sisu õiguspärasest, mistõttu süsteemi rakendamine võib tingida õiguspärase sisuga side blokeerimise. Vaidlust polegi selle üle, et vastus küsimusele edastuse õiguspärasuse kohta sõltub samuti autoriõiguses ette nähtud seaduslikest eranditest, mis on liikmesriigiti erinevad. Lisaks sellele võivad teatavad teosed teatavates liikmesriikides olla vabalt kasutatavad või autorid võivad olla teinud need võrgus tasuta kättesaadavaks (punkt 52).

⁶³ Seda kohtuotsust käsitleti 2011. aasta aastaaruandes, lk 37.

Euroopa Kohus tuvastas eelnevast tulenevalt, et kui liikmesriigi kohus kohustas oma ettekirjutusega Scarletit rakendama vaidlusalust filtreerimissüsteemi, on see liikmesriigi kohus jätnud täitmata nõude tagada õiglane tasakaal ühelt poolt intellektuaalomandi õiguse ja teiselt poolt ettevõtlusvabaduse, isikuandmete kaitse õiguse ja õiguse saada ja edastada teavet vahel (punkt 53).

[19. aprilli 2012. aasta kohtuotsus Bonnier Audio jt \(C-461/10, EU:C:2012:219\)](#)

Högsta domstolen (Rootsi kõrgeim kohus) pöördus eelotsusetaotlusega Euroopa Kohtu poole, paludes tõlgendada direktiive 2002/58/EÜ ja 2004/48/EÜ kohtuvaidluses ühelt poolt Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB ja Storyside AB (edaspidi koos „Bonnier Audio jt“) ning teiselt poolt Perfect Communication Sweden AB (edaspidi „ePhone“) vahel. Kohtuvaidlus puudutas viimase vastuväidet Bonnier Audio jt nõudele teha ettekirjutus andmete avaldamiseks.

Bonnier Audio jt on kirjastamisega tegelevad äriühingud, kellele kuuluvad muu hulgas ainuõigused 27 kuulderaamatu vormis esitatud teose reprodutseerimiseks, väljaandmiseks ja üldsusele kättesaadavaks tegemiseks. Bonnier Audio jt hinnangul oli nende ainuõigusi rikutud, kuna kõnealust 27 teost on ilma nende nõusolekuta üldsusele edastatud FTP („file transfer protocol“) serveri kaudu, mis võimaldab internetti ühendatud arvutite vahel faile vahetada ja andmeid edastada. Seetõttu pöördusid nad Rootsi kohtute poole taotlusega teha ettekirjutus avaldada selle isiku nimi ja aadress, kes kasutas IP-aadressi, kust kõnealused failid eeldatavalt edastati.

Niisuguses kontekstis pöördus Högsta domstolen, kes lahendas kassatsioonkaebust, Euroopa Kohtu poole küsimusega, kas liidu õigusega on vastuolus niisuguse riigisisese õigusnormi kohaldamine, mis on kehtestatud direktiivi 2004/48 artikli 8 alusel ja mis lubab tsiviilmenetluses abonendi kindlakstegemise eesmärgil kohustada internetiteenuste osutajat avaldama autoriõiguse omanikule või tema volitatud isikule selle abonendi andmed, kellele on antud IP-aadress, mida väidetavalt on kasutatud nimetatud õiguse kahjustamisel. Selleks eeldati esiteks, et ettekirjutuse taotleja on esitanud veenvad tõendid autoriõiguse kahjustamise kohta, ning teiseks, et taotletav meede on proportsionaalne.

Euroopa Kohus tuletas esmalt meelde, et direktiivi 2004/48 artikli 8 lõige 3 koostoimes direktiivi 2002/58 artikli 15 lõikega 1 ei välista liikmesriikide võimalust kehtestada kohustus edastada isikuandmeid eraõiguslikele isikutele, et võimaldada tsiviilasju lahendavas kohtus algatada menetlus autoriõiguse kahjustamise suhtes, kuid samas ei kohusta see säte ka liikmesriike niisugust kohustust ette nägema. Liikmesriikide ametiasutuste ja kohtute ülesanne ei ole siiski mitte ainult tõlgendada oma riigisisest õigust kooskõlas nende direktiividega, vaid ka jälgida, et nad ei tugineks asjaomaste direktiivide sellisele tõlgendusele, mis on vastuolus kõnealuste põhiõigustega või muude liidu õiguse üldpõhimõtetega, näiteks proportsionaalsuse põhimõttega (punktid 55 ja 56).

Euroopa Kohus märkis, et kõnealused riigisisemed õigusnormid nõuavad eelkõige, et selleks, et saaks teha asjaomaste andmete avaldamise ettekirjutuse, peavad esinema veenvad tõendid teosest tuleneva intellektuaalomandiõiguse kahjustamise kohta; nõutud teave peab hõlbustama sellise õiguse rikkumise või kahjustamise uurimist ning ettekirjutuse põhjendused peavad

kaaluma üles ebamugavuse või muu kahju, mille ettekirjutus võib selle adressaadile põhjustada, või mis tahes muu sellele vastupidise huvi (punkt 58).

Eeltoodust tulenevalt otsustas Euroopa Kohus, et direktiividega 2002/58 ja 2004/48 ei ole vastuolus niisugused riigisisised õigusnormid, nagu on kõne all põhikohtuasjas, kuna need õigusnormid võimaldavad liikmesriigi kohtul, kellele selleks õigustatud isik on esitanud taotluse teha isikuandmete avaldamise ettekirjutus, iga juhtumi asjaolude põhjal ja proportsionaalsuse põhimõttest tulenevaid nõudeid korrakohaselt arvesse võttes kaaluda asjas esinevaid vastandlikke huvisid (punkt 61 ja resolutsioon).

[17. juuni 2021. aasta kohtuotsus M.I.C.M. \(C-597/19, EU:C:2021:492\)](#)

Äriühing Mircom International Content Management & Consulting (M.I.C.M.) Limited (edaspidi „Mircom“) esitas Ondernemingsrechtbank Antwerpenile (Antwerpeni kaubanduskohus, Belgia; edaspidi „eelotsusetaotluse esitanud kohus“) internetiühenduse teenuseid pakkuva äriühingu Telenet BVBA vastu hagi teabe esitamise nõudes. Nimetatud haviga sooviti sellise otsuse tegemist, millega kohustatakse Teleneti esitama oma klientide identifitseerimisandmed IP-aadresside põhjal, mille teatav spetsialiseerunud ettevõtja oli Mircomi nimel kogunud. Teleneti klientide internetiühendust on kasutatud Mircomi kataloogis olevate filmide jagamiseks partnervõrgus (*peer-to-peer*) BitTorrent-protokolli abil. Telenet vaidles Mircomi hagile vastu.

Selles kontekstis küsis eelotsusetaotluse esitanud kohus Euroopa Kohtult kõigepealt, kas kaitstud teost sisaldava digifaili segmentide jagamine selles võrgus on üldsusele edastamine liidu õiguse tähenduses. Seejärel palus ta selgitada, kas intellektuaalomandi õiguste omaja, nagu Mircom, kes neid õigusi ise ei kasuta, vaid nõuab eeldatavalt rikkujatelt kahjuhüvitise sisse, võib õiguste jõustamiseks näiteks teabenõude esitamise kaudu tugineda liidu õiguses ette nähtud meetmetele, menetlustele ja õiguskaitsevahenditele. Lõpetuseks palus eelotsusetaotluse esitanud kohus Euroopa Kohtul selgitada, kas seaduslik on esiteks viis, kuidas Mircom on klientide IP-aadresse kogunud, ja teiseks andmete edastamine, mida Mircom on Telenetilt palunud.

Euroopa Kohus otsustas, et liidu õigusega⁶⁴ ei ole põhimõtteliselt vastuolus ei intellektuaalomandi õiguste omaja ja kolmanda isiku poolt selle õiguste omaja nimel partnervõrgu (*peer-to-peer*) nende kasutajate IP-aadresside süstemaatiline salvestamine, kelle internetiühendust on väidetavalt kasutatud autoriõigusi rikkuvateks tegevusteks (andmete eelnev töötlemine), ega nende kasutajate nimede ja aadresside edastamine kahjuhüvitise nõudmiseks vastavate õiguste omajale või kolmandale isikule (andmete hilisem töötlemine). Siiski peavad vastavad algatused ja nõuded olema põhjendatud, proportsionaalsed ega tohi olla kuritarvituslikud ning nende õiguslik alus peab olema riigisisene seadusandlik meede, millega piiratakse liidu õigusest tulenevate õiguste ja kohustuste ulatust. Euroopa Kohus täpsustas, et liidu õigus ei kohusta äriühingut, nagu Telenet, edastama eraõiguslikele isikutele isikuandmeid, et võimaldada esitada tsiviilkohtusse nõuet autoriõiguse rikkumisega seotud hagis. Liidu õigus lubab aga liikmesriikidel sellise kohustuse ette näha (punktid 97, 125–127 ja resolutsiooni punkt 3).

⁶⁴ Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f ja direktiivi 2002/58 artikli 15 lõige 1.

3. Isikuandmetele suunavate linkide eemaldamine

[24. septembri 2019. aasta kohtuotsus \(suurkoda\) GC jt \(delikaatsetele andmetele viitavate linkide eemaldamine\) \(C-136/17, ECLI:EU:C:2019:773\)⁶⁵](#)

Selles kohtuotsuses täpsustas suurkojana kokku tulnud Euroopa Kohus otsingumootori haldaja kohustusi delikaatsetele andmetele suunava lingi eemaldamise taotluse kontekstis.

Google keeldus rahuldamast nelja isiku taotlust eemaldada mitmesugused lingid tulemuste loetelust, mis kuvatakse otsingumootoris nende isikute nimedega tehtud otsingu tagajärjel ja mis viivad kolmandate isikute avaldatud veebilehtedele, muu hulgas meediaväljaannetes avaldatud artiklitele. Need neli isikut esitasid kaebuse Commission nationale de l'informatique et des libertés'le (riiklik andmetöötluse ja vabaduste komisjon, CNIL, Prantsusmaa), kes keeldus tegemast Google'ile ettekirjutust lingid taotlusele vastavalt eemaldada. Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu), kel tuli kohtuasi lahendada, palus Euroopa Kohtul täpsustada kohustusi, mis direktiivi 95/46 järgi lasuvad otsingumootori haldajal linkide eemaldamise taotlust menetledes.

Esimesena tuletas Euroopa Kohus meelde, et on keelatud töödelda isikuandmeid, mis paljastavad rassilise või etnilise päritolu, poliitilised vaated, usulised või filosoofilised veendumused, ametiühingusse kuulumise, ning isikuandmeid, mis käsitlevad tervislikku seisundit või seksuaalelu, kui sellest keelust ette nähtud eranditest ja piirangutest ei tulene teisiti⁶⁶. Mis puudutab süütegude, süüdimõistvate kohtuotsuste ja turvameetmetega seotud andmeid, siis võib neid töödelda ainult ametivõimude kontrolli all või juhul, kui riigisiseses õiguses on ette nähtud sobivad spetsiifilised tagatised⁶⁷ (punktid 39 ja 40).

Euroopa Kohus otsustas, et nimetatud eriliiki andmete töötlemisega seotud keeld ja piirangud on otsingumootori haldaja suhtes kohaldatavad samamoodi nagu mis tahes muu vastutava isikuandmete töötleja suhtes. Nende keeldude ja piirangute eesmärk on nimelt tagada tugevam kaitse sellise töötlemise eest, mis nende andmete erilise tundlikkuse tõttu võib kujutada endast eriti rasket sekkumist põhiõigusesse eraelu puutumatusse ja põhiõigusesse isikuandmete kaitsele (punktid 42–44).

Otsingumootori haldaja ei vastuta siiski mitte seetõttu, et isikuandmed sisalduvad kolmanda isiku poolt avaldatud veebilehel, vaid selle lehe otsingutulemustes sisaldumise eest. Neil asjaoludel saavad delikaatsete andmete töötlemisega seotud keeld ja piirangud kehtida haldaja suhtes üksnes lingi otsingutulemustes sisaldumise tõttu ja olla seega kohaldatavad kontrollimise

⁶⁵ Seda kohtuotsust käsitleti 2019. aasta aastaaruandes, lk 117 ja 118.

⁶⁶ Direktiivi 95/46 artikli 8 lõige 1 ja määruse 2016/679 artikli 9 lõige 1.

⁶⁷ Direktiivi 95/46 artikli 8 lõige 5 ja määruse 2016/679 artikkel 10.

kaudu, mis toimub pädevate riigisest ametivõimude kontrolli all taotluse alusel, mille andmesubjekt on esitanud (punktid 46 ja 47).

Teisena sedastas Euroopa Kohus, et kui otsingumootori haldajale on esitatud taotlus eemaldada link delikaatsetele andmetele, siis on ta põhimõtteliselt, kui teatud erandid välja arvata, kohustatud sellise taotluse rahuldama. Mis puudutab erandeid, siis võib haldaja keelduda taotlust rahuldamast muu hulgas siis, kui ta tuvastab, et lingid viivad andmeteni, mille andmesubjekt on ilmselgelt ise avalikustanud, ent tingimusel, et selliste linkide olemasolu vastab kõigile muudele isikuandmete töötlemise õiguspärasuse tingimustele⁶⁸, ja eeldusel, et andmesubjektil ei ole õigust esitada töötlemisele vastuväiteid tema konkreetse olukorraga seotud olulistel õiguspärasel põhjustel⁶⁹ (punktid 65 ja 69).

Igal juhul peab otsingumootori haldaja juhul, kui talle on esitatud taotlus linkide eemaldamiseks, kontrollima, kas kõnealuse delikaatseid andmeid sisaldava veebilehe lingi sisaldumine loetelus, mis kuvatakse andmesubjekti nimega tehtud otsingu tagajärjel, on vältimatult vajalik selleks, et internetikasutajad, kes võivad olla huvitatud sellise otsingu kaudu sellele veebilehele pääsemisest, saaksid teostada õigust teabevabadusele. Selle kohta rõhutas Euroopa Kohus, et kuigi põhiõigus eraelu puutumatusse ja põhiõigus isikuandmete kaitsele kaaluvad internetikasutajate teabevabaduse üldjuhul üles, võib see tasakaal konkreetsetel juhtudel siiski sõltuda kõnesoleva teabe laadist ja delikaatsusest andmesubjekti eraelu seisukohast ning üldsuse huvist seda teavet saada, mis omakorda võib varieeruda muu hulgas olenevalt sellest, milline on selle andmesubjekti roll avalikus elus (punktid 66 ja 68).

Kolmandana otsustas Euroopa Kohus, et lahendades taotlust eemaldada lingid, mis viivad veebilehtedele, millel on avaldatud andmesubjekti suhtes kriminaalasjas toimunud kohtumenetluse andmed, mis puudutavad selle menetluse varasemat etappi ega vasta enam hetkeolukorrale, peab otsingumootori haldaja hindama, kas pidades silmas kõiki juhtumi asjaolusid, on andmesubjektil õigus sellele, et kõnealused andmed ei oleks praeguses etapis enam seotud tema nimega tulemuste loetelus, mis kuvatakse selle nimega tehtud otsingu tagajärjel. Kui see aga ei ole nii asjaolu tõttu, et kõnealuse lingi sisaldumine tulemuste loetelus on tingimata vajalik, et ühitada andmesubjekti õigust eraelu puutumatusse ja andmekaitsele potentsiaalselt huvitatud internetikasutajate teabevabadusega, on haldaja igal juhul kohustatud hiljemalt siis, kui ta saab taotluse linkide eemaldamiseks, koostama tulemuste loetelu nii, et sellest internetikasutajale jääv üldpilt kajastaks kohtumenetluse praegust olukorda, ning see nõuab eelkõige, et lingid veebilehtedele, mis sisaldavad selleteemalisi andmeid, oleksid esitatud loetelu eesotsas (punktid 77 ja 78).

[24. septembri 2019. aasta kohtuotsus \(suurkoda\) Google \(territoriaalne ulatus, mis on õigusel linkide eemaldamisele\) \(C-507/17, ECLI:EU:C:2019:772\)](#)⁷⁰

Commission nationale de l'informatique et des libertés (riiklik andmetöötlemise ja vabaduste komisjon, CNIL, Prantsusmaa) tegi Google'ile ettekirjutuse, mille kohaselt juhul, kui kõnealune äriühing rahuldab andmesubjekti taotluse eemaldada tema nimega tehtud otsingu tagajärjel kuvatavate tulemuste loetelust lingid, mis viivad andmesubjekti puudutavaid andmeid sisaldavatele veebilehtedele, peab see äriühing need lingid eemaldama oma otsingumootori

⁶⁸ Direktiivi 95/46 artikli 8 lõike 2 punkt e ja määruse 2016/679 artikli 9 lõike 2 punkt e.

⁶⁹ Direktiivi 95/46 artikli 14 esimese lõigu punkt a ja määruse 2016/679 artikli 21 lõige 1.

⁷⁰ Seda kohtuotsust käsitleti 2019. aasta aastaaruandes, lk 118 ja 119.

kõigil domeeninime laienditel. Kuna Google keeldus seda ettekirjutust täitmast, määras CNIL äriühingule sanktsiooni summas 100 000 eurot. Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu), kelle poole Google pöördus, palus Euroopa Kohtul täpsustada, millise territoriaalse ulatusega on otsingumootori haldaja kohustus rakendada direktiivist 95/46 tulenevat õigust linkide eemaldamisele.

Esmalt tuletas Euroopa Kohus meelde, et liidu õigus võimaldab füüsilistel isikutel tugineda nende õigusele linkide eemaldamisele otsingumootori haldaja vastu, kellel on liidu territooriumil üks või mitu tegevuskohta, ning seda sõltumata küsimusest, kas isikuandmete töötlemine (kõnesoleval juhtumil lingid veebilehtedele, kus leidub vastava õiguse omaja isikuandmeid) toimub liidus või mitte⁷¹.

Mis puudutab ulatust, mis on õigusel linkide eemaldamisele, siis sedastas Euroopa Kohus, et otsingumootori haldaja on kohustatud lingid eemaldama mitte kõigist oma otsingumootori versioonidest, vaid kõigist liikmesriikides kasutusel olevatest otsingumootori versioonidest. Euroopa Kohus märkis sellega seoses, et kuigi linkide eemaldamine kõigist otsingumootori versioonidest on sobilik täielikult täitma liidu seadusandja eesmärki tagada isikuandmete kaitse kõrge tase kogu liidus, ei tulene liidu õigusest siiski, et niisuguse eesmärgi saavutamiseks oleks liidu seadusandja teinud valiku anda linkide eemaldamise õigusele ulatust, mis väljuks liikmesriikide territooriumilt⁷². Konkreetsemalt, ehkki liidu õiguses on küll nähtud ette liikmesriikide järelevalveasutuste vahelise koostöö mehhanismid, et jõuda ühisele otsusele, mis põhineb sellel, et kaalutakse ühelt poolt andmesubjekti õigust eraelu puutumatusse ja tema isikuandmete kaitsele ning teiselt poolt eri liikmesriikide üldsuse huvi teabega tutvuda, ei ole praegu ette nähtud selliseid mehhanisme seoses väljaspool liitu toimuva linkide eemaldamise ulatusega (punktid 62 ja 73).

Kehtiva liidu õiguse järgi on otsingumootori haldaja kohustatud taotluse kohaselt lingid eemaldama nii selles otsingumootori versioonis, mis on kasutusel linkide eemaldamise õiguse omaja elukoha liikmesriigis, kui ka teistes liikmesriikides kasutusel olevates otsingumootori versioonides, et muu hulgas tagada järjekindel ja kõrgetasemeline kaitse kogu liidus. Lisaks peab otsingumootori haldaja võtma vajaduse korral piisavalt tõhusaid meetmeid, et takistada liidu internetikasutajatel ligi pääseda – teatavatel juhtudel kolmandas riigis kasutatava otsingumootori kaudu – linkidele, mille kohta on esitatud linkide eemaldamise taotlus, või vähemalt tõsiselt pärssima nende tahet seda teha, ja liikmesriigi kohtul tuleb kontrollida, kas haldaja võetud meetmed vastavad sellele nõudele (punkt 70).

Viimaseks toonitas Euroopa Kohus, et kuigi kehtiv liidu õigus ei kohusta otsingumootori haldajat juhul, kui linkide eemaldamise taotlus rahuldatakse, eemaldama neid kõigist asjaomase otsingumootori versioonidest, ei ole see liidu õiguse kohaselt ka keelatud. Järelikult jääb liikmesriigi järelevalveasutusele või kohtule pädevus põhiõiguste kaitse riigisiseseid standardeid silmas pidades kaaluda ühelt poolt andmesubjekti õigust eraelu puutumatusse ja tema isikuandmete kaitsele ning teiselt poolt õigust teabevabadusele, ja kaalumise tulemusel vajaduse korral kohustada otsingumootori haldajat eemaldama lingid kõigist otsingumootori versioonidest (punktid 65 ja 72).

⁷¹ Direktiivi 95/46 artikli 4 lõike 1 punkt a ja määruse 2016/679 artikli 3 lõige 1.

⁷² Direktiivi 95/46 artikli 12 punkt b ja artikli 14 esimese lõigu punkt a ning määruse 2016/679 artikli 17 lõige 1.

4. Veebisaidi kasutaja nõusolek teabe salvestamiseks

[1. oktoobri 2019. aasta kohtuotsus \(suurkoda\) Planet49 \(C-673/17, ECLI:EU:C:2019:801\)](#)⁷³

Selles kohtuotsuses otsustas Euroopa Kohus, et nõusolek küpsiste abil teabe salvestamiseks veebisaidi kasutaja lõppseadmisse või juurdepääsuks sinna juba salvestatud teabele ei ole antud kehtivalt, kui luba on antud eeltäidetud märkeruudu abil, ja seda sõltumata sellest, kas kõnealuse teabe näol oli tegemist isikuandmetega või mitte. Lisaks täpsustas Euroopa Kohus, et teabe hulka, mille teenuseosutaja peab veebisaidi kasutajale andma, kuuluvad ka küpsiste kasutamise kestus ja asjaolu, kas kolmandatele isikutele antakse neile küpsistele juurdepääs või mitte.

Põhikohtuasjas oli kõne all müügiedendusliku auhinnamängu korraldamine Planet49 poolt veebisaidil www.dein-macbook.de. Internetikasutaja pidi mängus osalemiseks sisestama oma nime ja aadressi veebilehel, kus paiknesid märkeruudud. Märkeruut küpsiste paigaldamise lubamiseks oli eeltäidetud. Saksamaa tarbijakaitsekeskuste ja tarbijakaitseliitude föderatsiooni kassatsioonkaebust lahendanud Bundesgerichtshof (Saksamaa Liitvabariigi kõrgeim üldkohus) tekkisid kahtlused seoses sellega, kas tarbijatelt eeltäidetud märkeruudu abil saadud nõusolek on kehtiv ja millise ulatusega on teenuseosutajal lasuv teavitamiskohustus.

Eelotsusetaotlus puudutas sisuliselt seda, kuidas tõlgendada mõistet „nõusolek“ eraelu puutumatust ja elektroonilist sidet käsitlevas direktiivis 2002/58⁷⁴, koostoimes direktiiviga 95/46/EÜ⁷⁵ ning isikuandmete kaitse üldmäärusega⁷⁶.

Esimesena sedastas Euroopa Kohus, et direktiivi 95/46/EÜ artikli 2 punktis h, millele viitab eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi 2002/58 artikli 2 punkt f, on nõusolek määratletud kui „iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid“. Euroopa Kohus märkis, et andmesubjekti tahte „avaldamise“ nõue viitab selgelt aktiivsele, mitte passiivsele tegevusele. Eeltäidetud märkeruudu abil nõusoleku andmiseks ei ole aga vaja veebisaidi kasutaja aktiivset tegevust. Direktiivi 2002/58 artikli 5 lõike 3 – mis näeb sellesse direktiiviga 2009/136 tehtud muudatusest saadik ette, et andmesubjekt peab küpsiste paigaldamiseks olema „andnud [...] oma nõusoleku“ – kujunemislugu viitab lisaks sellele, et kasutaja nõusolekut ei tohi nüüdsest enam eeldada ja see peab nähtuma tema aktiivsest tegevusest. Viimaseks on aktiivne nõusolek nüüdseks ette nähtud üldmääruses⁷⁷, mille artikli 4 punkt 11 nõuab, et tahteavaldus oleks muu hulgas antud „selge nõusolekut väljendava tegevusega“ ja mille põhjenduses 32 on sõnaselgelt välistatud võimalus, et „vaikimist, eelnevalt märgistatud lahtreid või tegevusetust“ saaks pidada nõusolekuks (punktid 49, 52, 56 ja 62).

Euroopa Kohus otsustas sellest tulenevalt, et nõusolek ei ole antud kehtivalt, kui luba teabe salvestamiseks veebisaidi kasutaja lõppseadmisse või juurdepääs sinna juba salvestatud teabele on antud eeltäidetud märkeruudu abil, millest kasutaja peaks oma nõusolekust

⁷³ Seda kohtuotsust käsitleti 2019. aasta aastaaruandes, lk 120 ja 121.

⁷⁴ Direktiivi 2002/58, mida on muudetud Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiviga 2009/136/EÜ (ELT 2009, L 337, lk 11), artikli 2 punkt f ja artikli 5 lõige 3.

⁷⁵ Direktiivi 95/46 artikli 2 punkt h.

⁷⁶ Määruse 2016/679 artikli 6 lõike 1 punkt a.

⁷⁷ *Idem*.

keeldumiseks märgistuse eemaldama. Euroopa Kohus lisas, et asjaolust, et kasutaja klõpsab selle äriühingu korraldatud auhinnamängu osalemisnupul ei piisa selleks, et asuda seisukohale, et ta on andnud kehtiva nõusoleku küpsiste paigaldamiseks (punkt 63).

Teisena tõdes Euroopa Kohus, et direktiivi 2002/58 artikli 5 lõike 3 eesmärk on kaitsta kasutajat tema eraellu tungimise eest, olenemata sellest, kas selline sekkumine puudutab isikuandmeid. Sellest tuleneb, et mõistet „nõusolek“ ei tule tõlgendada erinevalt sõltuvalt sellest, kas teabe puhul, mis on salvestatud veebisaidi kasutaja lõppseadmesse või millele seal juurde pääsetakse, on või ei ole tegemist isikuandmetega (punktid 69 ja 71).

Kolmandana märkis Euroopa Kohus, et direktiivi 2002/58 artikli 5 lõige 3 nõuab, et kasutaja oleks andnud oma nõusoleku pärast seda, kui talle on esitatud selge ja igakülgne teave, muu hulgas andmete töötlemise eesmärgi kohta. Selge ja igakülgne teave peab võimaldama kasutajal hõlpsasti kindlaks määrata tema antava nõusoleku tagajärjed ja tagama, et see nõusolek oleks antud kõiki asjaolusid teades. Sellega seoses asus Euroopa Kohus seisukohale, et selge ja igakülgse teabe hulka, mille teenuseosutaja peab veebisaidi kasutajale andma, kuuluvad nii küpsiste kasutamise kestus kui ka kolmandate isikute võimalus neile juurde pääseda (punktid 73–75 ja 81).

VI. Riigisisised järelevalveasutused

1. Sõltumatuse nõude ulatus

[9. märtsi 2010. aasta kohtuotsus \(suurkoda\) komisjon vs. Saksamaa \(C-518/07, ECLI:EU:C:2010:125\)⁷⁸](#)

Komisjon palus oma hagis, et Euroopa Kohus tuvastaks, et Saksamaa Liitvabariik oli jätnud täitmata tal direktiivi 95/46 artikli 28 lõike 1 teise lõigu järgi lasuvad kohustused, sest ta allutas riiklikule järelevalvele asutused, kes on erinevates liidumaades pädevad tegema järelevalvet isikuandmete töötlemise üle erasektoris, ning võttis seega ebaõigelt üle andmekaitse tagamise eest vastutavate asutuste „täieliku sõltumatuse“ nõude.

Saksamaa Liitvabariik väitis, et direktiivi 95/46 artikli 28 lõike 1 teine lõik nõuab, et järelevalveasutused peavad oma tegevuses olema funktsionaalselt sõltumatud selles mõttes, et need asutused peavad olema sõltumatud erasektorist, mille üle nad järelevalvet teevad, ning et nad peavad olema vabad välisest mõjust. Tema arvates ei ole Saksamaa liidumaades tehtava riikliku järelevalve puhul tegemist mitte välise mõjuga, vaid haldusesisese järelevalvega, mida teevad järelevalveasutustega samasse haldusaparaati kuuluvad asutused, kes peavad samuti nagu järelevalveasutusedki täitma direktiivi 95/46 eesmäärke.

Euroopa Kohus otsustas, et liikmesriikide järelevalveasutuste sõltumatuse tagatis, mis on kehtestatud direktiivis 95/46, on kantud eesmärgist tagada isikuandmete töötlemisel üksikisikute kaitset käsitlevate sätete järgimise üle tehtava kontrolli tõhusus ja usaldusväärsus ning seda tuleb tõlgendada nimetatud eesmärki arvestades. Sõltumatuse tagatist ei kehtestatud mitte

⁷⁸ Seda kohtuotsust käsitleti 2010. aasta aastaaruandes, lk 34.

selleks, et anda nendele asutustele endile ning nende töötajatele eriline seisund, vaid eesmärgiga tugevdada nende isikute ja asutuste kaitset, keda järelevalveasutuste otsused puudutavad, millest järeldub, et oma ülesannete täitmisel peavad järelevalveasutused tegutsema objektiivselt ja erapooletult (punkt 25).

Euroopa Kohus asus seisukohale, et järelevalveasutused, kes on pädevad tegema järelevalvet isikuandmete töötlemise üle erasektoris, peavad olema sõltumatud, mis võimaldab neil täita oma ülesandeid välise mõjuta. See sõltumatus ei välista mitte ainult kontrollile allutatud asutuste mõju, vaid ka igasugused ettekirjutused ja muu otsese või kaudse välise mõju, mis võib seada kahtluse alla nimetatud järelevalveasutuste poolt oma kohustuse täitmise, milleks on eraelu puutumatus kaitse ning isikuandmete vaba liikumise vahel õiglase tasakaalu kehtestamine. Pelk oht, et riiklikku järelevalvet tegevad asutused võiksid poliitiliselt mõjutada järelevalveasutuste otsuseid, on piisav selleks, et takistada viimati nimetatute poolt nende ülesannete täitmisel sõltumatult tegutsemist. Esiteks võib seoses riiklikku järelevalvet tegeva asutuse otsustuspraktikaga kujuneda välja järelevalveasutuste „ennetav kuulekus“. Teiseks nõuab nendele järelevalveasutustele pandud eraelu puutumatus kaitsja roll, et nende otsused ning seega ka nemad ise oleksid väljaspool igasugust erapoolikuse kahtlust. Euroopa Kohtu hinnangul ei ole järelevalveasutuste üle tehtav riiklik järelevalve seega sõltumatuse nõudega kooskõlas (punktid 30, 36, 37 ja resolutsioon).

[16. oktoobri 2012. aasta kohtuotsus \(suurkoda\) komisjon vs. Austria \(C-614/10, EU:C:2012:631\)](#)

Komisjon palus oma hagnis, et Euroopa Kohus tuvastaks, et kuna Austria ei ole võtnud vastu kõiki vajalikke sätteid, et tema kehtivad õigusnormid vastaksid isikuandmete kaitse järelevalve asutusena loodud Datenschutzkommissioni (Austria andmekaitsekomisjon, edaspidi „DSK“) osas sõltumatuse kriteeriumile, siis on Austria rikkunud kohustusi, mis tulenevad direktiivi 95/46 artikli 28 lõike 1 teisest lõigust. Euroopa Kohus tuvastas, et Austria oli oma kohustusi rikkunud.

Euroopa Kohus leidis sisuliselt, et direktiivi 95/46 tulenevale järelevalveasutuse sõltumatuse nõudele ei vasta liikmesriik, kes kehtestab õigusliku raamistiku, mille kohaselt vastava järelevalveasutuse juhtivliige on föderaalametnik, kelle suhtes tehakse teenistuslikku järelevalvet; järelevalveasutuse büroo kuulub föderaalantantselei talituste juurde ning riigi valitsusjuhil on tingimusteta õigus saada teavet järelevalveasutuse juhtimise kõigi aspektide kohta (punkt 66 ja resolutsioon).

Euroopa Kohus tuletas esmalt meelde, et direktiivi 95/46 artikli 28 lõike 1 teises lõigus sätestatud mõisteid „täiesti sõltumatult“ tuleb tõlgendada nii, et järelevalveasutused peavad olema sõltumatud, mis võimaldab neil täita oma ülesandeid välise mõjuta. Ainuüksi asjaolust, et riigisisene järelevalveasutus on funktsionaalselt sõltumatu, kuna selle liikmed on sõltumatud ega ole oma ülesannete täitmisel seotud ühegi juhisega, ei piisa, et hoida nimetatud järelevalveasutust igasuguse välise mõju eest. Nõutud sõltumatusega ei ole tahetud välistada ainult otsest mõju juhiste vormis, vaid ühtlasi igasugust kaudset mõju, mis võiks järelevalveasutust otsuste tegemisel suunata. Pidades lisaks silmas järelevalveasutustele pandud eraelu puutumatus kaitsja rolli, peavad nende otsused ning seega ka nemad ise olema väljaspool igasugust erapoolikuse kahtlust (punktid 41–43 ja 52).

Euroopa Kohus täpsustas, et selleks, et vastata direktiivi 95/46 artikli 28 lõike 1 teises lõigus sätestatud sõltumatuse kriteeriumile, ei pea riigisisel järelevalveasutusel olema eraldiseisvat

eelarverida, nagu on ette nähtud määruse nr 45/2001 artikli 43 lõikes 3. Liikmesriigid ei ole tegelikult selleks, et tagada oma järelevalveasutus(t)e täielik sõltumatus, kohustatud kehtestama oma riigisisestes õigusaktides määruse nr 45/2001 V peatüki sätetega analoogilisi sätteid ning nad võivad ka eelarveõiguse osas ette näha, et järelevalveasutus sõltub konkreetse ministeeriumi ametkonnast. Sellest hoolimata ei või niisugusele asutusele vajaliku personali ja töövahendite andmine takistada asutusel oma ülesannete täitmist „täiesti sõltumatult“ direktiivi 95/46 artikli 28 lõike 1 teise lõigu tähenduses (punkt 58).

[8. aprilli 2014. aasta kohtuotsus \(suurkoda\) komisjon vs. Ungari \(C-288/12, EU:C:2014:237\)⁷⁹](#)

Selles kohtuasjas palus komisjon, et Euroopa Kohus tuvastaks, et kuna Ungari lõpetas enne tähtaega isikuandmete kaitse järelevalveasutuse ametiaja, oli ta rikkunud kohustusi, mis tulenevad direktiivist 95/46.

Euroopa Kohus otsustas, et liikmesriik, kes lõpetab enne tähtaega isikuandmete kaitse järelevalveasutuse ametiaja, on rikkunud kohustusi, mis tulenevad direktiivist 95/46/EÜ (punkt 62 ja resolutsiooni punkt 1).

Euroopa Kohtu hinnangul välistab sõltumatus, mis peab järelevalveasutustel nende andmete töötlemise üle järelevalve tegemisel olema, eelkõige igasugused ettekirjutused ja muu mis tahes vormis välise mõju, mis võib olla otsene või kaudne ning mis võib suunata nende otsuseid ja seada kahtluse alla nimetatud asutuste poolt oma ülesannete täitmise, mis on õiglase tasakaalu saavutamise eraelu puutumatus kaitse ja isikuandmete vaba liikumise vahel (punkt 51).

Euroopa Kohus tuletas lisaks meelde, et ainuüksi funktsionaalsest sõltumatusest ei piisa, et hoida järelevalveasutusi igasuguse välise mõju eest ning et pelk oht, et riiklikku järelevalvet tegevad asutused võiksid poliitiliselt mõjutada järelevalveasutuste otsuseid, on piisav selleks, et takistada viimati nimetatute poolt nende ülesannete täitmisel sõltumatult tegutsemist. Kui igal liikmesriigil oleks lubatud lõpetada järelevalveasutuse ametiaeg enne algul ette nähtud tähtaja lõppu, järgimata kohaldamisele kuuluvate õigusaktidega selleks kehtestatud eeskirju ja tagatisi, võiks seda asutust ähvardav ennetähtaegse ametiaja lõpetamise oht tuua kaasa asutuse teatava kuulekuse poliitilise võimu suhtes, mis ei oleks kooskõlas sõltumatuse nõudega. Niisuguses olukorras ei ole võimalik tõdeda, et järelevalveasutus tegutseb mis tahes olukorras väljaspool igasugust erapoolikuse kahtlust (punktid 52–55).

2. Kohaldatava õiguse ja pädeva järelevalveasutuse kindlaksmääramine

[1. oktoobri 2015. aasta kohtuotsus Weltimmo \(C-230/14, EU:C:2015:639\)⁸⁰](#)

Nemzeti Adatvédelmi és Információszabadság Hatóság (Ungari andmekaitse ja teabevahetuse amet) määras Slovakkias registreeritud äriühingule Weltimmo, kes haldab veebilehti, millel ta avaldab Ungaris asuva kinnisvara kuulutusi, trahvi, sest viimane ei kustutanud vastavasisulistele taotlustele vaatamata kuulutuste avaldajate isikuandmeid ja edastas need inkassofirmadele, et maksmata arvetele vastavad summad sisse nõutaks. Ungari järelevalveasutuse sõnul rikkus Weltimmo sellega Ungari õigusnormi, millega võeti üle direktiiv 95/46.

⁷⁹ Seda kohtuotsust käsitleti 2014. aasta aastaaruandes, lk 62.

⁸⁰ Seda kohtuotsust käsitleti 2015. aasta aastaaruandes, lk 55.

Kúrial (Ungari kõrgeim kohus), kellele esitati kassatsioonkaebus, tekkis kahtlus seoses kohaldatava õiguse kindlaksmääramise ja pädevusega, mida evib Ungari järelevalveasutus vastavalt direktiivi 95/46 artikli 4 lõikele 1 ja artiklile 28. Seetõttu esitas ta Euroopa Kohtule mitu eelotsuse küsimust.

Mis puudutab kohaldatavat liikmesriigi õigust, siis otsustas Euroopa Kohus, et direktiivi 95/46 artikli 4 lõike 1 punkt a võimaldab kohaldada muu liikmesriigi isikuandmekaitsealaseid õigusnorme kui see, kus nende andmete töötlemise eest vastutav isik on registreeritud, tingimusel et kõnealusel isikul on selle liikmesriigi territooriumil stabiilne asukoht, mille kaudu ta tegutseb tegelikult ja tulemuslikult, kas või minimaalselt, ning see töötlemine toimub selle tegevuse raames. Et määrata kindlaks, kas see on nii, võib eelotsusetaotluse esitanud kohus eelkõige võtta ühelt poolt arvesse asjaolu, et nimetatud töötlemise eest vastutava isiku tegevus, mille raames töötlemine toimub, seisneb veebilehe haldamises, millel avaldatakse selle liikmesriigi territooriumil asuva kinnisvara kuulutusi, mis on koostatud selle riigi keeles ja on seega peamiselt või isegi tervikuna suunatud nimetatud liikmesriiki. Eelotsusetaotluse esitanud kohus võib samuti arvestada asjaolu, et vastutaval isikul on nimetatud liikmesriigis esindaja, kes tegeleb sellisest tegevusest tulenevate nõuete sissenõudmisega ja esindab teda kõnealuste andmete töötlemist puudutavates haldus- ja kohtumenetlustes. Euroopa Kohus täpsustas, et see, millise riigi kodanikud on need isikud, keda andmete töötlemine puudutab, ei oma aga mingit tähtsust (punkt 41 ja resolutsiooni punkt 1).

Mis puudutab järelevalveasutuse pädevust ja volitusi kaebuse menetlemisel, siis leidis Euroopa Kohus, et liikmesriigi järelevalveasutus, kes direktiivi 95/46 artikli 28 lõike 4 alusel menetleb kaebusi seoses isikuandmete töötlemisega, võib vaadata kaebuse läbi sõltumata kohaldatavast õigusest, kui ei ole veel isegi teada, millise liikmesriigi õigus kuulub kõnesoleva töötlemise suhtes kohaldamisele (punkt 54). Kui ta jõuab aga järeldusele, et kohaldada tuleb teise liikmesriigi õigust, ei saa ta määrata sanktsioone väljaspool oma liikmesriigi territooriumi. Niisugusel juhul peab ta selle direktiivi artikli 28 lõikes 6 sätestatud lojaalse koostöö kohustust täites taotlema selle teise liikmesriigi järelevalveasutuselt, et see tuvastaks selle õiguse võimaliku rikkumise ja määraks sanktsiooni, kui kõnealune õigus seda võimaldab, tuginedes vajaduse korral teabele, mille esimese liikmesriigi järelevalveasutus talle edastas (punktid 57, 60 ja resolutsiooni punkt 2).

3. Riigisiseste järelevalveasutuste pädevus

[6. oktoobri 2015. aasta kohtuotsus \(suurkoda\) Schrems \(C-362/14, EU:C:2015:650\)](#)

Selles kohtuotsuses (vt ka IV alajaotus „Isikuandmete edastamine kolmandatesse riikidesse“) otsustas Euroopa Kohus muu hulgas, et riigisisised järelevalveasutused on pädevad, et teha järelevalvet isikuandmete kolmandatesse riikidesse edastamise üle.

Selleks on järelevalveasutustel lai valik volitusi, mis on direktiivi 95/46 artikli 28 lõikes 3 loetletud mitteammendavalt ja mis on nende kohustuste täitmiseks vajalikud vahendid. Nii on nendel asutustel muu hulgas uurimisvolitused, mille hulka kuulub õigus koguda oma järelevalvekohustuse täitmiseks vajalikku teavet, tõhusad sekkumisvolitused, mille hulka kuulub õigus keelata andmete töötlemine ajutiselt või alaliselt, ning volitused osaleda kohtumenetlustes (punkt 43).

Mis puudutab pädevust teha järelevalvet isikuandmete kolmandatesse riikidesse edastamise üle, siis otsustas Euroopa Kohus, et direktiivi 95/46 artikli 28 lõigetest 1 ja 6 nähtub tõepoolest, et liikmesriigi järelevalveasutuste pädevus puudutab isikuandmete töötlemist, mis toimub asutuse asukoha liikmesriigi territooriumil, mistõttu puudub neil artikli 28 kohaselt pädevus isikuandmete niisuguse töötlemise suhtes, mis leiab aset mõne kolmanda riigi territooriumil (punkt 44).

Ent toiming, mis seisneb isikuandmete edastamises liikmesriigist kolmandasse riiki, on iseenesest siiski käsitatav liikmesriigi territooriumil toimuva isikuandmete töötlemisena. Järelikult, kuna harta artikli 8 lõike 3 ja direktiivi 95/46 artikli 28 kohaselt on liikmesriigi järelevalveasutuste ülesanne kontrollida füüsiliste isikute kaitset reguleerivate liidu õigusnormide järgimist isikuandmete töötlemisel, on igal sellisel asutusel seega pädevus kindlaks teha, kas isikuandmete edastamine asutuse asukoha liikmesriigist kolmandasse riiki vastab kõnesoleva direktiiviga kehtestatud nõuetele (punktid 45 ja 47).

[5. juuni 2018. aasta kohtuotsus \(suurkoda\) Wirtschaftsakademie Schleswig-Holstein \(C-210/16, ECLI:EU:C:2018:388\)](#)

Selles kohtuotsuses (vt ka alajaotus II.5. „Mõiste „isikuandmete vastutav töötleja““), mis muu hulgas käsitleb direktiivi 95/46 artiklite 4 ja 28 tõlgendamist, võttis Euroopa Kohus seisukoha nende sekkumisvolituste ulatuse kohta, mis on järelevalveasutusel seoses isikuandmete töötlemisega, milles on hõlmatud mitu töötlemises osalejat.

Euroopa Kohus otsustas, et kui väljaspool Euroopa Liitu asutatud ettevõtjal (nagu Ameerika Ühendriikide ettevõtjal Facebook) on eri liikmesriikides mitu üksust, on ühe liikmesriigi järelevalveasutusel õigus kasutada talle selle direktiivi artikli 28 lõikega 3 antud volitusi selle ettevõtja üksuse suhtes, mis asub nimetatud liikmesriigi territooriumil (kõnesoleval juhtumil Facebook Germany), olgugi et vastavalt kontsernisisesele ülesannete jaotusele on see üksus ühelt poolt vastutav üksnes reklaamipinna müügi ja muu turundustegevuse eest selle liikmesriigi territooriumil ning teiselt poolt on isikuandmete kogumise ja töötlemise eest kogu Euroopa Liidu territooriumil ainuvastutav teises liikmesriigis asuv üksus (kõnesoleval juhtumil Facebook Ireland) (punkt 64 ja resolutsiooni punkt 2).

Lisaks täpsustas Euroopa Kohus, et kui ühe liikmesriigi järelevalveasutus soovib selle liikmesriigi territooriumil asuva üksuse suhtes kasutada talle direktiivi 95/46 artikli 28 lõikega 3 antud sekkumisvolitusi isikuandmete kaitse eeskirjade rikkumise tõttu, mille on toime pannud nende andmete töötlemise eest vastutav teises liikmesriigis asuv kolmas isik (kõnesoleval juhtumil Facebook Ireland), siis on see järelevalveasutus sõltumata teise liikmesriigi järelevalveasutusest (Iirimaa) pädev hindama sellise andmetöötluse seaduslikkust ja ta võib oma liikmesriigi territooriumil asuva üksuse suhtes kasutada oma sekkumisvolitusi, ilma et ta peaks enne paluma teise liikmesriigi järelevalveasutusel sekkuda (punkt 74 ja resolutsiooni punkt 3).

[15. juuni 2021. aasta \(suurkoda\) Facebook Ireland jt \(C-645/19, EU:C:2021:483\)](#)

Belgia eraelu puutumatus kaitse komisjoni (edaspidi „CPVP“) esimees algatas 11. septembril 2015 Facebook Irelandi, Facebook Inc-i ja Facebook Belgiumi vastu Nederlandstalige rechtbank van eerste aanleg Brusselis (Brüsseli hollandikeelne esimese astme kohus, Belgia) rikkumise lõpetamise menetluse eesmärgiga lõpetada andmekaitse õigusaktide rikkumised, mida Facebook väidetavalt toime pani. Need rikkumised seisnesid eelkõige Belgia internetikasutajate

veebikäitumist puudutava teabe kogumises ja kasutamises selliste erinevate tehnoloogiate abil nagu küpsised, sotsiaalmeedia pluginad⁸¹ või pikslid olenemata sellest, kas need kasutajad omasid Facebooki kontot või mitte.

See kohus tunnistas 16. veebruari 2018. aasta otsuses ennast selle menetluse osas pädevaks ja leidis sisulistes küsimustes, et suhtlusõrgustik Facebook ei teavitanud Belgia internetikasutajaid piisavalt asjaomase teabe kogumisest ja kasutamisest. Lisaks leidis see kohus, et internetikasutajate nõusolek selle teabe kogumiseks ja töötlemiseks oli kehtetu

Facebook Ireland, Facebook Inc. ja Facebook Belgium esitasid 2. märtsil 2018 selle kohtuotsuse peale apellatsioonkaebuse Hof van beroep te Brusselile (Brüsseli apellatsioonikohus), kes esitas käesolevas asjas eelotsusetaotluse. Belgia andmekaitseamet (edaspidi „APD“) osales apellatsioonimenetluses CPVP õigusjärglasena. Eelotsusetaotluse esitanud kohus leidis, et ta on pädev lahendama üksnes Facebook Belgiumi esitatud apellatsioonkaebust.

Eelotsusetaotluse esitanud kohus ei olnud kindel, kuidas mõjutab isikuandmete kaitse üldmääruses⁸² ette nähtud ühtse kontaktpunkti mehhanismi kohaldamine APD pädevust, ja täpsemalt tekkis tal küsimus, kas APD saab isikuandmete kaitse üldmääruse kohaldatavaks muutumisest, st 25. maist 2018, hilisemate asjaolude puhul algatada menetluse Facebook Belgiumi vastu, võttes arvesse, et asjasse puutuvate andmete töötlemise eest vastutava töötlejana on tuvastatud Facebook Ireland. Sellest kuupäevast alates ja isikuandmete kaitse üldmääruses ette nähtud ühtse kontaktpunkti põhimõtte kohaselt näib nimelt, et rikkumise lõpetamise menetluse algatamise pädevus on ainult liri andmekaitsevolinikul, kes allub üksnes liri kohtute kontrollile (punktid 36 ja 37).

Euroopa Kohus selgitas suurkoja tehtud kohtuotsuses pädevust, mille isikuandmete kaitse üldmäärus liikmesriikide järelevalveasutustele ette näeb. Täpsemalt otsustas ta, et piiriülese andmetöötlemise⁸³ korral saab liikmesriigi järelevalveasutus teatud tingimustel kasutada oma volitust juhtida selle liikmesriigi kohtu tähelepanu isikuandmete kaitse üldmääruse väidetavale rikkumisele ja osaleda kohtumenetluses ka juhul, kui ta ei ole selle andmetöötlemise osas juhtiv järelevalveasutus (resolutsiooni punkt 1).

Esiteks täpsustas Euroopa Kohus tingimusi, mille korral liikmesriigi järelevalveasutus, kes ei ole asjaomase piiriülese andmetöötlemise osas juhtiv järelevalveasutus, peab selle määrase kohaldamise tagamiseks kasutama oma volitust juhtida selle liikmesriigi kohtu tähelepanu isikuandmete kaitse üldmääruse väidetavale rikkumisele ja olenevalt asjaoludest osaleda kohtumenetluses. Selleks peab esimesena isikuandmete kaitse üldmääruse andma sellele järelevalveasutusele pädevuse võtta vastu otsus, millega tuvastatakse, et kõnealune töötlemine rikub selles määrases sisalduvaid norme, ja teisena tuleb järgida selles määrases ette nähtud koostöö ja järjepidevuse menetlusi⁸⁴ (punkt 75 ja resolutsiooni punkt 1).

⁸¹ Nt nupud „Meeldib“ või „Jagan“.

⁸² Isikuandmete kaitse üldmääruse artikli 56 lõikes 1 on sätestatud: „Ilma et see piiraks artikli 55 kohaldamist, on vastutava töötleja või volitatud töötleja peamise või ainsa tegevuskoha järelevalveasutus pädev tegutsema juhtiva järelevalveasutusena kõnealuse vastutava töötleja või volitatud töötleja tehtud piiriülese isikuandmete töötlemise toimingus suhtes kooskõlas artiklis 60 sätestatud menetlusega.“

⁸³ Isikuandmete kaitse üldmääruse artikli 4 punkti 23 tähenduses.

⁸⁴ Isikuandmete kaitse üldmääruse artiklites 56 ja 60 ette nähtud menetlused.

Piiriülese andmetöötuse jaoks näeb isikuandmete kaitse üldmäärus nimelt ette ühtse kontaktpunkti mehhanismi,⁸⁵ mis põhineb pädevuse jaotusel juhtiva järelevalveasutuse ja teiste asjasse puutuvate järelevalveasutuste vahel. See mehhanism nõuab nende asutuste tihedat, lojaalset ja tõhusat koostööd, et tagada isikuandmete kaitse normide järjepidev ja ühtne kohaldamine ning seeläbi säilitada nende soovitud toime. Sellega seoses annab isikuandmete kaitse üldmäärus juhtivale järelevalveasutusele põhimõttelise pädevuse teha otsus, et piiriülene andmetöötlus rikub selle määruse norme⁸⁶, samas kui teiste liikmesriikide järelevalveasutuste isegi ajutine pädevus sellist otsust teha kujutab endast erandit⁸⁷. Sellele vaatamata ei saa juhtiv järelevalveasutus oma pädevuse teostamisel loobuda vältimatust dialoogist ning lojaalsest ja tõhusast koostööst teiste asjasse puutuvate järelevalveasutustega. Seetõttu ei saa juhtiv järelevalveasutus selle koostöö raames eirata teiste asjaomaste järelevalveasutuste seisukohti ning iga asjakohaste järelevalveasutuste esitatud vastuväite tagajärjel peatub vähemalt ajutiselt ka juhtiva järelevalveasutuse kavandatud otsuse vastuvõtmine (punktid 50–53, 56–59 ja 63–65).

Euroopa Kohus täpsustas veel, et asjaolu, et liikmesriigi järelevalveasutus, mis ei ole asjaomase piiriülese andmetöötuse osas juhtiv järelevalveasutus, saab volitust juhtida selle liikmesriigi kohtu tähelepanu isikuandmete kaitse üldmääruse väidetavale rikkumisele ja olenevalt asjaoludest osaleda kohtumenetluses kasutada üksnes kooskõlas eeskirjadega, mis reguleerivad otsustuspädevuse jaotust juhtiva järelevalveasutuse ja teiste asjasse puutuvate järelevalveasutuste vahel⁸⁸, on vastavuses harta artiklitega 7, 8 ja 47, mis tagavad andmesubjektile õiguse tema isikuandmete kaitsele ja õiguse tõhusale õiguskaitsevahendile (punkt 67).

Teiseks otsustas Euroopa Kohus, et piiriülese andmetöötuse korral ei ole liikmesriigi järelevalveasutuse – kes ei ole juhtiv järelevalveasutus – volituse algatada kohtumenetlus⁸⁹ kasutamiseks nõutav, et isikuandmete piiriülese töötlemise eest vastutaval töötlejal või volitatud töötlejal, kelle vastu menetlus algatatakse, oleks peamine tegevuskoht või mõni muu tegevuskoht selle liikmesriigi territooriumil. Selle volituse kasutamine peab aga kuuluma isikuandmete kaitse üldmääruse territoriaalsesse kohaldamisalasse⁹⁰, mis eeldab, et piiriülese andmetöötuse eest vastutaval töötlejal või volitatud töötlejal on liidu territooriumil tegevuskoht (punktid 80, 83, 84 ja resolutsiooni punkt 2).

Kolmandaks otsustas Euroopa Kohus, et piiriülese andmetöötuse korral saab liikmesriigi järelevalveasutuse – kes ei ole juhtiv järelevalveasutus – volitust juhtida selle liikmesriigi kohtu tähelepanu isikuandmete kaitse üldmääruse väidetavale rikkumisele ja olenevalt asjaoludest osaleda kohtumenetluses kasutada nii isikuandmete piiriülese töötlemise eest vastutava töötleja peamise tegevuskoha vastu, mis asub selle järelevalveasutuse liikmesriigis, kui ka vastutava töötleja muu tegevuskoha vastu, tingimusel et kohtuasja ese on selle tegevuskoha tegevuse kontekstis toimunud andmetöötlus ja nimetatud järelevalveasutus on pädev seda volitust kasutama.

⁸⁵ Isikuandmete kaitse üldmääruse artikli 56 lõige 1.

⁸⁶ Isikuandmete kaitse üldmääruse artikli 60 lõige 7.

⁸⁷ Isikuandmete kaitse üldmääruse artikli 56 lõige 2 ja artikkel 66 näevad ette erandid põhimõttest, et otsustamispädevus on juhtival järelevalveasutusel.

⁸⁸ Ette nähtud isikuandmete kaitse üldmääruse artiklites 55 ja 56 koostoimes artikliga 60.

⁸⁹ Vastavalt isikuandmete kaitse üldmääruse artikli 58 lõikele 5.

⁹⁰ Isikuandmete kaitse üldmääruse artikli 3 lõikes 1 on ette nähtud, et seda määrust kohaldatakse liidus asuva vastutava töötleja või volitatud töötleja tegevuskoha tegevuse kontekstis toimuva isikuandmete töötlemise suhtes sõltumata sellest, kas töödeldakse liidus või väljaspool liitu.

Euroopa Kohus täpsustas siiski, et selle volituse kasutamine eeldab, et isikuandmete kaitse üldmäärus on kohaldatav. Kuna käesolevas kohtuasjas sai Facebooki kontserni Belgias asuva tegevuskoha tegevust pidada lahutamatu seotuks põhikohtuasjas kõne all olnud isikuandmete töötlemisega, mille eest liidu territooriumi osas vastutas Facebook Ireland, tuli sellist töötlemist pidada toimunuks „vastutava töötleja [...] tegevuskoha tegevuse kontekstis“ ja see kuulus seega isikuandmete kaitse üldmääruse kohaldamisalasse (punktid 94–96 ja resolutsiooni punkt 3).

Neljandaks otsustas Euroopa Kohus, et kui liikmesriigi järelevalveasutus, mis ei ole „juhtiv järelevalveasutus“, on algatanud kohtumenetluse seoses isikuandmete piiriülese töötlemisega enne isikuandmete kaitse üldmääruse kohaldatavaks muutumist, siis võib see menetlus liidu õiguse alusel jätkuda direktiivi 95/46 sätete alusel, kuna see direktiiv on jätkuvalt kohaldatav selles sätestatud normide rikkumise suhtes, mis on toime pandud kuni selle direktiivi kehtetuks tunnistamiseni. Lisaks võib nimetatud asutus algatada sellise menetluse pärast isikuandmete kaitse üldmääruse kohaldatavaks muutmise kuupäeva toime pandud rikkumiste suhtes, kui tegemist on ühega olukordadest, kus see määrus annab samale järelevalveasutusele erandina pädevuse võtta vastu otsus, milles tuvastatakse, et vaidlusaluse isikuandmete töötlemise puhul on rikutud selles määruses sisalduvaid norme, ja tingimusel, et selle otsuse tegemisel järgitakse määruses ette nähtud koostöömenetlusi (punkt 105 ja resolutsiooni punkt 4).

Viiendaks kinnitas Euroopa Kohus, et isikuandmete kaitse üldmääruse sättel, mille kohaselt peab iga liikmesriik seadusega ette nägema, et tema järelevalveasutus on volitatud juhtima õigusasutuste tähelepanu selle määruse rikkumistele ning olenevalt asjaoludest osalema kohtumenetluses, on vahetu õigusmõju. Seetõttu saab selline järelevalveasutus sellele sättele tugineda, et algatada menetlus eraõiguslike isikute vastu või seda menetlust jätkata, isegi kui seda sätet ei ole asjaomase liikmesriigi õiguses konkreetselt rakendatud (punkt 113 ja resolutsiooni punkt 5).

VII. Euroopa õigusaktide territoriaalne kohaldamine

[13. mai 2014. aasta kohtuotsus \(suurkoda\) Google Spain ja Google \(C-131/12, EU:C:2014:317\)](#)

Selles kohtuotsuses (vt ka alajaotus II.3. „Mõiste „isikuandmete töötlemine““ ning alajaotus V.1. „Õigus esitada isikuandmete töötlemisele vastuväiteid („õigus olla unustatud“)) tegi Euroopa Kohus otsuse ka direktiivi 95/46 territoriaalse kohaldamisala kohta.

Nii otsustas Euroopa Kohus, et isikuandmete töötlemine toimub liikmesriigi territooriumil paikneva vastutava töötleja asutuse tegevuse raames selle direktiivi 95/46 tähenduses, kui otsingumootori haldaja, kelle asukoht on küll kolmandas riigis, asutab liikmesriigis filiaali või tütarettevõtja, mille eesmärk on tagada otsingumootori reklaamipinna turustamine ja müük ning mille tegevus on suunatud selle liikmesriigi elanikele (punktid 55, 60 ja resolutsiooni punkt 2).

Niisuguses olukorras on otsingumootori haldaja tegevus ja tema liikmesriigis asuva asutuse tegevus, mis toimuvad küll teineteisest lahus, siiski omavahel lahutamatu seotud, kuna reklaamipinnaga seotud tegevus on vahend, et muuta otsingumootori tegevus majanduslikult tasuvaks, ning otsingumootor on samal ajal vahend, mis võimaldab seda tegevust sooritada (punkt 56).

VIII. Üldsuse õigus tutvuda Euroopa Liidu institutsioonide dokumentidega ja isikuandmete kaitse

[29. juuni 2010. aasta kohtuotsus \(suurkoda\) komisjon vs. Bavarian Lager \(C-28/08 P, EU:C:2010:378\)](#)

Äriühingul Bavarian Lager, mis asutati Saksa õlle importimiseks Ühendkuningriigis asuvatele alkoholse joogi jaemüügi kohtadele, ei õnnestunud oma tooteid müüa, kuna oluline osa alkoholsete jookide jaemüüjaist Ühendkuningriigis oli seotud ainuõiguslike ostukokkulepetega, mis kohustasid neid tellima oma õlle teatud kindlatelt õlletehastelt.

Vastavalt Ühendkuningriigi normidele õlle tarnimise kohta (edaspidi „külalisõlle säte“) pidid õlletehased andma publi pidajatele võimaluse osta üht õllesorti mõnelt teiselt õlletehaselt, ent seda tingimusel, et tegemist on vaadiõllega. Enamikku väljaspool Ühendkuningriiki toodetud õllesortidest ei saa aga pidada „vaadiõlleks“ külalisõlle sätte tähenduses ja seega ei kuulu nad selle sätte kohaldamisalasse. Kuna Bavarian Lager leidis, et külalisõlle säte on koguselise piiranguga samaväärse toimega meede, esitas ta komisjonile kaebuse.

Liikmesriigi kohustuste rikkumise menetluse raames, mille komisjon Ühendkuningriigi suhtes algatas, osalesid ühenduse ja Ühendkuningriigi ametkondade esindajad ja ühisturu õlleteootjate liidu (edaspidi „õlleteootjate liit“) esindajad koosolekul, mis toimus 11. oktoobril 1996. Pärast seda, kui Ühendkuningriigi ametiasutused olid teatanud kõnesolevate normide muutmise eelnõust, mille kohaselt võis pudeliõlut kui teistsuguse päritoluga õlut müüa niisamuti nagu vaadiõlut, teavitas komisjon Bavarian Lagerit sellest, et liikmesriigi kohustuste rikkumise menetlus on peatatud.

Bavarian Lager taotles 1996. aasta oktoobris toimunud koosoleku protokollis täielikku ärakirja, kus oleks mainitud kõigi koosolekul osalenute nimed, ent komisjon jättis selle taotluse 18. märtsi 2004. aasta otsusega rahuldamata, tuues põhjuseks nende isikute eraelu puutumatus kaitse, nii nagu see on tagatud määrusega 45/2001.

Bavarian Lager esitas seejärel hagi Üldkohtusse, nõudes, et komisjoni otsus tühistataks. Üldkohus tühistas komisjoni otsuse 8. novembri 2007. aasta otsusega, asudes eelkõige seisukohale, et asjasse puutuvate isikute nimede pelk lisamine nimekirja, kus olid ära toodud nende isikute nimed, kes oma teenistust esindades koosolekul osalesid, ei riivanud ega ohustanud nende isikute eraelu puutumatus. Komisjon, keda toetasid Ühendkuningriik ja nõukogu, esitas Euroopa Kohtule Üldkohtu otsuse peale apellatsioonkaebuse.

Euroopa Kohus märkis esmalt, et kui dokumentidele juurdepääsu käsitleva määruse nr 1049/2001⁹¹ alusel esitatud taotlusega soovitakse saada juurdepääsu isikuandmeid sisaldavatele dokumentidele, siis kohaldatakse kõiki määruse nr 45/2001 sätteid, sealhulgas sätet, mis kohustab isikuandmete vastuvõtjat tõendama nende andmete avaldamise vajalikkust, ning sätet, mis annab andmesubjektile võimaluse esitada igal ajal oma konkreetse seisundiga seotud veenvatel ja õigustatud põhjustel vastuväiteid endaga seotud andmete töötlemisele (punkt 63).

⁹¹ Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT 2001, L 145, lk 43).

Seejärel tõdes Euroopa Kohus, et liikmesriigi kohustuste rikkumise menetluse raames toimunud koosoleku protokollis olev koosolekul osalenute nimekiri sisaldab määruse nr 45/2001 artikli 2 punkti a tähenduses isikuandmeid, kuna on võimalik tuvastada koosolekul osalenud isikuid (punkt 70).

Lõpuks asus Euroopa Kohus seisukohale, et kui komisjon nõudis, et isikute osas, kes ei olnud selles protokollis sisalduvate oma isikuandmete avaldamiseks sõnaselget nõusolekut andnud, tõendataks nende andmete edastamise vajadust, siis käitus komisjon vastavalt määruse artikli 8 punkti b sätetele (punkt 77).

Nimelt, kui määruse nr 1049/2001 alusel esitatud taotluses protokolliga tutvuda ei ole esitatud ühtegi selget ja õiguspärast põhjendust ega ka veenvat argumenti, mis tõendaks nende isikuandmete edastamise vajadust, siis ei saa komisjon kaaluda asjaomaste poolte erinevaid huve. Ta ei saa ka kontrollida vastavalt määruse nr 45/2001 artikli 8 punktile b, kas on põhjust arvata, et andmete edastamine kahjustaks andmesubjektide õigustatud huve (punkt 78)⁹².

[16. juuli 2015. aasta kohtuotsus ClientEarth ja PAN Europe vs. EFSA \(C-615/13 P, EU:C:2015:489\)](#)

Euroopa Toiduohutusamet (EFSA) moodustas töögrupi, et töötada välja juhised, mis selgitaks määruse (EÜ) nr 1107/2009⁹³ artikli 8 lõike 5 rakendamist – sätte, mille kohaselt taimekaitsevahendi turulelaskmise loa taotleja lisab toimikule teaduslikud materjalid, mille kohta on koostatud võrdlevad teaduslikud eksperdihinnangud vastavalt EFSA antud määratlusele toimeaine ja selle oluliste metaboliitide kõrvaltoimete kohta tervisele, keskkonnale ja mittesihthilikele.

Juhise eelnõu esitati avalikuks aruteluks, mispeale ClientEarth ja Pesticide Action Network Europe (PAN Europe) esitasid omapoolsed seisukohad. Selles kontekstis esitasid nad koos EFSA-le taotluse tutvuda arvukate dokumentidega, mis on seotud juhise eelnõu väljatöötamisega, sealhulgas sooviti tutvuda välisekspertide seisukohtadega.

EFSA andis ClientEarthile ja PAN Europe'ile loa tutvuda muu hulgas individuaalsete seisukohtadega, mille välisekspertid olid juhise eelnõu kohta esitanud. EFSA selgitas aga, et märkustes varjas ta ekspertide nime, tuginedes määruse nr 1049/2001 artikli 4 lõike 1 punktile b ning liidu õigusnormidele isikuandmete kaitse kohta, eelkõige määrusele nr 45/2001. Ta märkis selle kohta, et ekspertide nime avalikustamist tuleb käsitada isikuandmete edastamisena määruse nr 45/2001 artikli 8 tähenduses, kuid selles sättes andmete edastamisele kehtestatud tingimused ei ole käesoleval juhul täidetud.

Seetõttu esitasid ClientEarth ja PAN Europe Üldkohtule hagi, milles nõudsid EFSA otsuse tühistamist. Üldkohus jättis selle hagi rahuldamata, mispeale ClientEarth ja PAN Europe esitasid Üldkohtu otsuse⁹⁴ peale apellatsioonkaebuse Euroopa Kohtule.

Euroopa Kohus märkis esiteks, et kuivõrd taotletud teave võimaldaks seostada konkreetse eksperdi vastava märkusega, puudutab see üheselt identifitseeritud füüsilisi isikuid ja kujutab

⁹² Seda kohtuotsust käsitleti 2010. aasta aastaaruandes, lk 14.

⁹³ Euroopa Parlamendi ja nõukogu 21. oktoobri 2009. aasta määrus (EÜ) nr 1107/2009 taimekaitsevahendite turulelaskmise ja nõukogu direktiivide 79/117/EMÜ ja 91/414/EMÜ kehtetuks tunnistamise kohta (ELT 2009, L 309, lk 1).

⁹⁴ Üldkohtu 13. septembri 2013. aasta otsus ClientEarth ja PAN Europe vs. EFSA (T-214/11, [EU:T:2013:483](#)).

endast järelkult isikuandmete kogumit määruse nr 45/2001 artikli 2 punkti a tähenduses. Kuna mõisted „isikuandmed“ määruse nr 45/2001 artikli 2 punkti a tähenduses ja „eraelu puudutavad andmed“ ei lange kokku, asus Euroopa Kohus seisukohale, et ClientEarthi ja PAN Europe'i väide, mille kohaselt ei oma vaidlusalune teave puutumust asjaomaste ekspertide eraeluga, ei saa järelkult olla tulemuslik (punktid 29 ja 32).

Teiseks käsitles Euroopa Kohus ClientEarthi ja PAN Europe'i argumenti, mis tugines umbusalduse õhkkonnale seoses EFSAga, keda süüdistatakse tihti erapoolikuses, kuna ta kasutab eksperte, kellel on isiklikud huvid tulenevalt seotusest tööstusringkondadega, ja vajadusele tagada selle ameti otsustamisprotsessi läbipaistvus. See argument tugines uuringule, mis näitab suurema osa EFSA töögrupis osalenud ekspertide seotust tööstusettevõtjaid esindavate survegruppidega. Euroopa Kohus otsustas kirjeldatud küsimuses, et vaidlusaluse teabe saamine oli vajalik selleks, et võimaldada kontrollida konkreetselt iga eksperdi erapooletust tema teaduslike ülesannete täitmisel EFSA huvides. Euroopa Kohus tühistas sellest tulenevalt Üldkohtu otsuse, leides, et Üldkohus eksis, kui ta otsustas, et ClientEarthi ja PAN Europe'i eespool esitatud argumendist ei piisa, et tõendada vaidlusaluse teabe edastamise vajalikkust (punktid 57–59).

Kolmandaks, et hinnata EFSA vaidlusaluse otsuse õiguspärasust, analüüsis Euroopa Kohus, kas on põhjust arvata, et andmete edastamine võis kahjustada andmesubjektide õigustatud huve. Sellega seoses tuvastas Euroopa Kohus, et EFSA väide, mille kohaselt ohustaks vaidlusaluse teabe avalikustamine nende ekspertide eraelu puutumatumust ja isikupuutumatumust, on üldine kaalutlus, mida ei toeta mingi muu käesolevas asjas esinev asjaolu. Euroopa Kohus leidis aga, et selline avalikustamine oleks iseenesest võimaldanud hajutada kõnealuseid kahtlusi erapoolikuses või andnud puudutatud ekspertidele vajaduse korral võimaluse vaidlustada olemasolevate õiguskaitsevahendite abil nende erapoolikuse kohta esitatud väited. Neid kaalutlusi arvesse võttes tühistas Euroopa Kohus EFSA otsuse (punktid 69 ja 73).

* * *

Käesolevas dokumendis refereeritud kohtuotsused asuvad kohtupraktika registri alajaotustes 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07, 4.11.11.01.