Oikeustapauskokoelma

JULKISASIAMIEHEN RATKAISUEHDOTUS
MANUEL CAMPOS SÁNCHEZ-BORDONA
15 päivänä tammikuuta 2020[1]

Yhdistetyt asiat C-511/18 ja C-512/18

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

(Ennakkoratkaisupyyntö – Conseil d'État (ylin hallintotuomioistuin, Ranska))

Ennakkoratkaisupyyntö – Henkilötietojen käsittely ja yksityiselämän suoja sähköisen viestinnän alalla – Kansallisen turvallisuuden suojelu ja terrorismin torjunta – Direktiivi 2002/58/EY – Soveltamisala – 1 artiklan 3 kohta – 15 artiklan 3 kohta – SEU 4 artiklan 2 kohta – Euroopan unionin perusoikeuskirja – 6, 7, 8, 11 ja 47 artikla ja 52 artiklan 1 kohta – Yhteystietojen ja tietojen, joiden perusteella voidaan tunnistaa sisältöjen luojat, yleinen ja erotuksetta tapahtuva säilyttäminen – Liikenne- ja paikkatietojen keruu – Oikeus tietojen saantiin

1. Unionin tuomioistuin on viime vuosina kehittänyt henkilötietojen säilyttämistä ja saantia koskevaa vakiintunutta oikeuskäytäntöä, josta merkittävimpinä on mainittava seuraavat ratkaisut:

– 8.4.2014 annettu tuomio Digital Rights Ireland ym.,[2] jossa unionin tuomioistuin totesi direktiivin 2006/24/EY[3] pätemättömäksi, koska se mahdollisti suhteettoman puuttumisen Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 7 ja 8 artiklassa taattuihin oikeuksiin

– 21.12.2016 annettu tuomio Tele2 Sverige ja Watson ym.,[4] jossa se tulkitsi direktiivin 2002/58/EY[5] 15 artiklan 1 kohtaa

– 2.10.2018 annettu tuomio Ministerio Fiscal,[6] jossa se vahvisti tästä samasta direktiivin 2002/58 säännöksestä antamansa tulkinnan.

1 Alkuperäinen kieli: espanja.

2 C-293/12 ja C-594/12, EU:C:2014:238; jäljempänä tuomio Digital Rights.

3 Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annettu Euroopan parlamentin ja neuvoston direktiivi (EUVL 2006, L 105, s. 54).

4 C-203/15 ja C-698/15, EU:C:2016:970; jäljempänä tuomio Tele2 Sverige ja Watson.

5 Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12.7.2002 annettu Euroopan parlamentin ja neuvoston direktiivi (sähköisen viestinnän tietosuojadirektiivi) (EYVL 2002, L 201, s. 37).

6 C-207/16, EU:C:2018:788; jäljempänä tuomio Ministerio Fiscal.

2. Joidenkin jäsenvaltioiden viranomaiset ovat huolestuneet näistä ratkaisuista (ja erityisesti toiseksi mainitusta ratkaisusta), koska ne katsovat, että ne niiden seurauksena menettävät välineen, jota ne pitävät välttämättömänä kansallisen turvallisuuden suojelun ja rikollisuuden ja terrorismin torjunnan kannalta. Tämän vuoksi jotkin näistä jäsenvaltioista ovat vaatineet kyseisen oikeuskäytännön kumoamista tai ainakin sen nyansoimista.

3. Tietyt jäsenvaltioiden tuomioistuimet ovat ilmaisseet tämän saman huolen neljässä ennakkoratkaisupyynnössä [7], joista kaikista esitän ratkaisuehdotukseni tänä samana päivänä.

4. Kyseisissä neljässä ennakkoratkaisuasiassa nousee esiin etenkin kysymys siitä, sovelletaanko direktiiviä 2002/58 kansalliseen turvallisuuteen ja terrorismin torjuntaan liittyvään toimintaan. Jos tätä direktiiviä sovelletaan kyseisessä asiayhteydessä, on selvitettävä, miltä osin jäsenvaltiot voivat rajoittaa siinä taattuja yksityisyyden suojaa koskevia oikeuksia. Lopuksi on määritettävä, missä määrin kyseisten eri jäsenvaltioiden (Yhdistynyt kuningaskunta, [8] Belgia [9] ja Ranska [10]) asiaa koskevat kansalliset lainsäädännöt ovat unionin oikeuden mukaisia, sellaisena kuin unionin tuomioistuin on sitä tulkinnut.

I Asiaa koskevat oikeussäännöt

A Unionin oikeus

1. Direktiivi 2002/58

5. Direktiivin 2002/58 1 artiklassa (”Soveltamisala ja tavoite”) säädetään seuraavaa:

”1. Tässä direktiivissä säädetään sellaisten kansallisten säännösten yhdenmukaistamisesta, joita tarvitaan samantasoisen perusoikeuksien ja -vapauksien, erityisesti yksityisyyttä ja luottamuksellisuutta koskevan oikeuden, suojan varmistamiseksi henkilötietojen käsittelyssä sähköisen viestinnän alalla sekä tällaisten tietojen ja sähköisten viestintälaitteiden ja -palvelujen vapaan liikkuvuuden varmistamiseksi yhteisössä.

– –

3. Tätä direktiiviä ei sovelleta Euroopan yhteisön perustamissopimuksen soveltamisalan ulkopuolelle jääviin toimiin, kuten niihin, joita Euroopan unionista tehdyn sopimuksen V ja VI osasto koskee, eikä missään tapauksessa yleistä turvallisuutta, puolustusta ja valtion turvallisuutta (mukaan lukien valtion taloudellinen hyvinvointi, kun toimet liittyvät valtion turvallisuuteen) koskeviin toimiin eikä valtion toimiin rikosoikeuden alalla.”

6. Sen 3 artiklassa (”Palvelut”) säädetään seuraavaa:

”Tätä direktiiviä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa yhteisössä, mukaan luettuina tiedonkeruu- ja tunnistuslaitteita tukevat yleiset viestintäverkot.”

7 Nyt käsiteltävät kaksi asiaa (C-511/18 ja C-512/18) sekä asia C-623/17, Privacy International, ja asia C-520/18, Ordre des barreaux francophones et germanophone ym.

8 Asia Privacy International, C-623/17.

9 Asia Ordre des barreaux francophones et germanophone ym., C-520/18.

10 Asia La Quadrature du Net ym., C-511/18 ja C-512/18.

7. Direktiivin 5 artiklan (”Viestinnän luottamuksellisuus”) 1 kohdassa säädetään seuraavaa:

”Jäsenvaltioiden on kansallisella lainsäädännöllä varmistettava yleisen viestintäverkon ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus. Niiden on erityisesti kiellettävä se, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä liikennetietoja, jollei se ole laillisesti sallittua 15 artiklan 1 kohdan mukaisesti. Mitä tässä kohdassa säädetään, ei estä teknistä tallentamista, joka on tarpeen viestinnän välittämiselle, tämän rajoittamatta luottamuksellisuuden periaatteen soveltamista.”

8. Direktiivin 6 artiklassa (”Liikennetiedot”) säädetään seuraavaa:

”1. Tilaajia ja käyttäjiä koskevat liikennetiedot, jotka yleisen viestintäverkon tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja käsittelee ja tallentaa, on poistettava tai tehtävä nimettömiksi, kun niitä ei enää tarvita viestinnän välittämiseen, sanotun kuitenkaan rajoittamatta tämän artiklan 2, 3 ja 5 kohdan sekä 15 artiklan 1 kohdan soveltamista.

2. Tilaajalaskutusta ja yhteenliittämismaksuja varten tarvittavia liikennetietoja voidaan käsitellä. Tällainen käsittely on sallittua ainoastaan sen ajanjakson loppuun asti, jona lasku voidaan laillisesti riitauttaa tai maksu periä.”

9. Direktiivin 15 artiklan (”Direktiivin 95/46/EY[11] tiettyjen säännösten soveltaminen”) 1 kohdassa säädetään seuraavaa:

”Jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan tämän direktiivin 5 artiklassa, 6 artiklassa, 8 artiklan 1, 2, 3 ja 4 kohdassa sekä 9 artiklassa säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos tällaiset rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi direktiivin 95/46/EY 13 artiklan 1 kohdan mukaisesti. Tätä varten jäsenvaltiot voivat muun muassa hyväksyä lainsäädännöllisiä toimenpiteitä, joissa säädetään tietojen säilyttämisestä sellaiseksi rajoitetuksi ajaksi, joka on perusteltua tässä kohdassa säädetyistä syistä. Kaikkien tässä kohdassa tarkoitettujen toimenpiteiden on oltava yhteisön oikeuden yleisten periaatteiden mukaisia, mukaan lukien Euroopan unionista tehdyn sopimuksen 6 artiklan 1 ja 2 kohdassa tarkoitetut periaatteet.”

2. Direktiivi 2000/31/EY[12]

10. Direktiivin 2000/31 14 artiklassa säädetään seuraavaa:

”1. Jos tietoyhteiskunnan palvelun tarjoaminen käsittää palvelun vastaanottajan toimittamien tietojen tallentamisen, jäsenvaltioiden on varmistettava, että palvelun tarjoaja ei ole vastuussa palvelun vastaanottajan pyynnöstä tallennettujen tietojen osalta, edellyttäen, että:

– –

11 Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annettu Euroopan parlamentin ja neuvoston direktiivi (EYVL 1995, L 281, s. 31).

12 Tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista 8.6.2000 annettu Euroopan parlamentin ja neuvoston direktiivi (”Direktiivi sähköisestä kaupankäynnistä”) (EYVL 2000, L 178, s. 1).

3. Tämä artikla ei vaikuta tuomioistuimen tai hallintoviranomaisen mahdollisuuteen vaatia jäsenvaltioiden oikeusjärjestelmän mukaisesti palvelun tarjoajaa lopettamaan tai estämään väärinkäytökset, eikä se myöskään vaikuta jäsenvaltioiden mahdollisuuteen vahvistaa menettelyjä, joita sovelletaan tietojen poistamiseen tai niihin pääsyn estämiseen."

11. Direktiivin 15 artiklassa säädetään seuraavaa:

"1. Jäsenvaltiot eivät saa asettaa palvelun tarjoajille 12, 13 ja 14 artiklassa tarkoitettujen palvelujen toimittamisen osalta yleistä velvoitetta valvoa siirtämiään ja tallentamiaan tietoja eivätkä yleistä velvoitetta pyrkiä aktiivisesti saamaan selville laitonta toimintaa osoittavia tosiasioita tai olosuhteita.

2. Jäsenvaltiot voivat asettaa tietoyhteiskunnan palvelun tarjoajille velvoitteita ilmoittaa viipymättä toimivaltaisille viranomaisille kyseisen palvelun vastaanottajien väitetysti toteuttamista, laittomiksi väitetyistä toimista tai antamista väitetysti laittomista tiedoista taikka velvoitteen toimittaa toimivaltaisille viranomaisille näiden pyynnöstä tietoja, joiden avulla on mahdollista tunnistaa ne toimitetun palvelun vastaanottajat, joiden kanssa palvelun tarjoajat ovat tehneet tallentamista koskevan sopimuksen."

3. Asetus (EU) 2016/679[13]

12. Asetuksen 2016/679 2 artiklassa ("Aineellinen soveltamisala") säädetään seuraavaa:

"1. Tätä asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

2. Tätä asetusta ei sovelleta henkilötietojen käsittelyyn,

a) jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan;

b) jota suorittavat jäsenvaltiot toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa;

c) jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa;

d) jota toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten.

_ _"

13 Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston asetus (Yleinen tietosuoja-asetus) (EUVL 2016, L 119, s. 1).

13. Asetuksen 23 artiklan (”Rajoitukset”) 1 kohdassa säädetään seuraavaa:

”Rekisterinpitäjään tai henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan lainsäädäntötoimenpiteellä rajoittaa 12–22 artiklassa ja 34 artiklassa sekä 5 artiklassa, siltä osin kuin sen säännökset vastaavat 12–22 artiklassa säädettyjä oikeuksia ja velvollisuuksia, säädettyjen velvollisuuksien ja oikeuksien soveltamisalaa, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide, jotta voidaan taata

a) kansallinen turvallisuus;

b) puolustus;

c) yleinen turvallisuus;

d) rikosten ennalta estäminen, tutkinta, paljastaminen tai rikoksiin liittyvät syytetoimet taikka rikosoikeudellisten seuraamusten täytäntöönpano, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu tai tällaisten uhkien ehkäisy;

e) muut unionin tai jäsenvaltion yleiseen julkiseen etuun liittyvät tärkeät tavoitteet, erityisesti unionille tai jäsenvaltiolle tärkeä taloudellinen tai rahoituksellinen etu, mukaan lukien rahaan, talousarvioon ja verotukseen liittyvät asiat sekä kansanterveys ja sosiaaliturva;

f) oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen suojelu;

g) säänneltyä ammattitoimintaa koskevan ammattietiikan rikkomisen torjunta, tutkinta, selvittäminen ja syytteeseenpano;

h) valvonta-, tarkastus- tai sääntelytehtävä, joka satunnaisestikin liittyy julkisen vallan käyttöön a–e ja g alakohdassa tarkoitetuissa tapauksissa;

i) rekisteröidyn suojelu tai muille kuuluvat oikeudet ja vapaudet;

j) yksityisoikeudellisten kanteiden täytäntöönpano.”

14. Asetuksen 95 artiklassa (”Suhde direktiiviin 2002/58/EY”) säädetään seuraavaa:

”Tällä asetuksella ei aseteta luonnollisille henkilöille tai oikeushenkilöille lisävelvoitteita sellaisen käsittelyn osalta, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa unionissa, suhteessa sellaisiin seikkoihin, joiden osalta niiden on noudatettava direktiivissä 2002/58/EY säädettyjä erityisiä velvoitteita, joilla on sama tavoite.”

B Kansallinen oikeus

1. Sisäisestä turvallisuudesta annettu laki (Code de la sécurité intérieure)

15. Sisäisestä turvallisuudesta annetun lain L. 851-1 §:ssä säädetään seuraavaa:

”Tämän osan II osaston 1 luvussa säädetyin edellytyksin voidaan sallia, että sähköisen viestinnän operaattoreilta ja henkilöiltä, jotka on mainittu postitoiminnasta ja sähköisestä viestinnästä annetun lain [code des postes et des communications électroniques] L. 34-1 §:ssä, sekä henkilöiltä, jotka on mainittu luottamuksesta digitaalisessa taloudessa 21.6.2004 annetun lain nro 2004-575 [loi pour la

confiance dans l'économie numérique] 6 §:n I momentin 1 ja 2 kohdassa, kerätään niiden sähköisissä viestintäverkoissa tai -palveluissa käsittelemiä tai säilyttämiä tietoja tai asiakirjoja, mukaan lukien tekniset tiedot, jotka liittyvät sähköisten viestintäpalvelujen tilaaja- tai yhteysnumeroiden tunnistamiseen, yksilöidyn henkilön kaikkien tilaaja- tai yhteysnumeroiden kartoittamiseen, käytettyjen päätelaitteiden paikantamiseen sekä tietyn tilaajan osalta yhteydenottoihin tietyssä luettelossa oleviin numeroihin tai olevista numeroista sekä puhelujen kestoon ja ajankohtaan – –."

16. Sisäisestä turvallisuudesta annetun lain L. 851-2 ja L. 851-4 §:ssä järjestetään eri tarkoituksia varten ja eri sääntöjen mukaisesti hallinnollinen pääsy reaaliajassa tällä tavoin säilytettyihin yhteystietoihin.

17. Sisäisestä turvallisuudesta annetun lain L. 851-2 §:n säännöksillä sallitaan yksinomaan terrorismin estämistä varten L. 851-1 §:ssä tarkoitettujen tietojen tai asiakirjojen kerääminen samoilta henkilöiltä. Tämä keruu, joka koskee vain yhtä tai useampaa sellaista henkilöä, joiden on etukäteen todettu olevan mahdollisesti yhteydessä terrorismin uhkaan, tapahtuu reaaliajassa. Sama pätee saman lain L. 851-4 §:ään, jossa sallitaan se, että operaattorit lähettävät reaaliajassa vain teknisiä tietoja, jotka liittyvät päätelaitteiden sijaintiin.[14]

18. Sisäisestä turvallisuudesta annetun lain L. 851-3 §:n säännösten perusteella voidaan määrätä, että sähköisen viestinnän operaattoreiden ja teknisten palvelujen tarjoajien on "huolehdittava verkoissaan automaattisesta tietojenkäsittelystä, jonka avulla kyetään havaitsemaan luvassa täsmennettyjen tekijöiden perusteella yhteyksiä, jotka saattavat paljastaa terrorismin uhan".[15]

19. Sisäisestä turvallisuudesta annetun lain L. 851-5 §:ssä täsmennetään, että "sellaisen teknisen laitteen käyttäminen, joka mahdollistaa henkilön, ajoneuvon tai esineen paikantamisen reaaliajassa, voidaan sallia", jos tietyt edellytykset täyttyvät.

20. L. 851-6 §:n I momentin mukaan "rikoslain [code pénal] 226-3 §:n 1 momentissa mainitulla teknisellä laitteella voidaan kerätä – – suoraan teknisiä yhteystietoja, jotka mahdollistavat päätelaitteen tai sen käyttäjän tilaajanumeron tunnistamisen, sekä käytettyjen päätelaitteiden sijaintiin liittyviä tietoja", jos tietyt edellytykset täyttyvät.

2. Postitoiminnasta ja sähköisestä viestinnästä annettu laki (code des postes et des communications électroniques)

21. Postitoiminnasta ja sähköisestä viestinnästä annetun lain L. 34-1 §:ssä, sellaisena kuin sitä sovelletaan käsiteltävän asian tosiseikkoihin, säädetään seuraavaa:

"I. Tätä pykälää sovelletaan henkilötietojen käsittelyyn, jota suoritetaan tarjottaessa sähköisiä viestintäpalveluja yleisölle; sitä sovelletaan erityisesti sellaisiin sähköisiin viestintäverkkoihin, joissa voidaan käyttää tiedonkeruu- ja tunnistuslaitteita.

II. Sähköisen viestinnän operaattorien ja erityisesti henkilöiden, joiden toimintaan kuuluu tarjota yleisölle pääsy verkkoviestintäpalveluihin, on poistettava tai anonymisoitava kaikki liikennetiedot, sanotun kuitenkaan rajoittamatta III, IV, V ja VI momentin soveltamista.

Toimijoiden, jotka tarjoavat yleisölle sähköisiä viestintäpalveluja, on edellisen momentin mukaisesti otettava käyttöön sisäisiä menettelyjä, jotta ne voivat vastata toimivaltaisten viranomaisten pyyntöihin.

14 Ennakkoratkaisua pyytäneen tuomioistuimen mukaan näillä menetelmillä ei aseteta asianomaisille palveluntarjoajille ylimääräistä säilyttämisvaatimusta verrattuna siihen, mikä on välttämätöntä niiden palvelujen laskutusta, markkinointia ja lisäarvoa sisältävien palvelujen suorittamista varten.

15 Ennakkoratkaisua pyytäneen tuomioistuimen mukaan tällä menetelmällä, joka ei merkitse yleistä ja erotuksetta tapahtuvaa säilyttämistä, pyritään ainoastaan keräämään rajoitetun ajan kuluessa kaikista näiden henkilöiden käsittelemistä yhteystiedoista sellaiset, jotka saattavat liittyä tällaiseen vakavaan rikokseen.

Toimijoiden, joiden pää- tai sivutoimialana on tarjota, myös ilmaiseksi, yleisölle verkkoviestintää verkkoyhteyden kautta, on noudatettava sähköisen viestinnän operaattoreihin tämän pykälän nojalla sovellettavia säännöksiä.

III. Toimenpiteitä, joiden tarkoituksena on poistaa tai anonymisoida tietyt teknisten tietojen ryhmät, voidaan lykätä enintään vuoden ajaksi, jos se on tarpeen rikosten tai henkisestä omaisuudesta annetun lain [code de la propriété intellectuelle] L. 336-3 §:ssä määritellyn velvoitteen laiminlyönnin tutkintaan, toteamiseen ja syytteeseenpanoon liittyvistä syistä taikka siinä tarkoituksessa, että estetään rikoslain 323-1–323-3-1 §:ssä tarkoitetut rangaistaviksi säädetyt hyökkäykset tietojen automaattisiin käsittelyjärjestelmiin, ja yksinomaan siinä tarkoituksessa, että mahdollistetaan tarvittaessa näiden tietojen asettaminen oikeusviranomaisen tai henkisestä omaisuudesta annetun lain L. 331-12 §:ssä mainitun korkean viranomaisen taikka maanpuolustuslain [code de la défense] L. 2321-1 §:ssä mainitun tietojärjestelmien turvallisuudesta vastaavan kansallisen viranomaisen saataville. Nämä tietoryhmät ja tietojen säilyttämisen kesto määritetään Conseil d'État'n [ylin hallintotuomioistuin, Ranska] kuulemisen jälkeen päätöksellä, joka tehdään Commission nationale de l'informatique et des libertés'n [tietojenkäsittelyn ja vapauksien kansallinen komitea] antaman lausunnon perusteella, jäljempänä VI momentissa vahvistetuin rajoituksin operaattoreiden toiminnan ja viestien laadun mukaan sekä mahdollisesti niiden yksityiskohtaisten sääntöjen mukaan, jotka koskevat hyvityksiä yksilöitävissä olevista erityisistä lisäkustannuksista, joita operaattoreille syntyy niiden tällä perusteella valtion vaatimuksesta suorittamista palveluista.

– –

VI. Tiedot, joita säilytetään ja käsitellään edellä III, IV ja V momentissa mainituin edellytyksin, voivat koskea yksinomaan operaattorien tarjoamien palvelujen käyttäjien tunnistamista, operaattorien mahdollistaman viestinnän teknisiä ominaisuuksia ja päätelaitteiden sijaintia.

Tiedot eivät missään tapauksessa saa liittyä tämän viestinnän yhteydessä vaihdettujen viestien tai haettujen tietojen sisältöön, olivat ne missä muodossa tahansa.

Tietojen säilytyksessä ja käsittelyssä on noudatettava tietojenkäsittelystä, tiedostoista ja vapauksista 6.1.1978 annetun lain [loi relative à l'informatique, aux fichiers et aux libertés] nro 78-17 säännöksiä.

Operaattorien on toteutettava kaikki toimenpiteet sen varmistamiseksi, että näitä tietoja ei käytetä muihin kuin tässä pykälässä säädettyihin tarkoituksiin."

22. Saman lain R. 10-13 §:n I momentin mukaan operaattorien on säilytettävä rikosten tutkintaa, toteamista ja syytteeseenpanoa varten seuraavat tiedot:

"a) tiedot, joiden perusteella käyttäjä voidaan tunnistaa

b) sähköisessä viestinnässä käytettyjä päätelaitteita koskevat tiedot

c) kunkin viestinnän tekniset ominaisuudet sekä päivämäärä, kellonaika ja kesto

d) tilattuja tai käytettyjä lisäpalveluja ja niiden tarjoajia koskevat tiedot

e) tiedot, joiden perusteella viestinnän vastaanottaja tai vastaanottajat kyetään tunnistamaan".

23. Saman pykälän II momentin mukaan operaattorin on puhelintoimintojen tapauksessa säilytettävä myös tiedot, jotka mahdollistavat puhelun alkuperän tunnistamisen ja sen paikantamisen.

24. Saman pykälän III momentin mukaan kyseisiä tietoja on säilytettävä vuoden ajan niiden tallennuspäivästä lukien.

3. Luottamuksesta digitaalisessa taloudessa 21.6.2004 annettu laki nro 2004-575 (loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)

25. Lain 2004-575 6 §:n II momentin 1 kohdassa säädetään, että henkilöt, joiden toimintaan kuuluu tarjota yleisölle pääsy verkkoviestintäpalveluihin, ja luonnolliset henkilöt ja oikeushenkilöt, jotka tarjoavat, myös ilmaiseksi, yleisölle verkkoviestintäpalvelujen kautta näiden palvelujen vastaanottajien toimittamien minkä tahansa merkkien, kirjoitusten, kuvien, äänien tai viestien tallennusta, ovat velvollisia ”pitämään hallussaan ja säilyttämään tiedot, joiden perusteella kyetään tunnistamaan kuka tahansa henkilö, joka on ollut osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä”.

26. Saman pykälän II momentin 3 kohdassa säädetään, että oikeusviranomainen voi velvoittaa nämä henkilöt ilmoittamaan sen 1 kohdassa mainitut tiedot.

27. Saman pykälän II momentin viimeisen kohdan mukaan ”1 kohdassa mainitut tiedot määritellään ja niiden säilytysaika ja säilyttämistavat vahvistetaan” Conseil d'État'n kuulemisen jälkeen annetulla asetuksella. [16]

II Tosiseikat ja ennakkoratkaisukysymykset

A Asia C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net ja Fédération des fournisseurs d'accès à internet associatifs (jäljempänä kantajat) vaativat Conseil d'État'ta kumoamaan useita sisäisestä turvallisuudesta annetun lain säännösten täytäntöön panemiseksi annettuja asetuksia. [17]

29. Tiivistettynä kantajat väittivät, että sekä riidanalaisilla asetuksilla että kyseessä olevilla sisäisestä turvallisuudesta annetun lain säännöksillä loukataan perusoikeuskirjan 7 taattua oikeutta yksityiselämään, sen 8 artiklassa taattua oikeutta henkilötietojen suojaan ja sen 47 artiklassa taattua oikeutta tehokkaisiin oikeussuojakeinoihin.

16 Näiden määrittelystä säädettiin sellaisten tietojen, jotka mahdollistavat kaikkien verkkoon ladatun sisällön luomiseen osallistuneiden henkilöiden tunnistamisen, säilyttämisestä ja toimittamisesta 25.2.2011 annetulla asetuksella nro 2011-219 (décret n.º 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). Kyseisestä asetuksesta on mainittava seuraavat säännökset: a) 1 §:n 1 momentti, jonka mukaan henkilöiden, jotka tarjoavat pääsyä verkkoviestintäpalveluihin, on säilytettävä seuraavat tiedot: yhteyden tunnistenumero, tilaajan tunnistenumero, yhteyden muodostukseen käytetyn päätelaitteen tunnistenumero, yhteyden alkamisen ja päättymisen päivämäärä ja kellonaika, tilaajayhteyden ominaisuudet; b) 1 §:n 2 momentin mukaan henkilöiden, jotka tarjoavat, myös ilmaiseksi, yleisölle verkkoviestintäpalvelujen kautta näiden palvelujen vastaanottajien toimittamien minkä tahansa merkkien, tekstien, kuvien, äänien tai viestien tallennusta, on säilytettävä kustakin tallennusoperaatiosta seuraavat tiedot: viestinnän aloittajan yhteystunniste, operaation kohteena olevan sisällön tunnistenumero, palveluun yhdistämisessä ja sisältöjen siirrossa käytetyt yhteyskäytännöt, operaation luonne, operaation päivämäärä ja kellonaika, operaation suorittajan käyttämä tunnistenumero; ja c) 1 §:n 3 momentissa säädetään, että edellisissä momenteissa mainittujen henkilöiden on säilytettävä seuraavat tiedot, jotka käyttäjä antaa sopimuksen tekemisen tai tilin luonnin yhteydessä: tilin luonnissa käytetyn yhteyden tunnistenumero; etunimi ja sukunimi tai toiminimi; postiosoite, käytetyt salanimet, sähköpostiosoitteet tai tilinumerot, puhelinnumerot, päivitetty salasana ja tiedot, joiden perusteella sitä voidaan tarkistaa tai muuttaa.

17 Niiden riitauttamat asetukset olivat seuraavat: a) erikoistuneiden tietopalvelujen nimeämisestä 28.9.2015 annettu asetus nro 2015-1185 (décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement); b) luvanvaraisten tietotekniikoiden soveltamisesta ja valtion turvallisuuteen vaikuttavista tiedostoista 1.10.2015 annettu asetus nro 2015-1211 (décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État); c) niiden palvelujen nimeämisestä, joilla on lupa käyttää sisäisestä turvallisuudesta annetun lain VIII osan V luvussa mainittuja tekniikoita ja jotka eivät ole erikoistuneita tietopalveluja, 11.12.2015 annettu asetus nro 2015-1639 (décret n.º 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 libre VIII du code de la sécurité intérieure) ja d) tiedonkeruutekniikoista 29.1.2016 annettu asetus nro 2016-67 (décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement).

30. Tässä tilanteessa Conseil d'État on esittänyt unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”1) Voidaanko – – direktiivin 2002/58 15 artiklan 1 kohdan sallivien säännösten nojalla asetettua yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevaa velvoitetta pitää asiayhteydessä, jolle ovat ominaisia vakavat ja jatkuvat uhat kansalliselle turvallisuudelle ja erityisesti terrorismin vaara, puuttumisena, joka on perusteltavissa – – perusoikeuskirjan 6 artiklassa taatulla oikeudella turvallisuuteen ja kansallisen turvallisuuden vaatimuksilla, joita koskeva vastuu kuuluu yksinomaan jäsenvaltioille SEU 4 artiklan nojalla?

2) Onko – – direktiiviä 2002/58, luettuna – – perusoikeuskirjan valossa, tulkittava siten, että siinä sallitaan lainsäädäntötoimet, kuten tiettyjen sellaisten henkilöiden liikenne- ja paikkatietojen kerääminen reaaliajassa, jotka vaikuttavat sähköisen viestintäpalvelun tarjoajien oikeuksiin ja velvollisuuksiin mutta joilla ei kuitenkaan aseteta niille erityistä velvollisuutta tietojen säilyttämiseen?

3) Onko – – direktiiviä 2002/58, luettuna – – perusoikeuskirjan valossa, tulkittava siten, että yhteystietojen keruuta koskevien menettelyjen sääntöjenmukaisuus edellyttää kaikissa tapauksissa sitä, että asianomaisille henkilöille ilmoitetaan asiasta, kun tällainen ilmoitus ei voi enää vaarantaa toimivaltaisten viranomaisten tutkimuksia, vai voidaanko tällaisia menettelyjä pitää sääntöjenmukaisina, kun otetaan huomioon kaikki muut olemassa olevat menettelylliset takeet, joissa varmistetaan muutoksenhakua koskevan oikeuden tehokkuus?”

B Asia C-512/18

31. Asian C-511/18 kantajat Igwan.netiä lukuun ottamatta vaativat myös, että Conseil d'État kumoaa (implisiittisen) hallinnollisen päätöksen, jolla hylättiin kantajien vaatimus postitoiminnasta ja sähköisestä viestinnästä annetun lain R. 10-13 §:n ja 25.2.2011 annetun asetuksen nro 2011-219 kumoamisesta.

32. Kantajien mukaan riidanalaisilla säännöksillä asetetaan liikenne-, paikka- ja yhteystietojen säilyttämistä koskeva velvoite, joka yleisen luonteensa vuoksi loukkaa suhteettomasti perusoikeuskirjan 7, 8 ja 11 artiklassa suojattuja oikeuksia yksityis- ja perhe-elämään, henkilötietojen suojaan ja sananvapauteen ja on direktiivin 2002/58 15 artiklan 1 kohdan vastainen.

33. Kyseisessä asiassa Conseil d'État esitti seuraavat ennakkoratkaisukysymykset:

”1) Voidaanko – – direktiivin 2002/58 15 artiklan 1 kohdan sallivien säännösten nojalla asetettua yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevaa velvoitetta pitää, kun otetaan huomioon erityisesti takeet ja valvonta, joita näiden yhteystietojen keruuseen ja käyttöön liittyy, puuttumisena, joka on perusteltavissa – – perusoikeuskirjan 6 artiklassa taatulla oikeudella turvallisuuteen ja kansallisen turvallisuuden vaatimuksilla, joita koskeva vastuu kuuluu yksinomaan jäsenvaltioille SEU 4 artiklan nojalla?

2) Onko – – direktiivin 2000/31 säännöksiä, luettuina yhdessä – – perusoikeuskirjan 6, 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan kanssa, tulkittava siten, että niissä sallitaan se, että valtio antaa kansallista lainsäädäntöä, jolla velvoitetaan henkilöt, joiden toimintaan kuuluu tarjota yleisölle pääsy verkkoviestintäpalveluihin, ja luonnolliset henkilöt tai oikeushenkilöt, jotka tarjoavat, myös ilmaiseksi, yleisölle verkkoviestintäpalvelujen kautta näiden palvelujen vastaanottajien toimittamien minkä tahansa merkkien, kirjoitusten, kuvien, äänien tai viestien säilytystä, säilyttämään tiedot, joiden perusteella kyetään tunnistamaan kuka tahansa henkilö, joka on ollut

osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä, jotta lainkäyttöviranomainen voi tarvittaessa pyytää niiden toimittamista siviili- tai rikosvastuuta koskevien sääntöjen noudattamisen varmistamiseksi?”

III Asian käsittely unionin tuomioistuimessa ja asianosaisten lausumat

34. Ennakkoratkaisupyynnöt saapuivat unionin tuomioistuimen kirjaamoon 3.8.2018.

35. Kirjallisia huomautuksia ovat esittäneet La Quadrature du Net, Fédération des fournisseurs d’accès à Internet associatifs, French Data Network, Saksan, Belgian, Yhdistyneen kuningaskunnan, Tšekin, Kyproksen, Tanskan, Espanjan, Viron, Ranskan, Unkarin, Irlannin, Puolan ja Ruotsin hallitukset sekä Euroopan komissio.

36. Nyt käsiteltäville asioille ja asioille C-623/17, Privacy International, ja C-520/18, Ordre des barreaux francophones et germanophone ym., 9.9.2019 pidettyyn yhteiseen istuntoon osallistuivat näiden neljän asian asianosaiset, edellä mainittujen jäsenvaltioiden ja Alankomaiden ja Norjan hallitukset sekä komissio ja Euroopan tietosuojavaltuutettu.

IV Asian tarkastelu

37. Conseil d’État’n esittämät ennakkoratkaisukysymykset voidaan jakaa seuraaviin kolmeen ryhmään:

– Ensinnäkin, voidaanko unionin oikeuden mukaisena pitää kansallista lainsäädäntöä, jossa sähköisten viestintäpalvelujen tarjoajat velvoitetaan yleisesti ja erotuksetta säilyttämään yhteystiedot (asioissa C-511/18 ja C-512/18 esitetty ensimmäinen ennakkoratkaisukysymys) ja erityisesti tiedot, joiden perusteella kyetään tunnistamaan palveluntarjoajien tarjoamien sisältöjen luomiseen osallistuneet henkilöt (asiassa C-512/18 esitetty toinen ennakkoratkaisukysymys)?

– Toiseksi, edellyttääkö yhteystietojen keruuta koskevien menettelyjen sääntöjenmukaisuus kaikissa tapauksissa sitä, että asianomaisille henkilöille ilmoitetaan asiasta, kun tällainen ilmoitus ei voi enää vaarantaa tutkimuksia (asiassa C-511/18 esitetty kolmas ennakkoratkaisukysymys)?

– Kolmanneksi, onko liikenne- ja paikkatietojen kerääminen reaaliajassa asettamatta kuitenkaan velvollisuutta näiden tietojen säilyttämiseen direktiivin 2002/58 mukaista, ja jos on, millaisin edellytyksin (asiassa C-511/18 esitetty toinen ennakkoratkaisukysymys)?

38. Käsiteltävissä asioissa on lopulta määriteltävä, voidaanko unionin oikeuden mukaisena pitää kansallista lainsäädäntöä, jossa sähköisten viestintäpalvelujen tarjoajille asetetaan kahdenlaisia velvoitteita, jotka koskevat a) yhtäältä tiettyjen tietojen *keräämistä* mutta eivät niiden säilyttämistä; b) toisaalta yhteystietojen ja tietojen, joiden perusteella kyetään tunnistamaan henkilöt, jotka ovat osallistuneet tarjottujen palvelujen sisällön luomiseen, *säilyttämistä*.

39. Ensin on kuitenkin selvitettävä, tuleeko direktiivi 2002/58 sovellettavaksi nimenomaan sen asiayhteyden [18] vuoksi, jossa tämä kansallinen lainsäädäntö on annettu (tilanteessa, jossa kansallinen turvallisuus voi vaarantua).

18 ”Asiayhteys, jolle ovat ominaisia vakavat ja jatkuvat uhat kansalliselle turvallisuudelle ja erityisesti terrorismin vaara”, kuten asiassa C-511/18 esitetyssä ensimmäisessä ennakkoratkaisukysymyksessä täsmennetään.

A Direktiivin 2002/58 sovellettavuus

40. Ennakkoratkaisua pyytänyt tuomioistuin pitää selvänä, että riidanalainen lainsäädäntö kuuluu direktiivin 2002/58 soveltamisalaan. Sen mukaan tämä ilmenee tuomioon Tele2 Sverige ja Watson perustuvasta oikeuskäytännöstä, joka vahvistettiin tuomiossa Ministerio Fiscal.

41. Tietyt ennakkoratkaisumenettelyyn osallistuneet hallitukset sitä vastoin väittävät, että riidanalainen lainsäädäntö ei kuulu kyseisen direktiivin soveltamisalaan. Näkemyksensä tueksi ne vetoavat muiden perustelujen ohella 30.5.2006 annettuun tuomioon parlamentti v. neuvosto ja komissio.[19]

42. Olen Conseil d'État'n kanssa samaa mieltä siitä, että riidan tämä osa on jo ratkaistu tuomiolla Tele2 Sverige ja Watson, jossa vahvistettiin, että direktiiviä 2002/58 on lähtökohtaisesti sovellettava tilanteessa, jossa sähköisten palvelujen tarjoajien on lain nojalla säilytettävä tilaajiaan koskevat tiedot ja sallittava viranomaisille pääsy näihin tietoihin. Tätä näkemystä ei muuta se, että nämä velvoitteet määrätään palveluntarjoajille kansalliseen turvallisuuteen liittyvistä syistä.

43. Huomautan jo tässä vaiheessa, että jos tuomion Tele2 Sverige ja Watson ja sitä edeltäneiden tuomioiden välillä ilmenee ristiriitaa, on ensisijaisena pidettävä ensin mainittua tuomiota, koska se on annettu viimeiseksi ja vahvistettu tuomiossa Ministerio Fiscal. Nähdäkseni mitään ristiriitaa ei kuitenkaan ole, kuten jäljempänä selitän.

1. Tuomio parlamentti v. neuvosto ja komissio

44. Tuomiolla parlamentti v. neuvosto ja komissio ratkaistuissa asioissa oli kyse

– lentoyhtiöiden PNR-tietojen (Passenger Name Records, matkustajarekisteritiedot) käsittelemistä ja siirtämistä Yhdysvaltojen viranomaisille koskevasta Euroopan yhteisön ja Amerikan yhdysvaltojen välisestä sopimuksesta[20]

– Yhdysvaltojen viranomaisille toimitettavien lentomatkustajia koskevaan matkustajarekisteriin sisältyvien henkilötietojen suojan riittävästä tasosta.[21]

45. Mainitun tuomion mukaan tietojen siirto oli käsittelyä, joka koski yleistä turvallisuutta ja rikosoikeuden alalla tapahtuvaa valtion toimintaa. Direktiivin 95/46 3 artiklan 2 kohdan ensimmäisen luetelmakohdan perusteella riidanalaiset päätökset eivät kuuluneet direktiivin 95/46 soveltamisalaan.

46. Lentoyhtiöt olivat alun perin keränneet nämä tiedot unionin oikeuden alaan kuuluvan toiminnan – lentolippujen myynnin – yhteydessä. Riidanalainen päätös ei kuitenkaan koskenut tietojen käsittelyä, joka "oli tarpeen palvelujen tarjoamiseksi, vaan se koski tietojen käsittelyä, jota pidettiin tarpeellisena yleisen turvallisuuden suojelemiseksi ja lainvalvontatarkoituksia varten"[22].

19 C-317/04 ja C-318/04, EU:C:2006:346; jäljempänä tuomio parlamentti v. neuvosto ja komissio.

20 Lentoyhtiöiden PNR-tietojen käsittelemistä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriön alaiselle tulli- ja rajavalvontalaitokselle koskevan Euroopan yhteisön ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä 17.5.2004 tehty neuvoston päätös 2004/496/EY (EUVL 2004, L 183, s. 83; oikaisu EUVL 2005, L 255, s. 168) (asia C-317/04).

21 Yhdysvaltojen tulli- ja rajavartiolaitokselle toimitettavien lentomatkustajia koskevaan matkustajarekisteriin sisältyvien henkilötietojen suojan riittävästä tasosta 14.5.2004 tehty komission päätös 2004/535/EY (EUVL 2004, L 235, s. 11) (asia C-318/04).

22 Tuomio parlamentti v. neuvosto ja komissio, kohta 57. Sen 58 kohdassa korostetaan, että "siitä, että yksityiset toimijat ovat keränneet – – tiedot kaupalliseen tarkoitukseen ja että ne järjestävät kyseisten tietojen siirron kolmanteen valtioon", ei kuitenkaan seuraa, että kyseessä oleva siirto ei olisi yksi niistä direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa mainituista tapauksista, joissa direktiiviä ei sovelleta, koska "tämä siirto tapahtuu julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen".

47. Mainitussa tuomiossa omaksuttiin näin teleologinen lähestymistapa, joka perustui tietojen käsittelyn tarkoitukseen: koska tietojen käsittelyllä pyrittiin suojaamaan yleistä turvallisuutta, sen oli katsottava jäävän direktiivin 95/46 soveltamisalan ulkopuolelle. Tämä tarkoitus ei kuitenkaan ollut ainoa ratkaiseva arviointiperuste,[23] minkä vuoksi tuomiossa korostettiin, että ”siirto tapahtui julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen”.[24]

48. Tuomio parlamentti v. neuvosto ja komissio auttaa siten ymmärtämään direktiivissä 95/46 olevien poissulkemislausekkeiden ja rajoituslausekkeiden (jotka vastaavat direktiivissä 2002/58 olevia lausekkeita) välisen eron. Pitää kuitenkin paikkansa, että molemmissa lausekelajeissa viitataan samankaltaisiin yleisen edun mukaisiin tavoitteisiin, mikä hämärtää niiden välistä eroa, kuten julkisasiamies Bot aikanaan varoitti.[25]

49. Tämä epäselvyys on todennäköisesti syynä niiden jäsenvaltioiden näkemyksiin, jotka katsovat, ettei direktiiviä 2002/58 sovelleta. Näiden jäsenvaltioiden mukaan kansallista turvallisuutta koskeva etu voidaan turvata ainoastaan direktiivin 2002/58 1 artiklan 3 kohdassa olevalla poissulkemislausekkeella. Tosiasia kuitenkin on, että tätä samaa etua palvelevat myös kyseisen direktiivin 15 artiklan 1 kohdassa sallitut rajoitukset, kuten kansallista turvallisuutta koskeva rajoitus. Jälkimmäinen säännös olisi tarpeeton, jos direktiiviä 2002/58 ei koskaan sovellettaisi tilanteessa, jossa vedotaan kansalliseen turvallisuuteen.

2. Tuomio Tele2 Sverige ja Watson

50. Tuomiossa Tele2 Sverige ja Watson oli kyse siitä, voitiinko unionin oikeuden mukaisina pitää kansallisia järjestelmiä, joissa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille asetettiin yleinen velvollisuus tätä viestintää koskevien tietojen säilyttämiseen. Siinä kyseessä olleet tapaukset olivat pääosin samanlaiset kuin tämän ennakkoratkaisumenettelyn taustalla olevat tapaukset.

51. Unionin tuomioistuin, jonka käsiteltäväksi oli jälleen kerran saatettu unionin oikeuden sovellettavuutta – sillä kertaa jo direktiivin 2002/58 osalta – koskeva kysymys, totesi aluksi, että ”direktiivin 2002/58 soveltamisalaa on arvioitava siten, että otetaan huomioon muun muassa direktiivin yleinen rakenne”.[26]

52. Tältä kannalta unionin tuomioistuin huomautti, että ”direktiivin 2002/58 15 artiklan 1 kohdassa tarkoitetut lainsäädännölliset toimenpiteet liittyvät tosin valtiolle tai valtion viranomaisille tyypillisiin toimintoihin, jotka eivät liity yksityisten henkilöiden toiminta-aloihin – –. Tavoitteet, joihin näillä toimenpiteillä on kyseisen säännöksen nojalla vastattava, eli tässä tapauksessa kansallisen turvallisuuden – – varmistaminen, käyvät pääasiallisesti yksiin direktiivin 1 artiklan 3 kohdassa tarkoitettujen toimintojen tavoitteiden kanssa.”[27]

23 Näin edesmennyt julkisasiamies Bot totesi ratkaisuehdotuksessaan Irlanti v. parlamentti ja neuvosto (C-301/06, EU:C:2008:558). Hän katsoi, että tuomio parlamentti v. neuvosto ja komissio ”ei voi – – tarkoittaa, että henkilötietojen käsittelyn sisältyminen direktiivillä 95/46 luodun tietosuojajärjestelmän soveltamisalaan määräytyisi yksinomaan tämän käsittelyn tavoitteen perusteella. Sen lisäksi on tarkistettava, millaisen toiminnan yhteydessä tietoja käsitellään. Tietojen käsittely jää direktiiviin 95/46 perustuvan yhteisössä sovellettavan henkilötietojen suojajärjestelmän ulkopuolelle kyseisen direktiivin 3 artiklan 2 kohdan ensimmäisen luetelmakohdan nojalla ainoastaan, jos se on valtiolle tai valtion viranomaisille tyypillistä toimintaa, joka ei liity yksityisten henkilöiden toiminta-aloihin. Euroopan unionin lainsäätäjän tehtävänä on silloin luoda yleinen tietosuojajärjestelmä, joka kattaa tietojen käsittelyn tällaisen valtiolle tyypillisen toiminnan puitteissa” (122 kohta).

24 Tuomio parlamentti v. neuvosto ja komissio, 58 kohta. Sopimuksessa pääasiallisesti vaadittiin, että kaikki kansainvälistä matkustajaliikennettä unionin ja Yhdysvaltojen välillä harjoittavat ulkomaiset lentoyhtiöt antavat Yhdysvaltojen viranomaisille sähköisen pääsyn matkustajarekisteritietoihin, joita säilytetään niiden automaattisissa varausjärjestelmissä tai lähtöselvitysjärjestelmissä. Sopimuksella luotiin näin sopimuspuolien välille eräänlainen kansainvälinen yhteistyö, jonka tavoitteena oli sekä terrorismin ja muun vakavan rikollisuuden torjunta että lentomatkustajien henkilötietojen suojaaminen. Tässä tilanteessa lentoyhtiöille asetettu velvoite ei juurikaan eronnut suorasta tietojenvaihdosta viranomaisten välillä.

25 Julkisasiamies Botin ratkaisuehdotus Irlanti v. parlamentti ja neuvosto (C-301/06, EU:C:2008:558, 127 kohta).

26 Tuomio Tele2 Sverige ja Watson, 67 kohta.

27 Ibidem, 72 kohta.

53. Niiden toimenpiteiden tavoite, joita jäsenvaltiot voivat direktiivin 2002/58 15 artiklan 1 kohdan nojalla toteuttaa rajoittaakseen oikeutta yksityisyyteen, käy siis (tältä osin) yksiin sen tavoitteen kanssa, jolla perustellaan tiettyjen valtion toimien jättämistä kyseisen direktiivin järjestelmän ulkopuolelle sen 1 artiklan 3 kohdan mukaisesti.

54. Unionin tuomioistuin kuitenkin katsoi, että ”kun otetaan huomioon direktiivin 2002/58 yleinen rakenne”, tämän seikan perusteella ”ei kuitenkaan voida päätellä, että direktiivin 2002/58 15 artiklan 1 kohdassa tarkoitetut lainsäädännölliset toimenpiteet olisi suljettu tämän direktiivin soveltamisalan ulkopuolelle, koska muutoin tältä säännökseltä riistettäisiin täysin sen tehokas vaikutus. Kyseinen säännös edellyttää väistämättä, että siinä tarkoitetut kansalliset toimenpiteet, kuten tietojen säilyttämistä koskevat toimenpiteet rikollisuuden torjumiseksi, kuuluvat tämän direktiivin soveltamisalaan, koska siinä nimenomaisesti sallitaan jäsenvaltioiden toteuttaa niitä vain siinä säädettyjä edellytyksiä noudattaen”. [28]

55. Se lisäsi, että direktiivin 2002/58 15 artiklan 1 kohdassa sallituilla rajoituksilla ”säännellään kyseisessä säännöksessä mainitussa tarkoituksessa sähköisten viestintäpalvelujen tarjoajien toimintaa”. Kyseistä säännöstä on, kun se luetaan yhdessä direktiivin 3 artiklan kanssa, ”siis tulkittava siten, että tällaiset lainsäädännölliset toimenpiteet kuuluvat tämän saman direktiivin soveltamisalaan”. [29]

56. Tämän perusteella unionin tuomioistuin katsoi, että direktiivin 2002/58 soveltamisalaan kuuluu sekä lainsäädännöllinen toimenpide, jossa palveluntarjoajat ”velvoitetaan säilyttämään liikenne- ja paikkatiedot, koska tällainen toiminta merkitsee väistämättä sitä, että ne käsittelevät henkilötietoja”, [30] että toimenpide, jossa säädetään kansallisten viranomaisten oikeudesta saada viestintäpalvelujen tarjoajien säilyttämiä tietoja. [31]

57. Tuomiossa Tele2 Sverige ja Watson annettu direktiivin 2002/58 tulkinta toistetaan tuomiossa Ministerio Fiscal.

58. Voitaisiinko väittää, että tuomiossa Tele2 Sverige ja Watson on enemmän tai vähemmän implisiittisesti poikettu tuomioon parlamentti v. neuvosto ja komissio perustuvasta oikeuskäytännöstä? Näin asiaa tulkitsee esimerkiksi Irlanti, jonka mukaan ainoastaan jälkimmäinen tuomio on yhteensopiva direktiivin 2002/58 oikeusperustan kanssa ja SEU 4 artiklan 2 kohdan mukainen. [32]

59. Ranskan hallitus katsoo, että tämä ristiriita voitaisiin ratkaista selittämällä se sillä, että tuomioon Tele2 Sverige ja Watson perustuvassa oikeuskäytännössä viitataan jäsenvaltioiden toimiin rikosoikeuden alalla, kun taas tuomiossa parlamentti v. neuvosto ja komissio vahvistettu oikeuskäytäntö koskee valtion turvallisuutta ja puolustusta. Käsiteltävään tapaukseen ei siten sovelleta tuomioon Tele2 Sverige ja Watson perustuvaa oikeuskäytäntöä, vaan siihen on sovellettava tuomiossa parlamentti v. neuvosto ja komissio omaksuttua ratkaisua. [33]

60. Kuten jo edellä totesin, uskoakseni nämä kaksi tuomiota voidaan sovittaa yhteen, mutta eri keinolla kuin se, jota Ranskan hallitus kannattaa. En ole jälkimmäisestä samaa mieltä, koska mielestäni tuomiossa Tele2 Sverige ja Watson esitettyjä toteamuksia, jotka koskevat nimenomaisesti terrorismin torjuntaa, [34] voidaan soveltaa mihin tahansa kansalliseen turvallisuuteen kohdistuvaan uhkaan (joista yksi on terrorismi).

28 Ibidem, 73 kohta.

29 Ibidem, 74 kohta.

30 Ibidem, 75 kohta.

31 Ibidem, 76 kohta.

32 Irlannin kirjalliset huomautukset, 15 ja 16 kohta.

33 Ranskan hallituksen kirjalliset huomautukset, 34–50 kohta.

34 Tuomio Tele2 Sverige ja Watson, 103 ja 119 kohta.

3. Mahdollisuus tuomion parlamentti v. neuvosto ja komissio ja tuomion Tele2 Sverige ja Watson sovittelevaan tulkintaan

61. Mielestäni unionin tuomioistuin otti tuomiossa Tele2 Sverige ja Watson ja tuomiossa Ministerio Fiscal huomioon poissulkemis- ja rajoituslausekkeiden tarkoituksen ja näiden kahden lauseketyypin välisen systemaattisen yhteyden.

62. Vaikka asiassa parlamentti v. neuvosto ja komissio vahvistettiin, että tietojen käsittely ei kuulunut direktiivin 95/46 soveltamisalaan, tämä johtui, kuten jo edellä muistutin, siitä, että unionin ja sen jäsenvaltioiden välisessä yhteistyössä, jota tehdään tyypillisesti kansainvälisissä puitteissa, on asetettava etusijalle toiminnan valtiollinen ulottuvuus, vaikka käsittelyllä olisi myös kaupallinen tai yksityinen ulottuvuus. Tuolloin yksi kiistellyistä kysymyksistä koski nimenomaan sitä, mikä oli asianmukainen oikeudellinen perusta riidanalaiselle päätökselle.

63. Sitä vastoin tuomioissa Tele2 Sverige ja Watson ja Ministerio Fiscal tarkasteltujen kansallisten toimenpiteiden tapauksessa unionin tuomioistuin asetti etusijalle tietojen käsittelyn kansallisen ulottuvuuden: lainsäädäntökehys, jossa tämä käsittely tapahtui, oli yksinomaan kansallinen, joten siltä puuttui tuomiossa parlamentti v. neuvosto ja komissio kyseessä olleelle käsittelylle ominainen ulkoinen ulottuvuus.

64. Koska tietojen käsittelyn kansainvälisellä ja kansallisella (kaupallisella ja yksityisellä) ulottuvuudella on eri painoarvot, ensin mainitussa tapauksessa oli sovellettava unionin oikeuden poissulkemislauseketta, koska se soveltui parhaiten kyseessä olleen yleisen edun eli kansallisen turvallisuuden suojaamiseen. Sitä vastoin jälkimmäisessä tapauksessa tämä sama etu voitiin tehokkaasti turvata direktiivin 2002/58 15 artiklan 1 kohdassa säädetyllä rajoituslausekkeella.

65. Näillä kahdella tuomiolla on toinenkin ero, joka liittyy asioiden erilaiseen normatiiviseen asiayhteyteen: ne kaksi säännöstä, joiden tulkintaan kyseisissä tuomioissa keskityttiin, eivät tarkemmin katsoen ole samat.

66. Tuomiossa parlamentti v. neuvosto ja komissio nimittäin tulkittiin direktiivin 95/46 3 artiklan 2 kohtaa ja tuomiossa Tele2 Sverige ja Watson direktiivin 2002/58 1 artiklan 3 kohtaa. Kyseisten artiklojen huolellisesta tarkastelusta ilmenee, että niiden välinen ero on riittävä tukeakseen unionin tuomioistuimen kummassakin tapauksessa antaman kaltaista ratkaisua.

67. Direktiivin 95/46 3 artiklan 2 kohdan mukaan ”tätä direktiiviä *ei sovelleta henkilötietojen käsittelyyn*, – – joka suoritetaan sellaisessa toiminnassa, joka ei kuulu yhteisön oikeuden soveltamisalaan, – – ja kaikissa tapauksissa *käsittely*, joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta (myös valtion taloudellista hyvinvointia, kun *käsittely*operaatio on sidoksissa valtion turvallisuutta koskeviin kysymyksiin) ja rikosoikeuden alalla tapahtuvaa valtion toimintaa”. [35]

68. Direktiivin 2002/58 1 artiklan 3 kohdan mukaan tätä direktiiviä ”*ei sovelleta* Euroopan yhteisön perustamissopimuksen soveltamisalan ulkopuolelle jääviin *toimiin*, – – eikä missään tapauksessa yleistä turvallisuutta, puolustusta ja valtion turvallisuutta (mukaan lukien valtion taloudellinen hyvinvointi, kun toimet liittyvät valtion turvallisuuteen) koskeviin *toimiin* eikä valtion *toimiin* rikosoikeuden alalla”. [36]

35 Kursivointi tässä.

36 Kursivointi tässä.

69. Direktiivin 95/46 3 artiklan 2 kohdassa siis jätetään tämän direktiivin soveltamisalan ulkopuolelle *tietojen käsittely*, joka koskee – nyt merkityksellisiltä osin – valtion turvallisuutta, kun taas direktiivin 2002/58 1 artiklan 3 kohdassa sen ulkopuolelle jätetään *toimet*, joiden tarkoituksena on suojata – niin ikään nyt merkityksellisin osin – valtion turvallisuutta.

70. Tämä ero ei suinkaan ole sattumanvarainen. Direktiivissä 95/46 jätettiin sen soveltamisalan ulkopuolelle tietty toiminta (”henkilötietojen käsittely”), jota kuka tahansa voi suorittaa. Sen soveltamisalan ulkopuolelle jäävänä toimintana mainittiin nimenomaisesti henkilötietojen käsittely, joka liittyy muun muassa valtion turvallisuutta koskeviin asioihin. Sillä, *kuka* tätä tietojen käsittelyä suorittaa, ei sitä vastoin ollut merkitystä. Direktiivin soveltamisalan ulkopuolelle jäävän toiminnan määrittelyssä käytettiin siis teleologista tai finaalista lähestymistapaa, jossa ei tehty eroa käsittelijöinä olevien henkilöiden välillä.

71. Näin ollen on tulkittava, että asiassa parlamentti v. neuvosto ja komissio otettiin ensisijaisesti huomioon tietojen käsittelyn tarkoitus. Merkitystä ei ollut sillä, että ”yksityiset toimijat olivat keränneet – – tiedot kaupalliseen tarkoitukseen ja että ne järjestivät kyseisten tietojen siirron kolmanteen valtioon”, vaan ratkaisevaa oli se, että ”siirto tapahtui julkishallinnon asettamissa puitteissa, jotka liittyivät yleiseen turvallisuuteen” [37].

72. Sitä vastoin asiassa Tele2 Sverige ja Watson tarkasteltuja ”valtion turvallisuutta koskevia toimia”, jotka eivät kuulu direktiivin 2002/58 soveltamisalaan, ei voi toteuttaa kuka tahansa henkilö vaan ainoastaan itse valtio. Näihin toimiin eivät sitä paitsi kuulu valtion lainsäädäntö- tai sääntelytehtävät vaan yksinomaan julkisen vallan toteuttamat konkreettiset toimenpiteet.

73. Direktiivin 2002/58 1 artiklan 3 kohdassa luetellut *toimet* nimittäin ”ovat kussakin tapauksessa valtiolle tai valtion viranomaisille tyypillisiä toimintoja, jotka eivät liity yksityisten henkilöiden toiminta-aloihin”. [38] Nämä ”toimet” eivät voi olla luonteeltaan normatiivisia. Jos näin olisi, direktiivin 2002/58 soveltamisalan ulkopuolelle jäisivät kaikki sellaiset jäsenvaltioiden henkilötietojen käsittelystä antamat säännökset, joita perustellaan sillä, että ne ovat välttämättömiä valtion turvallisuuden kannalta.

74. Yhtäältä tämä heikentäisi merkittävästi mainitun direktiivin tehokkuutta, koska jo pelkkä vetoaminen valtion turvallisuuden kaltaiseen epämääräiseen oikeudelliseen käsitteeseen riittäisi siihen, että jäsenvaltiot voisivat jättää soveltamatta takeita, jotka unionin lainsäätäjä on säätänyt kansalaisten henkilötietojen suojaamiseksi. Tätä suojaa on nimittäin käytännössä mahdoton antaa ilman jäsenvaltioiden myötävaikutusta, ja se taataan unionin kansalaisille myös suhteessa kansallisiin viranomaisiin.

75. Toisaalta tulkinnalla, jonka mukaan valtion toimien käsitteeseen sisältyisivät oikeussääntöjen antamiseen liittyvät toimet, vietäisiin direktiivin 2002/58 15 artiklalta sen tarkoitus, sillä kyseisessä artiklassa jäsenvaltiot nimenomaan valtuutetaan – muun muassa kansalliseen turvallisuuteen liittyvistä syistä – toteuttamaan ”lainsäädännöllisiä toimenpiteitä” tiettyjen samassa direktiivissä säädettyjen oikeuksien ja velvollisuuksien soveltamisalan rajoittamiseksi. [39]

37 Tuomio parlamentti v. neuvosto ja komissio, 58 kohta.

38 Tuomio Ministerio Fiscal, 32 kohta. Ks. vastaavasti tuomio Tele2 Sverige ja Watson, 72 kohta.

39 Olisi nimittäin vaikea väittää, että direktiivin 2002/58 15 artiklan 1 kohdassa sallittaisiin siinä säädettyjen oikeuksien ja velvollisuuksien rajoittaminen kansallisen turvallisuuden kaltaisella alalla, joka kyseisen direktiivin 1 artiklan 3 kohdan nojalla jää lähtökohtaisesti sen soveltamisalan ulkopuolelle. Kuten unionin tuomioistuin tuomion Tele2 Sverige ja Watson 73 kohdassa vahvisti, direktiivin 2002/58 15 artiklan 1 kohta ”edellyttää väistämättä, että siinä tarkoitetut kansalliset toimenpiteet – – kuuluvat tämän direktiivin soveltamisalaan, koska siinä nimenomaisesti sallitaan jäsenvaltioiden toteuttaa niitä vain siinä säädettyjä edellytyksiä noudattaen”.

76. Kuten unionin tuomioistuin asiassa Tele2 Sverige ja Watson totesi, ”direktiivin 2002/58 soveltamisalaa on arvioitava siten, että otetaan huomioon muun muassa direktiivin yleinen rakenne”[40]. Tältä kannalta tarkasteltuna ainoa direktiivin 2002/58 1 artiklan 3 kohdan ja 15 artiklan 1 kohdan tulkinta, joka selventää näiden säännösten merkitystä niiden tehokkuutta heikentämättä, on se, että ensin mainitussa säännöksessä jätetään jäsenvaltioiden kansallisen turvallisuuden alalla (ja muilla vastaavilla aloilla) toteuttamat *toimet* aineellisesti direktiivin soveltamisalan ulkopuolelle ja että jälkimmäisessä säännöksessä valtuutetaan jäsenvaltiot toteuttamaan *lainsäädännöllisiä toimenpiteitä* (eli antamaan yleisesti sovellettavia sääntöjä), joita kansallisen turvallisuuden suojaamiseksi sovelletaan jäsenvaltioiden lainkäyttövaltaan kuuluvien yksityisten toimintaan ja joilla rajoitetaan direktiivissä 2002/58 taattuja oikeuksia.

4. Kansallisen turvallisuuden poissulkeminen direktiivissä 2002/58

77. Kansallisesta turvallisuudesta (tai ”valtion turvallisuudesta”, joka, kuten 15 artiklan 1 kohdasta ilmenee, on sen synonyymi) säädetään direktiivissä 2002/58 kahdelta eri kannalta. Yhtäältä se on *poissulkemis*peruste, jonka nojalla direktiivin soveltamisalan ulkopuolelle voidaan jättää kaikki sellaiset jäsenvaltioiden toimet, jotka nimenomaisesti ”koskevat” kansallista turvallisuutta. Toisaalta se on lailla täytäntöön pantava *rajoittamis*peruste, jonka nojalla voidaan rajoittaa direktiivissä 2002/58 säädettyjä oikeuksia ja velvollisuuksia eli luonteeltaan yksityistä tai kaupallista toimintaa, joka ei kuulu julkisen vallan tehtäviin.[41]

78. Mihin toimiin direktiivin 2002/58 1 artiklan 3 kohdassa viitataan? Mielestäni Conseil d’État itse esittää niistä hyvän esimerkin viitatessaan sisäisestä turvallisuudesta annetun lain L. 851-5 ja L. 851-6 §:ään, jotka koskevat ”tiedonkeruumenetelmiä, joita valtio käyttää suoraan sääntelemättä sähköisten viestintäpalvelujen tarjoajien toimintaa määräämällä niille erityisiä velvoitteita”.[42]

79. Uskoakseni tämä on avain direktiivin 2002/58 1 artiklan 3 kohdan soveltamisalan ulkopuolelle jäävien toimien määrittämiseen. Sen soveltamisalaan eivät kuulu kansallisen turvallisuuden suojaamiseen liittyvät *toimet*, joita julkinen valta toteuttaa omaan lukuunsa edellyttämättä yksityisiltä yhteistyötä ja siten asettamatta niille mitään liiketoimintaan liittyviä velvoitteita.

80. Luetteloa niistä julkisen vallan toimista, jotka jäävät henkilötietojen käsittelyä koskevan yleisen järjestelmän soveltamisalan ulkopuolelle, on kuitenkin tulkittava suppeasti. *Kansallisen turvallisuuden*, josta kukin jäsenvaltio on SEU 4 artiklan 2 kohdan nojalla yksinomaisesti vastuussa, käsitettä ei siten voida laajentaa koskemaan muita, julkiseen elämään enemmän tai vähemmän läheisesti liittyviä aloja.

81. Koska nyt käsiteltävissä ennakkoratkaisupyynnöissä on kyse yksityisten (eli toimijoiden, jotka tarjoavat käyttäjille sähköisiä viestintäpalveluja) velvoittamisesta eikä pelkästään valtion viranomaisten toiminnasta, tässä ratkaisuehdotuksessa ei ole tarpeen käsitellä laajemmin sitä, miten kansallisen turvallisuuden käsite stricto sensu on rajattava.

40 Tuomio Tele2 Sverige ja Watson, 67 kohta.

41 Kuten julkisasiamies Saugmandsgaard Øe sivumennen ratkaisuehdotuksensa Ministerio Fiscal (C-207/16, EU:C:2018:300) 47 kohdassa huomautti, ”ei ole syytä sekoittaa toisiinsa henkilötietoja, jotka käsitellään *suoraan* valtion julkisen vallan tehtävien yhteydessä – – rikosoikeuteen kuuluvalla alalla, – – ja henkilötietoja, jotka käsitellään sähköisten viestintäpalvelujen tarjoajan kaupallisen toiminnan yhteydessä ja joita toimivaltaiset valtion viranomaiset käyttävät *sen jälkeen*”.

42 Asiassa C-511/18 esitetty ennakkoratkaisupyyntö, 18 ja 21 kohta.

82. Katson kuitenkin, että tähän voisi soveltua ohjenuoraksi puitepäätöksessä 2006/960/YOS [43] vahvistettu arviointiperuste, sillä sen 2 artiklan a alakohdassa tehdään ero yhtäältä lainvalvontaviranomaisen, jolla sanan laajassa merkityksessä tarkoitetaan ”jäsenvaltion poliisi-, tulli- tai muuta viranomaista, jolla on kansallisen lainsäädännön mukaan valta paljastaa, ehkäistä ja tutkia rikoksia tai rikollista toimintaa sekä käyttää julkista valtaa ja pakkokeinoja tämän toiminnan yhteydessä” – ja toisaalta sellaisten ”virastojen tai yksiköiden, jotka käsittelevät erityisesti kansallisia turvallisuuskysymyksiä”, välillä. [44]

83. Direktiivin 2002/58 johdanto-osan 11 perustelukappaleessa vahvistetaan, että tämä direktiivi ”samoin kuin direktiivi [95/46], ei koske perusoikeuksien ja -vapauksien turvaamista sellaisessa toiminnassa, joka ei kuulu [unionin] oikeuden soveltamisalaan”. Tästä syystä direktiivi 2002/58 ”ei vaikuta tasapainoon, joka tällä hetkellä vallitsee yksittäisten henkilöiden yksityisyyden suojan ja niiden tämän direktiivin 15 artiklan 1 kohdassa tarkoitettujen toimenpiteiden välillä, joita jäsenvaltiot voivat toteuttaa – – valtion turvallisuuden – – suojelemiseksi – –”.

84. Direktiivien 95/46 ja 2002/58 välillä on nimittäin tietty jatkumo siltä osin kuin on kyse jäsenvaltioiden toimivallasta kansallisen turvallisuuden alalla. Kummankaan direktiivin tavoitteena ei ole turvata perusoikeuksia tällä nimenomaisella alalla, jolla jäsenvaltioiden toiminta ”ei kuulu [unionin] oikeuden soveltamisalaan”.

85. ”Tasapaino”, johon kyseisessä johdanto-osan perustelukappaleessa viitataan, perustuu tarpeeseen kunnioittaa kullekin jäsenvaltiolle kansallisen turvallisuuden alalla kuuluvaa toimivaltaa silloin, kun ne käyttävät sitä *suoraan ja omin avuin*. Sitä vastoin silloin, kun tämän toimivallan käyttäminen, mukaan lukien kansalliseen turvallisuuteen liittyvistä syistä, edellyttää apua yksityisiltä, joille tässä yhteydessä asetetaan tiettyjä velvoitteita, sen on tämä seikan perusteella katsottava tapahtuvan alalla, joka kuuluu unionin oikeuden soveltamisalaan (eli kyseisten yksityisten toimijoiden yksityisyyden suojan alalla).

86. Sekä direktiivissä 95/46 että direktiivissä 2002/58 pyritään saavuttamaan tämä tasapaino sallimalla se, että yksityisten oikeuksia voidaan rajoittaa lainsäädännöllisillä toimenpiteillä, joita jäsenvaltiot toteuttavat ensin mainitun 13 artiklan 1 kohdan ja jälkimmäisen 15 artiklan 1 kohdan nojalla. Direktiiveissä ei tässä kohden ole mitään eroa.

87. Asetuksesta 2016/679, jossa vahvistetaan henkilötietojen suojaa koskeva (uusi) yleinen sääntelykehys, on todettava, että tämän asetuksen 2 artiklan 2 kohdan mukaan sitä ei sovelleta ”henkilötietojen käsittelyyn”, jota jäsenvaltiot ”suorittavat toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa”.

88. Direktiivissä 95/46 henkilötietojen käsittely määriteltiin pelkästään tarkoituksensa perusteella ottamatta huomioon sitä, kuka tätä käsittelyä suorittaa, kun taas asetuksessa 2016/679 sen soveltamisalan ulkopuolelle jäävä käsittely määritellään sekä tarkoituksensa että suorittajansa perusteella: sitä ei sovelleta käsittelyyn, jota jäsenvaltiot suorittavat sellaisen *toiminnan* yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan (2 artiklan 2 kohdan a ja b alakohta), ja jota toimivaltaiset viranomaiset suorittavat *rikosten torjuntaa* ja yleiseen turvallisuuteen kohdistuvilta uhkilta *suojelua* varten. [45]

43 Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta 18.12.2016 tehty neuvoston puitepäätös (EUVL 2006, L 386, s. 89).

44 Rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta 27.11.2008 tehdyn neuvoston puitepäätöksen 2008/977/YOS (EUVL 2008, L 350, s. 60) 1 artiklan 4 kohdassa säädettiin vastaavasti, että ”tämä puitepäätös ei vaikuta olennaisiin kansallisiin turvallisuusetuihin eikä kansallisen turvallisuuden alan erityisiin tiedustelutoimiin”.

45 Asetusta 2016/679 ei nimittäin sovelleta henkilötietojen käsittelyyn, jota jäsenvaltiot suorittavat sellaisen *toiminnan* yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan, eikä myöskään käsittelyyn, jota viranomaiset suorittavat yleisen turvallisuuden *suojelua* varten.

89. Tämä julkisen vallan toiminta on pakostikin määritettävä suppeasti, sillä muuten yksityisyyden suojaa koskeva unionin lainsäädäntö jää vaille tehokasta vaikutusta. Asetuksen 2016/679 23 artiklassa säädetään – direktiivin 2002/58 15 artiklan 1 kohdan mukaisesti – siinä säädettyjen oikeuksien ja velvollisuuksien rajoittamisesta *lainsäädäntötoimenpiteellä*, jos se on tarpeen muun muassa kansallisen turvallisuuden, puolustuksen ja yleisen turvallisuuden takaamiseksi. Jälleen kerran on todettava, että jos näiden tarkoitusten suojaaminen riittäisi jo yksinään asetuksen 2016/679 soveltamisalan ulkopuolelle jättämisen perusteeksi, valtion turvallisuuteen olisi tarpeetonta vedota perusteena kyseisessä asetuksessa säädettyjen oikeuksien rajoittamiseen lainsäädäntötoimenpiteillä.

90. Aivan kuten direktiivin 2002/58 tapauksessa, tässäkään ei olisi johdonmukaista katsoa, että asetuksen 2016/679 23 artiklassa (jossa siis sallitaan valtion rajoittaa kansalaistensa yksityisyyteen liittyviä oikeuksia kansalliseen turvallisuuteen perustuvista syistä) säädetyt lainsäädäntötoimenpiteet kuuluvat tämän asetuksen soveltamisalaan, ja samanaikaisesti, että valtion turvallisuuden kuuluminen sen soveltamisalaan tarkoittaa, että itse asetusta on suoralta kädeltä jätettävä soveltamatta, mikä merkitsisi sitä, että minkäänlaisia subjektiivisia oikeuksia ei tunnusteta.

B Tuomioon Tele2 Sverige ja Watson perustuvan oikeuskäytännön vahvistaminen ja kehittämismahdollisuudet

91. Asiassa C-520/18 esittämässäni ratkaisuehdotuksessa [46] tarkastelen yksityiskohtaisesti tätä aihetta koskevaa unionin tuomioistuimen oikeuskäytäntöä ja ehdotan tarkasteluni perusteella kyseisen oikeuskäytännön vahvistamista esittäen samalla joitakin tulkintakeinoja sen sisällön hahmottamiseksi.

92. Viittaan lyhyyden vuoksi kyseiseen tarkasteluun, jota mielestäni ei ole välttämätöntä tässä toistaa. Conseil d'État'n ennakkoratkaisukysymyksistä jäljempänä esittämiäni pohdintoja luettaessa on siten pidettävä mielessä asiassa C-520/18 esittämäni ratkaisuehdotuksen vastaavat osat.

C Vastaukset ennakkoratkaisukysymyksiin

1. Tietojen säilyttämistä koskeva velvoite (asioissa C-511/18 ja C-512/18 esitetty ensimmäinen ennakkoratkaisukysymys ja asiassa C-512/18 esitetty toinen ennakkoratkaisukysymys)

93. Sähköisten viestintäpalvelujen tarjoajille asetetun tietojen säilyttämistä koskevan velvoitteen osalta ennakkoratkaisua pyytänyt tuomioistuin haluaa erityisesti selvittää:

– merkitseekö tämä direktiivin 2002/58 15 artiklan 1 kohdan nojalla täytettävä velvoite perusteetonta puuttumista perusoikeuskirjan 6 artiklassa taattuun turvallisuutta koskevaan oikeuteen ja kansallisen turvallisuuden vaatimuksiin (asioissa C-511/18 ja C-512/18 esitetty ensimmäinen ennakkoratkaisukysymys ja asiassa C-511/18 esitetty kolmas ennakkoratkaisukysymys)

– sallitaanko direktiivissä 2000/31 sellaisten tietojen säilyttäminen, joiden perusteella kyetään tunnistamaan verkossa yleisesti saatavilla olevien sisältöjen luomiseen osallistuneet henkilöt (asiassa C-512/18 esitetty toinen ennakkoratkaisukysymys).

46 27–68 kohta.

a) Alustavat huomautukset

94. Conseil d'État viittaa perusoikeuskirjan 7 artiklassa (yksityis- ja perhe-elämän kunnioittaminen), 8 artiklassa (henkilötietojen suoja) ja 11 artiklassa (sananvapaus ja tiedonvälityksen vapaus) taattuihin perusoikeuksiin. Unionin tuomioistuimen oikeuskäytännön mukaan kansallisten viranomaisten sähköisten viestintäpalvelujen tarjoajille asettama velvoite säilyttää liikennetietoja saattaa nimittäin hyvinkin vaikuttaa näihin oikeuksiin.[47]

95. Ennakkoratkaisua pyytänyt tuomioistuin mainitsee myös perusoikeuskirjan 6 artiklassa suojatun oikeuden turvallisuuteen. Se kuitenkin viittaa siihen pikemminkin perusteena, jolla kyseisen velvoitteen asettaminen voitaisiin oikeuttaa, kuin kyseessä olevana oikeutena.

96. Olen komission kanssa samaa mieltä siitä, että tällainen viittaus 6 artiklaan voi olla monitulkintainen. Katson komission tavoin, ettei kyseistä määräystä pidä tulkita niin, että siihen sisältyy mahdollisuus ”asettaa unionille positiivinen velvollisuus toteuttaa toimenpiteitä henkilöiden suojelemiseksi rikoksilta”.[48]

97. Kyseisessä perusoikeuskirjan artiklassa taattu turvallisuus ei nimittäin tarkoita samaa kuin yleinen turvallisuus. Toisin sanoen yleinen turvallisuus voi liittyä yhtä hyvin ensin mainittuun oikeuteen kuin mihin tahansa muuhunkin perusoikeuteen, koska se on perusoikeuksien ja -vapauksien käyttämisen välttämätön edellytys.

98. Kuten komissio muistuttaa, perusoikeuskirjan 6 artikla vastaa Euroopan ihmisoikeussopimuksen 5 artiklaa, kuten perusoikeuskirjan selityksistä ilmenee. Euroopan ihmisoikeussopimuksen 5 artiklan sanamuodosta käy ilmi, että siinä suojatulla ”turvallisuudella” tarkoitetaan yksinomaan henkilökohtaista turvallisuutta, joka ymmärretään takeeksi oikeudesta fyysiseen vapauteen, joka suojaa mielivaltaiselta pidättämiseltä tai säilöönotolta. Viime kädessä turvallisuudella tarkoitetaan sitä, ettei keneltäkään saa riistää hänen vapauttaan, paitsi laissa säädetyin edellytyksin ja lain määräämässä järjestyksessä.

99. Kyse on siis *henkilökohtaisesta turvallisuudesta*, joka liittyy edellytyksiin, joilla henkilöiden fyysistä vapautta voidaan rajoittaa,[49] eikä valtion olemassaoloon erottamattomasti kuuluvasta *yleisestä turvallisuudesta*, joka kehittyneessä yhteiskunnassa on ehdoton edellytys sille, että julkisen vallan käyttö voidaan sovittaa yhteen yksilön oikeuksien käytön kanssa.

100. Jotkin hallitukset kuitenkin pyytävät, että oikeus jälkimmäiseen näistä turvallisuuden muodoista otettaisiin nykyistä paremmin huomioon. Todellisuudessa unionin tuomioistuin ei suinkaan ole jättänyt huomiotta yleistä turvallisuutta, vaan se on vieläpä nimenomaisesti maininnut sen antamissaan tuomioissa[50] ja lausunnoissa[51]. Unionin tuomioistuin ei milloinkaan ole kiistänyt niiden yleisen edun mukaisten tavoitteiden merkitystä, jotka liittyvät kansallisen turvallisuuden ja yleisen järjestyksen suojaamiseen[52] ja kansainvälisen terrorismin torjumiseen kansainvälisen rauhan ja turvallisuuden

47 Tuomio Tele2 Sverige ja Watson, 92 kohta, jossa viitataan analogisesti tuomion Digital Rights 25 ja 70 kohtaan.

48 Komission huomautukset, 37 kohta.

49 Näin asiaa tulkitsee Euroopan ihmisoikeustuomioistuin. Euroopan ihmisoikeustuomioistuimen tuomio 5.7.2016, Buzadji v. Moldavian tasavalta (ECHR:2016:0705JUD002375507), jonka 84 kohdassa vahvistetaan, että Euroopan ihmisoikeussopimuksen 5 artiklassa tunnustetun oikeuden olennainen tavoite on estää yksilön vapauden mielivaltainen tai perusteeton riistäminen.

50 Tuomio Digital Rights, 42 kohta.

51 Lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017 (EU:C:2017:592, 149 kohta oikeuskäytäntöviittauksineen; jäljempänä lausunto 1/15).

52 Tuomio 15.2.2016, N (C-601/15 PPU, EU:C:2016:84, 53 kohta).

ylläpitämiseksi sekä vakavien rikosten torjumiseen yleisen turvallisuuden takaamiseksi,[53] ja näitä se on aivan oikein pitänyt ”ensisijaisen tärkeänä”.[54] Kuten unionin tuomioistuin aikanaan totesi, ”yleisen turvallisuuden suojaaminen myötävaikuttaa myös muiden henkilöiden oikeuksien ja vapauksien suojeluun”.[55]

101. Tässä voitaisiin käyttää hyväksi nyt käsiteltävien ennakkoratkaisupyyntöjen tarjoamaa tilaisuutta ja painottaa entistä selvemmin tasapainon etsimistä yhtäältä turvallisuutta koskevan oikeuden ja toisaalta yksityisyyden suojaa ja henkilötietojen suojaa koskevien oikeuksien välillä. Näin vältettäisiin arvostelut siitä, että jälkimmäisiä suositaan ensin mainitun kustannuksella.

102. Tähän tasapainoon mielestäni juuri viitataan direktiivin 2002/58 johdanto-osan 11 perustelukappaleessa ja sen 15 artiklan 1 kohdassa, kun niissä puhutaan *demokraattisen yhteiskunnan* toimenpiteille asetetuista välttämättömyyden ja oikeasuhteisuuden vaatimuksista. Oikeus turvallisuuteen on, kuten edellä jo totesin, demokratian olemassaolon ja selviytymisen luontainen edellytys, mikä oikeuttaa sen, että se otetaan täysimääräisesti huomioon toimenpiteiden oikeasuhteisuutta arvioitaessa. Toisin sanoen, vaikka tietojen luottamuksellisuuden periaatteen suojaa pidetään demokraattisessa yhteiskunnassa ensisijaisen tärkeänä, ei myöskään turvallisuuden merkitystä voida aliarvioida.

103. Asiayhteys, jossa kansalliseen turvallisuuteen kohdistuu vakavia ja jatkuvia uhkia ja erityisesti terrorismin vaara, on siten otettava huomioon tuomion Tele2 Sverige ja Watson 119 kohdan viimeisessä virkkeessä todetun mukaisesti. Kansallisessa järjestelmässä voidaan vastata siihen kohdistuviin uhkiin oikeasuhteisesti sen mukaan, minkä luonteisia ja miten suuria nämä uhat ovat, eikä vastatoimien välttämättä tarvitse olla samanlaisia kuin muissa jäsenvaltioissa.

104. Lopuksi on lisättävä, että edellä esittämäni toteamukset eivät suinkaan estä sitä, että kansallisessa lainsäädännössä varataan sellaisissa *poikkeuksellisissa* tilanteissa, joissa välitön vaara tai epätavallinen riski oikeuttaa julistamaan jäsenvaltioon virallisen hätätilan, mahdollisuus määrätä rajoitetuksi ajaksi niin laaja tietojen säilyttämisvelvollisuus kuin on välttämätöntä.[56]

105. Molemmissa ennakkoratkaisupyynnöissä esitetty ensimmäinen ennakkoratkaisukysymys olisi siten muotoiltava uudelleen niin, että siinä tiedustellaan lähinnä sitä, onko kyseistä puuttumista mahdollista perustella kansalliseen turvallisuuteen liittyvillä syillä. Kysymys koskisi näin ollen siitä, onko sähköisiä viestintäpalveluja tarjoaville operaattoreille asetettu velvoite yhteensopiva direktiivin 2002/58 15 artiklan 1 kohdan kanssa.

b) Arviointi

1) Kansallisten säännösten, sellaisina kuin ne esitetään ennakkoratkaisupyynnöissä, luonnehdinta unionin tuomioistuimen oikeuskäytännön valossa

106. Ennakkoratkaisupyyntöjen mukaan pääasioissa riitautetussa lainsäädännössä asetetaan tietojen säilyttämistä koskeva velvoite

– sähköisen viestinnän operaattoreille ja erityisesti niille, jotka tarjoavat yleisölle pääsyä verkkoviestintäpalveluihin; ja

53 Tuomio Digital Rights, 42 kohta oikeuskäytäntöviittauksineen.

54 Ibidem, 51 kohta.

55 Lausunto 1/15, 149 kohta.

56 Ks. asiassa C-520/18 esittämäni ratkaisuehdotus, 105–107 kohta.

– luonnollisille henkilöille ja oikeushenkilöille, jotka tarjoavat, myös ilmaiseksi, yleisölle verkkoviestintäpalvelujen kautta näiden palvelujen vastaanottajien toimittamien minkä tahansa merkkien, kirjoitusten, kuvien, äänien tai viestien tallennusta.[57]

107. Operaattorien on säilytettävä vuoden ajan niiden tallennuksesta lukien tiedot, joiden perusteella kyetään tunnistamaan käyttäjä, viestinnässä käytettyjä päätelaitteita koskevat tiedot, kunkin viestinnän tekniset ominaisuudet sekä päivämäärä, kellonaika ja kesto, tilattuja tai käytettyjä oheispalveluja ja niiden tarjoajia koskevat tiedot sekä tiedot, joiden perusteella kyetään tunnistamaan viestinnän vastaanottaja ja, jos kyse on puhelintoiminnasta, puhelun alkuperä ja sijainti.[58]

108. Erityisesti internetiin pääsyä ja tiedontallennusta koskevien palvelujen osalta kansallisessa lainsäädännössä vaaditaan säilyttämään IP-osoitteet,[59] salausavaimet ja, jos on käytetty maksullista sopimusta tai tiliä, maksulaji, maksun viitenumero sekä maksutapahtuman summa, päivämäärä ja kellonaika.[60]

109. Tämä säilyttämisvelvollisuus voidaan asettaa rikosten tutkintaan, toteamiseen ja syytteeseenpanoon liittyvistä syistä.[61] Päinvastoin kuin – kuten jäljempänä käy ilmi – liikenne- ja paikkatietojen *keruuta* koskevan velvoitteen, niiden *säilyttämistä* koskevan velvoitteen yksinomaisena tarkoituksena ei ole terrorismin ennaltaehkäisy.[62]

110. Säilytettyjen tietojen *saantia* koskevien edellytysten osalta käsiteltävien asioiden asiakirja-aineistoon sisältyvistä tiedoista ilmenee, että joko tietojen saannissa noudatetaan yleisessä järjestelmässä säädettyjä edellytyksiä (oikeusviranomaisen osallistuminen menettelyyn) tai niiden saanti rajoitetaan erikseen nimetyille ja valtuutetuille virkamiehille, mikä edellyttää pääministerin riippumattomalta hallintoviranomaiselta saaman ei-sitovan lausunnon perusteella antamaa lupaa.[63]

111. Voidaan helposti ymmärtää, kuten komissio huomautti,[64] että tiedot, joiden säilyttämistä kansallisissa säännöksissä edellytetään, ovat olennaisin osin samat kuin unionin tuomioistuimen tuomioissa Digital Rights ja Tele2 Sverige ja Watson[65] tarkastelemat tiedot. Kuten niihin, myös nyt tarkasteltaviin tietoihin kohdistuu ”yleistä ja erotuksetta tapahtuvaa säilyttämistä koskeva velvoite”, kuten Conseil d’État ennakkoratkaisupyyntönsä alussa avoimesti toteaa.

112. Jos näin todella on, minkä arvioiminen on viime kädessä ennakkoratkaisua pyytäneen tuomioistuimen asia, on vain todettava, että kyseisen lainsäädännön merkitsemä ”puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin on laajamittaista, ja se on katsottava erityisen vakavaksi”.[66]

57 Tämä ilmenee sisäisestä turvallisuudesta annetun lain L. 851-1 §:stä, jossa viitataan postitoiminnasta ja sähköisestä viestinnästä annetun lain L. 34-1 §:ään ja luottamuksesta digitaalisessa taloudessa annetun lain nro 2004-575 6 §:ään.

58 Näin säädetään postitoiminnasta ja sähköisestä viestinnästä annetun lain R. 10-13 §:ssä.

59 Ennakkoratkaisua pyytäneen tuomioistuimen asiana on tarkistaa tämä seikka, josta esitettiin istunnossa eriäviä näkemyksiä.

60 Asetuksen nro 2011-219 1 §.

61 Postitoiminnasta ja sähköisestä viestinnästä annetun lain R. 10-13 §.

62 Sekä La Quadrature du Net että Fédération des founisseurs d’accès à Internet associatifs tuovat esiin, että säilyttämisellä on monia eri tarkoituksia, että viranomaiset käyttävät harkintavaltaa niiden arvioinnissa, ettei niiden määrittelylle ole objektiivisia arviointiperusteita ja että tältä kannalta merkityksellisinä pidetään sellaisia rikollisuuden muotoja, joita ei voida luokitella vakaviksi.

63 Commission nationale de contrôle des techniques de renseignement (tietotekniikan kansallinen sääntelyviranomainen). Ks. tältä osin Ranskan hallituksen huomautukset, 145–148 kohta.

64 Komission huomautukset, 60 kohta.

65 Todellisuudessa kyseisessä lainsäädännössä mennään vielä pidemmälle, koska vaikuttaa siltä, että siinä edellytetään internetyhteyspalvelujen tapauksessa myös IP-osoitteen tai salausavainten säilyttämistä.

66 Tuomio Tele2 Sverige ja Watson, 100 kohta.

113. Yksikään asianosaisista ole kiistänyt sitä, että tämänkaltainen lainsäädäntö merkitsee puuttumista näihin oikeuksiin. Tätä kysymystä ei siten ole tarpeen käsitellä tarkemmin edes sen esiin tuomiseksi, että näiden oikeuksien loukkaaminen murentaa väistämättä sellaisen yhteiskunnan perusteita, jossa – muiden arvojen ohella – pyritään kunnioittamaan perusoikeuskirjassa taattua yksityisyyden suojaa.

114. Tuomioon Tele2 Sverige ja Watson perustuvan ja tuomiossa Ministerio Fiscal vahvistetun oikeuskäytännön soveltamisen perusteella voitaisiin luontevasti väittää, että nyt riitautetun kaltainen säännöstö ”ylittää – – täysin välttämättömän rajat, eikä sitä voida pitää perusteltuna demokraattisessa yhteiskunnassa siten kuin edellytetään direktiivin 2002/58 15 artiklan 1 kohdassa, kun se luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa”. [67]

115. Tuomiossa Tele2 Sverige ja Watson tarkastellun lainsäädännön tavoin nyt käsiteltävä lainsäädäntö nimittäin ”kattaa yleisesti kaikki tilaajat ja rekisteröidyt käyttäjät ja koskee kaikkia sähköisiä viestintävälineitä ja kaikkia liikennetietoja, ei tee mitään erottelua eikä aseta rajoituksia tai poikkeuksia asetetun tavoitteen perusteella”. [68] Näin ollen ”sitä sovelletaan siis myös henkilöihin, joiden osalta ei ole mitään seikkaa, jonka perusteella voitaisiin olettaa, että heidän toimintansa voisi olla edes epäsuorasti tai kaukaisesti yhteydessä vakavaan rikollisuuteen”, ja siinä ei myöskään säädetä minkäänlaisesta poikkeuksesta, ”joten sitä sovelletaan jopa henkilöihin, joiden viestintään sovelletaan kansallisen lainsäädännön mukaan salassapitovelvollisuutta”. [69]

116. Riidanalaisessa säännöstössä ei myöskään ”vaadita minkäänlaista yhteyttä säilytettäviksi säädettyjen tietojen ja yleistä turvallisuutta koskevan uhan välillä. Siinä ei varsinkaan rajoituta säilyttämään joko tiettyyn ajanjaksoon ja/tai maantieteellisesti määriteltyyn alueeseen ja/tai sellaisten tiettyjen henkilöiden piiriin, jotka voisivat olla sekaantuneita tavalla tai toisella vakavaan rikollisuuteen, liittyviä tietoja, tai henkilöihin, joiden tietojen säilyttäminen voisi muilla perusteilla myötävaikuttaa rikollisuuden torjumiseen, liittyviä tietoja.” [70]

117. Edellä esitetystä seuraa, että tämä lainsäädäntö ”ylittää – – täysin välttämättömän rajat, eikä sitä voida pitää perusteltuna demokraattisessa yhteiskunnassa siten kuin edellytetään direktiivin 2002/58 15 artiklan 1 kohdassa, kun se luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa”. [71]

118. Unionin tuomioistuimelle tämä oli riittävä peruste todeta, että kyseiset kansalliset säännöt eivät olleet yhteensopivia direktiivin 2002/58 15 artiklan 1 kohdan kanssa, koska niissä ”säädettiin rikollisuuden torjumiseksi kaikkien tilaajien ja rekisteröityjen käyttäjien liikenne- ja paikannustietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä kaikkien sähköisten viestintävälineiden osalta”. [72]

119. Tässä vaiheessa herääkin kysymys, voitaisiinko henkilötietojen säilyttämistä koskevaa unionin tuomioistuimen oikeuskäytäntöä tarkastella uudelleen tai ainakin nyansoida silloin, kun tämän ”yleisesti ja erotuksetta tapahtuvan” säilyttämisen tarkoituksena on terrorismin torjunta. Asiassa C-511/18 esitetty ensimmäinen ennakkoratkaisukysymys on muotoiltu nimenomaan ”asiayhteydessä, jolle ovat ominaisia vakavat ja jatkuvat uhat kansalliselle turvallisuudelle ja erityisesti terrorismin vaara”.

67 Ibidem, 107 kohta.

68 Ibidem, 105 kohta.

69 Sama.

70 Tuomio Tele2 Sverige ja Watson, 106 kohta.

71 Ibidem, 107 kohta.

72 Ibidem, 112 kohta.

120. Vaikka tämä on tietojen säilyttämisvelvoitteen asettamisen *tosiasiallinen asiayhteys*, sen *normatiivinen asiayhteys* ei kuitenkaan liity yksinomaan terrorismiin. Tietojen säilyttämistä ja saantia koskevassa järjestelmässä, josta Conseil d'État'ssa vireillä olevassa oikeudenkäynnissä on kyse, tämä säilyttämisvelvollisuus voidaan asettaa rikosten tutkintaan, toteamiseen ja syytteeseenpanoon liittyvistä yleisistä syistä.

121. Muistutan joka tapauksessa, että tuomion Tele2 Sverige ja Watson perusteluissa ei suinkaan jätetty huomiotta terrorismin torjuntaa ja että tuolloin unionin tuomioistuin katsoi, ettei tämä rikollisuuden muoto millään tavoin oikeuttanut sitä poikkeamaan oikeuskäytännöstään.[73]

122. Näin ollen ja lähtökohtaisesti katson, että ennakkoratkaisua pyytäneen tuomioistuimen esittämään kysymykseen, joka koskee terrorismin uhkan muodostamaa erityistapausta, on vastattava samalla tavoin kuin kysymykseen, jonka unionin tuomioistuin ratkaisi tuomiossa Tele2 Sverige ja Watson.

123. Kuten ratkaisuehdotuksessani Stichting Brein totesin, "vaikka oikeuden soveltamisen varmuus ei velvoitakaan tuomioistuimia soveltamaan ehdottomasti ennakkotapausoppia, niiden on kuitenkin noudatettava omia ratkaisujaan, jotka ne ovat huolellisen harkinnan jälkeen tehneet tietystä oikeuskysymyksestä".[74]

2) Rajoitettu tietojen säilyttäminen tilanteessa, jossa valtion turvallisuuteen kohdistuu uhkia, kuten terrorismin uhka

124. Olisiko tätä oikeuskäytäntöä kuitenkin mahdollista nyansoida tai täydentää, kun otetaan huomioon sen seuraukset terrorismin torjunnalle tai valtion suojelulle muilta vastaavilta kansallisen turvallisuuden vaarantavilta uhkilta?

125. Korostin jo edellä, että henkilötietojen säilyttäminen merkitsee jo yksinään puuttumista perusoikeuskirjan 7, 8 ja 11 artiklassa taattuihin oikeuksiin.[75] Riippumatta siitä, että säilyttämisen tarkoituksena on viime kädessä mahdollistaa tietojen *saanti* tiettynä ajankohtana, joko jälkikäteen tai samanaikaisesti,[76] jo pelkkä tietojen säilyttäminen, joka ylittää sen, mikä on ehdottoman välttämätöntä viestinnän välittämiseksi tai palveluntarjoajan suorittamien palvelujen laskuttamiseksi, tarkoittaa direktiivin 2002/58 5 ja 6 artiklassa vahvistettujen rajojen noudattamatta jättämistä.

126. Näiden palvelujen käyttäjillä (joita kehittyneimmissä yhteiskunnissa ovat lähes kaikki kansalaiset) on tai on voitava olla perusteltu luottamus siihen, että heistä ei ilman heidän suostumustaan säilytetä muita tietoja kuin ne, jotka on tallennettu kyseisten säännösten mukaisesti. Direktiivin 2002/58 15 artiklan 1 kohdan poikkeuksia on tulkittava tästä lähtökohdasta käsin.

73 Ibidem, 103 kohta.

74 C-527/15, EU:C:2016:938, 41 kohta.

75 Kuten unionin tuomioistuin lausunnon 1/15 124 kohdassa muistutti, "henkilötietojen välittäminen kolmannelle, kuten viranomaiselle, merkitsee puuttumista perusoikeuskirjan 7 artiklassa vahvistettuun perusoikeuteen välitettyjen tietojen myöhemmästä käytöstä riippumatta. Sama koskee henkilötietojen säilyttämistä sekä pääsyä kyseisiin tietoihin niiden käyttämiseksi viranomaisissa. Tässä yhteydessä ei ole merkitystä sillä, ovatko kyseessä olevat yksityiselämään liittyvät tiedot arkaluonteisia vai eivät tai onko asianomaisille mahdollisesti aiheutunut haittaa tästä puuttumisesta".

76 Kuten julkisasiamies Cruz Villalón totesi ratkaisuehdotuksensa Digital Rights (C-293/12 ja C-594/12, EU:C:2013:845) 72 kohdassa, "kuitenkin se, että valtaviin tietokantoihin kerätään, ja erityisesti se, että niissä säilytetään lukuisia tietoja, jotka on luotu tai joita on käsitelty unionin kansalaisten tavanomaisesta sähköisestä viestinnästä suurimman osan yhteydessä, merkitsee vakavaa puuttumista heidän yksityiselämäänsä, vaikka sillä vain luotaisiin edellytykset mahdollisuudelle valvoa taannehtivasti heidän sekä yksityistä että ammatillista toimintaansa. Näiden tietojen keräämisellä luodaan edellytykset valvonnalle, joka – vaikka sitä harjoitettaisiin vain taannehtivasti tietojen hyödyntämisen yhteydessä – uhkaa kuitenkin pysyvästi koko tietojen säilyttämisen ajan unionin kansalaisten oikeutta yksityisyyden suojaan. Valvontaa koskevan laajalle levinneen mielikuvan vuoksi kysymys tietojen säilyttämisajasta nousee erityisen voimakkaasti esille".

127. Kuten jo edellä selitin, tuomiossa Tele2 Sverige ja Watson unionin tuomioistuin katsoi kielletyksi myös sellaisen henkilötietojen yleisen ja erotuksetta tapahtuvan säilyttämisen, joka liittyy terrorismin torjuntaan.[77]

128. Vaikka kyseiseen tuomioon perustuva oikeuskäytäntö on saanut osakseen arvostelua, nähdäkseni siinä ei suinkaan vähätellä terrorismin uhkaa. Terrorismihan on erityisen vakava rikollisuuden muoto, jossa pyritään avoimesti uhmaamaan valtiovaltaa ja horjuttamaan tai tuhoamaan sen perusrakenteita. Valtiolle terrorismin torjunta on kirjaimellisesti elintärkeää, ja sen onnistuminen on kiistatta oikeusvaltion yleisen edun mukainen tavoite.

129. Käytännössä kaikki ennakkoratkaisumenettelyyn osallistuneet hallitukset ovat komission tavoin todenneet, että henkilötietojen osittainen ja valikoitu säilyttäminen olisi paitsi teknisesti vaikeaa, sillä myös vietäisiin kansallisilta tiedustelupalveluilta mahdollisuus hankkia yleiseen turvallisuuteen ja valtion puolustukseen kohdistuvien uhkien tunnistamisen ja terrori-iskujen tekijöiden syytteeseenpanon kannalta välttämättömiä tietoja.[78]

130. Tästä näkemyksestä on mielestäni aiheellista huomauttaa, ettei terrorismin torjuntaa pidä tarkastella pelkästään sen tehokkuuden kannalta. Terrorismin torjunnan vaikeus, mutta myös sen vahvuus, on juuri siinä, että sen keinojen ja menetelmien on vastattava oikeusvaltion vaatimuksia, mikä tarkoittaa ennen muuta sitä, että toimivaltuudet ja voimankäyttö pidetään lainsäädännön rajoissa ja että niissä erityisesti noudatetaan oikeusjärjestystä, jonka koko olemassaolon syy ja tarkoitus on puolustaa perusoikeuksia.

131. Kun terrorismiin käytettyjen keinojen ainoana oikeuttamisperusteena on vallitsevaan järjestykseen kohdistettujen iskujen puhdas (ja maksimaalinen) vaikuttavuus, oikeusvaltiossa tehokkuutta arvioidaan perusteilla, jotka eivät salli sitä, että oikeusvaltion puolustamisessa voitaisiin poiketa niistä menettelyistä ja takeista, jotka nimenomaan tekevät siitä laillisen järjestyksen. Antautuessaan suoraa päätä tehokkuuden tavoitteluun oikeusvaltio menettäisi ominaisuutensa, joka erottaa sen muista järjestyksistä, ja voisi äärimmäisissä tapauksissa itse muuttua uhkaksi kansalaisille. Kukaan ei voi taata, ettei julkinen valta silloin, kun se turvautuu rikosten syytteeseen panemiseksi liiallisiin keinoihin, joilla loukataan tai heikennetään perusoikeuksia, tällä hallitsemattomalla ja täysin vapaalla toiminnallaan rajoita lopulta kaikkien vapautta.

132. Kuten jo edellä totesin, julkisen vallan tehokkuuden viimeisenä rajana ovat unionin kansalaisten perusvapaudet, joita perusoikeuskirjan 52 artiklan 1 kohdan mukaan voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen, ”jos [nämä rajoitukset] ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia”.[79]

133. Niiden edellytysten osalta, joilla tietojen *valikoiva* säilyttäminen voitaisiin tuomion Tele2 Sverige ja Watson mukaan sallia, viittaan asiassa C-520/18 esittämääni ratkaisuehdotukseen.[80]

77 Tuomio Tele2 Sverige ja Watson, 103 kohta: se ”ei – – yksin voi oikeuttaa sitä, että kansallista säännöstöä, jossa säädetään kaikkien liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä, pidetään välttämättömänä mainitun torjumisen kannalta”.

78 Näin asian tulkitsee esimerkiksi Ranskan hallitus, joka havainnollistaa näkemystään käytännön esimerkeillä siitä, miten hyödyllistä on tietojen yleinen säilyttäminen, joka mahdollisti valtion vastatoimet Ranskassa viime vuosina tapahtuneissa vakavissa terrori-iskuissa (Ranskan hallituksen huomautukset, 107 ja 122–126 kohta).

79 Tuomio 15.2.2016, N (C-601/15 PPU, EU:C:2016:84, 50 kohta). Kyse on siis yleisen järjestyksen ja jo mainitsemani vapauden välisestä vaikeasti saavutettavasta tasapainosta, johon kaikessa unionin lainsäädännössä lähtökohtaisesti pyritään. Esimerkkinä voidaan mainita terrorismin torjumisesta sekä neuvoston puitepäätöksen 2002/475/YOS korvaamisesta sekä neuvoston päätöksen 2005/671/YOS muuttamisesta 15.3.2017 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2017/541 (EUVL 2017, L 88, s. 6). Sen 20 artiklan 1 kohdassa säädetään, että jäsenvaltioiden on varmistettava, että rikoksia tutkivilla tai niistä syytteeseen panevilla henkilöillä, yksiköillä tai muilla tahoilla ”on käytettävissä tehokkaat tutkintakeinot”, ja sen johdanto-osan 21 perustelukappaleessa todetaan samanaikaisesti, että tällaisten tehokkaiden keinojen käytön ”olisi oltava kohdennettua, ja siinä olisi otettava huomioon suhteellisuusperiaate sekä tutkinnan kohteena olevien rikosten luonne ja vakavuus ja siinä olisi kunnioitettava oikeutta henkilötietojen suojaan”.

80 87–95 kohta.

134. Olosuhteissa, joissa turvallisuuspalvelujen hallussa olevien tietojen perusteella on perusteltua syytä epäillä terrori-iskun valmistelua, voi olla perusteltua asettaa tiettyjen tietojen säilyttämistä koskeva velvollisuus. Sitäkin perustellumpaa tämän velvollisuuden asettaminen on silloin, kun tämä isku on tosiasiallisesti tehty. Vaikka jälkimmäisessä tapauksessa rikoksen tekeminen voi jo yksinään riittää toimenpiteen oikeuttamisperusteeksi, silloin, kun kyseessä on pelkkä epäily terrori-iskun yrityksestä, sitä tukevien seikkojen on välttämättä täytettävä tietty uskottavuuden vähimmäisvaatimus, jotta todisteita, jolla tätä epäilyä perustellaan, voitaisiin arvioida objektiivisesti.

135. Sekä niiden tietoryhmien, joiden säilyttämistä pidetään välttämättömänä, että asianomaisten henkilöiden piirin määrittäminen tarkasti ja objektiivisilla perusteilla on toki vaikeaa, muttei suinkaan mahdotonta. *Käytännöllisintä ja tehokkainta* olisi tietysti asettaa sähköisten viestintäpalvelujen tarjoajille yleinen ja syrjimätön velvoite säilyttää kaikki keräämänsä tiedot, mutta totesin jo edellä, ettei tätä kysymystä voida ratkaista *käytännön tehokkuuden* vaan *oikeudellisen tehokkuuden* perusteella ja oikeusvaltion ehdoilla.

136. Tämä määritystyö tapahtuu tyypillisesti antamalla lainsäädäntöä unionin tuomioistuimen oikeuskäytännössä vahvistetuissa rajoissa. Viittaan jälleen siihen, mitä asiassa C-520/18 esittämässäni ratkaisuehdotuksessa [81] totean tästä näkökohdasta.

3) Säilytettyjen tietojen saanti

137. Edellyttäen, että operaattorit ovat noudattaneet tietojen keruussa direktiivin 2002/58 säännöksiä ja että tietoja on säilytetty sen 15 artiklan 1 kohdan mukaisesti, [82] toimivaltaisille viranomaisille on annettava oikeus saada näitä tietoja, jos ne täyttävät unionin tuomioistuimen vahvistamat edellytykset, joita tarkastelen asiassa C-520/18 esittämässäni ratkaisuehdotuksessa, johon tässä viittaan. [83]

138. Kansallisessa lainsäädännössä on kuitenkin myös tällaisessa tilanteessa säädettävä aineellisista ja menettelyllisistä edellytyksistä, joiden täyttyessä toimivaltaiset viranomaiset voivat saada säilytettyjä tietoja. [84] Nyt käsiteltävien ennakkoratkaisupyyntöjen yhteydessä tämä oikeus voidaan myöntää vain sellaisten henkilöiden tietoihin, joiden epäillään suunnittelevan, tekevän tai tehneen terroriteon tai olevan jollakin tavalla mukana tällaisessa teossa. [85]

139. Kaiken kaikkiaan olennaista on se, että toimivaltaisten kansallisten viranomaisten oikeus saada säilytettyjä tietoja edellyttää lähtökohtaisesti asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta joko tuomioistuimen tai riippumattoman hallinnollisen elimen etukäteisvalvontaa ja sitä, että kyseisen tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä, jonka nämä viranomaiset esittävät. [86] Tällä tavoin tilanteessa, jossa lainsäädäntöön perustuva abstrakti arviointi ei ole mahdollista, pystytään takaamaan riippumattoman viranomaisen tekemä *konkreettinen* arviointi, jossa otetaan tasapuolisesti huomioon sekä valtion turvallisuuden takaaminen että kansalaisten perusoikeuksien suojelu.

81 100–107 kohta.

82 Kunhan tuomion Tele2 Sverige ja Watson 122 kohdassa mainittuja edellytyksiä noudatetaan: unionin tuomioistuin muistutti, että direktiivin 2002/58 15 artiklan 1 kohdassa ei sallita jäsenvaltioiden poiketa direktiivin 4 artiklan 1 kohdasta eikä 4 artiklan 1 a kohdasta, jossa edellytetään, että palveluntarjoajat toteuttavat toimenpiteitä, joilla voidaan varmistaa säilytettyjen tietojen suoja väärinkäytön vaaraa ja kaikenlaista laitonta saantia vastaan. Tämän perusteella se totesi, että ”kun otetaan huomioon säilytettyjen tietojen määrä, niiden arkaluonteisuus sekä niiden lainvastaista saantia koskeva vaara, sähköisten viestintäpalvelujen tarjoajien on mainittujen tietojen täyden koskemattomuuden ja luottamuksellisuuden takaamiseksi varmistettava erityisen korkea suojan ja turvan taso turvautumalla asianmukaisiin teknisiin ja organisatorisiin toimiin. Kansallisessa säännöstössä on erityisesti säädettävä tietojen säilyttämisestä unionin alueella ja tietojen lopullisesta hävittämisestä, kun niiden säilyttämisaika päättyy”.

83 52–60 kohta.

84 Tuomio Tele2 Sverige ja Watson, 118 kohta.

85 Ibidem, 119 kohta.

86 Ibidem, 120 kohta.

4) Velvollisuus säilyttää tiedot, joiden perusteella kyetään tunnistamaan sisältöjen luomiseen osallistuneet henkilöt, direktiivin 2000/31 kannalta tarkasteltuna (asiassa C-512/18 esitetty toinen ennakkoratkaisukysymys)

140. Ennakkoratkaisua pyytänyt tuomioistuin viittaa direktiiviin 2000/31, jota se pitää lähtökohtana määritettäessä, onko tietyt henkilöt[87] ja operaattorit, jotka tarjoavat yleisölle sähköisiä viestintäpalveluja, mahdollista velvoittaa säilyttämään tiedot, ”joiden perusteella kyetään tunnistamaan kuka tahansa henkilö, joka on ollut osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä, jotta lainkäyttöviranomainen voi tarvittaessa pyytää niiden toimittamista siviili- tai rikosvastuuta koskevien sääntöjen noudattamisen varmistamiseksi”.

141. Olen komission kanssa samaa mieltä siitä, että tämän velvoitteen yhteensopivuutta direktiivin 2000/31[88] kanssa ei voida tutkia, koska kyseisen direktiivin 1 artiklan 5 kohdan b alakohdassa jätetään sen soveltamisalan ulkopuolelle ”direktiivien 95/46/EY ja 97/66/EY soveltamisalaan kuuluviin tietoyhteiskunnan palveluihin liittyvät kysymykset”, ja viimeksi mainitut säädökset vastaavat nykyään asetusta N:o 2006/679 ja direktiiviä 2002/58[89], joiden 23 artiklan 1 kohtaa ja 15 artiklan 1 kohtaa on mielestäni tulkittava edellä esitetyn mukaisesti.

2. Velvollisuus kerätä liikenne- ja paikkatietoja reaaliajassa (asiassa C-511/18 esitetty toinen ennakkoratkaisukysymys)

142. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan sisäisestä turvallisuudesta annetun lain L. 851-2 §:ssä sallitaan yksinomaan terrorismin estämistä varten tietojen kerääminen reaaliajassa henkilöistä, joilla on etukäteen todettu olevan mahdollisia yhteyksiä terrorismin uhkaan. Kyseisen lain L. 851-4 §:ssä vastaavasti sallitaan se, että operaattorit siirtävät reaaliajassa teknisiä tietoja, jotka liittyvät päätelaitteiden sijaintiin.

143. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan näillä menetelmillä ei aseteta palveluntarjoajille ylimääräistä säilyttämisvaatimusta verrattuna siihen, mikä on välttämätöntä niiden palvelujen laskutusta ja markkinointia varten.

144. Sisäisestä turvallisuudesta annetun lain L. 851-3 §:n sanamuodon mukaan sähköisen viestinnän operaattorit ja teknisten palvelujen tarjoajat voidaan velvoittaa ”huolehtimaan verkoissaan automaattisesta tietojenkäsittelystä, jonka avulla kyetään havaitsemaan luvassa täsmennettyjen tekijöiden perusteella yhteyksiä, jotka saattavat paljastaa terrorismin uhan”. Tämä menetelmä ei sisällä yleisesti ja erotuksetta tapahtuvaa tietojen säilyttämistä koskevaa velvoitetta, vaan sillä pyritään ainoastaan keräämään rajoitetun ajan kuluessa kaikista näiden henkilöiden käsittelemistä yhteystiedoista sellaiset, jotka saattavat liittyä terrorismirikokseen.

145. Mielestäni samoja säilytettyjen henkilötietojen saannille asetettuja edellytyksiä on sovellettava myös sähköisessä viestinnässä syntyneiden tietojen reaaliaikaiseen saantiin. Näin ollen viittaan edellä tästä näkökohdasta esittämiini näkemyksiin. Sillä, onko kyse säilytetyistä tiedoista vai reaaliaikaisista tiedoista, ei ole merkitystä, koska saadut tiedot ovat kummassakin tapauksessa henkilötietoja riippumatta siitä, ovatko ne peräisin menneeltä vai nykyiseltä ajalta.

87 Henkilöt, ”jotka tarjoavat – – suurelle yleisölle verkkoviestintäpalvelujen kautta näiden palvelujen vastaanottajien toimittamien minkä tahansa merkkien, kirjoitusten, kuvien, äänien tai viestien säilytystä – –”.

88 Tämä direktiivi mainitaan kansallisen tuomioistuimen asiassa C-512/18 esittämässä toisessa ennakkoratkaisukysymyksessä ainoastaan yleisesti ja yksilöimättä mitään tiettyä säännöstä.

89 Komission huomautukset, 112 ja 113 kohta.

146. Jos siis reaaliaikainen pääsy tietoihin on seurausta yhteyksien havaitsemisesta sisäisestä turvallisuudesta annetun lain L. 851-3 §:ssä tarkoitetun kaltaisessa automaattisessa käsittelyssä, tätä käsittelyä varten ennalta vahvistettujen mallien ja kriteerien on oltava erityisiä, luotettavia ja syrjimättömiä, jotta niiden avulla voidaan tunnistaa henkilöt, joihin voi kohdistua kohtuullinen epäily osallistumisesta terrorismirikoksiin. [90]

3. Velvollisuus ilmoittaa tiedonkeruusta asianomaisille henkilöille (asiassa C-511/18 esitetty kolmas ennakkoratkaisukysymys)

147. Unionin tuomioistuin on vahvistanut, että toimivaltaisten kansallisten viranomaisten, joille on annettu oikeus saada säilytettyjä tietoja, on tiedotettava tästä asianomaisille henkilöille sovellettavien kansallisten menettelyjen mukaisesti heti, kun tämä tiedoksianto ei vaaranna kyseisten viranomaisten vireillä olevia tutkimuksia. Tämän velvoitteen syynä on se, että tällainen tiedottaminen on välttämätöntä, jotta nämä henkilöt voivat käyttää oikeussuojakeinoja, joista nimenomaisesti säädetään direktiivin 2002/58 15 artiklan 2 kohdassa, jos heidän oikeuksiaan loukataan. [91]

148. Conseil d'État haluaa asiassa C-511/18 esittämällään kolmannella ennakkoratkaisukysymyksellä selvittää, onko tätä ilmoittamisvaatimusta sovellettava ehdottomasti kaikissa tapauksissa vai voidaanko siitä poiketa silloin, kun on säädetty muita takeita, kuten ennakkoratkaisupyynnössä mainitut takeet.

149. Ennakkoratkaisua pyytäneen tuomioistuimen selostuksen [92] mukaan mainitut takeet muodostuvat siitä, että kenellä tahansa, joka haluaa varmistaa, että mitään tiedustelumenetelmää ei ole käytetty sääntöjenvastaisesti, on mahdollisuus saattaa asiansa Conseil d'État'n käsiteltäväksi. Tämä tuomioistuin voi tapauksen mukaan kumota toimenpiteelle annetun luvan ja määrätä kerättyjen tietojen tuhoamisesta menettelyssä, jossa ei noudateta oikeudenkäyntimenettelyille ominaista kontradiktorista periaatetta.

150. Ennakkoratkaisua pyytänyt tuomioistuin katsoo, ettei tällä lainsäädännöllä loukata oikeutta tehokkaaseen oikeussuojaan. Nähdäkseni tämä näkemys voi teoriassa pitää paikkansa niiden henkilöiden kohdalla, jotka päättävät tarkastaa, ovatko he tiedusteluoperaation kohteena. Kyseistä oikeutta ei sitä vastoin kunnioiteta, jos henkilöille, jotka ovat tai ovat olleet tällaisen operaation kohteina, ei ilmoiteta siitä ja jos he eivät siten voi saada selville edes sitä, onko heidän oikeuksiaan loukattu.

151. Oikeussuojatakeet, joihin ennakkoratkaisua pyytänyt tuomioistuin viittaa, vaikuttavat olevan riippuvaisia sen henkilön oma-aloitteisuudesta, joka epäilee, että hänestä kerätään henkilötietoja. Oikeus saattaa asiansa tehokkaasti tuomioistuimen käsiteltäväksi oikeuksiensa puolustamiseksi kuuluu kuitenkin kaikille, mikä tarkoittaa, että jokaisella, jonka henkilötietoja on käsitelty, on oltava mahdollisuus riitauttaa tämän käsittelyn lainmukaisuus tuomioistuimessa, ja että hänelle on siten ilmoitettava sen suorittamisesta.

152. Kuten toimitetuista tiedoista ilmenee, tuomioistuinmenettely voidaan panna vireille viran puolesta tai hallintoviranomaisen aloitteesta, mutta asianomaiselle henkilölle on joka tapauksessa annettava mahdollisuus saattaa itse asia vireille, minkä vuoksi on välttämätöntä, että hänelle ilmoitetaan, että hänen henkilötietojaan on käsitelty. Kyseisen henkilön oikeuksien puolustaminen ei voi olla sen varassa, että hän saa tämän käsittelyn tietoonsa kolmansilta osapuolilta tai omin avuin.

153. Näin ollen kyseiselle henkilölle on ilmoitettava tietojen saannista heti, kun tämä tiedoksianto ei vaaranna tutkimuksia, joita varten oikeus säilytettyjen tietojen saantiin on myönnetty.

90 Tuomio Digital Rights, 59 kohta.

91 Tuomio Tele2 Sverige ja Watson, 121 kohta.

92 Ennakkoratkaisupyynnön 8–11 kohta.

154. Kokonaan toinen kysymys on, että kun asianomainen henkilö on saattanut tuomioistuinmenettely vireille sen jälkeen, kun hänelle on ilmoitettu näiden tietojen saannista, tätä seuraavassa oikeudenkäyntimenettelyssä on noudatettava luottamuksellisuuden ja pidättyvyyden vaatimuksia, jotka kuuluvat erottamattomasti sellaisten toimenpiteiden laillisuusvalvontaan, joita julkinen valta toteuttaa valtion turvallisuuden ja puolustuksen kaltaisilla arkaluonteisilla aloilla. Tämä kysymys ei kuitenkaan kuulu nyt käsiteltäviin ennakkoratkaisupyyntöihin, joten unionin tuomioistuimen ei mielestäni tarvitse lausua siitä.

V Ratkaisuehdotus

155. Edellä esitetyn perusteella ehdotan, että unionin tuomioistuin vastaa Conseil d'État'n ennakkoratkaisukysymyksiin seuraavasti:

Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12.7.2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) 15 artiklan 1 kohtaa, luettuna yhdessä Euroopan unionin perusoikeuskirjan 7, 8 ja 11 artiklan ja 52 artiklan 1 kohdan kanssa, on tulkittava siten, että

1) se on esteenä kansalliselle lainsäädännölle, jossa sähköisten viestintäpalvelujen operaattoreille ja tarjoajille asetetaan asiayhteydessä, jolle ovat ominaisia vakavat ja jatkuvat uhat kansalliselle turvallisuudelle ja erityisesti terrorismin vaara, yleisesti ja erotuksetta velvollisuus säilyttää kaikkien tilaajiensa liikenne- ja paikkatiedot sekä tiedot, joiden perusteella kyetään tunnistamaan henkilöt, jotka ovat osallistuneet näiden palveluntarjoajien tarjoaman sisällön luomiseen

2) se on esteenä kansalliselle lainsäädännölle, jossa ei aseteta velvoitetta ilmoittaa asianomaisille henkilöille, että toimivaltaiset viranomaiset ovat käsitelleet heidän henkilötietojaan, ellei tämä ilmoitus vaaranna kyseisten toimivaltaisten viranomaisten toimenpiteitä

3) se ei ole esteenä kansalliselle lainsäädännölle, jossa sallitaan yksityishenkilöitä koskevien liikenne- ja paikkatietojen reaaliaikainen keruu, edellyttäen, että nämä toimenpiteet toteutetaan laillisesti säilytettyjen henkilötietojen saantia koskevien menettelyjen mukaisesti ja noudattaen sitä koskevia takeita.