



## Kohtulahendite kogumik

KOHTUJURISTI ETTEPANEK  
MANUEL CAMPOS SÁNCHEZ-BORDONA  
esitatud 15. jaanuaril 2020<sup>1</sup>

**Liidetud kohtuasjad C-511/18 ja C-512/18**

**La Quadrature du Net,  
French Data Network,  
Fédération des fournisseurs d'accès à Internet associatifs,  
Igwam.net (C-511/18)  
*versus*  
Premier ministre,  
Garde des Sceaux, ministre de la Justice,  
Ministre de l'Intérieur,  
Ministre des Armées**

(eelotsusetaotlus, mille on esitanud Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu))

Eelotsusetaotlus – Isikuandmete töötlemine ja eraelu puutumatus kaitse elektroonilise side sektoris – Riigi julgeoleku kaitse ja terrorismivastane võitlus – Direktiiv 2002/58/EÜ – Kohaldamisala – Artikli 1 lõige 3 – Artikli 15 lõige 3 – ELL artikli 4 lõige 2 – Euroopa Liidu põhiõiguste harta – Artiklid 6, 7, 8, 11, 47 ja artikli 52 lõige 1 – Ühendusandmete ja sisuloojaid tuvastada võimaldavate andmete üldine ja vahet tegemata säilitamine – Võrguliiklus- ja asukohaandmete kogumine – Andmetele juurdepääs

1. Euroopa Kohus on viimastel aastatel hoidnud isikuandmete säilitamise ja neile juurdepääsu asjus väljakujunenud kohtupraktika joont, mille märkimisväärsed tähised on:

- 8. aprilli 2014. aasta kohtuotsus Digital Rights Ireland jt,<sup>2</sup> milles ta tunnistas direktiivi 2006/24/EÜ<sup>3</sup> kehtetuks, kuna see võimaldab ebaproportsionaalset sekkumist Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artiklitega 7 ja 8 tunnustatud õigustesse.
- 21. detsembri 2016. aasta kohtuotsus Tele2 Sverige ja Watson jt,<sup>4</sup> milles ta tõlgendas direktiivi 2002/58/EÜ<sup>5</sup> artikli 15 lõiget 1.
- 2. oktoobri 2018. aasta kohtuotsus Ministerio Fiscal,<sup>6</sup> milles ta kinnitas direktiivi 2002/58 selle sama sätte tõlgendust.

1 Algeel: hispaania.

2 Kohtuasjad C-293/12 ja C-594/12, edaspidi „kohtuotsus Digital Rights“, EU:C:2014:238.

3 Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiv, mis käsitleb üldkasutatavate elektroonilise side teenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (ELT 2006, L 105, lk 54).

4 Kohtuasjad C-203/15 ja C-698/15, edaspidi „kohtuotsus Tele2 Sverige ja Watson“, EU:C:2016:970.

5 Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatus kaitset elektroonilise side sektoris (eraelu puutumatus ja elektroonilist sidet käsitlev direktiiv) (EÜT 2002, L 201, lk 37; ELT eriväljaanne 13/29, lk 514).

6 Kohtuasi C-207/16, edaspidi „kohtuotsus Ministerio Fiscal“, EU:C:2018:788.

2. Need kohtuotsused (eriti teine) teevad mõne liikmesriigi ametiasutustele muret, sest nende arvates jäävad nad nende kohtuotsuste tagajärjel ilma töövahendist, mida nad peavad vajalikuks riigi julgeoleku kaitsmiseks ning kuritegevuse ja terrorismi vastu võitlemiseks. Seepärast peavad mõned nendest liikmesriikidest õigeks see kohtupraktika tühistada või seda nüansseerida.

3. Teatavad liikmesriikide kohtud on seda muret rõhutanud neljas eelotsusetaotluses,<sup>7</sup> mille kohta loetakse minu ettepanekut samal kuupäeval.

4. Nendes neljas kohtuasjas tõstatatakse eelkõige probleem seoses direktiivi 2002/58 kohaldamisega riigi julgeoleku ja terrorismivastase võitlusega seotud tegevustele. Kui see direktiiv on selles kontekstis kohaldatav, siis tuleks järgmiseks välja selgitada, mil määral võivad liikmesriigid piirata eraelu puutumatuse õigusi, mida see direktiiv kaitseb. Viimasena tuleb analüüsida, millisel määral vastavad erinevad riigisisised õigusnormid (Ühendkuningriigi,<sup>8</sup> Belgia<sup>9</sup> ja Prantsuse õigusnormid<sup>10</sup>) selles valdkonnas liidu õigusele, nagu seda on tõlgendanud Euroopa Kohus.

## I. Õiguslik raamistik

### A. Liidu õigus

#### 1. Direktiiv 2002/58

5. Artiklis 1 („Reguleerimisala ja eesmärk“) on ette nähtud:

„1. Käesoleva direktiiviga nähakse ette nende siseriiklike sätete ühtlustamine, mis on vajalikud põhiõiguste ja -vabaduste, eelkõige eraelu puutumatuse ja konfidentsiaalsuse kaitse võrdväärse taseme tagamiseks isikuandmete töötlemise puhul elektroonilise side sektoris ja selliste andmete ning elektrooniliste sideseadmete ja -teenuste vaba liikumise tagamiseks ühenduses.

[...]

3. Käesolevat direktiivi ei kohaldata tegevuse suhtes, mis jääb väljapoole Euroopa Ühenduse asutamislepingu reguleerimisala, nagu näiteks Euroopa Liidu lepingu V ja VI jaotise kohane tegevus, ja igal juhul sellise tegevuse suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (kaasa arvatud riigi majanduslik heaolu, kui tegevus on seotud riigi julgeolekuga) ja riigi sunnijõuga kriminaalõiguse valdkonnas.“

6. Artiklis 3 („Asjaomased teenused“) on märgitud:

„Käesolevat direktiivi kohaldatakse isikuandmete töötlemisele, mis toimub seoses üldkasutatavate elektrooniliste sideteenuste osutamisega ühenduse üldkasutatavates sidevõrkudes, sealhulgas andmete kogumist ja tuvastusseadmeid toetavates üldkasutatavates sidevõrkudes.“

<sup>7</sup> Lisaks nendele kahele (kohtuasjad C-511/18 ja C-512/18) kohtuasjad C-623/17, Privacy International, ja C-520/18, Ordre des barreaux francophones et germanophone jt.

<sup>8</sup> Kohtuasi Privacy International, C-623/17.

<sup>9</sup> Kohtuasi Ordre des barreaux francophones et germanophone jt, C-520/18.

<sup>10</sup> Kohtuasjad La Quadrature du Net jt, C-511/18 ja C-512/18.

7. Artikli 5 („Side konfidentsiaalsus“) lõikes 1 on sätestatud:

„Liikmesriigid tagavad üldkasutatava sidevõrgu ja üldkasutatavate elektrooniliste sideteenuste kaudu toimuva side ja sellega seotud liiklusandmete konfidentsiaalsuse siseriiklike õigusaktidega. Eelkõige keelatakse nende õigusaktidega isikutel, kes ei ole kasutajad, kuulata, salaja pealt kuulata, salvestada või muul viisil pealt kuulata või jälgida sidet ja sellega seotud liiklusandmeid ilma asjaomaste kasutajate loata, kui see ei ole õiguspärane artikli 15 lõike 1 kohaselt. Käesolev lõige ei takista side edastamiseks vajalikku tehnilist salvestamist, ilma et see piiraks konfidentsiaalsuse põhimõtet.“

8. Artiklis 6 („Liiklusandmed“) on sätestatud:

„1. Abonentide ja kasutajatega seotud liiklusandmed, mida töötleb üldkasutatava sidevõrgu pakkuja või üldkasutatavate elektrooniliste sideteenuste osutaja, tuleb kustutada või muuta anonüümseks, kui neid ei ole enam vaja side edastamiseks, ilma et see piiraks käesoleva artikli lõigete 2, 3 ja 5 ning artikli 15 lõike 1 kohaldamist.“

2. Töödelda võib liiklusandmeid, mis on vajalikud abonentide arvete ja sidumistasude jaoks. Selline töötlemine on lubatud ainult selle tähtaja lõpuni, mille jooksul võib arve õiguspäraselt vaidlustada või mille jooksul võib võtta meetmeid arve sissenõudmiseks.“

9. Artikli 15 (Direktiivi 95/46/EÜ<sup>[11]</sup> teatavate sätete rakendamine“) lõikes 1 on märgitud:

„Liikmesriigid võivad võtta seadusandlikke meetmeid, millega piiratakse käesoleva direktiivi artiklites 5 ja 6, artikli 8 lõigetes 1, 2, 3 ja 4 ning artiklis 9 sätestatud õiguste ja kohustuste ulatust, kui selline piiramine on vajalik, otstarbekas ja proportsionaalne abinõu selleks, et kaitsta direktiivi 95/46/EÜ artikli 13 lõikes 1 nimetatud riiklikku julgeolekut (s.t riigi julgeolekut), riigikaitset, avalikku korda, kriminaalkuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamist, uurimist, avastamist ja kohtus menetlemist. Selleks võivad liikmesriigid muu hulgas võtta seadusandlikke meetmeid, millega nähakse ette andmete säilitamine piiratud aja jooksul käesolevas lõikes sätestatud põhjustel. Kõik käesolevas lõikes osutatud meetmed on kooskõlas ühenduse õiguse üldpõhimõtetega, kaasa arvatud Euroopa Liidu lepingu artikli 6 lõigetes 1 ja 2 osutatud põhimõtetega.“

## 2. *Direktiiv 2000/31/EÜ*<sup>12</sup>

10. Artiklis 14 on ette nähtud:

„1. Kui osutatakse infoühiskonna teenust, mis seisneb teenuse saaja poolt pakutava teabe talletamises, tagavad liikmesriigid, et teenuseosutaja ei vastuta teenuse saaja taotluse põhjal talletatava teabe eest järgmistel tingimustel:

[...]

3. Käesolev artikkel ei mõjuta kohtu või haldusasutuse võimalust nõuda vastavalt liikmesriikide õigussüsteemidele teenuse osutajalt rikkumise lõpetamist või vältimist ega liikmesriikide võimalust kehtestada kord, kuidas teave kõrvaldada või juurdepääs sellele tõkestada.“

11 Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT 1995, L 281, lk 31; ELT eriväljaanne 13/15, lk 355).

12 Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 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).

11. Artiklis 15 on sätestatud:

„1. Liikmesriigid ei kehtesta artiklites 12, 13 ja 14 käsitletud teenuste osutajatele üldist kohustust jälgida teavet, mida nad edastavad või talletavad, ega üldist kohustust otsida ebaseaduslikku tegevust näitavaid fakte ja asjaolusid.

2. Liikmesriigid võivad kehtestada infoühiskonna teenuse osutajatele kohustuse kiiresti teatada pädevatele ametivõimudele nende teenuse saajate väidetavalt ebaseaduslikest tegevustest või pakutavast teabest või kohustuse edastada pädevatele asutustele nende taotluse põhjal teavet, mis võimaldab identifitseerida nende teenuse saajaid, kellega teenuseosutajal on talletamise kohta lepingud.“

**3. Määrus (EL) 2016/679<sup>13</sup>**

12. Artiklis 2 („Sisuline kohaldamisala“) on sätestatud:

„1. Käesolevat määrust kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatakse andmete kogumisse kanda.

2. Käesolevat määrust ei kohaldata, kui:

- a) isikuandmeid töödeldakse muu kui liidu õiguse kohaldamisalasse kuuluva tegevuse käigus;
- b) liikmesriigid töötlevad isikuandmeid sellise tegevuse käigus, mis kuulub ELi lepingu V jaotise 2. peatüki kohaldamisalasse;
- c) isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus;
- d) isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.

[...]“.

13. Artikli 23 („Piirangud“) lõige 1 näeb ette:

„Vastutava töötleja või volitatud töötleja suhtes kohaldatavas liidu või liikmesriigi õiguses võib seadusandliku meetmega piirata artiklites 12–22 ja artiklis 34, samuti artiklis 5 sätestatud kohustuste ja õiguste ulatust, kuivõrd selle sätted vastavad artiklites 12–22 sätestatud õigustele ja kohustustele, kui selline piirang austab põhiõiguste ja -vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada:

- a) riigi julgeolek;
- b) riigikaitse;
- c) avalik julgeolek;

<sup>13</sup> Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46 kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT 2016, L 119, lk 1).

- d) süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine;
- e) liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus;
- f) kohtusüsteemi sõltumatuse ja kohtumenetluse kaitse;
- g) reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine;
- h) jälgimine, kontrollimine või regulatiivsete ülesannete täitmine, mis on kas või juhtumipõhiselt seotud avaliku võimu teostamisega punktides a–e ja g osutatud juhtudel;
- i) andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse;
- j) tsiviilõiguslike nõuete täitmise tagamine.“

14. Artiklis 95 („Seos direktiiviga 2002/58/EÜ“) on sätestatud:

„Käesoleva määrusega ei panda füüsilistele ega juriidilistele isikutele lisakohustusi isikuandmete töötlemise suhtes, mis toimub seoses üldkasutatavate elektrooniliste sideteenuste osutamisega üldkasutatavates sidevõrkudes liidus ja mis on seotud küsimustega, mille puhul kehtivad nende suhtes direktiivis 2002/58/EÜ sätestatud erikohustused, millel on sama eesmärk.“

## **B. Liikmesriigi õigus**

### **1. Sisejulgeoleku seadustik (Code de la sécurité intérieure)**

15. Artiklis L. 851-1 on ette nähtud:

„Käesoleva raamatu II jaotise 1. peatükis sätestatud tingimustel võib anda loa koguda elektroonilise side teenuste pakkujatel ning posti- ja elektroonilise side seadustiku (code des postes et des communications électroniques) artiklis L. 34-1 nimetatud isikutelt, samuti usaldust digitaalmajanduses käsitleva [...] seaduse nr 2004-575 (loi n°2004-575 [...] pour la confiance dans l'économie numérique) artikli 6I punkti lõigetes 1 ja 2 nimetatud isikutelt nende võrgus või nende poolt elektroonilise side teenuste osutamisel töödeldud või säilitatud teavet ja dokumente, sealhulgas tehnilisi andmeid, mis seonduvad abonentnumbrite või elektroonilise side teenuste kasutamise tuvastamisega, teatud konkreetse isiku kõigi ühenduste või abonentnumbritega, kasutatud lõppseadme asukohaga ning konkreetse abonendi ühendustega, mis hõlmab väljaminevate ja sissetulevate kõnede nimekirja, kestust ja side kuupäeva [...]“.

16. Sisejulgeoleku seadustiku artiklid L. 851-2 ja L. 851-4 reguleerivad sõltuvalt eesmärgist ja viisist asutustele reaajas juurdepääsu andmist selliselt säilitatud ühendusandmetele.

17. Artikliga L. 851-2 on lubatud üksnes terrorismi tõkestamise eesmärgil koguda samadelt isikutelt artiklis L. 851-1 nimetatud teavet või dokumente. See andmete kogumine ühe või mitme konkreetse isiku kohta, kelle puhul on eelnevalt tuvastatud, et nad võivad olla seotud terrorismiohuga, toimub reaajas. Samamoodi on see ka artikliga L. 851-4, mis lubab teenusepakkujatel reaajas edastada

ainult lõppseadmete asukoha tehnilisi andmeid.<sup>14</sup>

18. Artikkel L. 851-3 võimaldab panna elektroonilise side teenuse pakkujatele ja tehniliste teenuste osutajatele kohustuse „rakendada oma võrkudes automatiseeritud andmetöötlusmeetmeid selleks, et tuvastada loas täpsustatud parameetrite alusel sideühendused, millest võib ilmneda terrorismioht“.<sup>15</sup>

19. Artiklis L. 851-5 on täpsustatud, et teatavatel tingimustel „võib olla lubatud kasutada tehnilist seadet, millega saab reaajas määrata isiku, sõiduki või objekti asukohta“.

20. Artikli L. 851-6 I lõike kohaselt on teatavatel tingimustel võimalik „karistusseadustiku (code pénal) artikli 226-3 lõikes 1 nimetatud aparadi või tehnilise seadmega vahetult [...] koguda tehnilisi ühendusandmeid, mis võimaldavad tuvastada lõppseadme või selle kasutaja abonendinumbril, ning kasutatava lõppseadmete asukoha andmeid“.

## **2. Posti ja elektroonilise side seadustik**

21. Asjaoludele kohaldatavas artikli L. 34-1 redaktsioonis on sätestatud:

„I. Käesolevat artiklit kohaldatakse isikuandmete töötlemisele üldkasutatavate elektroonilise side teenuste osutamisel; eelkõige kohaldatakse seda andmekogumis- ja -tuvastusseadmete võrkudele.

II. Elektroonilise side operaatorid ja eelkõige isikud, kes pakuvad üldsusele juurdepääsu interneti sideteenustele, kustutavad või muudavad anonüümseks kõik liiklusandmed, ilma et see piiraks III, IV, V ja VI lõike kohaldamist.

Isikud, kes pakuvad üldsusele elektroonilise side teenuseid, kehtestavad eelmise lõigu nõudeid järgides sisenemenetlused pädevate ametiasutuste nõudmistele vastamiseks.

Isikud, kes kutsealase põhi- või kõrvaltegevusena pakuvad üldsusele, sh tasuta, ühendust, mis võimaldab internetisidet veebiühenduse teel, on kohustatud täitma käesoleva artikli alusel elektroonilise side operaatoritele kohaldatavaid õigusnorme.

III. Süütegude või intellektuaalomandi seadustiku (code de la propriété intellectuelle) artiklis L. 336-3 sätestatud kohustuse rikkumise uurimiseks, tuvastamiseks ja menetlemiseks või karistusseadustiku (code pénal) artiklites 323-1 kuni 323-3-1 nimetatud automatiseeritud andmetöötlussüsteemi kahjustamise ennetamiseks ning üksnes eesmärgiga teha need andmed vajaduse korral kättesaadavaks kohtule või intellektuaalomandi seadustiku artiklis L. 331-12 nimetatud asutusele või kaitseseadustiku (code de défense) artiklis 2321-1 nimetatud riiklikule infosüsteemide turvalisuse asutusele võib teatud tehniliste andmete kustutamise või anonüümseks muutmise peatada kuni üheks aastaks. Conseil d'État'le (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) edastatud dekreediga, mis võeti vastu pärast riikliku andmetöötluse ja vabaduste komisjoni [(Commission nationale de l'informatique et des libertés)] arvamust, täpsustatakse VI lõikes märgitud piirides need andmekategooriad ja nende säilitamise kestus sõltuvalt operaatorite tegevusest ja side laadist ning vajaduse korral riigi taotlusel operaatorite tagatud teenuste osutamisega kaasnevate kindlaks määratavate ja spetsiifiliste lisakulutuste hüvitamise kord.

[...]

<sup>14</sup> Eelotsusetaotluse esitanud kohtu sõnul ei panda nende tehnikatega teenuseosutajatele täiendavat kohustust säilitada andmeid lisaks nendele, mis on vajalik nende osutatavate teenuste eest arveldamise, osutatavate teenuste turustamise ja lisandväärtust omavate teenuste osutamise seisukohast.

<sup>15</sup> Eelotsusetaotluse esitanud kohtu sõnul seisneb see tehnika, mis ei eelda andmete üldist ja vahet tegemata säilitamist, üksnes piiratud aja jooksul kõigi nende isikute poolt töödeldavate ühendusandmete hulgast nende andmete kogumises, millel võib olla seos selliste raskete õigusrikkumistega.



VI. Andmed, mida säilitatakse ja töödeldakse III, IV ja V lõikes sätestatud tingimustel, puudutavad ainult operaatorite osutatud teenuste kasutajate tuvastamist, operaatorite pakutava side tehnilisi tunnuseid ja lõppseadmete asukohta.

Need ei tohi mingil juhul puudutada selle side raames mis tahes kujul kirjavahetuse või vaadatud teabe sisu.

Andmete säilitamine ja töötlemine toimub vastavuses 6. jaanuari 1978. aasta infotehnoloogia, failide ja vabaduste seaduse nr 78–17 sätetega.

Operaatorid võtavad kõik meetmed, et takistada nende andmete kasutamist muudel kui käesolevas artiklis ette nähtud eesmärkidel.“

22. Artikli R. 10-13 lõike I alusel säilitavad operaatorid süütegude uurimise, tuvastamise ja süütegude eest vastutusele võtmise eesmärgil järgmisi andmeid:

- „a) kasutaja tuvastamist võimaldavad andmed;
- b) kasutatud terminali sideseadmete andmed;
- c) iga sideseansi tehnilised tunnused, nagu kuupäev, kellaeg ja kestus;
- d) taotletud või kasutatud lisateenuste ja nende osutajate andmed;
- e) andmed, mis võimaldavad tuvastada side adressaati või adressaate.“

23. Sama artikli II lõike kohaselt peab telefonsidetegevuse korral operaator lisaks säilitama andmed, mis võimaldavad tuvastada side lähtepunkti ja asukohta.

24. Sama artikli III lõike kohaselt tuleb nimetatud andmeid säilitada üks aasta alates nende salvestamisest.

**3. Usaldust digitaalmajanduses käsitlev 21. juuni 2004. aasta seadus nr 2004-575 (Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)**

25. Seaduse 2004-575 artikli 6 II lõike esimeses lõigus on sätestatud, et isikud, kes pakuvad üldsusele juurdepääsu interneti sideteenustele, ning füüsilised või juriidilised isikud, kes talletavad, isegi kui nad teevad seda tasuta, üldkasutatavate interneti sideteenuste teel üldsusele kättesaadavaks tegemise eesmärgil nende teenuste adressaatide poolt edastatud mis tahes liiki signaale, tekste, pilte, helisid või sõnumeid, „haldavad ja säilitavad andmeid nii, et see võimaldab tuvastada nende poolt osutatavate teenuste sisu või selle osa loomises osalenud isikud“.

26. Sama artikli II lõike kolmandas lõigus on sätestatud, et kohus võib neilt isikutelt nõuda esimeses lõigus nimetatud andmeid.

27. II lõike viimases lõigus on sätestatud, et Conseil d'État „määrab kindlaks esimeses lõigus nimetatud andmed ja nende säilitamise tähtaja ja korra“<sup>16</sup>.

## II. Faktilised asjaolud ja eelotsuse küsimused

### A. Kohtuasi C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net ja Fédération des fournisseurs d'accès à internet associatifs (edaspidi „kaebajad“) esitasid Conseil d'État'le kaebuse nõudega tühistada mitu sisejulgeoleku seadustiku teatavate sätete rakendamise dekreeti.<sup>17</sup>

29. Kaebajad väitsid sisuliselt, et nii vaidlustatud dekreedid kui ka need sisejulgeoleku seadustiku sätted on vastuolus õigusega eraelu puutumatusse, isikuandmete kaitsele ja tõhusale õiguskaitsevahendile, mis on tagatud vastavalt harta artiklitega 7, 8 ja 47.

30. Nendel asjaoludel esitab Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) Euroopa Kohtule järgmised küsimused:

- „1. Kas elektroonilise side teenuste pakkujatele direktiivi 2002/58 artikli 15 lõike 1 sätete alusel, mis annavad selleks loa, pandud andmete üldise ja vahet tegemata säilitamise kohustust tuleks olukorras, mida iseloomustavad tõsised ja pidevad ohud riigi julgeolekule, eelkõige terrorismioht, käsitada riivena, mis on põhjendatud [...] harta artikliga 6 tagatud õigusega turvalisusele ja riigi julgeoleku kaitsmise vajadusega, mille eest vastutavad [ELL] artikli 4 kohaselt ainult liikmesriigid?
2. Kas [...] direktiivi 2002/58 tuleb [...] hartat arvestades tõlgendada nii, et selle kohaselt on lubatud sellised seadusandlikud meetmed nagu kindlaksmääratud isikute kohta liiklus- ja asukohaandmete kogumine reaalajas, mis puudutavad küll elektroonilise side teenuste osutajate õigusi ja kohustusi, ent millega ei panda neile siiski spetsiaalset kohustust oma andmete säilitamiseks?
3. Kas [...] direktiivi 2002/58 tuleb [...] hartat arvestades tõlgendada nii, et selle kohaselt on ühendusandmete kogumise menetluse õiguspärasuse eelduseks igal juhul see, et asjaomast isikut informeeritakse, kui see informeerimine pädevate ametiasutuste poolt läbi viidavat uurimist enam kahjustada ei saa, või saab selliseid menetlusi käsitada õiguspärasena, võttes arvesse kõiki teisi olemasolevaid menetluslikke tagatise, kuna need tagavad tõhusalt kaebeõiguse?“

16 Määratlus anti 25. veebruari 2011. aasta dekreediga nr 2011-219 kõiki veebisisu loomises osalenud isikuid tuvastada võimaldavate andmete säilitamise ja edastamise kohta (décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne). Sellest dekreedist võib välja tuua: a) artikli 1 lõike 1, mille kohaselt peavad interneti sideteenustele juurdepääsu pakkuvad isikud säilitama järgmiseid andmeid: ühenduse identifikaator, abonendile määratud identifikaator, ühenduseks kasutatava terminali identifikaator, ühenduse alguse ja lõpu kuupäev ja kellaaeg, abonendi liini tehnilised omadused; b) artikli 1 lõike 2 alusel peavad isikud, kes talletavad, isegi kui nad teevad seda tasuta, üldkasutatavate interneti sideteenuste teel üldsusele kättesaadavaks tegemise eesmärgil nende teenuste aadressaaside poolt edastatud mis tahes liiki signaale, tekste, pilte, helisid või sõnumeid, säilitama iga toimingu kohta järgmiseid andmeid: ühenduse identifikaator side lähtepunktis, toimingu objektiks olevale sisule määratud identifikaator, teenusega ühendamiseks ja sisu edastamiseks kasutatud protokollitüübid, toimingu laad, toimingu kuupäev ja kellaaeg, toimingu autori kasutatud identifikaator; ja c) lõpuks on artikli 1 lõikes 3 sätestatud, et eelmistes lõigetes nimetatud isikud peavad säilitama järgmiseid andmeid, mille on kasutaja andnud lepingu sõlmimise või konto loomise ajal: konto loomise ajal kasutatud ühenduse identifikaator; eesnimi, perekonnanime või ärinimi; seonduvad postiaadressid, kasutatud pseudonüümid, seonduvad e-posti või konto aadressid, telefoninumbrid, uuendatud parool ja andmed, mis võimaldavad seda kontrollida või muuta.

17 Vaidlustatud dekreedid olid järgmised: a) 28. septembri 2015. aasta dekreet nr 2015-1185, mis käsitleb luureteenistusi (décret n°2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement); b) 1. oktoobri 2015. aasta dekreet nr 2015-1211, mis käsitleb loa nõudega luuretehnikate rakendamise ja riigi julgeolekut puudutavate failide vaidlustamist (décret n°2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressants la sûreté de l'État); c) 11. detsembri 2015. aasta dekreet nr 2015-1639 luureteenistuste hulka mitte kuuluvate asutuste kohta, kellel on õigus kasutada sisejulgeoleku seadustiku VIII raamatu V jaotises nimetatud luureandmete kogumise tehnikaid (décret n°2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure); ja d) 29. jaanuari 2016. aasta dekreet nr 2016-67 luureandmete kogumise tehnikate kohta (décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement).



## B. Kohtuasi C-512/18

31. Kaebajad palusid vaidluses, mille alusel algatati kohtuasi C-511/18, välja arvatud Igwan.net, Conseil d'État'l (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) samuti tühistada (haldusastutuse vaikimisi tehtud) otsus, millega jäeti rahuldamata nende taotlus tunnistada kehtetuks posti- ja elektroonilise side seadustiku (code des postes et des communications électroniques) artikkel R. 10-13 ja 25. veebruari 2011. aasta dekreet nr 2011-219.

32. Nende kaebajate hinnangul pannakse vaidlustatud õigusnormidega võrguliiklus-, asukoha- ja ühendusandmete säilitamise kohustus, mis oma üldise laadi tõttu rikub ebaproportsionaalselt õigust era- ja perekonnaelu austamisele, isikuandmete kaitsele ja sõnavabadusele, mis on kaitstud harta artiklitega 7, 8 ja 11, rikkudes direktiivi 2002/58 artikli 15 lõiget 1.

33. Sellest kaebuses esitas Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) selle eelotsuse küsimuse:

- „1. Kas elektroonilise side teenuste osutajatele [...] direktiivi 2002/58 artikli 15 lõike 1 sätete alusel, mis annavad selleks loa, pandud andmete üldise ja vahet tegemata säilitamise kohustust tuleks, võttes iseäranis arvesse nende ühendusandmete kogumise ja kasutamisega seotud tagatise ja kontrollimehhanisme, käsitada riivena, mis on põhjendatud [...] harta artikliga 6 tagatud õigusega turvalisusele ja riigi julgeoleku kaitsmise vajadusega, mille eest vastutavad [ELL] artikli 4 kohaselt ainult liikmesriigid?
2. Kas [...] direktiivi 2000/31 sätteid tuleks [...] harta artikleid 6, 7, 8 ja 11 ning artikli 52 lõiget 1 arvestades tõlgendada nii, et need lubavad liikmesriigil kehtestada riigisisised normid, millega pannakse isikutele, kes pakuvad üldsusele juurdepääsu interneti sideteenustele, ning füüsilistele või juriidilistele isikutele, kes tagavad, isegi kui nad teevad seda tasuta, interneti teel üldsusele andmete edastamise teenuste kaudu üldsusele edastamise eesmärgil nende teenuste kasutajate poolt edastatud mis tahes liiki signaalide, tekstide, piltide, helide või sõnumite talletamise, kohustus säilitada andmeid, mis võimaldavad tuvastada kõik nende poolt osutatavate teenuste sisu või selle osa loomises osalenud isikud, et kohus saaks vajaduse korral nõuda nende andmete esitamist tsiviil- või karistusõiguslikku vastutust reguleerivate sätete kohaldamiseks?“

## III. Menetlus Euroopa Kohtus ja poolte seisukohad

34. Eelotsusetaotlus registreeriti Euroopa Kohtus 3. augustil 2018.

35. Kirjalikud seisukohad on esitanud lisaks komisjonile La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, Saksamaa, Belgia, Ühendkuningriigi, Tšehhi, Küprose, Taani, Hispaania, Eesti, Prantsuse, Ungari, Iirimaa, Poola ja Rootsi valitsus.

36. Avalik kohtuistung peeti 9. septembril 2019 koos kohtuasjade C-623/17, Privacy International, ja C-520/18, Ordre des barreaux francophones et germanophone jt, kohtuistungiga, millel osalesid nelja eelotsusetaotluse pooled, eespool nimetatud valitsused ning Madalmaade ja Norra valitsus, samuti komisjon ja Euroopa andmekaitseinspektor.

#### IV. Õiguslik analüüs

37. Conseil d'État' (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) küsimused võib rühmitada kolmeks küsimuseks:

- Esiteks, kas riigisisised õigusnormid, millega pannakse elektroonilise side teenuste osutajatele kohustus säilitada üldiselt ja vahet tegemata ühendusandmeid (esimene küsimus kohtuasjas C-511/18 ja kohtuasjas C-512/18) ja konkreetselt andmeid, mis võimaldavad tuvastada nende teenuseosutajate pakutava sisu loojaid (teine küsimus kohtuasjas C-512/18), on liidu õigusega kooskõlas?
- Teiseks, kas ühendusandmete kogumise menetluste õiguspärasus sõltub igal juhul kohustusest asjaomaseid isikuid informeerida, kui sellega uurimisi ei ohustata (kolmas küsimus kohtuasjas C-511/18).
- Kolmandaks, kas liiklus- ja asukohaandmete kogumine, ilma nende säilitamise kohustuseta, on – ja mis tingimustel – direktiiviga 2002/58 kooskõlas (teine küsimus kohtuasjas C-511/18).

38. Lõppkokkuvõttes tuleb kindlaks määrata, kas liidu õigusega on kooskõlas liikmesriigi õigusnorm, millega pannakse elektroonilise side teenuste osutajatele kahte tüüpi kohustused: a) ühelt poolt *koguda* teatavaid andmeid, kuid neid mitte säilitada; b) teiselt poolt *säilitada* ühendusandmeid ja andmeid, mis võimaldavad tuvastada teenuseosutajate osutatud teenuste sisu loojaid.

39. Kõigepealt tuleb välja selgitada, kas just nimelt selle konteksti<sup>18</sup> tõttu, milles see riigisisene õigusnorm vastu võeti (s.t asjaoludel, milles võib esineda oht riigi julgeolekule), on kohaldatav direktiiv 2002/58.

#### A. Direktiivi 2002/58 kohaldatavus

40. Eelotsusetaotluse esitanud kohus peab tuvastatuks, et vaidlusalune õigusnorm kuulub direktiivi 2002/58 kohaldamisalasse. Nii nähtub tema hinnangul kohtuotsuses Tele2 Sverige ja Watson sedastatud ning kohtuotsuses Ministerio Fiscal kinnitatud kohtupraktikast.

41. Mõned menetluse astunud valitsused seevastu väidavad, et vaidlusalused õigusnormid sellesse kohaldamisalasse ei kuulu. Oma seisukoha kaitseks viitavad nad muude argumentide hulgas 30. mai 2006. aasta kohtuotsusele parlament vs. nõukogu ja komisjon<sup>19</sup>.

42. Nõustun Conseil d'État'ga (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu), et kohtuotsusega Tele2 Sverige ja Watson lahendati vaidluse see osa, kinnitades, et direktiiv 2002/58 on põhimõtteliselt kohaldatav, kui elektrooniliste teenuste osutajad on seadusega kohustatud oma abonentide andmeid säilitama ja võimaldama ametivõimudel neid andmeid kasutada. Seda põhiseisukohta ei muuda asjaolu, et kohustused on teenuseosutajatele pandud riikliku julgeoleku kaalutlustel.

43. Pean kohe ette ütleva, et kui kohtuotsuse Tele2 Sverige ja Watson ning eelnevate kohtuotsuste vahel peaks olema lahknevusi, siis tuleb ülekaalukaks lugeda just seda kui hilisemat ja kohtuotsusega Ministerio Fiscal üle kinnitatud kohtuotsust. Arvan siiski, et seda lahknevust ei ole, nagu ma edaspidi selgitan.

<sup>18</sup> „Olukorras [...] [kus on] tõsised ja pidevad ohud riigi julgeolekule, eelkõige terrorismioht“, nagu on täpsustatud kohtuasja C-511/18 esimeses küsimuses.

<sup>19</sup> Kohtuasjad C-317/04 ja C-318/04, edaspidi „kohtuotsus parlament vs. nõukogu ja komisjon“, EU:C:2006:346.

## 1. Kohtuotsus parlament vs. nõukogu ja komisjon

44. Kohtuotsusega parlament vs. nõukogu ja komisjon lahendatud kohtuasjad puudutasid:

- Euroopa Ühenduse ja Ameerika Ühendriikide vahelist lepingut lennuettevõtjate poolt PNR (Passenger Name Records) ehk reisijate isikuandmete töötlemise ja edastamise kohta Ameerika Ühendriikide ametiasutustele.<sup>20</sup>
- Nimetatud ametiasutustele edastatud reisijaregistris sisalduvate isikuandmete kaitse piisavust.<sup>21</sup>

45. Euroopa Kohus järeldas sellest, et nende andmete edastamine oli andmete töötlemine riigi julgeoleku ja kriminaalasjades riigi toimingute tegemise eesmärgil. Direktiivi 95/46 artikli 3 lõike 2 esimese taande kohaselt ei kuulu kaks vaidlusalust otsust direktiivi 95/46 kohaldamisalasse.

46. Algselt olid andmeid kogunud lennuettevõtjad tegevuse – piletimüük – raames, mis kuulub liidu õiguse kohaldamisalasse. Nende andmete töötlemine, nagu see oli ette nähtud vaidlusaluses direktiivis, aga „ei [ole vajalik] teenuse osutamiseks [...], vaid sellega peetakse silmas riigi julgeoleku kaitset ning õiguskaitse eesmärke“<sup>22</sup>.

47. Euroopa Kohus lähtus peaaegu teleoloogilisest käsitlusviisist, arvestades andmete töötlemise eesmärki: kui sellega püütakse tagada riigi julgeolek, tuleb see direktiivi 95/46 kohaldamisalast välja arvata. See eesmärk ei olnud aga ainus määrav kriteerium,<sup>23</sup> mistõttu kohtuotsuses rõhutati, et „toimub sellises ametivõimude poolt loodud raamistikus, mille eesmärk on tagada riigi julgeolek“<sup>24</sup>.

48. Kohtuotsus parlament vs. nõukogu ja komisjon võimaldab seega täheldada erinevust direktiivi 95/46 välistamisklausli ja piirangu- või piiramisklauslite vahel (mis on analoogsed direktiivi 2002/58 klauslitega). Siiski on tõsi, et mõlemat tüüpi klauslitel on sarnased üldise huvi eesmärgid, mis tekitab mõningast segadust nende vastava ulatuse suhtes, nagu hoiatas omal ajal kohtujurist Bot.<sup>25</sup>

49. Sellest segadusest arvatavasti tulebki nende liikmesriikide põhiseisukoht, kes leiavad, et direktiiv 2002/58 ei ole selles kontekstis kohaldatav. Tema hinnangul kaitstakse riigi julgeoleku huvi ainult direktiivi 2002/58 artikli 1 lõikes 3 sätestatud välja jätmisega. Kindel on siiski, et sama huvi teenivad ka nimetatud direktiivi artikli 15 lõikega 1 lubatud piirangud, sealhulgas piirang riigi julgeoleku suhtes. Viimati nimetatud säte oleks ülearune, kui direktiiv 2002/58 ei oleks riigi julgeolekule tuginemise korral kohaldatav.

20 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, ja parandus: ELT 2005, L 255, lk 168) (kohtuasi C-317/04).

21 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) (kohtuasi C-318/04).

22 Kohtuotsus parlament vs. nõukogu ja komisjon, punkt 57. Punktis 58 on rõhutatud, et „sellest, et kuna eraõiguslikud ettevõtjad kogusid PNR-andmeid kommertseesmärgil ning just nemad korraldavad nende edastamist kolmandasse riiki“, ei järeldu, et kõnealune ei ole üks nendest direktiivi 95/46 artikli 3 lõike 2 esimeses taandes loetletud juhtudest, kus see direktiiv ei ole kohaldatav, sest see „[e]dastamine toimub sellises ametivõimude poolt loodud raamistikus, mille eesmärk on tagada riigi julgeolek“.

23 Nii rõhutas seda kadunud kohtujurist Bot hiljem oma ettepanekus kohtuasjas Iirimaa vs. parlament ja nõukogu (C-301/06, EU:C:2008:558). Ta väitis, et kohtuotsusega parlament vs. nõukogu ja komisjon „ei taheta [...] näidata, nagu piisaks ainuüksi isikuandmete töötlemise eesmärgi uurimisest, et otsustada, kas kõnealune andmetöötlus kuulub direktiivis 95/46 ette nähtud andmekaitse süsteemi reguleerimisalasse. Lisaks tuleb kontrollida, millise tegevusvaldkonna raames andmeid töödeldakse. Andmetöötlus jääb direktiivist 95/46 tulenevast ühenduse isikuandmete kaitse süsteemist välja kõnealuse direktiivi artikli 3 lõike 2 esimese taande kohaselt vaid juhul, kui kõnealune andmetöötlus leiab aset selliste toimingute teostamiseks, mis on iseloomulikud riigile või riigi ametiasutustele ega ole omased eraisikute tegevusvaldkondadele“ (punkt 122).

24 Kohtuotsus parlament vs. nõukogu ja komisjon, punkt 58. Lepingu peamine eesmärk oli nõuda lennuettevõtjalt reisijateveoteenustega liidu ja Ameerika Ühendriikide vahel, et nad võimaldaksid Ameerika Ühendriikide ametiasutustel elektrooniliselt kasutada oma broneeringute ja väljumiste kontrollimise infosüsteemides olevaid PNR broneeringuandmeid. Sellega kehtestati seega liidu ja Ühendriikide vahel teatud vormis rahvusvaheline koostöö võitlemiseks terrorismi ja muude raskete kuritegude vastu, püüdes seda eesmärki ühitada reisijate isikuandmete kaitsega. Selles kontekstis ettevõtjatele pandud kohustus ei olnud väga erinev otsesest andmevahetusest ametiasutuste vahel.

25 Kohtujurist Boti ettepanek kohtuasjas Iirimaa vs. parlament ja nõukogu (C-301/06, EU:C:2008:558, punkt 127).

## 2. Kohtuotsus Tele2 Sverige ja Watson

50. Kohtuotsuses Tele2 Sverige ja Watson arutati, kas liidu õigusega olid kooskõlas teatavad liikmesriikide korrad, kus kehtestati üldkasutatavate elektroonilise side teenuste osutajatele üldine kohustus säilitada nende sideteenuste andmeid. Need juhtumid olid seega sisuliselt identsed nendega, mida lahendatakse nendes eelotsusetaotlustes.

51. Kuna on taas tõstatatud küsimus liidu õiguse – nüüd juba direktiivi 2002/58 kehtivusaajal – kohaldatavusest, märkis Euroopa Kohus alustuseks, et „direktiivi 2002/58 kohaldamisala ulatust tuleb tõlgendada eelkõige lähtuvalt selle direktiivi üldisest ülesehitusest“<sup>26</sup>.

52. Seda silmas pidades juhtis Euroopa Kohus tähelepanu asjaolule, et „[m]õistagi seonduvad direktiivi 2002/58 artikli 15 lõikes 1 nimetatud seadusandlikud meetmed riigi ametiasutustele tüüpiliste ülesannetega, mis ei puutu üksikisikute tegevusvaldkonda [...] Lisaks kattuvad eesmärgid, millele niisugused meetmed peavad selle sätte kohaselt vastama, ehk antud juhul riigi julgeoleku, [...], tagamine [...] suures ulatuses eesmärkidega, mida on mainitud selle direktiivi artikli 1 lõikes 3“<sup>27</sup>.

53. Nii on nende meetmete eesmärk, mida liikmesriigid võivad direktiivi 2002/58 artikli 15 lõike 1 kohaselt võtta, et piirata õigust eraelu puutumatusse, (selles osas) kattuv eesmärgiga, mis õigustab selle direktiivi artikli 1 lõike 3 kohaselt teatavate riiklike tegevuste vabastamist selle direktiiviga kehtestatud korrast.

54. Euroopa Kohus on siiski leidnud, et „[d]irektiivi 2002/58 üldist ülesehitust arvestades“ ei võimaldanud see asjaolu siiski „järeldata, et direktiivi 2002/58 artikli 15 lõikes 1 mainitud seadusandlikud meetmed on selle direktiivi kohaldamisalast välistatud, vastasel juhul jääks see säte täielikult ilma oma soovitatavast toimest. Kõnealune säte eeldab nimelt tingimata, et selles nimetatud riigisisised meetmed [...] kuuluvad selle direktiivi kohaldamisalasse, sest direktiiv lubab liikmesriikidel sõnaselgelt võtta neid meetmeid ainult seal ette nähtud tingimustel“<sup>28</sup>.

55. Eelöeldule lisandub, et direktiivi 2002/58 artikli 15 lõikes 1 lubatud piirangud reguleerivad „selles sättes nimetatud otstarbel elektroonilise side teenuste osutajate tegevust“. Seetõttu tuleb seda sätet koostoides sama direktiivi artikliga 3 „tõlgendada nii, et niisugused seadusandlikud meetmed kuuluvad selle direktiivi kohaldamisalasse“<sup>29</sup>.

56. Seetõttu on Euroopa Kohus leidnud, et direktiivi 2002/58 kohaldamisalasse kuulub nii seadusandlik meede, mis paneb teenuseosutajatele „kohustuse säilitada liiklusandmed ja asukohaandmed, kuna see tegevus hõlmab tingimata ka isikuandmete töötlemist nende teenuseosutajate poolt“,<sup>30</sup> kui ka meede, mis reguleerib ametiasutuste juurdepääsu nende teenuseosutajate säilitatavatele andmetele<sup>31</sup>.

57. Kohtuotsuses Tele2 Sverige ja Watson Euroopa Kohtu järgitud direktiivi 2002/58 tõlgendust kinnitatakse kohtuotsuses Ministerio Fiscal.

58. Kas võib asuda seisukohale, et kohtuotsus Tele2 Sverige ja Watson on suuremal või väiksemal määral pööre kohtuotsuses parlament vs. nõukogu ja komisjon sedastatud kohtupraktika suhtes? Nii mõistab seda näiteks Iirimaa valitsus, kelle arvates on ainult see viimati nimetatud direktiivi 2002/58 õigusliku alusega kooskõlas ja vastavuses ELL artikli 4 lõikega 2.<sup>32</sup>

26 Kohtuotsus Tele2 Sverige ja Watson, punkt 67.

27 *Ibidem*, punkt 72.

28 *Ibidem*, punkt 73.

29 *Ibidem*, punkt 74.

30 *Ibidem*, punkt 75.

31 *Ibidem*, punkt 76.

32 Iirimaa valitsuse kirjalike seisukohtade punktid 15 ja 16.

59. Prantsuse valitsus leiab omalt poolt, et vastuolu saaks vältida, kui arvestada, et kohtuotsuse Tele2 Sverige ja Watson doktriinis on viidatud liikmesriikide tegevusele karistusõiguse valdkonnas, samas kui kohtuotsuses parlament *vs.* nõukogu ja komisjon sedastatud doktriin seondub riigi julgeolekuga ja riigikaitsega. Seega ei ole kohtuotsuse Tele2 Sverige ja Watson doktriin tema arvates praegu analüüsitaval juhul kohaldatav, kuna selles tuleb lähtuda lahendusest, milleni jõuti kohtuotsuses parlament *vs.* nõukogu ja komisjon<sup>33</sup>.

60. Nagu ma juba märkisin, arvan, et võib leida teistsuguse viisi neid kahte kohtuotsust omavahel ühendada kui see, mille pakub välja Prantsuse valitsus. Viimati nimetatud võimalusega ma ei nõustu, sest minu arvates on kohtuotsuses Tele2 Sverige ja Watson sõnaselgelt terrorismivastase võitluse kohta antud põhjendused<sup>34</sup> laiendatavad igale muule riigi julgeolekut ähvardavale ohule (millest terrorism on vaid üks).

### ***3. Kohtuotsust parlament vs. nõukogu ja komisjon kohtuotsusega Tele2 Sverige ja Watson ühendava tõlgendamise võimalus***

61. Minu arvates võttis Euroopa Kohus kohtuotsustes Tele2 Sverige ja Watson ning Ministerio Fiscal arvesse välistamis- ja piiramisklauslite mõtet ning süstemaatilist seost nende kahte tüüpi klauslite vahel.

62. Kui kohtuasjas parlament *vs.* nõukogu ja komisjon otsustas Euroopa Kohus, et andmete töötlemine ei kuulu direktiivi 95/46 valdkonda, siis – nagu ma juba meenutasin – seetõttu, et Euroopa Liidu ja Ühendriikide vahelise koostöö kontekstis tüüpilises rahvusvahelises raamistikus pidi tegevuse riiklik mõõde üles kaaluma asjaolu, et see töötlemine hõlmas ka ärilist või eraõiguslikku mõõdet. Üks tookord arutatud küsimustest oligi just nimelt vaidlusaluse otsuse õige õiguslik alus.

63. Seevastu kohtuotsustes Tele2 Sverige ja Watson ning Ministerio Fiscal analüüsitud riiklike meetmete puhul seadis Euroopa Kohus esiplaanile andmetöötluse riigisisese ulatuse: õiguslik raamistik, milles see toimus, oli eranditult riigisisene, nii et sellel puudus väline mõõde, mis iseloomustas kohtuotsuse parlament *vs.* nõukogu ja komisjon eset.

64. Andmetöötluse rahvusvahelise ja riigisisese (ärilise ja eraõigusliku) mõõtme erineva kaalu tagajärjel osutus esimesel selle üldise huvi kaitseks, milleks on riigi julgeolek, sobivamaks liidu õigusest välistamise klausel. Teisel juhul seevastu sai seda sama huvi tõhusalt teenida direktiivi 2002/58 artikli 15 lõikes 1 ette nähtud piiramisklausliga.

65. Tuleks siiski hinnata veel ühte erinevust, mis on seotud erineva normatiivse kontekstiga: mõlemas nendes kohtuotsuses keskenduti kahe niisuguse sätte tõlgendamisele, mis lähemal vaatamisel ei ole võrdsed.

66. Nii võeti kohtuotsuses parlament *vs.* nõukogu ja komisjon seisukoht direktiivi 95/46 artikli 3 lõike 2 tõlgendamise suhtes, samas kui kohtuotsus Tele2 Sverige ja Watson tehti direktiivi 2002/58 artikli 1 lõike 3 kohta. Nende artiklite tähelepanelikul lugemisel ilmneb piisav erinevus selleks, et põhjendada Euroopa Kohtu otsuste erinevust kummalgi juhul.

<sup>33</sup> Prantsuse valitsuse kirjalike seisukohtade punktid 34–50.

<sup>34</sup> Kohtuotsus Tele2 Sverige ja Watson, punktid 103 ja 119.



67. Direktiivi 95/46 artikli 3 lõikes 2 on sätestatud, et „[k]äesolevat direktiivi *ei kohaldata isikuandmete töötlemise suhtes* [...] kui see toimub sellise tegevuse käigus, mis jääb väljapoole ühenduse õigust [...] ja igal juhul sellise *töötlemise* suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealhulgas riigi majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas“<sup>35</sup>.

68. Direktiivi 2002/58 artikli 1 lõikes 3 on omakorda märgitud, et seda direktiivi „*ei kohaldata tegevuse suhtes*, mis jääb väljapoole Euroopa Ühenduse asutamislepingu reguleerimisala [...] ja igal juhul *sellise tegevuse suhtes*, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (kaasa arvatud riigi majanduslik heaolu, kui *tegevus* on seotud riigi julgeolekuga) ja riigi sunnijõuga kriminaalõiguse valdkonnas“<sup>36</sup>.

69. Kui direktiivi 95/46 artikli 3 lõikega 2 on selle direktiivi kohaldamisalast välistatud *andmetöötlus*, mille eesmärk on – käesolevas asjas oluline – riigi julgeolek, siis direktiivi 2002/58 artikli 1 lõikega 3 on välistatud *tegevus*, mille eesmärk on – samuti käesolevas asjas oluline – riigi julgeoleku säilitamine.

70. Erinevus ei ole tähtsusetu. Direktiiv 95/46 jättis oma kohaldamisalast välja tegevuse („isikuandmete töötlemine“), mida igaüks võib teha. Sellest tegevusest olid konkreetselt välja arvatud töötlemised, mille ese oli muu hulgas riigi julgeolek. Seevastu ei omanud tähtsust selle *isiku* olemus, kes andmeid töötleb. Välja jäetud toimingute kindlaks tegemiseks järgitud käsitusviis oli seega teleoloogiline või eesmärgist lähtuv ning isikutel kui toimingute tegijatel ei tehtud vahet.

71. Seega on arusaadav, et kohtuasjas parlament *vs.* nõukogu ja komisjon lähtus Euroopa Kohus esmajoones andmete töötlemise eesmärgist. Ei olnud oluline see, „et kuna eraõiguslikud ettevõtjad kogusid [...] andmeid kommertseesmärgil ning just nemad korralda[si]d nende edastamist kolmandasse riiki“, kuna põhitähtis oli, et see „[e]dastamine toimu[s] sellises ametivõimude poolt loodud raamistikus, mille eesmärk o[li] tagada riigi julgeolek“<sup>37</sup>.

72. Seevastu kohtuasjas Tele2 Sverige ja Watson analüüsitud „tegevust, mille eesmärk on riigi julgeolek“, mis ei kuulu direktiivi 2002/58 kohaldamisalasse, ei saa eeldada iga isiku, vaid ainult riigi puhul. Lisaks ei kuulu selle hulka riigi normatiivsed või regulatiivsed funktsioonid, vaid rangelt avalike võimuorganite sisulised toimingud.

73. Direktiivi 2002/58 artikli 1 lõikes 3 loetletud tegevused nimelt „kujutavad endast igal juhul toiminguid, mis on iseloomulikud riigile või riigi ametiasutustele, ega ole omased eraõiguslike isikute tegevusvaldkondadele“<sup>38</sup>. Need „tegevused“ ei saa siiski olla normatiivset laadi. Kui see oleks nii, jääksid kõik isikuandmete töötlemisega seoses liikmesriikide poolt vastu võetud sätted direktiivi 2002/58 kohaldamisalast välja, kui neid püütaks vähegi põhjendada vajalikena riigi julgeoleku tagamiseks.

74. Ühelt poolt tähendaks see nimetatud direktiivi tõhususe märkimisväärset kadu, sest ainuüksi nii määramatu õigusmõiste nagu riigi julgeolek põhjenduseks toomisest piisaks selleks, et muuta kodanike isikuandmete kaitsmiseks ette nähtud liidu seadusandja kaitsemeetmed liikmesriikide suhtes mitte kohaldatavateks. Seda kaitse ei saa praktikas rakendada ilma liikmesriikide abita ja selle tagamine on kodanikele kindlustatud ka riikide võimuorganite ees.

<sup>35</sup> Kohtujuristi kursiiv.

<sup>36</sup> Kohtujuristi kursiiv.

<sup>37</sup> Parlament *vs.* nõukogu ja komisjon, punkt 58.

<sup>38</sup> Kohtuotsus Ministerio Fiscal, punkt 32. Samas mõttes kohtuotsus Tele2 Sverige ja Watson, punkt 72.



75. Teiselt poolt muudaks mõiste „riiklik tegevus“ niisugune tõlgendus, mis hõlmaks tegevust, mis väljendub normide ja õigusnormide väljakuulutamises, direktiivi 2002/58 artikli 15 sisutühjaks, sest selle artikliga just nimelt volitatakse liikmesriike – muu hulgas riigi julgeoleku kaitse põhjustel – võtma „seadusandlikke meetmeid“ selleks, et piirata samas direktiivis sätestatud õiguste ja kohustuste ulatust.<sup>39</sup>

76. Nagu Euroopa Kohus kohtuasjas Tele2 Sverige ja Watson rõhutas, tuleb „direktiivi 2002/58 kohaldamisala ulatust [...] tõlgendada eelkõige lähtuvalt selle direktiivi üldisest ülesehitusest“<sup>40</sup>. Sellest vaatevinklist on direktiivi 2002/58 artikli 1 lõike 3 ja artikli 15 lõike 1 tõlgendus, mis annab neile tähenduse nende tõhusust vähendamata, niisugune, milles tehakse esimese nimetatud sätetest tõlgendamisel kindlaks see, mis on liikmesriikide tegevusest riigi julgeoleku (ja samaväärses) valdkonnas sisuliselt välistatud, ja teise puhul õigus anda seadusandlikke meetmeid (s.t üldkohaldatavaid õigusnorme), mis riigi julgeoleku huvides mõjutavad üksikisikute tegevust, kes tegutsevad liikmesriikide sunnil, piirates direktiiviga 2002/58 tagatud õigusi.

#### 4. Riikliku julgeoleku välistamine direktiivis 2002/58

77. Riiklikku julgeolekut (või sünonüümiga väljendatud „riigi julgeolekut“), nagu on välja toodud direktiivi 2002/58 artikli 15 lõikes 1, on selles direktiivis arvesse võetud kahekordselt. Ühelt poolt on see liikmesriikide kõikide nende tegevuste, „mis on seotud“ riigi julgeolekuga, (selle direktiivi kohaldamisalast) *välja jätmise* alus. Teiselt poolt on see direktiiviga 2002/58 ette nähtud õiguste ja kohustuste *piiramise* aluseks, mis tuleb rakendada seadusega, s.t eraõigusliku või äritegevuse suhtes, mis ei ole seotud era- või äritegevusega, mis ei kuulu valitseja tegevuse valdkonda.<sup>41</sup>

78. Milliste tegevuste kohta direktiivi 2002/58 artikli 1 lõige 3 käib? Minu arvates toob Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) ise hea näite, nimetades sisejulgeoleku seadustiku artikleid L. 851-5 ja L. 851-6, milles on nimetatud „teabe kogumise tehnikaid, mida kasutab otseselt riik, kuid mis ei reguleeri elektroonilise side teenuste osutajate tegevust, pannes neile erikohustusi“<sup>42</sup>.

79. Usun, et siin ongi võti direktiivi 2002/58 artikli 1 lõikes 3 ette nähtud välistamise piiritlemiseks. Selle korda ei kohaldata *tegevuse* suhtes, mida teostavad riigi julgeoleku tagamiseks enda nimel avaliku võimu organid, nõudmata eraõiguslike isikute koostööd ja seega kehtestamata neile kohustusi nende ettevõtluse juhtimises.

80. Loetelu avaliku või organite tegevustest, mille puhul on tehtud isikuandmete töötlemise üldisest korrast erand, tuleb siiski tõlgendada kitsalt. Täpsemalt ei või mõistet „riigi julgeolek“, mis jääb vastavalt ELL artikli 4 lõikele 2 iga liikmesriigi ainuvastutusse, laiendada teistele sektoritele, mis on avalikule elule rohkem või vähem lähedased.

81. Kuna nendes eelotsuse küsimustes on tegemist eraõiguslike isikute (s.t kasutajatele elektroonilise side teenuseid osutavate isikute) kaasamisega, mitte üksnes riigiasutuste sekkumisega, ei ole vaja põhjalikult piiritleda mõistet „riiklik julgeolek“ otseses mõttes.

39 Oleks nimelt raske väita, et direktiivi 2002/58 artikli 15 lõige 1 võimaldab piirata õigusi ja kohustusi, mis on selle direktiiviga välja kuulutatud valdkonnas, mis on – nagu riigi julgeolek – selle direktiivi artikli 1 lõikega 3 põhimõtteliselt selle direktiivi kohaldamisalast välja jäetud. Nagu kinnitas Euroopa Kohus kohtuotsuses Tele2 Sverige ja Watson, punkt 73, eeldab direktiivi 2002/58 artikli 15 lõige 1 „tingimata, et selles nimetatud riigisisesed meetmed [...] kuuluvad selle direktiivi kohaldamisalasse, sest direktiiv lubab liikmesriikidel sõnaselgelt võtta neid meetmeid ainult seal ette nähtud tingimustel“.

40 Kohtuotsus Tele2 Sverige ja Watson, punkt 67.

41 Nagu märkis muuseas kohtujurist Saugmandsgaard Øe oma ettepanekus kohtuasjas Ministerio Fiscal (C-207/16, EU:C:2018:300, punkt 47): „segamini ei tohi ajada isikuandmeid, mida töödeldakse *otseselt* (avaliku võimu teostamise iseloomuga) riigi kriminaalõiguse valdkonda kuuluvate riigi sunnijõuga seotud tegevuste raames, ning andmeid, mida töödeldakse elektrooniliste sideteenuste osutaja (ärilise iseloomuga) tegevuste raames ja mida pädevad riigiasutused *hiljem* kasutavad“.

42 Kohtuasjas C-511/18 esitatud eelotsusetaotluse punktid 18 ja 21.

82. Leian siiski, et orientiiriks võib olla raamotsuses 2006/960/JSK<sup>43</sup>, mille artikli 2 punktis a eristatakse ühelt poolt õiguskaitseasutusi laias mõttes – mis on muu hulgas „riiklik politsei-, tolli- või mõni teine asutus, mida siseriiklike õigusaktidega on volitatud avastama, ennetama ja uurima süütegusid või kuritegelikkude tegevust ning kasutama oma volitusi ja võtma sunnimeetmeid selliste tegevuste puhul“ – ja teiselt poolt „asutusi või üksusi, mis tegelevad eelkõige riikliku julgeoleku küsimustega“, antud kriteerium<sup>44</sup>.

83. Direktiivi 2002/58 põhjenduses 11 on kinnitatud, et selles direktiivis „[n]agu direktiivis 95/46/EÜ, ei käsitleta ka käesolevas direktiivis põhiõiguste ja -vabaduste kaitsmist selliste toimingute puhul, mis ei kuulu [liidu] õiguse reguleerimisalasse“. Seega ei muuda direktiiv 2002/58 „senist tasakaalu üksikisiku eraelu puutumatus õiguse ja liikmesriikide võimaluse vahel võtta käesoleva direktiivi artikli 15 lõikes 1 osutatud meetmeid, mis on vajalikud [...] riigi julgeoleku [...] kaitse [...] seisukohast“.

84. Direktiiv 95/46 ja direktiiv 2002/58 on nimelt omavahel järjepidevad selles osas, mis puutub liikmesriikide pädevusaladesse riigi julgeoleku suhtes. Kummagi eesmärk ei ole kaitsta põhiõigusi selles konkreetnes valdkonnas, milles liikmesriikide tegevus ei „kuulu [liidu] õiguse reguleerimisalasse“.

85. Selles põhjenduses nimetatud „tasakaal“ tuleneb vajadusest järgida liikmesriikide pädevust riigi julgeoleku valdkonnas, kui nad teostavad pädevust *otse ja oma vahenditega*. Seevastu juhul, kui – isegi kui tegemist on samade riigi julgeoleku kaalutlustega – abiks on vaja eraõiguslikke isikuid, kellele pannakse teatavad kohustused, tähendab see sisenemist liidu õiguse reguleerimisalasse (eraelu puutumatus kaitse, mida nõutakse nendelt eraõiguslikelt isikutelt).

86. Nii direktiiv 95/46 kui ka direktiiv 2002/58 püüavad saavutada seda tasakaalu, lubades isikute õigusi piirata normatiivsete meetmete alusel, mille võtavad liikmesriigid vastavalt nende direktiivide artikli 13 lõike 1 ja artikli 15 lõike 1 alusel. Selles aspektis ei ole nende kahe direktiivi vahel mingit erinevust.

87. Mis puutub määrusesse 2016/679, millega on ette nähtud (uus) isikuandmete kaitse üldine raamistik, siis selle artikli 2 lõige 2 välistab selle määruse kohaldamise „isikuandmete töötlemisele“ liikmesriikide „sellise tegevuse käigus, mis kuulub EL lepingu V jaotise 2. peatüki kohaldamisalasse“.

88. Nii nagu direktiivis 95/46 oli isikuandmete töötlemine kvalifitseeritud ainult selle eesmärgi järgi, olenemata isikust, kes seda teeb, on määruses 2016/679 välistatud töötlemine identifitseeritud nii selle eesmärgi kui ka tegijate järgi: välja on jätetud töötlemine, mida liikmesriigid teevad niisuguse *tegevuse* teostamisel, mis ei kuulu liidu õiguse kohaldamisalasse (artikli 2 lõike 2 punktid a ja b), ja mida teostavad ametiasutused *süütegude vastu võitlemiseks ja kaitseks* avalikku julgeolekut ähvardavate ohtude eest.<sup>45</sup>

89. Need avaliku võimu tegevused tuleb tingimata kindlaks määrata kitsalt, vastasel korral kaotaksid liidu õigusnormid, mis käsitlevad eraelu puutumatus kaitset, oma soovitud toime. Määruse 2016/679 artiklis 23 on – samamoodi nagu direktiivi 2002/58 artikli 15 lõikes 1 – ette nähtud selles sätestatud õiguste ja kohustuste piiramine *seadusandlike meetmetega*, kui see on vajalik muude eesmärkide hulgas riigi julgeoleku, kaitse või avaliku julgeoleku tagamiseks. Jällegi, kui nende eesmärkide kaitset piisaks selleks, et see määraks määruse 2016/679 kohaldamisalast välja jätmise, siis oleks riigi julgeoleku toomine selle määrusega tagatud õiguste seadusandlike meetmetega piiramise põhjenduseks ülearune.

43 Nõukogu 18. detsembri 2006. aasta raamotsus Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jältusteabe vahetamise lihtsustamise kohta (ELT 2006, L 386, lk 89).

44 Samamoodi oli nõukogu 27. novembri 2008. aasta raamotsuse 2008/977/JSK kriminaalajajades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta (ELT 2008, L 350, lk 60) artikli 1 lõikes 4 ette nähtud, et [selle raamotsusega] „ei piirata riigi julgeoleku olulisi huve ega riigi julgeolekuga seotud luuretegevust“.

45 Määrus 2016/679 välistab nimelt andmetöötluse, mida teevad liikmesriigid niisuguse *tegevuse* teostamisel, mis ei kuulu liidu õiguse kohaldamisalasse, lisaks tegevusele, mida teostavad ametiasutused avaliku julgeoleku *kaitse eesmärkidel*.

90. Samamoodi nagu direktiivi 2002/58 puhul, ei oleks loogiline, et määruse 2016/679 (mis, ma kordan, lubab riikidel riigi julgeoleku kaalutlustel kodanike eraelu puutumatusse õigusi piirata) artiklis 23 ette nähtud seadusandlikud meetmed kuuluvad selle määruse kohaldamisalasse ja samal ajal, et riigi julgeoleku kaitse muudab määruse enda lihtsalt kohaldamatuks, mis tähendaks mis tahes subjektiivse õiguse mitte tunnustamist.

## **B. Tele2 Sverige ja Watsoni kohtupraktika kinnitamine ja selle arendamise võimalused**

91. Oma ettepanekus kohtuasjas C-520/18 analüüsin ma üksikasjalikult<sup>46</sup> Euroopa Kohtu praktikat selles valdkonnas, mille tulemusel teen ettepaneku seda kinnitada, soovitades samas mõnda tõlgendamisviisi selle sisu täpsustamiseks.

92. Viitan sellele analüüsile, mida ma ei pea tingimata vajalikuks lihtsalt aja kokkuvõtte mõttes praegu ära tuua. Minu järgnevat arutluskäiku Conseil d'État' (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) esitatud eelotsuse küsimuste kohta tuleb seega lugeda kohtuasjas C-520/18 esitatud ettepaneku vastavatest punktidest lähtudes.

## **C. Vastus eelotsuse küsimustele**

### ***1. Andmete säilitamise kohustus (esimene eelotsuse küsimus kohtuasjades C-511/18 ja C-512/18 ning teine eelotsuse küsimus kohtuasjas C-512/18)***

93. Mis puutub elektroonilise side teenuste osutajatele kehtestatud andmete säilitamise kohustusse, siis soovib eelotsusetaotluse esitanud kohus konkreetselt teada:

- kas see kohustus, mida tuleb täita direktiivi 2002/58 artikli 15 lõike 1 alusel, on riive, mis on põhjendatud harta artikliga 6 tagatud „õigusega julgeolekule“ ja riigi julgeoleku nõuetega (esimene küsimus kohtuasjades C-511/18 ja C-512/18 ning kolmas küsimus kohtuasjas C-511/18);
- kas direktiiviga 2000/31 on lubatud säilitada andmeid, mille järgi on võimalik tuvastada isikuid, kes on osalenud üldsusele kättesaadava veebisisu loomises (teine küsimus kohtuasjas C-512/18).

#### ***a) Sissejuhatav märkus***

94. Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) viitab harta artiklites 7 (era- ja perekonnaelu austamine), 8 (isikuandmete kaitse) ja 11 (sõna- ja teabevabadus) sätestatud põhiõigustele. Need on need põhiõigused, mida võib Euroopa Kohtu hinnangul kahjustada liiklusandmete säilitamise kohustus, mille panevad liikmesriikide ametiasutused elektroonilise side teenuste osutajatele.<sup>47</sup>

95. Eelotsusetaotluse esitanud kohus viitab ka harta artikliga 6 kaitstud õigusele turvalisusele. Enam kui õiguse, mida võidakse kahjustada, esitab ta selle pigem kui teguri, mis võib muuta selle kohustuse kehtestamise õiguspäraseks.

96. Nõustun komisjoniga, et artiklile 6 tuginemine nendel tingimustel võib olla eksitav. Leian niisamuti nagu komisjon, et seda sätet ei saa tõlgendada nii, et sellega saab „panna liidule positiivse kohustuse võtta meetmeid isikute kaitsmiseks kuritegude eest“<sup>48</sup>.

<sup>46</sup> Punktid 27–68.

<sup>47</sup> Nii tuleneb kohtuotsust Tele2 Sverige ja Watson, punkt 92, kus on analogia alusel viidatud kohtuotsusele Digital Rights, punktid 25 ja 70.

<sup>48</sup> Komisjoni kirjalike seisukohtade punkt 37.

97. Harta selle artikliga tagatud turvalisust ei samastata avaliku julgeolekuga. Või, kui eelistate, on selle viimasega seost sama palju nagu mis tahes muu põhiõigusega, kuna avalik julgeolek on põhiõiguste ja -vabaduste kasutamiseks tingimata vajalik eeltingimus.

98. Nagu komisjon meelde tuletab, vastab harta artikkel 6 Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni (edaspidi „EIÕK“) artiklile 5, nagu nähtub ka harta kohta antud selgitustest. EIÕK artiklist 5 nähtub, et „turvalisus“, mida selles kaitstakse, on kitsalt isiklik turvalisus, mida mõistetakse nii, et see tagab õiguse füüsilisele vabadusele meelevaldse vahistamise või kinnipidamise eest. Lõppkokkuvõttes turvalisus, et kelleltki ei või võtta vabadust, välja arvatud seaduses sätestatud juhtudel, nõuete kohaselt ja korras.

99. Tegemist on seega *isikliku turvalisusega*, mis puudutab tingimusi, mille korral võib isikute füüsilist vabadust piirata,<sup>49</sup> mitte *avaliku julgeolekuga*, mis on sisemiselt omane riigi olemasolule, mis on arenenud ühiskonnas tingimata vajalik eeltingimus selleks, et ühitada avalik-õiguslike volituste teostamine individuaalsete õiguste kasutamiseks.

100. Mõned valitsused paluvad siiski, et võetaks rohkem arvesse õigust turvalisusele teises nendest tähendustest. Tegelikult ei ole Euroopa Kohus seda eiranud, vaid on, veelgi enam, seda sõnaselgelt nimetanud oma kohtuotsustes<sup>50</sup> ja arvamustes<sup>51</sup>. Euroopa Kohus ei ole kunagi eitanud niisuguste üldise huvi eesmärkide tähtsust nagu riigi julgeolek ja avalik kord,<sup>52</sup> rahvusvahelise terrorismi vastu võitlemine rahvusvahelise rahu ja julgeoleku hoidmises ning raskete kuritegude vastu võitlemine avaliku julgeoleku tagamiseks,<sup>53</sup> mida ta on õigesti nimetaud „esmatähtsaks“<sup>54</sup>. Nagu ta tookord märkis, „aitab avaliku julgeoleku kaitse kaasa ka teiste isikute õiguste ja vabaduste kaitsmisele“<sup>55</sup>.

101. Võiks kasutada nende eelotsusetaotlustega antud võimalust, et teha selgemalt ettepanek leida tasakaal ühelt poolt õiguse turvalisusele ning teiselt poolt õiguse eraelu puutumatusel ja isikuandmete kaitsele vahel. Sellega saaks vältida kriitikat, et teisi soodustatakse esimese kahjuks.

102. Sellele tasakaalule viitavad minu arvates direktiivi 2002/58 põhjendus 11 ja artikli 15 lõige 1, kui seal on juttu meetmete vajalikkuse ja proportsionaalsuse nõuetest *demokraatlikus ühiskonnas*. Õigus turvalisusele, kordan, on olemuslik demokraatia olemasolule ja püsima jäämisele endale, mis õigustab seda, et seda õigust võetakse selle proportsionaalsuse hindamisel täielikult arvesse. Teisisõnu, kuigi andmete konfidentsiaalsuse põhimõtte kaitse on demokraatlikus ühiskonnas esmatähtis, ei tohi alahinnata ka selle ühiskonna turvalisust.

103. Riigi julgeolekut ähvardavate tõsiste ja püsivate ohtude konteksti, eelkõige terrorismi ohtu tuleb seega arvesse võtta, nagu on kinnitatud kohtuotsuse Tele2 Sverige ja Watson punkti 119 viimases lauses. Liikmesriigi süsteem võib vastata proportsionaalselt riiki ähvardavate ohtude olemusele ja intensiivsusele, ilma et see vastus peaks tingimata olema identne teiste liikmesriikide vastusega.

104. Pean lõpuks lisama, et eeltoodud mõttekäik ei takista seda, et otseses mõttes *erandlikes* olukordades, mida iseloomustab vahetu või erakorraline oht, mis õigustavad liikmesriigis ametlikku hädaolukorra väljakuulutamist, on riigisisestes õigusaktides ette nähtud võimalus kehtestada piiratud ajaks nii ulatuslik ja üldine andmete säilitamise kohustus, kui peetakse möödapääsmatult vajalikuks.<sup>56</sup>

49 Nii tõlgendab seda EIK. Muu hulgas 5. juuli 2016. aasta kohtuotsus Buzadji vs. Moldova Vabariik, ECHR:2016:0705JUD002375507, mille punktis 84 kinnitatakse, et EIÕK artikliga 5 tunnustatud põhiõiguse eesmärk on ära hoida meelevaldset või õigustamatut isikuvabaduse võtmist.

50 Kohtuotsus Digital Rights, punkt 42.

51 26. juuli 2017. aasta arvamus 1/15 (Kanada ja Euroopa Liidu vaheline broneeringuinfo leping) (edaspidi „arvamus 1/15“, EU:C:2017:592, punkt 149 ja seal viidatud kohtupraktika).

52 15. veebruari 2016. aasta kohtuotsus N. (C-601/15 PPU, EU:C:2016:84, punkt 53).

53 Kohtuotsus Digital Rights, punkt 42 ja seal viidatud kohtupraktika.

54 *Ibidem*, punkt 51.

55 Arvamus 1/15, punkt 149.

56 Vt kohtuasjas C-520/18 minu esitatud ettepaneku punktid 105–107.

105. Järelikult tuleb mõlema eelotsusetaotluse esimene küsimus ümber sõnastada nii, et see on esitatud pigem selle kohta, kas riivet on võimalik õigustada riigi julgeoleku kaalutlustega. Küsimus oleks seega selles, kas elektroonilise side teenuste operaatoritele kehtestatud kohustus on kooskõlas direktiivi 2002/58 artikli 15 lõikega 1.

## **b) Õiguslik hinnang**

### *1) Eelotsusetaotlustes esitatud riigisiseste õigusnormide iseloomustamine Euroopa Kohtu doktriini seisukohast*

106. Eelotsusemenetlustest nähtub, et põhikohtuasjades vaidlusalune õigusnorm paneb andmete säilitamise kohustuse:

- elektroonilise side operaatoritele ja eelkõige neile, kes pakuvad üldsusele juurdepääsu interneti sideteenustele; ja
- füüsilistele või juriidilistele isikutele, kes talletavad, isegi kui nad teevad seda tasuta, üldsusele kättesaadavaks tegemise eesmärgil nende teenuste adressaatide poolt edastatud mis tahes liiki signaale, tekste, helisid, pilte või sõnumeid.<sup>57</sup>

107. Operaatorid peavad säilitama üks aasta alates andmete salvestamise päevast teavet, millega saab kasutajat tuvastada, kasutatud terminali sideseadmete andmeid, iga kõne tehnilisi tunnuseid, nagu kuupäev, kellaaeg ja kestus, taotletud või kasutatud lisateenuste ja nende osutajate andmeid ning andmeid, mis võimaldavad tuvastada side adressaati ja telefonsidetegevuse korral side lähtepunkti ja asukohta.<sup>58</sup>

108. Näib, et konkreetselt internetiühenduse teenuste ja talletusteenuste puhul on riigisiseses õigusnormis nõutud IP-aadresside,<sup>59</sup> pöördusvõtmete ja, kui registreerumine toimub lepingu sõlmimise või maksekonto kaudu, tehtud makseviisi, samuti selle viitenumbri, summa, tehingu kuupäeva ja kellaaaja säilitamist<sup>60</sup>.

109. Seda säilitamiskohustust nõutakse kuritegude uurimiseks, tuvastamiseks ja nende eest vastutusele võtmiseks.<sup>61</sup> Täheleb, et erinevalt – nagu selgub – sellest, nagu see on liiklus- ja asukohaandmete kogumise kohustuse puhul, ei ole *andmete säilitamise* kohustuse ainus eesmärk terrorismi ennetamine.<sup>62</sup>

110. Mis puutub säilitatavatele andmetele *juurdepääsu* tingimustesse, siis nähtub kohtutoimiku teabest, et need tingimused on kas ühise korra puhul ette nähtud tingimused (õigusasutuse sekkumine) või siis on juurdepääs ainult eraldi nimetatud ja volitatud ametiisikutel sõltumatu haldusasutuse mittesiduva arvamuse alusel peaministri väljastatud loa alusel.<sup>63</sup>

57 Nii tuleneb sisejulgeoleku seadustiku artiklist L. 851-1, milles on viidatud posti- ja elektroonilise side seadustiku artiklile L. 34-1 ning usaldust digitaalmajanduses käsitleva seaduse nr 2004-575 artiklile 6.

58 Nii on see märgitud posti ja elektroonilise side seadustiku artiklis R. 10-13.

59 Seda asjaolu, mille suhtes väljendati kohtuistungil lahknevaid seisukohti, tuleb kontrollida eelotsusetaotluse esitanud kohtul.

60 Dekreedi nr 2011-219 artikkel 1.

61 Posti ja elektroonilise side seadustiku artikkel R. 10-13.

62 Nii La Quadrature du Net kui ka Fédération des fournisseurs d'accès à Internet associatifs rõhutavad nende eesmärkide suurt ulatust, mille jaoks andmeid säilitatakse, ametiasutustele antud kaalutusõigust, objektiivsete kriteeriumide puudumist selle määratlemisel ja nende kuritegevuse vormide olulisust, mida ei saa kvalifitseerida rasketeks.

63 Commission nationale de contrôle des techniques de renseignement (riiklik luuretehnikate kontrolli komisjon). Vt selle kohta Prantsuse valitsuse kirjalike seisukohtade punktid 145–148.



111. On lihtne märgata, et – nagu märkis komisjon<sup>64</sup> – andmed, mille säilitamist riigisiseste õigusnormidega nõutakse, vastavad sisuliselt andmetele, mida Euroopa Kohus analüüsis kohtuotsustes Digital Rights ning Tele2 Sverige ja Watson<sup>65</sup>. Samamoodi nagu tookord, on nende andmete suhtes kehtestatud „üldise ja vahet tegemata säilitamise kohustus“, nagu toob täiesti ausalt välja Conseil d’État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) oma eelotsuse küsimuste alguses.

112. Kui see on nii, mida peab lõpuks hindama eelotsusetaotluse esitanud kohus, siis tuleb vaid järeldada, et kõnealused õigusnormid kujutavad endast „harta artiklites 7 ja 8 ette nähtud põhiõiguste ulatusliku riive[t], mida tuleb pidada eriti raskeks“<sup>66</sup>.

113. Ükski esindatud pooltest ei ole seadnud kahtluse alla, et niisuguste tunnustega õigusnormid kujutavad nende õiguste riivet. Sellel aspektil ei ole vaja praegu peatuda, isegi mitte selleks, et meelde tuletada, et nende õiguste riive kahjustab paratamatult niisuguse ühiskonna aluseid, mis väidetavalt austab muude väärtuste hulgas isikliku eraelu puutumatumust, mida toetab harta.

114. Kohtuotsuses Tele2 Sverige ja Watson kehtestatud ja kohtuotsuses Ministerio Fiscal kinnitatud doktriini kohaldamisel tuleb loomulikult väita, et niisugused õigusnormid, nagu on siin vaidlusalused, „väljuvad [...] rangelt vajaliku piiridest ja demokraatlikus ühiskonnas ei saa neid lugeda põhjendatuks, nagu nõuab direktiivi 2002/58 artikli 15 lõige 1, tõlgendatuna harta artiklite 7, 8 ja 11 ning artikli 52 lõike 1 alusel“<sup>67</sup>.

115. Samamoodi nagu kohtuotsuses Tele2 Sverige ja Watson analüüsitud õigusnormid, hõlmavad ka need, millega on tegemist praegu, „üldiselt kõiki abonentide ja registreeritud kasutajaid ning kõiki elektroonilise side vahendeid ja liiklusandmeid [ega ei näe] ette mingeid taotletavast eesmärgist lähtuvaid eristamisi, piiranguid või erandeid“<sup>68</sup>. Järelikult „on need kohaldatavad ka isikutele, kelle kohta pole mingeid tõendeid, mille põhjal võiks arvata, et nende käitumisel oleks kas või kaudne või kaugel seos raskete kuritegudega“, ja seda ilma mingite eranditeta, „mistõttu on need kohaldatavad ka isikutele, kelle sideseansid kuuluvad liikmesriigi õiguse kohaselt ametisaladuse alla“<sup>69</sup>.

116. Samamoodi ei nõua vaidlusalused õigusnormid „mingi seose olemasolu säilitatavate andmete ja ohu vahel avalikule julgeolekule. Eelkõige ei piira need säilitamist andmetega, mis kuuluvad kindlasse ajavahemikku ja/või kindlasse geograafilisse piirkonda ja/või puudutavad teatavaid isikuid, kes võivad olla mingil viisil seotud raske kuriteoga, või isikutega, kelle andmete säilitamine võib muul põhjusel kaasa aidata raskete kuritegude ennetamisele, avastamisele või menetlemisele“<sup>70</sup>.

117. Eespool öeldust nähtub, et need õigusnormid „väljuvad seega rangelt vajaliku piiridest ja demokraatlikus ühiskonnas ei saa neid lugeda põhjendatuks, nagu nõuab direktiivi 2002/58 artikli 15 lõige 1, tõlgendatuna harta artiklite 7, 8 ja 11 ning artikli 52 lõike 1 alusel“<sup>71</sup>.

118. Eespool öeldust piisas selleks, et Euroopa Kohus järeldaks, et vastavad riigisisemed õigusnormid ei olnud direktiivi 2002/58 artikli 15 lõikega 1 kooskõlas, kuna nendes oli nähtud „kuritegevuse vastu võitlemise eesmärgil ette kõiki elektroonilise side vahendeid puudutav[...] kohustus[...] säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed“<sup>72</sup>.

64 Komisjoni kirjalike seisukohtade punkt 60.

65 Tegelikult lähevad need veidi kaugemale, sest näib, et nendes on ette nähtud internetiühenduse teenuste puhul IP-aadressi või pöördusvõtmete säilitamine.

66 Kohtuotsus Tele2 Sverige ja Watson, punkt 100.

67 *Ibidem*, punkt 107.

68 *Ibidem*, punkt 105.

69 *Loc. ult. cit.*

70 Kohtuotsus Tele2 Sverige ja Watson, punkt 106.

71 *Ibidem*, punkt 107.

72 *Ibidem*, punkt 112.



119. Küsimus, mis praegu tekib, on, kas Euroopa Kohtu praktikat isikuandmete säilitamise valdkonnas võib juhul, kui eesmärk, mida see „üldine ja vahet tegemata“ säilitamine teenib, on võitlemine terrorismi vastu, kui mitte ümber kujundada, siis vähemalt nüansseerida. Esimene küsimus kohtuasjas C-511/18 on sõnastatud just nimelt „olukorras, mida iseloomustavad tõsised ja pidevad ohud riigi julgeolekule, eelkõige terrorismioht“.

120. Kuna *faktilised asjaolud*, milles on andmete säilitamise kohustus kehtestatud, on aga sellised, ei ole selle normatiivne kontekst kindlasti seotud ainult terrorismiga. Conseil d'État' (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) menetluses olevas andmete säilitamise ja kasutamise korras on selle kohustuse tingimuseks seatud üldised kuritegude uurimise, tuvastamise ja nende eest vastutusele võtmise eesmärgid.

121. Igal juhul tuletan meelde, et terrorismivastane võitlus ei jäänud kohtuotsuse Tele2 Sverige ja Watson argumentidest välja, ilma et Euroopa Kohus oleks tookord leidnud, et selle kuritegevuse liigi tõttu oleks vaja tema doktriini kuidagi kohandada.<sup>73</sup>

122. Seepärast, ja põhimõtteliselt, leian ma, et eelotsusetaotluse esitanud kohtu küsimusele, mis keskendub terrorismiohu eripärale, tuleks vastata samas tähenduses, nagu otsustas Euroopa Kohus kohtuotsuses Tele2 Sverige ja Watson.

123. Nagu ma väitsin ettepanekus kohtuasjas Stichting Brein, „[õ]iguse kindel kohaldamine sunnib kohtuid, kui mitte kohaldama *stare decisis*'t absoluutses mõttes, siis kindlasti hoolikalt lähtuma sellest, mida nad on ise pärast põhjalikku kaalumist teatud konkreetse õigusprobleemi kohta otsustanud“<sup>74</sup>.

## 2) Piiratud andmete säilitamine riigi julgeolekut ähvardavate ohtude, sealhulgas terrorismiohu korral

124. Kas seda doktriini oleks siiski võimalik nüansseerida või täiendada, arvestades selle tagajärgi terrorismivastasele võitlusele või riigi kaitsesele muude sarnaste riigi julgeolekut ähvardavate ohtude vastu?

125. Rõhutasin juba, et ainult isikuandmete säilitamine tähendab harta artiklitega 7, 8 ja 11 tagatud õiguste riivet.<sup>75</sup> Sõltumata sellest, et lõppastmes tahetakse sellega võimaldada tagantjärele või samaaegset *juurdepääsu* andmetele kindlal ajahetkel,<sup>76</sup> tähendab juba ainuüksi andmete säilitamine side edastamiseks või teenuseosutaja osutatud teenuste eest arve esitamiseks rangelt vajalikku ületaval määral direktiivi 2002/58 artiklites 5 ja 6 ette nähtud piiride eiramist.

126. Nende teenuste kasutajatel (arenenumates ühiskondades tegelikult peaaegu kõik kodanikud) on või peab olema õiguspärane ootus, et ilma nende nõusolekuta ei säilitata rohkem nende andmeid kui need, mida talletatakse vastavalt nende säetetele. Direktiivi 2002/58 artikli 15 lõikes 1 sätestatud erandeid tuleb tõlgendada sellest eeldusest lähtudes.

<sup>73</sup> *Ibidem*, punkt 103.

<sup>74</sup> Kohtuasi C-527/15, EU:C:2016:938, punkt 41.

<sup>75</sup> Nagu Euroopa Kohus arvamuse 1/15 punktis 124 meelde tuletas, „kujutab isikuandmete edastamine kolmandale isikule, näiteks ametiasutusele, endast harta artikliga 7 tagatud põhiõiguse riivet, olenemata sellest, kuidas edastatud teavet hiljem kasutatakse. Sama kehtib isikuandmete säilitamise ning isikuandmetele juurdepääsu suhtes, mis antakse ametiasutustele, et nad saaksid andmeid kasutada. Sellega seoses ei ole oluline, kas asjassepuutuvad eraelulised andmed on delikaatsed või mitte või kas puudutatud isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi või mitte“.

<sup>76</sup> Nagu märkis kohtujurist Cruz Villalón kohtuasja Digital Rights, C-293/12 ja C-594/12 (EU:C:2013:845), ettepaneku punktis 72: „paljude selliste andmete kogumine ja eelkõige säilitamine hiigelsuurtes andmebaasides, mis tekivad või mida töödeldakse liidu kodanike suurema osa igapäevase elektroonilise side raames, kujutab endast nende eraelu selget riivet, kuigi see loob üksnes tingimused nende isikliku ja kutsealase tegevuse tagantjärele kontrollimise võimaldamiseks. Nende andmete kogumine loob sellise jälgimise tingimused, mis küll toimub nende kasutamisel tagantjärele, kuid mis siiski ohustab kogu nende säilitamise aja vältel alaliselt liidu kodanike õigust oma eraelu saladusele. Tekitavad üldlevinud tunne, et ollakse jälgimise all, tõstatab eriti teravalt andmete säilitamise kestuse küsimuse“.

127. Nagu ma juba selgitasin, ei pidanud Euroopa Kohus kohtuotsuses *Tele2 Sverige ja Watson* samuti seoses terrorismivastase võitlusega isikuandmete üldist ja vahet tegemata säilitamist õigeks.<sup>77</sup>

128. Saadud kriitikat arvestades ei usu ma, et selles kohtuotsuses sedastatud kohtupraktika alahindaks terrorismiohtu, kuna see on eriti raske kuritegevuse vorm, millel on otsene eesmärk hakata vastu riigi võimule ja selle institutsioonid ebastabiilseks muuta või hävitada. Terrorismivastane võitlus on otseses mõttes eluliselt tähtis riigi ja selle edu jaoks, üldise huvi eesmärk, mis on õigusriigi puhul vältimatu.

129. Praktiliselt kõik menetluses esindatud valitsused lisaks komisjonile märkisid üksmeelselt, et lisaks sellele, et osaline ja eristatud isikuandmete säilitamine tekitab tehnilisi raskusi, jätab see väidetavalt riigi luureteenistused ilma võimalusest kasutada andmeid, mis on tingimata vajalikud avalikku julgeolekut ja riigikaitset ähvardavate ohtude tuvastamiseks ning terrorismirünnakute toimepanijate vastutusele võtmiseks.<sup>78</sup>

130. Seda hinnangut arvestades on minu arvates oluline märkida, et terrorismivastast võitlus ei tule käsitleda ainult selle tõhususele mõeldes. Selles seisnebki selle raskus, aga ka selle suurusjärg, kui selle vahendid ja meetodid vastavad õigusriigi nõuetele, mis on eelkõige seada võimule ja jõule õiguslikud piirid ning konkreetselt allutada need õiguskorrale, mille olemasolu mõte ja eesmärk seisneb põhiõiguste kaitses.

131. Kui terrorismi puhul ei lähtu selle vahendite õigustatus muust kriteeriumist kui puhtast (ja maksimaalsest) rünnakute tõhususest kehtestatud korra vastu, siis õigusriigi puhul mõõdetakse tõhusust sellega, et selle kaitsel ei sallita niisuguste menetluste ja tagatiste piiramist, mis määratlevad õigusriiki kui õiguspärasest korda. Lastes endal minna lihtsalt üksnes tõhususe teed, kaotaks õigusriik staatuse, mis teda eristab, ja võiks äärmuslikel juhtudel ise muutuda kodaniku jaoks ähvardavaks ohuks. Miski ei võimaldaks tagada, et kui avalik võim on ennast süüteo eest vastutusele võtmiseks varustanud liialdatud vahenditega, millega ta võiks eirata või väärata põhiõigusi, võib tema kontrollimatu ja täiesti vaba tegutsemine lõpuks omandada sellised mõõtmed, mis on kõikide vabaduse kahjuks.

132. Kordan, et avaliku võimu tõhususele on ületamatuks tõkkeks kodanike põhiõigused, millele võib piiranguid seada, nagu on ette nähtud harta artikli 52 lõikes 1 ainult seadusega ja nende põhisisu järgides, „kui need [piirangud] on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi“.<sup>79</sup>

133. Tingimuste osas, mille korral oleks vastavalt kohtuotsusele *Tele2 Sverige ja Watson* lubatav *eesmärgipärane* andmete säilitamine, viitan oma ettepanekule kohtuasjas C-520/18<sup>80</sup>.

<sup>77</sup> Kohtuotsus *Tele2 Sverige ja Watson*, punkt 103: „ei saa [...] iseenesest õigustada, et riigisiseseid õigusnorme, mis näevad ette kohustuse säilitada üldiselt ja valimatult kõiki liiklusandmeid ja asukohaandmeid, võiks pidada selle võitluse jaoks vajalikuks“.

<sup>78</sup> Nii tõlgendab seda näiteks Prantsuse valitsus, kes illustreerib seda väidet konkreetsete näidetega andmete üldise säilitamise tarvilikkusest, mis võimaldas riigil reageerida rasketele terrorismirünnakutele, mille all on tema riik viimastel aastatel kannatanud (Prantsuse valitsuse kirjalike seisukohtade punktid 107 ja 122–126).

<sup>79</sup> 15. veebruari 2016. aasta kohtuotsus N. (C-601/15 PPU, EU:C:2016:84, punkt 50). Seega on tegemist avaliku korra ja vabaduse vahel keerulise tasakaalu leidmisega, mida ma juba nimetasin ja mille poole püüdlavad põhimõtteliselt kõik liidu õigusnormid. Selle näiteks on Euroopa Parlamendi ja nõukogu 15. märtsi 2017. aasta direktiiv (EL) 2017/541 terrorismivastase võitluse kohta, millega asendatakse nõukogu raamotsus 2002/475/JSK ning muudetakse nõukogu otsust 2005/671/JSK (ELT 2017, L 88, lk 6). Kuigi selle artikli 20 lõikes 1 on sätestatud, et liikmesriigid tagavad, et isikutele, kelle ülesanne on terrorismikuritegevuse uurimine või nende eest süüdistuse esitamine, „on kättesaadavad tulemuslikud uurimismeetmed“, on samas põhjenduses 21 avaldatud, et nende tõhusate vahendite kasutamine peab „olema sihipärane ja arvesse peaks võtma proportsionaalsuse põhimõtet ning uurimise all olevate kuritegevuse olemust ja raskusastet ning tuleks austada õigust isikuandmete kaitsel“.

<sup>80</sup> Punktid 87–95.

134. Asjaoludel, mille korral võimaldab kättesaadav teave õiguskaitseasutuste käes pidada põhjendatuks terrorismiatentaadi ettevalmistamise kahtlust, võib olla õiguspärane kehtestada kohustus teatavoid andmeid säilitada. Seda enam võib seda õigustada tegelik atentaadi toimepanek. Kui sellel viimasel juhul võib kuriteo toimepanemine iseenesest olla selle meetme võtmist õigustav asjaolu, siis ainuüksi võimaliku atentaadi kahtluse korral oleks vaja, et kahtluse aluseks olevad asjaolud viitaksid vähimalgi määral tõenäosusele, mis on tingimata vajalik nende näitajate objektiivseks kaalumiseks, mis võiksid seda õigustada.

135. Kuigi nii andmekategooriaid, mille säilitamist peetakse tingimata vajalikuks, kui ka asjaomaste isikute ringi on keeruline täpselt ja objektiivsete kriteeriumide alusel kindlaks määrata, ei ole see võimatu. Kindlasti oleks kõige *praktilisem ja tõhusam* üldiselt ja vahet tegemata säilitada nii palju andmeid, kui elektroonilise side teenuste osutajad kätte saavad, kuid ma juba märkisin, et seda küsimust ei saa lahendada mitte *praktilise tõhususe*, vaid *õigusliku tõhususe* seisukohast ja õigusriigi kontekstis.

136. See kindlaksmääramise töö on tüüpiliselt seadusandlik, Euroopa Kohtu praktikas määratud piirides. Viitan taas sellele, mida ma selle kohta esitan oma ettepanekus kohtuasjas C-520/18<sup>81</sup>.

### 3) Säilitatavatele andmetele juurdepääs

137. Seega, kui lähtuda eeldusest, et operaatorid on kogunud andmeid kooskõlas direktiivi 2002/58 sätetega ja nende säilitamine toimus artikli 15 lõike 1 alusel,<sup>82</sup> siis peab pädevate asutuste juurdepääs sellele teabele vastama niisugustele tingimustele, nagu seda on nõudnud Euroopa Kohus ja mida mina omakorda analüüsin oma ettepanekus kohtuasjas C-520/18, millele ma viitan<sup>83</sup>.

138. Seega tuleb ka käesoleval juhul liikmesriigi õigusnormides ette näha materiaal- ja menetlusõiguslikud tingimused, mis reguleerivad riigi pädevate asutuste juurdepääsu säilitatavatele andmetele.<sup>84</sup> Nende eelotsusetaotluste kontekstis on kõnealuste nõuetega lubatud kasutada niisuguste isikute andmeid, kelle puhul kahtlustatakse, et nad kavatsevad panna toime, panevad toime, on toime pannud terroriakti või võivad olla seotud terroriakti toime panemisega.<sup>85</sup>

139. Peamine on aga see, et – välja arvatud nõuetekohaselt põhjendatud kiireloomulistel juhtudel – kõnealuste andmetega tutvumine toimub kohtu või sõltumatu haldusasutuse eelneva kontrolli all, kelle otsusega vastatakse pädevate ametiasutuste põhjendatud taotlusele.<sup>86</sup> Seega on seal, kuhu abstraktne seaduse otsus ei ulatu, tagatud selle sõltumatu asutuse *konkreetne* otsus, kes tegutseb samamoodi riigi julgeoleku tagamise ja kodanike põhiõiguste kaitse nimel.

81 Punktid 100–107.

82 Eeldusel, et järgitakse kohtuotsuse Tele2 Sverige ja Watson punktis 122 nimetatud tingimusi: Euroopa Kohus meenutas, et direktiivi 2002/58 artikli 15 lõige 1 ei luba teha erandit artikli 4 lõigetest 1 ja 1a, mis nõuavad, et teenuseosutajad võtaksid meetmed, mis võimaldavad tagada säilitatavate andmete kaitse kuritarvitamise ohu ja ebaseadusliku juurdepääsu eest. Selle kohta tuvastas ta, et „[a]rvestades säilitatavate andmete hulka, delikaatsust ja neile ebaseaduslikult juurde pääsemise ohtu, peavad elektroonilise side teenuste osutajad, selleks et kindlustada säilitatavate andmete terviklikkus ja konfidentsiaalsus, tagama nende andmete eriti kõrgetasemelise kaitse ja turvalisuse, kasutades selleks sobivaid tehnilisi ja korralduslikke meetmeid. Täpsemalt peavad liikmesriigi õigusnormid nägema ette andmete säilitamise liidu territooriumil ja nende pöördumatu hävitamise pärast säilitamistähtaja lõppu“.

83 Punktid 52–60.

84 Kohtuotsus Tele2 Sverige ja Watson, punkt 118.

85 *Ibidem*, punkt 119.

86 *Ibidem*, punkt 120.

*4) Sisu autoreid tuvastada võimaldavate andmete säilitamise kohustus direktiivi 2000/31 seisukohast (teine eelotsuse küsimus kohtuasjas C-512/18)*

140. Eelotsusetaotluse esitanud kohus viitab direktiivile 2000/31 kui võrdluspunktile, millest lähtuvalt teha kindlaks, kas on võimalik kohustada teatavaid isikuid<sup>87</sup> ja operaatoreid, kes pakuvad üldsusele sideteenuseid, säilitama andmeid, „mis võimaldavad tuvastada kõik nende poolt osutatavate teenuste sisu või selle osa loomises osalenud isikud, et kohus saaks vajaduse korral nõuda nende andmete esitamist tsiviil- või karistusõiguslikku vastutust reguleerivate sätete kohaldamiseks“.

141. Nõustun komisjoniga selles, et oleks kohatu analüüsida selle kohustuse kooskõla direktiiviga 2000/31,<sup>88</sup> kuna selle direktiivi artikli 1 lõike 5 punktiga b on „direktiivide 95/46/EÜ ja 97/66/EÜ rakendusallas kuuluvate infoühiskonna teenustega seotud küsimus[ed]“ selle direktiivi kohaldamisalast välja jäetud; nendele õigusnormidele vastavad nüüd määrus 2006/679 ja direktiiv 2002/58,<sup>89</sup> mille vastavat artikli 23 lõige 1 ja artikli 15 lõiget 1 tuleb minu arvates tõlgendada nii, nagu on eespool selgitatud.

*2. Liiklus- ja asukohaandmete reaajas kogumise kohustus (teine eelotsuse küsimus kohtuasjas C-511/18)*

142. Eelotsusetaotluse esitanud kohus on seisukohal, et sisejulgeoleku seadustiku artikliga L. 851-2 on lubatud koguda reaajas teavet isikute kohta, kes on eelnevalt tuvastatud terrorismiohuga seotuses kahtlustatavatena, ainult terrorismi ennetamise eesmärkidel. Samamoodi on selle seadustiku artikliga L. 851-4 lubatud teenusepakujatel reaajas edastada lõppseadmete asukoha tehnilisi andmeid.

143. Eelotsusetaotluse esitanud kohtu sõnul ei pane need tehnikad teenuseosutajatele täiendavat säilitamiskohustust lisaks sellele, mida tal on vaja teenuste eest arvete esitamiseks ja oma teenuste turustamiseks.

144. Lisaks võib sisejulgeolekuseadustiku artikli L. 851-3 kohaselt elektroonilise side teenuse pakujatele ja tehniliste teenuste pakujatele panna kohustuse „rakendada oma võrkudes automatiseeritud andmetöötlusmeetmeid selleks, et tuvastada loas täpsustatud parameetrite alusel sideühendused, millest võib ilmneda terrorismioht“. See tehnika ei hõlma andmete üldist ja vahet tegemata säilitamist ning selle eesmärk on koguda piiratud aja jooksul neid ühendusandmeid, mis võivad olla seotud terroristliku kuriteoga.

145. Minu arvates tuleb säilitatud isikuandmetele juurdepääsuks nõutavaid tingimusi kohaldada ka elektroonilise side ajal loodavatele andmetele juurdepääsule reaajas. Ma viitan seega selle üksikasja kohta öeldule. Ei ole oluline, kas tegemist on säilitatavate andmetega või vahetult saadud andmetega, sest mõlemal juhul saadakse teada isikuandmeid, ilma et oleks tähtsust sellel, kas need on mineviku või praegused andmed.

146. Täpsemalt, kui reaajas juurdepääs on automaatse töötlemise käigus tuvastatud ühenduste tagajärg, nagu on sätestatud sisejulgeoleku seadustiku artiklis L. 851-3, siis peavad selle töötlemise kohta eelnevalt kehtestatud mudelid ja kriteeriumid olema konkreetsed, usaldusväärsed ja mittediskrimineerivad, nii et need võimaldavad tuvastada isikuid, kelle puhul võib mõistlikult kahtlustada, et nad osalevad terroristlikus tegevuses.<sup>90</sup>

<sup>87</sup> Need, kes „talletavad [...] üldkasutatavate interneti sideteenuste teel üldsusele kättesaadavaks tegemise eesmärgil nende teenuste adressaatide poolt edastatud mis tahes liiki signaale, tekste, pilte, helisid või sõnumeid [...]“.

<sup>88</sup> Seda direktiivi on eelotsusetaotluse esitanud kohus üldsõnaliselt ja konkreetseid sätteid täpsustamata nimetanud kohtuasja C-512/18 teises küsimuses.

<sup>89</sup> Komisjoni kirjalike seisukohtade punktid 112–113.

<sup>90</sup> Kohtuotsus Digital Rights, punkt 59.

### **3. Asjaomaste isikute teavitamise kohustus (kolmas eelotsuse küsimus kohtuasjas C-511/18)**

147. Euroopa Kohus on kinnitanud, et ametiasutused, kellele antakse juurdepääs andmetele, peavad asjaomaseid isikuid sellest asjaolust teavitama, tingimusel et see ei kahjusta pooleliolevaid uurimisi. Selle kohustuse põhjus tuleneb sellest, et nimetatud teavitamine on vajalik selleks, et need isikud saaksid nende õiguste rikkumise korral kasutada oma õigust tõhusale kohtulikule kaitsele, mis on sõnaselgelt sätestatud direktiivi 2002/58 artikli 15 lõikes 2.<sup>91</sup>

148. Conseil d'État (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) soovib kohtuasjas C-511/18 esitatud kolmanda küsimusega teada, kas see teavitamisnõue on igal juhul vältimatu või võib selle ära jätta, kui on ette nähtud muud tagatised, nagu on eelotsusetaotluses kirjeldatud.

149. Vastavalt eelotsusetaotluse esitanud kohtu selgitusele<sup>92</sup> seisnevad need tagatised selles, et nendel, kes soovivad kontrollida, kas luuretehnikat on rakendatud ebaseaduslikult, on võimalik pöörduda isiklikult Conseil d'État'sse (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu). See organ võib vajaduse korral meetme võtmise loa tühistada ja anda korralduse kogutud andmed hävitada menetluses, milles ei ole ette nähtud tavapärasest kohtumenetluste võistlevuse põhimõtet.

150. Eelotsusetaotluse esitanud kohus on seisukohal, et need õigusnormid ei riku õigust tõhusale kohtulikule kaitsele. Arvan siiski, et see võib olla teoreetiliselt lubatud isikute puhul, kes otsustavad kontrollida, kas nende suhtes toimub luureoperatsioon. Seevastu ei järgita seda õigust siis, kui isikuid, kelle suhtes see operatsioon toimub, sellest asjaolust ei hoiatata ja nad seega ei saa isegi välja selgitada, kas nende õigusi on rikutud või mitte.

151. Näib, et õiguslikud tagatised, millele eelotsusetaotluse esitanud kohus viitab, sõltuvad selle isiku algatusest, kes kahtlustab, et tema isiku kohta kogutakse teavet. Siiski peab oma õiguste kaitseks kohtusse pöördumise võimalus olema tõhus kõikide jaoks, mis tähendab, et isikul, kelle isikuandmeid on töödeldud, peab olema võimalus selle töötlemise õiguspärasust kohtus vaidlustada ja järelikult tuleb teda sellest töötlemisest teavitada.

152. Nagu esitatud teabest nähtub, võib kohtuasja algatada omal algatusel või halduskaebuse alusel, kuid igal juhul peab asjaomasel isikul olema võimalik seda ise algatada, milleks on vaja, et talle antaks teada, et tema isikuandmeid on teatud viisil töödeldud. Tema õiguste kaitset ei saa usaldada selle hooleks, et ta saab sellest töötlemisest teada kolmandatelt isikutelt või oma vahenditega.

153. Seega, kui ei kahjustata uurimiste käiku, mille jaoks on lubatud juurdepääs säilitatavatele andmetele, tuleb andmesubjektile sellest juurdepääsust teatada.

154. Teine asi on see, kui kohtumenetluses, mille asjaomane isik algatab pärast seda, kui teda on tema andmetele juurdepääsust teavitatud, järgitakse järgnevas kohtumenetluses konfidentsiaalsuse ja kaitsenõudeid, mis on omased järelevalvele avalike võimuorganite tegevuse suhtes niisugustes tundlikes valdkondades nagu riigi julgeolek ja riigikaitse. See küsimus ei ole siiski nende eelotsusetaotluste küsimus, nii et minu arvates ei ole Euroopa Kohtul vaja selles osas seisukohta võtta.

91 Kohtuotsus Tele2 Sverige ja Watson, punkt 121.

92 Eelotsusetaotluse punktid 8–11.

## V. Ettepanek

155. Esitatut arvestades teen Euroopa Kohtule ettepaneku vastata Conseil d'État'le (Prantsusmaa kõrgeima halduskohtuna tegutsev riiginõukogu) järgmiselt:

Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatus kaitset elektroonilise side sektoris (eraelu puutumatus ja elektroonilist sidet käsitlev direktiiv), artikli 15 lõiget 1 koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7, 8, 11 ja artikli 52 lõikega 1 tuleb tõlgendada nii, et:

1. sellega on vastuolus riigisisesed õigusnormid, millega pannakse olukorras, mida iseloomustavad tõsised ja pidevad ohud riigi julgeolekule, eelkõige terrorismioht, elektroonilise side teenuste operaatoritele ja teenuseosutajatele kohustus säilitada üldiselt ja vahet tegemata kõikide abonentide liiklus- ja asukohaandmed ning andmed, mis võimaldavad tuvastada nende teenuseosutajate pakutava sisu loojaid;
2. sellega on vastuolus riigisisesed õigusnormid, mis ei kehtesta kohustust teavitada asjaomaseid isikuid nende isikuandmete töötlemisest pädevate asutuste poolt, välja arvatud juhul, kui selline teatamine kahjustab nende ametiasutuste tegevust;
3. sellega ei ole vastuolus riigisisesed õigusnormid, mis võimaldavad reaalselt koguda konkreetse isiku liiklus- ja asukohaandmeid, kui sellised toimingud tehakse õiguspäraselt säilitatavate isikuandmetega tutvumiseks kehtestatud korras ja samade tagatistega.