Oikeustapauskokoelma

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

Asia C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY ja
XX
vastaan
Conseil des ministres,
sekä muuna osapuolena
Child Focus

(Ennakkoratkaisupyyntö – Cour constitutionnelle (perustuslakituomioistuin, Belgia)

Ennakkoratkaisupyyntö – Henkilötietojen käsittely ja yksityisyyden suoja sähköisen viestinnän alalla – Direktiivi 2002/58/EY – Soveltamisala – 1 artiklan 3 kohta – 15 artiklan 1 kohta – SEU 4 artiklan 2 kohta – Euroopan unionin perusoikeuskirja – 4, 6, 7, 8 ja 11 artikla ja 52 artiklan 1 kohta – Liikenne- ja paikkatietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä koskeva velvollisuus – Rikostutkinnan tehokkuus ja muut yleistä etua koskevat tavoitteet

1. Unionin tuomioistuin on viime vuosina noudattanut henkilötietojen säilyttämistä ja saantia koskevaa vakiintuneen oikeuskäytännön mukaista linjaa, jonka kannalta merkittäviä tuomioita ovat

– 8.4.2014 annettu tuomio Digital Rights Ireland ym.,[2] jossa unionin tuomioistuin totesi direktiivin 2006/24/EY[3] pätemättömäksi, koska siinä sallittiin suhteeton puuttuminen Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa tunnustettuihin oikeuksiin

1 Alkuperäinen kieli: espanja.

2 Asiat 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).

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

– 2.10.2018 annettu tuomio Ministerio Fiscal,[6] jossa unionin tuomioistuin vahvisti direktiivin 2002/58 saman säännöksen tulkinnan.

2. Nämä tuomiot (erityisesti toiseksi mainittu) huolestuttavat joidenkin jäsenvaltioiden viranomaisia, koska ne katsovat menettävänsä niiden seurauksena välineen, jota ne pitävät välttämättömänä kansallisen turvallisuuden suojaamisen ja rikollisuuden ja terrorismin torjunnan kannalta. Siksi jotkut näistä jäsenvaltioista puoltavat kyseisen oikeuskäytännön kumoamista tai nyansoimista.

3. Tietyt jäsenvaltioiden tuomioistuimet ovat tuoneet esiin saman huolenaiheen neljässä ennakkoratkaisupyynnössä[7], joista esitän ratkaisuehdotukseni samana päivänä nyt käsiteltävän ennakkoratkaisupyynnön kanssa.

4. Näissä neljässä asiassa on kyse ennen kaikkea direktiivin 2002/58 soveltamisesta, kun kyse on kansallisen turvallisuuden suojaamiseen ja terrorismin torjuntaan liittyvistä toimista. Jos kyseistä direktiiviä sovelletaan tässä yhteydessä, on seuraavaksi selvitettävä, missä määrin jäsenvaltiot voivat rajoittaa sillä turvattavaa oikeutta yksityisyyden suojaan. Viimeiseksi on tutkittava, missä määrin tätä alaa koskeva kansallinen lainsäädäntö (Yhdistyneen kuningaskunnan,[8] Belgian[9] ja Ranskan[10] lainsäädäntö) on unionin oikeuden, sellaisena kuin unionin tuomioistuin on sitä tulkinnut, mukainen.

5. Saatuaan tiedon tuomiosta Digital Rights Cour constitutionnelle (perustuslakituomioistuin, Belgia) kumosi kansallisen lainsäädännön, jolla direktiivi 2006/24, joka todettiin pätemättömäksi kyseisessä tuomiossa, oli saatettu osittain osaksi kansallista oikeutta. Belgian lainsäätäjä antoi tuolloin uuden säädöksen, ja myös sen yhteensoveltuvuus unionin oikeuden kanssa on asetettu kyseenalaiseksi tuomion Tele2 Sverige ja Watson johdosta.

6. Nyt käsiteltävän ennakkoratkaisupyynnön erityispiirre on se, että siinä annetaan mahdollisuus pidentää väliaikaisesti sellaisen kansallisen lain vaikutuksia, joka kansallisten tuomioistuinten on kumottava unionin oikeuden vastaisena.

I Asiaa koskevat oikeussäännöt

A Unionin oikeus

7. Viittaan asioissa C-511/18 ja C-512/18 esittämäni ratkaisuehdotuksen vastaavaan kohtaan.

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

7 Nyt käsiteltävän asian (C-520/18, Ordre des barreaux francophones et germanophone ym.) lisäksi kyseessä ovat asiat C-511/18 ja C-512/18, La Quadrature du Net ym. ja C-623/17, Privacy International.

8 Asia Privacy International, C-623/17.

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

10 Yhdistetyt asiat La Quadrature du Net ym., C-511/18 y C-512/18.

B Belgian oikeus. Tietojen keräämisestä ja säilyttämisestä sähköisen viestinnän alalla 29.5.2016 annettu laki [11]

8. Lain 4 §:ssä säädetään, että sähköisestä viestinnästä 13.6.2005 annetun lain [12] (loi du 13 juin 2005 relative aux communications électroniques) 126 §:ssä säädetään seuraavaa:

”1. Toimijat, jotka toimittavat yleisesti saatavilla olevia puhelinpalveluja, myös internetin välityksellä, internetyhteyden tai sähköpostipalveluja internetin välityksellä, ja operaattorit, jotka tarjoavat yleisesti saatavilla olevia sähköisiä viestintäverkkoja, sekä operaattorit, jotka tarjoavat jotain näistä palveluista, säilyttävät 3 momentissa tarkoitetut tiedot, joita ne luovat tai käsittelevät asianomaisten viestintäpalvelujen suorittamisen yhteydessä, tämän rajoittamatta yksityiselämän suojelusta henkilötietojen käsittelyssä 8.12.1992 annetun lain [loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel] soveltamista.

Tämä pykälä ei koske viestinnän sisältöä.

– –

2. Vain seuraavat viranomaiset voivat saada hakemuksesta 1 momentin 1 kohdassa tarkoitetuilta toimittajilta ja operaattoreita tämän pykälän nojalla säilytettyjä tietoja jäljempänä mainittuihin tarkoituksiin ja jäljempänä säädetyin edellytyksin:

1° oikeusviranomaiset rikosten tutkintaa, selvittämistä ja syyteharkintaa varten rikostutkintalain [Code d’instruction criminelle] 46bis ja 88bis §:ssä tarkoitettujen toimenpiteiden toteuttamista varten ja kyseisissä pykälissä vahvistetuin edellytyksin

2° tiedustelu- ja turvallisuusyksiköt hoitaakseen tiedustelutehtäviä tiedustelu- ja turvallisuuspalveluista 30.11.1998 annetun lain [loi du 30 novembre 1998 organique des services de renseignement et de Sécurité [13]] 16/2, 18/7 ja 18/8 §:ssä säädettyjen tiedonkeruumenetelmien avulla ja tässä laissa säädetyin edellytyksin

3° kuka tahansa Institut [belge des services postaux et des télécommunicationsin (Belgian posti- ja televiestintälaitos)] poliisivirkamies [verkkoturvallisuussääntöjen] ja tämän pykälän rikkomisten tutkintaa, selvittämistä ja syyteharkintaa varten

4° pelastusyksiköt, jotka tarjoavat ensiapua, jos ne eivät saa hätäpuhelun jälkeen kyseiseltä toimittajalta tai operaattorilta soittajan tunnistustietoja – – tai saavat puutteellisia tai virheellisiä tietoja. Pyynnön kohteena voivat olla vain soittajan tunnistustiedot, ja pyyntö on esitettävä 24 tunnin kuluessa puhelusta

5° Cellule des personnes disparues de la Police Fédéralen [liittovaltion poliisin kadonneiden henkilöiden yksikkö, Belgia] poliisivirkamies, kun hänen tehtävänään on avustaa vaarassa olevaa henkilöä ja etsiä henkilöitä, joiden katoaminen aiheuttaa huolta, ja kun voidaan olettaa tai on olemassa vakavia viitteitä siitä, että kadonneen henkilön fyysinen koskemattomuus on

11 Tietojen keräämisestä ja säilyttämisestä sähköisen viestinnän alalla 29.5.2016 annettu laki (loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, jäljempänä 29.5.2016 annettu laki) (Moniteur belge 18.7.2016, s. 44717).

12 Jäljempänä vuonna 2005 annettu laki (Moniteur belge 20.6.2005, s. 28070).

13 Jäljempänä vuonna 1998 annettu laki (Moniteur belge 18.12.1998, s. 40312).

välittömässä vaarassa. Asianomaiselta toimittajalta tai operaattorilta voidaan pyytää kuninkaan nimeämän poliisiyksikön välityksellä vain 3 momentin 1 ja 2 kohdassa tarkoitettuja tietoja, jotka liittyvät kadonneeseen henkilöön ja jotka on säilytetty 48 tunnin ajan ennen tietopyynnön esittämistä

6° Service de médiation pour les télécommunications [televiestinnän välitysyksikkö] sellaisen henkilön tunnistamiseksi, joka on käyttänyt vilpillisesti verkkoa tai sähköistä viestintäpalvelua – –. Pyynnön kohteena voivat olla vain tunnistustiedot.

Edellä 1 momentin 1 kohdassa tarkoitetut toimittajat ja operaattorit huolehtivat siitä, että 3 momentissa tarkoitetut tiedot ovat rajattomasti saatavilla Belgiasta ja että nämä tiedot ja kaikki muut näihin tietoihin liittyvät tarvittavat seikat voidaan toimittaa viipymättä ja yksinomaan tässä momentissa tarkoitetuille viranomaisille.

Edellä 1 momentin 1 kohdassa tarkoitetut toimittajat ja operaattorit eivät voi käyttää 3 momentin nojalla säilytettyjä tietoja muihin tarkoituksiin, jollei toisin ole lailla säädetty.

3. Tiedot, joilla tunnistetaan käyttäjä tai tilaaja ja viestintävälineet, lukuun ottamatta 2 ja 3 kohdassa nimenomaisesti säädettyjä tietoja, säilytetään 12 kuukauden ajan päivämäärästä, jona viestintä on viimeistä kertaa mahdollista käytetyn palvelun avulla.

Tiedot, jotka liittyvät päätelaitteen verkkoliittymään sekä tämän laitteen palveluun ja sijaintiin, mukaan lukien verkkopääte, säilytetään 12 kuukauden ajan viestintäpäivästä.

Viestintätiedot, sisältöä lukuun ottamatta, mukaan lukien lähtöpaikka ja määränpää, säilytetään 12 kuukauden ajan viestintäpäivästä.

Kuningas vahvistaa Belgian hallituksen toteuttaman yhteiskäsittelyn jälkeen oikeusministerin ja ministerin ehdotuksesta ja saatuaan Commission de la protection de la vie privéen ja laitoksen lausunnon tiedot, jotka on säilytettävä 1–3 kohdassa tarkoitettujen ryhmien mukaisesti, sekä vaatimukset, jotka näiden tietojen on täytettävä.

4. Edellä 3 momentissa tarkoitettujen tietojen säilyttämistä varten 1 momentin 1 kohdassa tarkoitetut toimittajat ja operaattorit

1° takaavat, että säilytetyt tiedot ovat samanlaatuisia ja että niitä koskevat samat tietoturvaa ja -suojaa koskevat vaatimukset kuin verkossa olevia tietoja

2° huolehtivat siitä, että säilytettyihin tietoihin kohdistetaan asianmukaisia teknisiä ja organisatorisia toimenpiteitä, jotta niitä voidaan suojata tahattomalta tai lainvastaiselta hävittämiseltä, tahattomalta katoamiselta tai muuttumiselta taikka luvattomalta tai lainvastaiselta varastoinnilta, käsittelyltä, tutustumiselta tai julkistamiselta

3° takaavat, että oikeus tutustua säilytettyihin tietoihin 2 momentissa tarkoitettujen viranomaisten pyyntöihin vastaamiseksi on vain yhdellä tai useammalla 126/1 §:n 1 momentissa tarkoitetun koordinointiyksikön jäsenellä

4° säilyttävät tiedot Euroopan unionin alueella

5º toteuttavat teknisiä suojatoimenpiteitä, joiden ansiosta säilytetyt tiedot eivät ole niiden rekisteröinnin jälkeen sellaisten henkilöiden luettavissa eivätkä käytettävissä, joilla ei ole lupaa tutustua niihin

6º tuhoavat säilytetyt tiedot kaikilta alustoilta sen jälkeen kun näihin tietoihin sovellettava 3 momentissa vahvistettu säilyttämisaika on päättynyt, tämän rajoittamatta 122 ja 123 §:n soveltamista

7º varmistavat säilytettyjen tietojen käytön jäljitettävyyden jokaisen 2 momentissa tarkoitetun viranomaisen näitä tietoja koskevan pyynnön osalta.

Edellä 1 momentin 7 kohdassa tarkoitettu jäljitettävyys toteutetaan lokikirjan avulla. Laitos ja Commission pour la protection de la vie privée voivat tutustua tähän lokikirjaan tai vaatia jäljennöstä, joka käsittää koko lokikirjan tai osan siitä. Laitos ja Commission pour la protection de la vie privée tekevät yhteistyöpöytäkirjan tutustumisesta lokikirjan sisältöön ja sen sisällön valvonnasta.

5. Oikeusministeri ja ministeri huolehtivat siitä, että edustajainhuoneelle toimitetaan vuosittain tilastoja, jotka koskevat yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämistä.

Näihin tilastoihin sisältävät erityisesti

1º tapaukset, joissa tiedot on toimitettu toimivaltaisille viranomaisille sovellettavien oikeussääntöjen mukaisesti

2º aika, joka kului siitä päivämäärästä, josta alkaen tietoja on säilytetty, siihen päivämäärään, jona toimivaltaiset viranomaiset pyysivät niiden toimittamista

3º tapaukset, joissa tietopyyntöjä ei ole voitu täyttää.

Nämä tilastot eivät voi sisältää henkilötietoja.

– –”

9. Lain 5 §:ssä säädetään, että vuonna 2005 annettuun lakiin on lisättävä 126/1 §, jonka sanamuoto on seuraava:

”1. Jokaiseen operaattoriin ja jokaiseen 126 §:n 1 momentin 1 kohdassa tarkoitettuun toimittajayritykseen perustetaan koordinointiyksikkö, jonka tehtävänä on antaa laillisesti valtuutetuille Belgian viranomaisille niiden pyynnöstä 122, 123 ja 126 §:n nojalla säilytettyjä tietoja, 107 §:n 2 momentin 1 kohdan nojalla soittajan tunnistustietoja tai tietoja, joita voidaan pyytää rikostutkintalain 46bis, 88bis ja 90ter §:n nojalla ja [vuonna 1998 annetun lain] 18/7, 18/8, 18/16 ja 18/17 §:n nojalla.

– –

2. Jokainen 126 §:n 1 momentin 1 kohdassa tarkoitettu operaattori ja toimittaja luo sisäisen menettelyn, jossa voidaan vastata viranomaisten pyyntöön saada käyttäjien henkilötietoja. Se

toimittaa pyynnöstä laitoksen käyttöön tietoja näistä menettelyistä, vastaanotettujen pyyntöjen lukumäärästä, esitetystä oikeusperustasta ja vastauksestaan.

– –

3. Jokainen 126 §:n 1 momentin 1 kohdassa tarkoitettu operaattori ja toimittaja nimeää henkilötietojen suojeluun yhden tai useamman valtuutetun, jonka on täytettävä kaikki 1 momentin 3 kohdassa luetellut edellytykset.

– –

Henkilötietojen suojelusta vastaava valtuutettu toimii tehtäviään hoitaessaan täysin riippumattomasti, ja hänellä on oikeus tutustua kaikkiin viranomaisille toimitettaviin henkilötietoihin sekä kaikkiin toimittajan tai operaattorin asianomaisiin toimitiloihin.

– –

4. Kuningas vahvistaa Belgian hallituksen toteuttaman yhteiskäsittelyn jälkeen ja Commission pour la protection de la vie privéen lausunnon saatuaan

– –

2° vaatimukset, jotka koordinointiyksikön on täytettävä, kun otetaan huomioon sellaisten operaattoreiden ja toimittajien tilanne, jotka saavat vain vähän pyyntöjä oikeusviranomaisilta, koska niillä ei ole toimipaikkaa Belgiassa tai ne toimivat pääasiallisesti ulkomailla

3° tiedot, jotka on toimitettava laitokselle ja Commission pour la protection de la vie privéelle 1 ja 3 momentin mukaisesti, sekä viranomaiset, joilla on oikeus tutustua näihin tietoihin

4° muut säännöt, jotka koskevat 126 §:n 1 momentin 1 kohdassa tarkoitettujen operaattoreiden ja toimittajien yhteistyötä Belgian viranomaisten tai tiettyjen Belgian viranomaisten kanssa 1 momentissa tarkoitettujen tietojen toimittamiseksi, mukaan lukien, mikäli tarpeen ja kulloisenkin viranomaisen osalta täsmennettynä, pyynnön muoto ja sisältö.

– –”

10. Lain 8 §:n nojalla rikostutkintalain 46bis §:n 1 momentti muutetaan seuraavan sisältöiseksi:

”1. Yleinen syyttäjä voi rikoksia selvittäessään perustellulla ja kirjallisella päätöksellä – tarvittaessa sähköisen viestintäverkon operaattorin, sähköisen viestintäpalvelun tarjoajan tai kuninkaan nimeämän poliisin yksikön myötävaikutuksella – kaikkien hallussaan olevien tietojen perusteella tai tutustumalla operaattorien tai palveluntarjoajien asiakkaiden tiedostoihin

1° tunnistaa sähköisen viestintäpalvelun tilaajan tai tavanomaisen käyttäjän taikka käytetyn sähköisen viestintävälineen

2° tunnistaa ne sähköiset viestintäpalvelut, jotka tietty henkilö on tilannut tai joita tietty henkilö tavanomaisesti käyttää.

Perustelut on suhteutettava yksityiselämän kunnioittamiseen, ja ne ovat toissijaisia mihin tahansa muuhun selvittämisvelvoitteeseen nähden.

Erittäin kiireellisessä tapauksessa jokainen poliisivirkamies voi virallisen syyttäjän suullisella ja etukäteisellä suostumuksella ja perustellulla ja kirjallisella päätöksellä pyytää tällaisia tietoja. Poliisivirkamiehen on ilmoitettava tällaisesta perustellusta ja kirjallisesta päätöksestä sekä saaduista tiedoista 24 tunnissa viralliselle syyttäjälle ja perusteltava toimenpiteen erityinen kiireellisyys.

Yleinen syyttäjä tai erityisen kiireellisessä tapauksessa poliisivirkamies voi vaatia rikoksista, joista ei voi seurata pääseuraamuksena yhden vuoden ehdotonta vankeusrangaistusta tai ankarampaa rangaistusta, 1 kohdassa tarkoitettuja tietoja vain päätöstään edeltävien kuuden kuukauden ajalta. – –

2. Kaikkien sähköisten viestintäverkkojen operaattoreiden ja sähköisen viestintäpalvelun tarjoajien, joita vaaditaan toimittamaan edellä 1 momentissa tarkoitetut tiedot, on annettava viralliselle syyttäjälle tai poliisivirkamiehelle pyydetyt tiedot kuninkaan vahvistamassa määräajassa – –.

– –

Kaikilla henkilöillä, jotka saavat tehtäviensä vuoksi tiedon toimenpiteestä tai osallistuvat siihen, on salassapitovelvollisuus. Salassapitovelvollisuuden laiminlyönnistä määrätään seuraamus rikoslain [Code pénal] 458 §:n mukaisesti.

Tietojen toimittamatta jättämisestä määrätään rangaistuksena sakko, jonka suuruus on 26–10 000 euroa.”

11. Lain 9 artiklan nojalla rikostutkintalain 88bis §:n sanamuoto on seuraava:

”1. Jos on olemassa vakavia viitteitä siitä, että rikkomiset saattavat johtaa pääseuraamuksena yhden vuoden vankeusrangaistukseen tai ankarampaan rangaistukseen, ja tutkintatuomari arvioi, että on olemassa seikkoja, joiden vuoksi sähköisen viestinnän jäljittäminen tai sähköisen viestinnän lähtöpaikan tai määränpään paikantaminen on välttämätöntä totuuden selvittämiseksi, hän voi tarvittaessa suoraan tai kuninkaan nimeämän poliisin yksikön välityksellä sähköisten viestintäverkkojen operaattorilta tai sähköisen viestintäpalvelun tarjoajalta saamansa teknisen avun turvin

1° jäljittää liikennetietoja sellaisten sähköisten viestintävälineiden osalta, joista sähköinen viestintä on lähtöisin tai joille se on osoitettu

2° paikantaa sähköisen viestinnän lähtöpaikan tai määränpään.

Edellä 1 kohdassa tarkoitetuissa tapauksissa ilmoitetaan kunkin sähköisen viestintävälineen osalta, jonka puhelutiedot jäljitetään tai jonka osalta televiestinnän lähtöpaikka tai määränpää paikannetaan, päivä, kellonaika, kesto ja tarvittaessa sähköisen viestinnän paikka, ja tiedot merkitään pöytäkirjaan.

Tutkintatuomari ilmoittaa perustellulla määräyksellä asiaan liittyvät tosiseikat, joiden vuoksi toimenpide on perusteltu, sen oikeasuhteisuuden yksityiselämän kunnioittamiseen nähden ja toissijaisuuden kaikkiin muihin selvittämisvelvoitteisiin nähden.

Se täsmentää myös, miten pitkään toimenpidettä voidaan soveltaa tulevaisuudessa, jolloin sen kesto ei voi olla pidempi kuin kaksi kuukautta määräyksen päivämäärästä, tämän rajoittamatta toimenpiteen uudistamista ja tarvittaessa menneisyyteen ulottuvaa ajanjaksoa, johon määräys ulottuu 2 momentin perusteella.

– –

2. Siltä osin kuin kyseessä on 1 momentin 1 kohdassa tarkoitetun toimenpiteen soveltaminen liikenne- tai paikkatietoihin, jotka on säilytetty [vuonna] 2005 annetun lain 126 §:n nojalla, sovelletaan seuraavia säännöksiä:

– rikoslain II kirjan I ter osastossa tarkoitetun rikoksen osalta tutkintatuomari voi määräyksessään vaatia tietoja määräystä edeltäneiden 12 kuukauden ajanjaksolta

– 90 ter §:n 2–4 momentissa tarkoitetun muun rikoksen osalta, jota ei tarkoiteta ensimmäisessä luetelmakohdassa, tai sellaisen rikoksen osalta, johon on syyllistytty rikoslain 324bis §:ssä tarkoitetun järjestäytyneen rikollisryhmän yhteydessä, tai sellaisen rikoksen osalta, joka saattaa johtaa pääseuraamuksena viiden vuoden vankeusrangaistukseen tai ankarampaan rangaistukseen, tutkintatuomari voi määräyksessään vaatia tietoja määräystä edeltäneiden 9 kuukauden ajanjaksolta

– muiden rikosten osalta tutkintatuomari voi vaatia tietoja vain määräystä edeltäneiden kuuden kuukauden ajanjaksolta.

3. Toimenpide voi koskea asianajajan tai lääkärin sähköisiä viestintävälineitä vain, jos tämän itsensä epäillään syyllistyneen 1 momentissa tarkoitettuun rikokseen tai osallistuneen siihen tai jos täsmällisten tosiseikkojen perusteella voidaan olettaa, että kolmannet henkilöt, joiden epäillään syyllistyneen 1 kohdassa tarkoitettuun rikokseen, käyttävät hänen sähköisiä viestintävälineitään.

Toimenpidettä ei voida toteuttaa, ellei tapauksen mukaan asianajajayhteisön puheenjohtajalle tai lääkäreiden alueyhdistyksen edustajalle ilmoiteta tästä. Tutkintatuomari ilmoittaa näille samoille henkilöille seikoista, joiden hän katsoo kuuluvan salassapitovelvollisuuden piiriin. Näitä seikkoja ei kirjata pöytäkirjaan.

4. – –

Kaikilla henkilöillä, jotka saavat tehtäviensä vuoksi tiedon toimenpiteestä tai osallistuvat siihen, on salassapitovelvollisuus. Salassapitovelvollisuuden laiminlyönnistä määrätään seuraamus rikoslain 458 §:n mukaisesti.

– –”

12. Lain 12 §:n nojalla vuonna 1998 annetun lain 13 §:n sanamuoto on seuraava:

”Tiedustelu- ja turvallisuusyksiköt voivat etsiä, kerätä, vastaanottaa ja käsitellä tietoja ja henkilötietoja, jotka voivat olla hyödyllisiä niiden tehtävän hoitamisen kannalta, ja pitää ajan tasalla asiakirja-aineistoa, joka liittyy erityisesti tapahtumiin, ryhmittymiin ja henkilöihin, joilla on merkitystä heidän tehtäviensä hoitamisen kannalta.

Asiakirja-aineistoon sisältyvillä tiedoilla on oltava yhteys tiedoston tarkoitukseen, ja niiden on koskettava vain siitä johtuvia velvoitteita.

Tiedustelu- ja turvallisuusyksiköt huolehtivat niiden lähteisiin liittyvien tietojen turvallisuudesta ja näiden lähteiden toimittamien tietojen ja henkilötietojen turvallisuudesta.

Tiedustelu- ja turvallisuusyksiköiden tutkijoilla on oikeus tutustua tietoihin, selvityksiin ja henkilötietoihin, joita heidän yksikkönsä on kerännyt ja käsitellyt, siltä osin kuin ne ovat hyödyllisiä heidän hoitaessaan tehtäväänsä tai toimeksiantoaan.”

13. Lain 14 §:ssä annetaan vuonna 18/3 §:lle uusi sanamuoto. Lain 18/3 §:ssä säädetään sittemmin seuraavaa:

”1. Edellä 18/2 §:n 1 momentissa tarkoitettuja erityisiä tiedonkeruumenetelmiä voidaan soveltaa, kun otetaan huomioon 18/1 §:ssä tarkoitettu mahdollinen uhka, jos tavanomaisia tiedonkeruumenetelmiä pidetään riittämättöminä, jotta kyetään keräämään tiedustelutehtävän onnistumiseksi tarvittavat tiedot. Erityinen menetelmä on valittava sen mukaan, miten suuri on mahdollinen uhka, jota varten sitä sovelletaan.

Erityinen menetelmä voidaan ottaa käyttöön vasta yksikön johtajan kirjallisen ja perustellun päätöksen jälkeen ja sen jälkeen, kun tämä päätös on annettu tiedoksi komitealle.

2. Yksikön johtajan päätöksessä mainitaan seuraavat asiat:

1° erityisen menetelmän luonne

2° tilanteen mukaan luonnolliset henkilöt tai oikeushenkilöt, järjestöt tai ryhmittymät, kohteet, paikat, tapahtumat ja tiedot, joihin sovelletaan erityistä menetelmää

3° mahdollinen uhka, joka oikeuttaa erityisen menetelmän soveltamisen

4° tosiseikat, jotka oikeuttavat erityisen menetelmän soveltamisen, toissijaisuusperiaatteeseen ja oikeasuhteisuuteen liittyvät perustelut, mukaan lukien 2 ja 3 kohdan välinen yhteys

5° ajanjakso, jonka aikana erityistä menetelmää voidaan soveltaa, lukien päätöksen tiedoksiannosta komissiolle

– –

9° tarvittaessa vakavat viitteet, jotka osoittavat, että asianajaja, lääkäri tai toimittaja osallistuu tai on osallistunut henkilökohtaisesti ja aktiivisesti mahdollisen uhan syntymiseen tai kehittymiseen

10º mikäli sovelletaan 18/8 §:ää, perustelut sen ajanjakson kestolle, johon tietojen keruu liittyy

– –

8. Yksikön johtaja lopettaa erityisen menetelmän soveltamisen, jos sen oikeutuksena oleva mahdollinen uhka on hävinnyt, jos menetelmä ei ole enää hyödyllinen siihen tarkoitukseen, jota varten se on otettu käyttöön, tai jos lainvastaisuus on todettu. Se ilmoittaa päätöksestään mahdollisimman nopeasti komissiolle.”

14. Vuonna 1988 annetun lain 18/8 §:ssä säädetään sittemmin seuraavaa:

”1. Tiedustelu- ja turvallisuusyksiköt voivat tehtäviään hoitaessaan tarvittaessa pyytämällä tähän sähköisen viestintäverkon operaattorilta tai sähköisen viestintäpalvelun toimittajalta teknistä tukea

1º jäljittää tai pyytää jäljittämään niiden sähköisten viestintävälineiden liikennetiedot, joista tai joihin sähköinen viestintä osoitetaan tai on osoitettu

2º paikantaa tai pyytää paikantamaan sähköisen viestinnän lähtöpaikan tai määränpään.

– –

2. Siltä osin kuin kyseessä on 1 momentissa tarkoitetun menetelmän soveltaminen tietoihin, jotka on säilytetty [vuonna] 2005 annetun lain 126 §:n perusteella, sovelletaan seuraavia säännöksiä:

1º sen mahdollisen uhkan osalta, joka liittyy toimintaan, joka saattaa olla yhteydessä järjestäytyneisiin rikollisryhmiin tai haitallisiin ääriliikkeisiin, yksikön johtaja voi vaatia päätöksessään tietoja vain päätöstä edeltävien kuuden kuukauden ajanjaksolta

2º muun kuin 1 ja 3 kohdassa tarkoitetun mahdollisen uhkan osalta yksikön johtaja voi vaatia päätöksessään tietoja päätöstä edeltävien yhdeksän kuukauden ajanjaksolta

3.º sellaisen mahdollisen uhkan osalta, joka liittyy toimintaan, joka saattaa olla yhteydessä terrorismiin tai ääriliikkeisiin, yksikön johtaja voi vaatia päätöksessään tietoja päätöstä edeltävien 12 kuukauden ajanjaksolta. – –”.

II Tosiseikat ja ennakkoratkaisukysymykset

15. Cour constitutionnelle kumosi 11.6.2015 antamassaan tuomiossa [14] vuonna 2005 annetun lain 126 §:n uudelleen laaditun toisinnon samoista syistä, joiden takia unionin tuomioistuin oli tuomiossa Digital Rights todennut direktiivin 2006/24 pätemättömäksi.

16. Kansallinen lainsäätäjä antoi tämän kumoamisen johdosta (ennen tuomion Tele 2 Sverige ja Watson antamista) 29.5.2016 annetun lain.

[14] Tuomio 84/2015, Moniteur belge 11.8.2015.

17. VZ ym., Ordre des barreaux francophones et germanophone (jäljempänä Ordre des barreaux), Liga voor Mensenrechten ASBL (jäljempänä LMR), Ligue des Droits de l'Homme ASBL (jäljempänä LDH) ja Académie Fiscale ASBL (jäljempänä Académie Fiscale) nostivat ennakkoratkaisua pyytäneessä tuomioistuimessa useita mainitun lain perustuslainmukaisuutta koskevia kanteita ja väittivät lähinnä, että siinä ylitettiin se, mikä oli ehdottoman välttämätöntä, ja ettei siinä säädetty suojaa koskevista riittävistä takeista.

18. Tässä tilanteessa Cour constitutionnelle on esittänyt unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”1 Onko direktiivin 2002/58/EY 15 artiklan 1 kohtaa, kun sitä luetaan yhdessä Euroopan unionin perusoikeuskirjan [(jäljempänä perusoikeuskirja)] 6 artiklassa taatun turvallisuutta koskevan oikeuden ja – – perusoikeuskirjan 7 ja 8 artiklassa sekä 52 artiklan1 kohdassa taatun henkilötietojen suojaa koskevan oikeuden kanssa, tulkittava siten, että se on esteenä kyseessä olevan kaltaiselle kansalliselle säännöstölle, jossa säädetään operaattoreita ja sähköisten viestintäpalvelujen tarjoajia koskevasta yleisestä velvollisuudesta säilyttää direktiivissä 2002/58/EY tarkoitetut kyseisten palvelujen suorittamisen yhteydessä luodut tai käsitellyt liikenne- ja paikkatiedot ja jonka tavoitteena ei ole ainoastaan vakavien rikosten tutkinta, selvittäminen ja syyteharkinta vaan myös valtion turvallisuuden, maanpuolustuksen ja yleisen turvallisuuden takaaminen, muiden tekojen kuin vakavan rikollisuuden tutkinta, selvittäminen ja syyteharkinta tai sähköisten viestintäjärjestelmien kielletyn käytön torjuminen taikka jonkin muun [luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston] asetuksen (EU) 2016/679 [(yleinen tietosuoja-asetus) (EUVL 2016, L 119, s. 1)] 23 artiklan 1 kohdassa yksilöidyn tavoitteen toteuttaminen ja jota lisäksi koskevat kyseisessä säännöstössä tietojen säilyttämisen ja tietoihin tutustumisen osalta asetetut täsmälliset takeet?

2) Onko direktiivin 2002/58/EY 15 artiklan 1 kohtaa, kun sitä luetaan yhdessä – – perusoikeuskirjan 4, 7, 8, ja 11 artiklan sekä 52 artiklan 1 kohdan kanssa, tulkittava siten, että se on esteenä kyseessä olevan kaltaiselle kansalliselle säännöstölle, jossa säädetään operaattoreita ja sähköisten viestintäpalvelujen tarjoajia koskevasta yleisestä velvollisuudesta säilyttää direktiivissä 2002/58/EY tarkoitetut kyseisten palvelujen suorittamisen yhteydessä luodut tai käsitellyt liikenne- ja paikkatiedot, jos kyseisillä säännöksillä on tarkoitus muun muassa toteuttaa viranomaisille perusoikeuskirjan 4 ja 8 artiklan perusteella kuuluvat positiiviset velvollisuudet eli säätää lainsäädännöllisestä kehyksestä, jolla mahdollistetaan tehokas rikostutkinta ja tehokas seuraamusten määrääminen alaikäisiin kohdistuvasta seksuaalisesta hyväksikäytöstä sekä tällaisen rikoksentekijän tunnistaminen tehokkaasti myös silloin, kun tekijä käyttää sähköisiä viestintävälineitä?

3) Jos Cour constitutionnelle tekisi ensimmäiseen tai toiseen ennakkoratkaisukysymykseen annettavien vastausten perusteella sen päätelmän, että riidanalaisessa laissa jätetään huomiotta yksi tai useampi näissä kysymyksissä mainituista säännöksistä ja määräyksistä johtuva velvollisuus, voisiko se pitää väliaikaisesti voimassa [riidanalaisen] lain vaikutukset, jotta vältetään oikeudellinen epävarmuus ja mahdollistetaan aikaisemmin kerättyjen ja säilytettyjen tietojen käyttäminen lakisääteisiin tarkoituksiin?”

III Asian käsittelyn vaiheet unionin tuomioistuimessa

19. Ennakkoratkaisupyyntö kirjattiin saapuneeksi unionin tuomioistuimeen 2.8.2018.

20. Kirjallisia huomautuksia ovat esittäneet VZ ym., Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), Saksan, Belgian, Yhdistyneen kuningaskunnan, Tšekin, Kyproksen, Tanskan, Espanjan, Viron, Ranskan, Unkarin, Irlannin, Alankomaiden, Puolan ja Ruotsin hallitukset sekä komissio.

21. Yhdessä asioiden C-511/18, C-512/18 ja C-623/17 kanssa pidettiin 9.9.2019 julkinen istunto, johon osallistuivat neljän ennakkoratkaisupyynnön asianosaiset, edellä mainitut hallitukset ja Norjan hallitus sekä Euroopan komissio ja Euroopan tietosuojavaltuutettu.

IV Asian tarkastelu

22. Ensimmäinen ennakkoratkaisukysymys on olennaisilta osin sama kuin asioissa C-511/18 ja C-512/18 esitetyt kysymykset. Se eroaa kuitenkin viimeksi mainituista kysymyksistä kansalliselle lainsäädännölle asetettujen tavoitteiden osalta: niitä eivät ole vain terrorismin ja rikollisuuden vakavimpien muotojen torjuminen tai kansallisen turvallisuuden suojaaminen vaan myös ”maanpuolustuksen ja yleisen turvallisuuden takaaminen, muiden tekojen kuin vakavan rikollisuuden tutkinta, selvittäminen ja syyteharkinta” ja yleisesti mikä tahansa asetuksen N:o 2016/679 23 artiklan 1 kohdassa säädetyistä tavoitteista.

23. Toinen kysymys liittyy ensimmäiseen ja täydentää sitä, koska siinä pohditaan, voidaanko kyseessä olevia toimenpiteitä perustella julkiselle vallalle kuuluvilla positiivisilla velvoitteilla, jotka koskevat alaikäisiin kohdistuvan seksuaalisen hyväksikäytön tutkintaa ja kyseisestä rikoksesta määrättäviä seuraamuksia.

24. Kolmas kysymys esitetään siinä tapauksessa, että kansallinen lainsäädäntö on ristiriidassa unionin oikeuden kanssa. Ennakkoratkaisua pyytänyt tuomioistuin pyrkii selvittämään, voiko se tällaisessa tapauksessa pitää väliaikaisesti voimassa 29.5.2016 annetun lain vaikutukset.

25. Käsittelen näitä kysymyksiä tutkimalla ensin direktiivin 2002/58 sovellettavuutta, ja viittaan sitä varten näissä muissa ennakkoratkaisupyynnöissä esittämiini ratkaisuehdotuksiin. Esittelen toiseksi lyhyesti asiaa koskevan unionin tuomioistuimen oikeuskäytännön päälinjat ja sen mahdolliset tulkinnat. Lopuksi esitän ratkaisun kuhunkin ennakkoratkaisukysymykseen.

A Direktiivin 2002/58 sovellettavuus

26. Muiden ennakkoratkaisupyyntöjen tavoin tässäkin ennakkoratkaisupyynnössä on kyseenalaistettu direktiivin 2002/58 sovellettavuus. Koska jäsenvaltioiden tässä asiassa puoltamat näkemykset ovat samanlaiset, viittaan tältä osin asioissa C-511/18 ja C-512/18 esittämiini ratkaisuehdotuksiin. [15]

[15] 40 kohta ja sitä seuraavat kohdat.

B Unionin tuomioistuimen oikeuskäytäntö, joka koskee viranomaisilla direktiivin 2002/58 nojalla olevaa oikeutta säilyttää henkilötietoja ja tutustua niihin

1. Viestinnän ja siihen liittyvien tietojen luottamuksellisuuden periaate

27. Direktiivin 2002/58 säännöksillä ”täsmennetään ja täydennetään” direktiiviä 95/46/EY [16], jotta varmistetaan henkilötietojen suojan korkea taso sähköisten viestintäpalvelujen tarjoamisen yhteydessä. [17]

28. Direktiivin 2002/58 5 artiklan 1 kohdan mukaan jäsenvaltioiden on kansallisessa lainsäädännössä varmistettava yleisen viestintäverkon ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän sekä vastaavien liikennetietojen luottamuksellisuus.

29. Viestinnän luottamuksellisuus edellyttää muun muassa (direktiivin 2002/58 5 artiklan 1 kohdan toinen virke) sen kieltämistä, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta tallentavat sähköiseen viestintään liittyviä liikennetietoja. Poikkeuksia ovat ”henkilöt, joiden – – toiminta on – – laillisesti sallittua, ja tekninen tallentaminen, joka on tarpeen viestinnän välittämiselle”. [18]

30. Direktiivin 2002/58 5 ja 6 artiklan ja 9 artiklan 1 kohdan tarkoituksena on säilyttää viestinnän ja siihen liittyvien tietojen luottamuksellisuus ja minimoida väärinkäytön vaara. Sen soveltamisalaa on arvioitava suhteessa kyseisen direktiivin johdanto-osan 30 perustelukappaleeseen, jonka mukaan ”sähköisiä viestintäverkkoja ja -palveluita tarjoavat järjestelmät olisi suunniteltava niin, että tarvittavien henkilötietojen määrä rajoitetaan mahdollisimman *pieneksi*”. [19]

31. Näiden tietojen osalta voidaan erottaa toisistaan

– *liikennetiedot*, joiden käsittely ja tallentaminen on sallittua vain siinä määrin ja niin kauan kuin palvelujen laskuttaminen ja markkinointi sekä lisäarvopalveluiden tarjoaminen sitä edellyttävät (direktiivin 2002/58 6 artikla). Tämän määräajan päätyttyä käsitellyt ja tallennetut tiedot on poistettava tai tehtävä nimettömiksi. [20]

– muita kuin liikennettä koskevia *paikkatietoja* saa käsitellä vain tietyin edellytyksin ja sen jälkeen, kun ne on tehty nimettömiksi tai jos käyttäjät tai tilaajat ovat antaneet siihen suostumuksensa (direktiivin 2002/58 9 artiklan 1 kohta). [21]

16 Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annettu direktiivi (EYVL 1995, L 281, s. 31). Ks. direktiivin 2002/58 1 artiklan 2 kohta. Direktiivi 95/46 kumottiin 25.5.2018 alkaen asetuksella N:o 2016/679. Siltä osin kuin direktiivissä 2002/58 viitataan direktiiviin 95/46 tai siinä ei anneta omia säännöksiä on välttämätöntä ottaa huomioon kyseisen asetuksen säännökset (ks. asetuksen N:o 2016/679 94 artiklan 1 ja 2 kohta).

17 Tuomio Tele2 Sverige ja Watson, 82 ja 83 kohta.

18 Ibidem, 85 kohta oikeuskäytäntöviittauksineen.

19 Ibidem, 87 kohta. Kursivointi tässä.

20 Ibidem, 86 kohta oikeuskäytäntöviittauksineen.

21 Ibidem, 86 kohdan loppu.

2. Direktiivin 2002/58 15 artiklan 1 kohdassa säädetty rajoituslauseke

32. Direktiivin 2002/58 15 artiklan 1 kohdan mukaan 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”.

33. Rajoitusten on oltava ”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] 13 artiklan 1 kohdan mukaisesti”.

34. Kyseinen tavoitteiden luettelo on luonteeltaan tyhjentävä:[22] voidaan hyväksyä esimerkiksi (”muun muassa”) ”lainsäädännöllisiä toimenpiteitä, joissa säädetään tietojen säilyttämisestä sellaiseksi rajoitetuksi ajaksi, joka on perusteltua tässä kohdassa säädetyistä syistä”.

35. Joka tapauksessa ”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”. Direktiivin 2002/58 15 artiklan 1 kohtaa on näin ollen tulkittava perusoikeuskirjassa taattujen perusoikeuksien valossa.[23]

36. Näistä perusoikeuskirjassa tunnustetuista oikeuksista unionin tuomioistuin on maininnut nyt käsiteltävän asian kannalta merkityksellisinä oikeuden yksityisyyteen (7 artikla), oikeuden henkilötietojen suojaan (8 artikla) ja sananvapauden (11 artikla).[24]

37. Unionin tuomioistuin on samoin korostanut direktiivin 2002/58 15 artiklan 1 kohdan tulkintaperiaatteena, että viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuuden takaamista koskevan velvollisuuden rajoituksia on tulkittava suppeasti.

38. Se on hylännyt erityisesti sen, että ”velvollisuudesta ja erityisesti kyseisen direktiivin 5 artiklassa säädetystä tietojen tallentamista koskevasta kiellosta tehtävästä poikkeuksesta tulisi sääntö – tällöin tehtäisiin viimeksi mainitun säännöksen sisältö laajalti tyhjäksi”.[25]

39. Nämä kaksi huomautusta ovat mielestäni ratkaisevia sen ymmärtämiseksi, miksi unionin tuomioistuin katsoi sähköiseen viestintään liittyvien liikenne- ja paikkatietojen yleisen ja erotuksetta tapahtuvan säilyttämisen olevan ristiriidassa direktiivin 2002/58 kanssa.

22 Ibidem, 90 kohta.

23 Ibidem, 91 kohta oikeuskäytäntöviittauksineen.

24 Ibidem, 93 kohta oikeuskäytäntöviittauksineen.

25 Ibidem, 89 kohta.

40. Näin todetessaan unionin tuomioistuin ainoastaan sovelsi ”ehdottomasti”[26] jo aikaisemmin käyttämäänsä oikeasuhteisuuden edellytystä:[27] ”yksityiselämän kunnioitusta koskevan perusoikeuden suoja unionin tasolla edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset on toteutettava täysin välttämättömän rajoissa.”[28]

3. Tietojen säilyttämisen oikeasuhteisuus

a) Yleisen ja erotuksetta tapahtuvan säilyttämisen suhteettomuus

41. Unionin tuomioistuin myönsi, että vakavan rikollisuuden, muun muassa järjestäytyneen rikollisuuden ja terrorismin, torjuminen on ensisijaisen tärkeää yleisen turvallisuuden takaamiseksi, ja tämän torjumisen tehokkuus voi riippua suuressa määrin nykyaikaisten tutkintatekniikkojen käytöstä. Se lisäsi, että ”tällainen yleisen edun mukainen tavoite, niin perustavanluonteinen kuin se onkaan, ei kuitenkaan yksin voi oikeuttaa katsomaan direktiivissä 2006/24 säädetyn kaltaista säilyttämistoimenpidettä välttämättömäksi mainitun torjumisen kannalta”.[29]

42. Ratkaistakseen, rajoittuuko tämäntyyppinen toimenpide siihen, mikä on ehdottoman välttämätöntä, unionin tuomioistuin painotti ennen kaikkea, että sillä puututaan erityisen vakavasti perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin.[30] Erityisen vakava puuttuminen johtuu nimenomaisesti siitä, että kansallisessa lainsäädännössä säädettiin ”*kaikkien tilaajien ja rekisteröityjen käyttäjien liikenne- ja paikkatietojen* yleisestä ja erotuksetta tapahtuvasta säilyttämisestä *kaikkien sähköisten viestintävälineiden osalta* ja että siinä velvoitetaan sähköisten viestintäpalvelujen tarjoajat säilyttämään nämä tiedot *systemaattisesti ja jatkuvasti ilman mitään poikkeuksia*”.[31]

43. Tähän toimenpiteeseen liittyvä puuttuminen kansalaisten elämään ilmenee näistä unionin tuomioistuimen arvioista, jotka koskevat tietojen säilyttämisen vaikutuksia.

Nämä tiedot[32]

– ”sisältävät viestinnän lähteen ja kohteen jäljittämiseksi ja tunnistamiseksi tarvittavat tiedot, viestinnän päivämäärän, kellonajan, keston ja tyypin sekä käyttäjien viestintälaitteen määrittämiseksi tarvittavat tiedot sekä matkaviestintälaitteen sijainnin tunnistamiseksi tarvittavat tiedot.”[33]

– ”Näiden tietojen avulla voidaan muun muassa saada selville, kuka on se henkilö, jonka kanssa tilaaja tai rekisteröity käyttäjä on viestinyt, ja millä laitteella, sekä määrittää viestinnän

26 Tämän adverbin käyttö tuomion Tele2 Sverige ja Watson 95 kohdassa perustuu direktiivin 2002/58 johdanto-osan 11 perustelukappaleeseen.

27 Tuomio Digital Rights, 48 kohta: ”Kun otetaan huomioon yhtäältä henkilötietojen suojan tärkeä rooli yksityiselämän kunnioitusta koskevan perusoikeuden kannalta ja toisaalta sen tähän oikeuteen puuttumisen laajuus ja vakavuus, jonka direktiivi 2006/24 sisältää, unionin lainsäätäjän harkintavalta on – – pieni, joten valvonnan on oltava tarkkaa.”

28 Tuomio Tele2 Sverige ja Watson, 96 kohta oikeuskäytäntöviittauksineen.

29 Tuomio Digital Rights, 51 kohta. Tämän mukaisesti tuomio Tele2 Sverige ja Watson, 103 kohta.

30 Tuomio Digital Rights, 65 kohta ja tuomio Tele2 Sverige ja Watson, 100 kohta.

31 Tuomio Tele2 Sverige ja Watson, 97 kohta. Kursivointi tässä.

32 Joihin kuuluvat muun muassa tilaajan tai rekisteröidyn käyttäjän nimi ja osoite, soittajan puhelinnumero ja valittu numero sekä internetpalvelujen IP-osoite.

33 Tuomio Tele2 Sverige ja Watson, 98 kohta.

ajankohta sekä paikka, josta käsin viestintä tapahtui. Niiden avulla voidaan lisäksi saada tietoon, kuinka tiheästi tilaaja tai rekisteröity käyttäjä on viestinyt tiettyjen henkilöiden kanssa tietyn ajanjakson aikana.” [34]

– ”Näiden tietojen kokonaisuus voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituisista tai tilapäisistä oleskelupaikoista, päivittäisestä tai muusta liikkumisesta, tekemisestä sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään.” [35]

– ”– – näiden tietojen perusteella voidaan laatia asianomaisten henkilöiden profiili, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö.” [36]

44. Puuttuminen voi lisäksi aiheuttaa ”kyseisille ihmisille – – tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun kohteena”, sillä ”[tietoja säilytetään] ilman, että sähköisten viestintäpalvelujen käyttäjille ilmoitetaan siitä”. [37]

45. Kun otetaan huomioon puuttumisen laajuus, ainoa peruste tietojen säilyttämistoimenpiteelle, jolla on tällaisia ominaispiirteitä, olisi vakavan rikollisuuden torjuminen. [38] Kyseisestä toimenpiteestä ei voi kuitenkaan tulla sääntö, sillä ”direktiivillä 2002/58 käyttöön otettu järjestelmä edellyttää, että tämä tietojen säilyttäminen on poikkeus.” [39]

46. Toimenpiteellä oli lisäksi kaksi ominaispiirrettä, jotka johtuivat siitä, ettei siinä tehdä ”mitään erottelua eikä aseteta rajoituksia tai poikkeuksia asetetun tavoitteen perusteella” [40] eikä ”vaadita minkäänlaista yhteyttä säilytettäviksi säädettyjen tietojen ja yleistä turvallisuutta koskevan uhan välillä”: [41]

– Yhtäältä toimenpide koski ”yleisellä tavalla sähköisiä viestintäpalveluja käyttäviä kaikkia henkilöitä ilman, että henkilöt, joiden tietoja säilytetään, olisivat edes epäsuorasti sellaisessa tilanteessa, joka voisi johtaa rikosoikeudellisiin toimiin. – – Siinä ei myöskään säädetä minkäänlaisesta poikkeuksesta, joten sitä sovelletaan jopa henkilöihin, joiden viestintään sovelletaan kansallisen lainsäädännön mukaan salassapitovelvollisuutta”. [42]

– Toisaalta ”siinä ei – – 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”. [43]

34 Ibidem, 98 kohta.
35 Ibidem, 99 kohta.
36 Ibidem, 99 kohdan loppu.
37 Ibidem, 100 kohta.
38 Ibidem, 102 kohta.
39 Ibidem, 104 kohta.
40 Ibidem, 105 kohta.
41 Ibidem, 106 kohta.
42 Ibidem, 105 kohta.
43 Ibidem, 106 kohta.

47. Tarkasteltu kansallinen lainsäädäntö ei tässä tilanteessa ollut täysin välttämätöntä. Näin ollen sitä ei voitu pitää perusteltuna demokraattisessa yhteiskunnassa siten kuin edellytetään direktiivin 2002/58 15 artiklan 1 kohdassa, kun se luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä52 artiklan 1 kohdan valossa. [44]

b) Mahdollisuus tietojen valikoivaan säilyttämiseen

48. Unionin tuomioistuin on hyväksynyt sen, että kansallinen lainsäädäntö, ”joka sallii liikenne- ja paikkatietojen kohdennetun säilyttämisen vakavan rikollisuuden torjumiseksi”, on unionin oikeuden mukaista. [45]

49. Tietojen valikoivan säilyttämisen pätevyyden edellytyksenä on, että ”tietojen säilyttäminen on, siltä osin kuin kyse on säilytettävistä tietoluokista, tarkoitetuista viestintävälineistä, asianomaisista henkilöistä ja aiotun säilytyksen kestosta, rajoitettu täysin välttämättömään”.

50. Ohjeet, joita tuomiossa Tele2 Sverige ja Watson annetaan sen selvittämiseksi, milloin nämä edellytykset täyttyvät, eivät ole (eivät kenties voineet olla) tyhjentävät, ja niiden sanamuoto on varsin yleisluonteinen. Niiden täyttämiseksi jäsenvaltioiden

– on säädettävä selvistä ja täsmällisistä tällaisen tietojen säilyttämistoimenpiteen laajuutta ja soveltamista koskevista säännöistä [46]

– on säädettävä ”[objektiiviset perusteet] – –, joilla luodaan yhteys säilytettävien tietojen ja asetetun tavoitteen välille”, [47] ja

– säännöstön on ”perustuttava objektiivisiin seikkoihin, joiden perusteella voidaan [valikoida] yleisö, jonka tiedot voivat paljastaa ainakin välillisen yhteyden vakavaan rikollisuuteen, myötävaikuttaa tavalla tai toisella vakavan rikollisuuden torjumiseen tai ehkäistä yleistä turvallisuutta kokeva uhka”. [48]

51. Unionin tuomioistuin mainitsee näihin objektiivisiin seikkoihin liittyvänä esimerkkinä mahdollisuuden rajata yleisö ja mahdolliset tilanteet maantieteellisen kriteerin avulla. Vaikka unionin tuomioistuin on maininnut vain tämän kriteerin, jota jotkin jäsenvaltiot ovat arvostelleet, mielestäni sen tarkoituksena ei ollut rajata valintaperusteena käytettäviä tekijöitä yksinomaan siihen.

44 Ibidem, 107 kohta.

45 Ibidem, 108 kohta. Kursivointi tässä.

46 Ibidem, 109 kohta. Niiden on erityisesti ilmoitettava, ”missä olosuhteissa ja millä edellytyksillä tietojen säilyttämistoimenpide voidaan toteuttaa ennaltaehkäisevästi, jotta taataan, että toimenpide rajoittuu täysin välttämättömään”.

47 Ibidem, 110 kohta.

48 Ibidem, 111 kohta.

4. Tietojen saannin oikeasuhteisuus

a) Tuomio Tele2 Sverige ja Watson

52. Unionin tuomioistuin käsittelee kansallisten viranomaisten oikeutta *saada* tietoja riippumatta sähköisten viestintäpalvelujen tarjoajille asetetun tietojen *säilyttämistä* koskevan velvollisuuden laajuudesta ja etenkin siitä, onko tietojen säilyttäminen yleistä vai kohdennettua. [49]

53. Vaikka tietojen säilyttämisen johdonmukaisena tarkoituksena on helpottaa tietojen myöhempää saantia, säilyttäminen ja saanti voivat johtaa erilaisiin perusoikeuskirjassa turvattujen perusoikeuksien loukkauksiin. Tämä erottelu ei kuitenkaan merkitse sitä, ettei joitakin säilyttämiseen liittyviä näkökohtia voitaisi soveltaa myös säilytettävien tietojen saantiin.

54. Tämän mukaisesti tietojen saannin

– ”on vastattava tosiasiallisesti ja täysin jotakin näistä tavoitteista”, jotka on lueteltu direktiivin 2002/58 15 artiklan 1 kohdan ensimmäisessä virkkeessä. Myös oikeuksiin puuttumisen vakavuuden ja asetetun tavoitteen on vastattava toisiaan. Jos puuttumista pidetään vakavana, sitä voidaan perustella ainoastaan vakavan rikollisuuden torjunnalla. [50]

– salliminen on mahdollista vain täysin välttämättömän rajoissa. [51] Lisäksi lainsäädännöllisissä toimenpiteissä on ”oltava selkeät ja täsmälliset säännöt, joissa ilmaistaan, missä olosuhteissa ja millä edellytyksillä sähköisten viestintäpalvelujen tarjoajien on annettava toimivaltaisille kansallisille viranomaisille oikeus saada tietoja. Tällaisen toimenpiteen on myös oltava kansallisen oikeuden mukaan sitova”. [52]

– Erityisesti kansallisessa säännöstössä on säädettävä ”aineellisista ja menettelyllisistä edellytyksistä, joilla toimivaltaiset kansalliset viranomaiset voivat saada säilytettyjä tietoja”. [53]

55. Edellä esitetystä voidaan päätellä, että ”yleisen kaikkien säilytettyjen tietojen saamista koskevan oikeuden, joka on riippumaton siitä, onko olemassa mitään edes välillistä yhteyttä asetettuun tavoitteeseen nähden, ei voida katoa olevan rajattu täysin välttämättömään”. [54]

56. Unionin tuomioistuimen mukaan ”asianomaisen kansallisen säännöstön on perustuttava objektiivisiin kriteereihin niiden olosuhteiden ja edellytysten määrittelemiseksi, joilla toimivaltaisille kansallisille viranomaisille on annettava oikeus saada tilaajien tai rekisteröityjen käyttäjien tietoja”. [55] Tältä osin ”oikeus voidaan lähtökohtaisesti myöntää rikollisuuden torjumisen tavoitteen yhteydessä vain *sellaisten henkilöiden tietoihin, joiden epäillään suunnittelevan, tekevän tai tehneen vakavan rikoksen tai olevan jollakin tavalla mukana tällaisessa rikoksessa*”. [56]

49 Ibidem, 113 kohta.

50 Ibidem, 115 kohta.

51 Ibidem, 116 kohta.

52 Ibidem, 117 kohta.

53 Ibidem, 118 kohta.

54 Ibidem, 119 kohta.

55 Idem.

56 Idem. Kursivointi tässä.

57. Toisin sanoen kansallisten säännösten, joilla kansallisille toimivaltaisille viranomaisille annetaan oikeus saada säilytettyjä tietoja, soveltamisalan on oltava riittävän suppea. Asianomaisten henkilöiden ja asetetun tavoitteen välillä on oltava yhteys, jotta tietojen saanti ei kata huomattavaa määrää tai jopa kaikkia henkilöitä, kaikkia sähköisiä viestintävälineitä ja kaikkia tallennettuja tietoja.

58. Näitä sääntöjä voidaan kuitenkin lieventää tietyissä olosuhteissa. Unionin tuomioistuimen mukaan tämä on mahdollista ”erityisissä tilanteissa, kuten niissä, joissa kansallisen turvallisuuden, maanpuolustuksen tai yleisen turvallisuuden elintärkeitä intressejä uhkaa terrorismi”. Tällaisissa tilanteissa ”oikeus saada muiden henkilöiden tietoja voidaan kuitenkin myöntää myös, jos olemassa on objektiivisia seikkoja, joiden perusteella voidaan katsoa, että näillä tiedoilla voidaan konkreettisessa tapauksessa tosiasiallisesti myötävaikuttaa tällaisen toiminnan torjumiseen”. [57]

59. Tämä unionin tuomioistuimen selvennys antaa jäsenvaltioille mahdollisuuden ottaa käyttöön tietojen saantia koskevan laajemman erityisjärjestelmän silloin, kun se on poikkeuksellisesti tarpeen valtion ensisijaisiin intresseihin (kansallinen turvallisuus, maanpuolustus ja yleinen turvallisuus) kohdistuvien uhkien torjumiseksi, [58] ja siten, että se käsittää myös henkilöt, jotka liittyvät edes epäsuorasti kyseisiin riskeihin.

60. Kansallisten viranomaisten oikeudelle saada säilytettyjä tietoja on tietojen tyypistä riippumatta kolme edellytystä:

– Se edellyttää ”lähtökohtaisesti asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta joko tuomioistuimen tai riippumattoman hallinnollisen elimen etukäteisvalvontaa”. Kyseisen tuomioistuimen tai elimen ratkaisu on annettava ”perustellusta pyynnöstä, jonka nämä viranomaiset esittävät rikoksen estämis-, selvittämis- tai syyteharkintamenettelyssä”. [59]

– ”Toimivaltaiset kansalliset viranomaiset, joille on annettu oikeus saada säilytettyjä tietoja, tiedottavat tästä asianomaisille henkilöille sovellettavien kansallisten menettelyjen mukaisesti heti, kun tämä tiedoksianto ei vaaranna kyseisten viranomaisten suorittamia tutkimuksia”. [60]

– Jäsenvaltioiden on annettava sähköisten viestintäpalvelujen tarjoajien hallussa olevien tietojen turvaa ja suojaa koskevia sääntöjä näiden tietojen väärinkäytön ja laittoman saannin estämiseksi. [61]

b) Tuomio Ministerio Fiscal

61. Kyseisessä asiassa tutkittiin, oliko sellainen kansallinen säännös, jonka mukaan toimivaltaisilla viranomaisilla on oikeus saada tiettyjen SIM-korttien haltijoiden henkilöllisyyttä koskevia tietoja, yhteensopiva direktiivin 2002/58 15 artiklan 1 kohdan, sellaisena kuin sitä tulkitaan perusoikeuskirjan 7 ja 8 artiklan valossa, kanssa.

57 Idem.

58 Tätä poikkeusta voidaan terrorismin lisäksi perustella muilla satunnaisilla tapahtumilla, kuten valtion kriittisiin infrastruktuureihin kohdistuvalla laajamittaisella kyberhyökkäyksellä tai ydinaseiden leviämiseen liittyvällä uhkalla.

59 Tuomio Tele2 Sverige ja Watson, 120 kohta.

60 Ibidem, 121 kohta.

61 Ibidem, 122 kohta.

62. Unionin tuomioistuin totesi, että direktiivin 2002/58 15 artiklan 1 kohdan ensimmäisessä virkkeessä ei rajata rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa koskevaa tavoitetta vain vakaviin rikoksiin, vaan se koskee ”rikoksia” yleisesti. [62]

63. Se lisäsi, että toimivaltaisten kansallisten viranomaisten oikeus saada tietoja edellyttää, että oikeuksiin puuttumisen vakavuus ja kyseessä olevien rikosten vakavuus vastaavat toisiaan. Näin ollen

– ”Vakava puuttuminen voi olla oikeutettu rikosten ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla vain sellaisen rikollisuuden torjumisen tavoitteella, joka on myös luokiteltavissa ’vakavaksi’”. [63]

– Sen sijaan ”silloin, kun puuttuminen, jota tällainen tietojensaanti merkitsee, ei ole vakavaa, se voidaan oikeuttaa yleisesti ’rikosten’ ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla”. [64]

64. Tästä lähtökohdasta käsin ja toisin kuin tuomiossa Tele2 Sverige ja Watson unionin tuomioistuin ei katsonut ”vakavaksi” puuttumista perusoikeuskirjan 7 ja 8 artiklassa suojattuihin oikeuksiin, koska tietojen saantia koskevan pyynnön ”ainoa tavoite [oli] varastetun matkapuhelimen IMEI-koodilla 12 päivän aikana aktivoitujen SIM-korttien haltijoiden tunnistaminen”. [65]

65. Painottaakseen puuttumisen vähäisempää vakavuutta se selitti, että ”tiedoilla, joita pääasiassa kyseessä oleva tietojensaantipyyntö koskee, voidaan ainoastaan liittää tietyn ajanjakson ajan yhteen se SIM-kortti tai ne SIM-kortit, jotka aktivoitiin varastetulla matkapuhelimella, ja näiden SIM-korttien haltijoiden henkilöllisyys. Ilman näillä SIM-korteilla suoritettua viestintää koskevien tietojen ja paikkatietojen yhdistämistä toisiinsa näiden tietojen perusteella ei voida selvittää kyseisellä SIM-kortilla tai kyseisillä SIM-korteilla suoritetun viestinnän päivämäärää, kellonaikaa, kestoa ja vastaanottajia, eikä paikkoja, joissa viestintä on tapahtunut, tai sen tiheyttä tiettyjen henkilöiden kanssa tiettynä ajanjaksona. Näiden tietojen perusteella ei siis voida tehdä täsmällisiä päätelmiä niiden henkilöiden yksityiselämästä, joiden tiedoista on kyse”. [66]

66. Tuomiolla Ministerio Fiscal ratkaistussa asiassa ei ollut kyse siitä, olivatko sähköisten viestintäpalvelujen tarjoajat säilyttäneet tiedonsaantioikeuden kohteena olevat henkilötiedot direktiivin 2002/58 15 artiklan 1 kohdassa, tulkittuna perusoikeuskirjan 7 ja 8 artiklan valossa, säädettyjen edellytysten mukaisesti. [67] Myöskään kysymystä siitä, täyttyivätkö muut kyseiseen artiklaan perustuvat tietojensaantiedellytykset, ei käsitelty.

67. Näin ollen tuomion Ministerio Fiscal perusteella ei voida päätellä, että unionin tuomioistuimen oikeuskäytäntö, joka koskee sellaisen kansallisen järjestelmän, jolla sallitaan tuomiossa Tele2 Sverige ja Watson tarkoitettu tietojen yleinen ja erotuksetta tapahtuva säilyttäminen, yhteensopimattomuutta unionin oikeuden kanssa, olisi muuttunut.

62 Tuomio Ministerio Fiscal, 53 kohta.

63 Ibidem, 56 kohta.

64 Ibidem, 57 kohta.

65 Ibidem, 59 kohta. Pyyntö koski tiedon saantia ”näitä SIM-kortteja vastaavista puhelinnumeroista sekä näiden korttien haltijoiden henkilöllisyydestä, kuten heidän etu- ja sukunimestään ja mahdollisesti osoitteestaan. Nämä tiedot eivät sen sijaan, kuten sekä Espanjan hallitus että syyttäjäviranomainen vahvistivat istunnossa, koske varastetulla matkapuhelimella suoritettua viestintää eivätkä puhelimen paikkatietoja”.

66 Ibidem, 60 kohta.

67 Tuomio Ministerio Fiscal, 49 kohta.

68. Olen kuitenkin sitä mieltä, että tunnustaessaan sellaisen järjestelmän pätevyyden, jossa oikeus saada tietoja rajataan tiettyihin henkilötietoihin (SIM-korttien haltijoiden henkilöllisyyttä koskeviin tietoihin) unionin tuomioistuin hyväksyy implisiittisesti sen, että palveluntarjoajat säilyttävät nämä samat tiedot.

C Unionin tuomioistuimen oikeuskäytännöstä esitetty pääasiallinen kritiikki

69. Sekä ennakkoratkaisua pyytänyt tuomioistuin että suurin osa huomautuksia esittäneistä jäsenvaltioista kehottavat unionin tuomioistuinta selventämään, nyansoimaan tai jopa harkitsemaan uudelleen useita näkökohtia sen oikeuskäytännössä, josta ne esittävät kritiikkiä.

70. Suuri osa tästä epäsuorasta ja suorasta kritiikistä on jo esitetty asiassa Digital Rights annetun tuomion yhteydessä ja hylätty tuomiossa Tele 2 Sverige ja Watson. Se toistetaan nyt lähinnä sen korostamiseksi, että sähköisten viestintäpalvelujen tarjoajien hallussa olevien tietojen saantia koskevat tiukat säännökset, joilla voitaisiin tietyllä tapaa kompensoida näiden samojen tietojen yleisen ja erotuksetta tapahtuvan säilyttämisen merkitsemän puuttumisen vakavuutta, ovat niiden mukaan riittäviä.

71. Lukuisissa kritiikeissä korostetaan myös sitä, että turvallisuutta koskevien vakavien uhkien ja yleisesti rikollisuuden torjumiseksi on tarpeen toteuttaa todella tehokkaita toimenpiteitä, ja unionin tuomioistuinta pyydetään ottamaan huomioon oikeus turvallisuuteen (perusoikeuskirjan 6 artikla) sekä jäsenvaltioiden harkintavalta kansallisen turvallisuuden suojaamisen alalla. Joissakin tapauksissa unionin tuomioistuinta kritisoidaan lisäksi siitä, ettei se ole arvioinut turvallisuus- ja tiedustelupalvelujen toimien ennaltaehkäisevää luonnetta.

D Arvio esitetystä kritiikistä ja täsmennyksistä, joita unionin tuomioistuimen oikeuskäytäntöön voidaan tehdä

72. Mielestäni unionin tuomioistuimen on pidettävä voimassa aiemmissa tuomioissa omaksumansa periaatteellinen kanta: kaikkien tilaajien ja rekisteröityjen käyttäjien liikenne- ja paikkatietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä koskeva velvollisuus loukkaa suhteettomasti perusoikeuskirjan 7, 8 ja 11 artiklassa suojattuja perusoikeuksia.

73. Käänteisesti kansallinen lainsäädäntö, jossa säädetään asianmukaiset rajoitukset joidenkin tällaisten sähköisten viestintäpalvelujen tarjoamisen yhteydessä tuotettavien tietojen säilyttämiselle, voi olla unionin oikeuden mukainen. Keskeisessä asemassa on siis näiden tietojen *säilyttäminen rajoitetusti*.

74. Jäljempänä esittämäni perusteella rajoitetulla säilyttämisellä ei pitäisi tarkoittaa vain säilyttämistä, joka koskee tiettyä maantieteellistä aluetta tai tiettyä henkilöiden ryhmää: näistä säilyttämisperusteista käydyistä keskusteluista ilmenee, että niitä voi olla mahdoton toteuttaa tai ettei niillä saavuteta asetettuja päämääriä tehokkaasti tai että ne saattavat jopa olla syrjiviä.

75. Olen ensinnäkin eri mieltä kriittisestä kaksiosaisesta perusteesta, jonka mukaan ”laajempaa säilyttämistä kompensoidaan rajoittamalla oikeutta saada tietoja”. Olen samaa mieltä unionin tuomioistuimen päättelystä, jonka mukaan tietojen säilyttäminen ja saanti tarkoittavat kahta erityyppistä puuttumista. Vaikka tietojen säilyttämisellä on merkitystä toimivaltaisten viranomaisten mahdollista myöhempää tietojen saantia ajatellen, jokainen puuttuminen on perusteltava erikseen tutkimalla se erityisesti asetetun tavoitteen kannalta.

76. Näin ollen kansallista järjestelmää, jossa säädetään tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä, ei voida oikeuttaa sillä perusteella, että asiaa koskevilla säännöksillä asetetaan samaan aikaan näiden tietojen saannille tiukat aineelliset ja menettelylliset vaatimukset.

77. On siis oltava erityisesti tietojen säilyttämiseen liittyvät säännöt, joissa säilyttämiselle asetetaan joitakin edellytyksiä, jotka estävät yleisen ja erotuksetta tapahtuvan säilyttämisen. Vain näin taataan sen yhteensopivuus direktiivin 2002/58 15 artiklan 1 kohdan kanssa, kun otetaan huomioon perusoikeuskirjan 7, 8 ja 11 artikla sekä 52 artiklan 1 kohta.

78. Tämä on muutenkin se lähestymistapa, jonka neuvostossa kokoontuneet työryhmät omaksuivat määrittääkseen unionin tuomioistuimen oikeuskäytännön mukaiset tietojen säilyttämistä ja saantia koskevat säännöt, kun ne tarkastelivat rinnakkain molempia puuttumisen muotoja.[68]

79. Soveltamalla rajoituksia kumpaakin näistä kahdesta oikeuksiin puuttumisen muodosta voidaan arvioida, onko niiden mahdollinen kumulatiivinen vaikutus yhdistettynä tehokkaaseen suojaan sellainen, että se lieventää tietojen säilyttämisen vaikutusta perusoikeuskirjan 7, 8 ja 11 artiklassa suojattuihin perusoikeuksiin ja takaa samalla tutkimusten tehokkuuden.

80. Näiden oikeuksien suojaamiseksi järjestelmässä on

– säädettävä tietojen säilyttämisestä, johon liittyy tiettyjä tavoiteltuun päämäärään perustuvia rajoituksia ja eroja

– säänneltävä oikeutta näiden tietojen saantiin sen mukaan, mikä on ehdottoman välttämätöntä tavoitellun päämäärän saavuttamiseksi, ja siten, että saanti tapahtuu tuomioistuimen tai riippumattoman hallintoviranomaisen valvonnassa.

81. Peruste, jolla sähköisten viestintäpalvelujen tarjoajat oikeutetaan säilyttämään tiettyjä tietoja muutenkin kuin käyttäjiä koskevien sopimusvelvoitteidensa hallinnointia varten, laajenee rinnan tekniikan kehityksen kanssa. Koska myönnetään, että tietojen säilyttämisestä on hyötyä rikollisuuden ehkäisyn ja torjumisen kannalta (mitä on vaikea kiistää[69]), ei vaikuta johdonmukaiselta rajata sitä koskemaan pelkästään niiden tietojen käyttöä, joita operaattorit säilyttävät liiketoimintansa harjoittamista varten, ja vain sen aikaa kuin kyseinen toiminta edellyttää.

82. Kun on myönnetty, että tietojen säilyttämistä koskeva velvollisuus, joka menee pidemmälle kuin operaattoreiden velvollisuus säilyttää niitä teknisiä ja kaupallisia tarpeitaan varten, on hyödyllinen kansallisen turvallisuuden suojaamiseksi ja rikollisuuden torjumiseksi, on välttämätöntä määrittää tämän velvollisuuden rajat.

83. Jokainen säilyttämistä koskeva järjestelmä on mukautettava tarkasti vastaamaan tavoiteltua päämäärää siten, ettei säilyttäminen voi muuttua erotuksetta tapahtuvaksi.[70] Järjestelmällä on samoin suljettava pois se, että tietoja yhdistämällä saadaan muodostettua asianomaisesta henkilöstä (toisin sanoen hänen tavanomaisista toimistaan ja sosiaalisista suhteistaan) vastaava tai samankaltainen *kuva* kuin saataisiin tutustumalla viestinnän sisältöön.

68 Jäsenvaltiot ovat vuodesta 2017 osallistuneet työryhmään, jonka tarkoituksena on mukauttaa niiden lainsäädäntö tätä asiaa koskevassa unionin tuomioistuimen oikeuskäytännössä vahvistettuihin perusteisiin (tietojenvaihto- ja tietosuojatyöryhmä, DAPIX).

69 Tekniikoiden määrittäminen ja niiden tehokkuuden arviointi kuuluvat joka tapauksessa jäsenvaltioiden harkintavaltaan.

70 Tuomion Digital Rights 57 kohta ja tuomion Tele2 Sverige ja Watson 105 kohta.

84. Erehdysten ja väärinkäsitysten selvittämiseksi on tärkeää ottaa huomioon se, mitä unionin tuomioistuin *ei todennut* tuomioissaan Digital Rigths ja Tele2 Sverige ja Watson. Niissä ei pidetty tuomittavana varsinaisen tietojen säilyttämistä koskevan järjestelmän olemassaoloa hyödyllisenä rikollisuuden torjumisen välineenä. Päinvastoin siinä myönnettiin rikosten estämistä ja niistä rankaisemista koskeva tavoite oikeutetuksi sekä tietojen säilyttämistä koskeva järjestelmä hyödylliseksi tämän tavoitteen saavuttamisen kannalta.

85. Toistan, että unionin tuomioistuin hylkäsi sitten ehdottomasti sen, että unioni ja sen jäsenvaltiot voisivat tähän tavoitteeseen vedoten määrätä *kaikkien* sähköisten viestintäpalvelujen tarjoamisen yhteydessä tuotettavien tietojen erotuksetta tapahtuvasta säilyttämisestä ja yleisestä oikeudesta saada kyseisiä tietoja.

86. Näin ollen on tarpeen löytää sellaisia tietojen säilyttämisen tapoja, jotka eroavat perusoikeuskirjan 7, 8 ja 11 artiklassa edellytetyn suojan vastaisista ominaisuuksista (”yleinen ja erotuksetta tapahtuva”).

87. Yksi näistä tavoista on joko jotakin kohderyhmää (teoriassa sitä, jolla on tiettyjä enemmän tai vähemmän suoria yhteyksiä vakavimpiin uhkiin) tai maantieteellistä aluetta koskevien tietojen *valikoiva* säilyttäminen.

88. Tämä lähestymistapa on kuitenkin jossain määrin ongelmallinen:

– Mahdollisen rikollisryhmän tunnistaminen ei todennäköisesti olisi riittävää, jos se käyttää anonymisointitekniikoita tai vääriä henkilöllisyyksiä. Kyseisten ryhmien valitseminen voisi lisäksi luoda tiettyjä väestöryhmiä koskevan yleiseen epäluuloon perustuvan järjestelmän ja osoittautua syrjiväksi valinnassa käytetyn algoritmin perusteella.

– Maantieteellisin perustein tehty valinta (jonka tehokkuus edellyttää, että se koskee melko laajoja alueita) synnyttää nämä samat ongelmat ja aiheuttaa lisäksi uusia, kuten Euroopan tietosuojavaltuutettu istunnossa totesi, koska se voi leimata tietyt alueet.

89. Johonkin kohderyhmään tai maantieteelliseen alueeseen kohdistuva ennaltaehkäisevä säilyttäminen voi myös olla jossain määrin ristiriidassa sen kanssa, että rikoksentekijät eivät tunne toisiaan eivätkä rikoksentekopaikkaa ja -hetkeä ennakolta.

90. Ei kuitenkaan pidä sulkea pois sitä, että on olemassa näihin kriteereihin perustuvia valikoivan säilyttämisen muotoja, jotka ovat hyödyllisiä edellä esitettyjen tavoitteiden saavuttamiseksi. Lainsäätäjän on kussakin jäsenvaltiossa tai unionin tasolla suunniteltava nämä järjestelyt siten, että niissä kunnioitetaan unionin tuomioistuimen takaamaa perusoikeuksien suojaa.

91. Olisi virhe kuvitella, että tiettyä kohderyhmää tai maantieteellistä aluetta koskevien tietojen valikoiva säilyttäminen on ainoa muoto, jonka unionin tuomioistuin katsoo olevan direktiivin 2002/58 15 artiklan 1 kohdan mukainen, kun se luetaan perusoikeuskirjan 7 ja 8 artiklan valossa.

92. Korostan, että on mahdollista löytää muitakin tietojen valikoivan säilyttämisen tapoja kuin ne, jotka kohdistuvat tiettyihin henkilöryhmiin tai maantieteellisiin alueisiin. Näin ovat yksimielisesti katsoneet ne neuvoston työryhmät, joihin jo viittasin: niiden mukaan selvittämiskeinoja voisivat

olla erityisesti säilytettävien tietojen luokkien rajoittaminen,[71] tietojen pseudonymisointi,[72] rajoitettujen säilytysaikojen käyttöönotto,[73] tiettyjen sähköisten viestintäpalvelujen tarjoajien ryhmien jättäminen huomiotta,[74] uusittavissa olevat tallennusluvat,[75] velvollisuus säilyttää tallennetut tiedot unionin alueella tai se, että riippumaton hallintoviranomainen valvoo systemaattisesti ja säännöllisesti takeita, jotka sähköisten viestintäpalvelujen tarjoaja antaa tietojen luvatonta käyttöä vastaan.

93. Jotta säilyttäminen olisi unionin tuomioistuimen oikeuskäytännön mukaista, on mielestäni ensisijaista säilyttää väliaikaisesti tiettyjen liikenne- ja paikkatietojen *luokat*, jotka rajataan tiukkojen turvallisuusvaatimusten perusteella ja joista ei kokonaisuutena voida saada täsmällistä ja yksityiskohtaista kuvaa asianomaisten henkilöiden elämästä.

94. Käytännössä tämä tarkoittaa sitä, että kahdesta pääluokasta (liikennetiedot ja paikkatiedot) säilytetään sopivien suodattimien avulla *vähimmäistiedot*, jotka katsotaan ehdottoman välttämättömiksi rikollisuuden tehokkaan ehkäisemisen ja valvonnan sekä kansallisen turvallisuuden suojaamisen kannalta.

95. Jäsenvaltioiden tai unionin toimielinten on toteutettava lainsäädäntöteitse (omien asiantuntijoidensa avulla) tämä valintamenettely ja torjuttava kaikki pyrkimykset määrätä kaikkien liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä.

96. Sen lisäksi, että säilytettävät tiedot rajataan luokkien mukaan, niitä voidaan säilyttää vain tietyn tallennusajan, jotta niistä ei ole mahdollista saada yksityiskohtaista kuvaa asianomaisten henkilöiden elämästä. Säilytysaika on lisäksi mukautettava tietojen luonteeseen, jotta ne tiedot, joista kyseisten henkilöiden elämäntyyli ja -tavat ilmenevät tarkemmin, säilytetään lyhimmän aikaa.[76]

97. Toisin sanoen on tutkittava mahdollisuutta toteuttaa menettely, jossa kuhunkin luokkaan kuuluvien tietojen säilytysaika on erilainen sen mukaan, miten hyödyllisiä ne ovat turvallisuustavoitteiden saavuttamisen kannalta. Rajaamalla kummankin tietoluokan samanaikaista säilytysaikaa (jonka kuluessa niitä voidaan siis käyttää asianomaisten henkilöiden elämäntyyliä ilmentävien vastaavuuksien etsimiseen) laajennetaan perusoikeuskirjan 8 artiklassa turvatun oikeuden suojaa.

71 Säilyttämisvelvollisuus ei koske tietoja, jotka eivät ole ehdottoman välttämättömiä ja objektiivisesti tarpeellisia rikosten ehkäisemisen ja syyteharkinnan tai yleisen turvallisuuden suojaamisen kannalta. On erityisesti täsmennettävä asetetun tavoitteen mukaisesti, minkä tyyppiset tilaaja-, liikenne- ja paikkatiedot on ehdottomasti säilytettävä mainitun tavoitteen saavuttamiseksi. Velvollisuuden ulkopuolelle jäävät erityisesti ne tiedot, joita ei pidetä välttämättöminä rikosten tutkimisen ja syyteharkinnan kannalta.

72 Voidaan harkita mahdollisuutta muuttaa säilytysaikoja eri tietoluokkien mukaan ottaen huomioon se, kuinka suuressa määrin niillä loukataan henkilöiden yksityisyyttä. Lisäksi on säädettävä tietojen poistamisesta pysyvästi säilytysajan päätyttyä.

73 Lupajärjestelmät voivat perustua kussakin jäsenvaltiossa säännöllisesti tehtäviin uhka-arvioihin. On varmistettava, että yhteys säilytettyjen tietojen ja asetetun tavoitteen välillä luodaan ja että sitä mukautetaan kunkin jäsenvaltion erityistilanteeseen. Näin ollen on mahdollista, että palveluntarjoajille myönnetyt säilytysluvat voivat johtaa tietynlaisten tietojen säilyttämiseen uhka-arviosta riippuen. Nämä luvat voisi antaa riippumaton tuomioistuin tai hallintoviranomainen, ja niiden perusteella säilyttämisen välttämättömyyttä tarkasteltaisiin uudelleen säännöllisesti.

74

75

76 Tätä järjestelmää käytetään ilmeisesti Saksan liittotasavallassa, jonka hallitus ilmoitti istunnossa, että liikennetietojen säilytysaika on sen lainsäädännön mukaan kymmenen viikkoa, kun taas paikkatietojen säilytysaika on vain neljä viikkoa. Sitä vastoin Ranskan tasavallan mukaan liikenne- ja paikkatiedot on välttämätöntä säilyttää yhden vuoden ajan. Kyseisen jäsenvaltion mukaan yhden vuoden määräajan lyhentäminen vähentäisi rikospoliisin yksiköiden tehokkuutta.

98. Euroopan tietosuojavaltuutettu esitti istunnossa samansuuntaisen toteamuksen: mitä enemmän säilytettyjen metatietojen luokkia on ja mitä pidempi on tallennusaika, sitä helpompi on määritellä henkilön yksityiskohtainen profiili, ja päinvastoin.[77]

99. Muilta osin, kuten istunnossakin kävi ilmi, rajan vetäminen tiettyjen sähköisen viestinnän metatietojen ja tämän saman viestinnän sisällön välille on vaikeaa. Jotkin metatiedot voivat olla yhtä paljastavia tai paljastavampia kuin kyseisen viestinnän varsinainen sisältö: tämä voi koskea niiden verkkosivujen URL-osoitteita, joilla käyttäjä on vieraillut.[78] Siksi tämäntyyppisiin ja muihin vastaaviin tietoihin on kiinnitettävä erityistä huomiota, jotta rajataan mahdollisimman paljon niiden säilyttämisen tarvetta ja kestoa.

100. Tasapainoisen ratkaisun löytäminen ei ole helppoa, koska ristiintarkistamalla säilytettyjä tietoja ja selvittämällä niiden vastaavuussuhteet valvontaviranomaiset voivat tapauksen mukaan tunnistaa epäillyn henkilön tai uhkan. Tästäkin huolimatta tietojen säilyttämisessä on aste-ero sen mukaan, paljastaako se kyseisen epäillyn henkilön tai uhkan vai saadaanko sen tuloksena yksityiskohtainen kuva henkilön elämästä.

101. Ennen kuin tätä erityisalaa varten laaditaan koko unionia koskevaa yhteistä sääntelyä, en usko, että unionin tuomioistuinta voidaan pyytää ottamaan hoitaakseen sääntelytehtäviä ja täsmentämään yksityiskohtaisesti, mitä tietoluokkia voidaan säilyttää ja kuinka pitkään. Sen jälkeen, kun rajat, jotka unionin tuomioistuimen mukaan perustuvat perusoikeuskirjaan, on vedetty, on unionin toimielinten ja jäsenvaltioiden tehtävä löytää tasapaino turvallisuuden varmistamisen ja perusoikeuskirjassa suojattujen perusoikeuksien välille.

102. On totta, että jättämällä huomiotta tiedot, jotka ovat pääteltävissä suuremmasta määrästä säilytettyjä tietoja, voidaan joissakin tapauksissa vaikeuttaa mahdollisten uhkien torjumista. Tämä on kuitenkin yksi hinta muiden joukossa, joka viranomaisten on maksettava, kun ne asettavat itselleen velvoitteen suojella perusoikeuksia.

103. Kenenkään mielestä ei ole suositeltavaa asettaa ennakolta velvollisuutta, joka koskee yksityisen sähköisen viestinnän *sisältöjen* yleistä ja erotuksetta tapahtuvaa säilyttämistä (silloinkaan, kun laeilla taataan rajattu oikeus tutustua mainittuihin sisältöihin myöhemmin), ja vastaavasti myöskään kyseisen viestinnän metatietojen, jotka voivat paljastaa sen varsinaisen sisällön kanssa yhtä arkaluonteisia tietoja, erotuksetta tapahtuvan ja yleisen tallentamisen ei pidä olla mahdollista.

104. Myönnän, että on vaikea määrittää lainsäädännössä tarkasti ne tilanteet ja edellytykset, joiden toteutuessa tiedot voidaan säilyttää valikoidusti, mutta se ei oikeuta jäsenvaltioita muuttamaan poikkeusta säännöksi siten, että ne tekevät henkilötietojen yleisestä säilyttämisestä lainsäädäntönsä keskeisen periaatteen. Jos näin olisi, hyväksyttäisiin henkilötietojen suojaa koskevan oikeuden loukkauksen jatkuminen määräämättömän ajan.

105. Lisään, ettei mikään estä sitä, että varsinaisissa *poikkeustilanteissa*, joihin liittyy välitön uhka tai erityinen riski, jonka perusteella jäsenvaltiossa voidaan virallisesti julistaa hätätila, kansallisessa lainsäädännössä säädetään mahdollisuudesta asettaa rajoitetuksi ajaksi niin laaja ja yleinen tietojen säilyttämistä koskeva velvoite kuin pidetään välttämättömänä.

[77] On luonnollisesti taattava, että sähköisten viestintäpalvelujen tarjoajat poistavat tiedot pysyvästi säilytysajan päätyttyä (lukuun ottamatta niitä tietoja, jotka säilyttämistä voidaan direktiivin 2002/58 mukaisesti jatkaa liiketoimintaa varten).

[78] Ranskan hallitus totesi istunnossa, että URL-osoitteet jätettiin pois sisäänkirjautumistiedoista, joiden osalta sen lainsäädännössä säädetään yleisestä säilyttämisvelvollisuudesta.

106. Tässä yhteydessä voitaisiin antaa lainsäädäntöä, jossa nimenomaisesti sallitaan laajempi tietojen säilyttäminen (ja saanti) sellaisin edellytyksin ja sellaisten menettelyjen mukaisesti, joilla varmistetaan näiden toimenpiteiden poikkeuksellisuus niiden aineellisen soveltamisalan ja keston osalta sekä vastaavat oikeudelliset takeet.

107. Perustuslain mukaisia hätätilanteita sääntelevien sääntelyjärjestelmien vertailusta käy ilmi, ettei ole mahdotonta rajata tilanteita, jotka ovat syynä sellaisen erityisen sääntelyjärjestelmän soveltamiseen, jossa säännellään sitä, mikä viranomainen voi tehdä tällaisen päätöksen, millä edellytyksillä ja kenen valvonnassa. [79]

E Kolmeen ennakkoratkaisukysymykseen annettavat vastaukset

1. Alustava huomautus

108. Kansallinen tuomioistuin pyytää tulkitsemaan direktiivin 2002/58 15 artiklan 1 kohtaa suhteessa useisiin perusoikeuskirjassa taattuihin oikeuksiin: yksityis- ja perhe-elämän kunnioittamista koskevaan oikeuteen (7 artikla), henkilötietojen suojaa koskevaan oikeuteen (8 artikla) ja sananvapautta ja tiedonvälityksen vapautta koskevaan oikeuteen (11 artikla).

109. Kuten selitän ratkaisuehdotuksissa C-511/18 ja C-512/18, nämä ovat tosiasiallisesti ne oikeudet, joihin saatetaan unionin tuomioistuimen mukaan näissä tapauksissa vaikuttaa.

110. Cour constitutionnelle viittaa myös perusoikeuskirjan 4 ja 6 artiklaan, joista edellinen mainitaan toisessa ja jälkimmäinen ensimmäisessä ennakkoratkaisukysymyksessä.

111. Siltä osin kuin on kyse perusoikeuskirjan 6 artiklasta, jossa taataan oikeus vapauteen ja turvallisuuteen, siihen on vedottu myös asioissa C-511/18 ja C-512/18, ja sen merkityksellisyyttä olen käsitellyt vastaavissa ratkaisuehdotuksissa, joihin viittaan. [80]

112. Perusoikeuskirjan 4 artiklan osalta on todettava, että koska vastaus ei riipu niinkään kansallisen lainsäädännön tutkimisesta sen vertailemiseksi unionin oikeuden kanssa kuin kyseisen säännöksen tulkinnasta, siihen on mielestäni vastattava ensimmäiseksi.

2. Toinen ennakkoratkaisukysymys

113. Kidutuksen sekä epäinhimillisen tai halventavan rangaistuksen ja kohtelun kieltoon, joka taataan perusoikeuskirjan 4 artiklassa, on tosiasiallisesti viitattu yksinomaan tässä ennakkoratkaisukysymyksessä, minkä vuoksi olen velvollinen kiinnittämään siihen huomiota.

114. Mainitessaan perusoikeuskirjan 4 artiklan ennakkoratkaisua pyytänyt tuomioistuin haluaa tuoda selvästi esiin, että kansallisen lain tavoitteena on myös täyttää viranomaisille kuuluva *positiivinen velvollisuus* säätää ”lainsäädännöllisestä kehyksestä, jolla mahdollistetaan tehokas

[79] Ackerman, B., ”The Emergency Constitution”, *Yale Law Journal*, nide 113, 2004, s. 1029–1092; Ferejohn, J. ja Pasquino, P., ”The Law of the Exception: A typology of Emergency Powers”, *International Journal of Constitutional Law*, nide 2, 2004, s. 210–239.

[80] Ratkaisuehdotukset C-511/18 ja C-512/18, 95 kohta ja sitä seuraavat kohdat.

rikostutkinta ja tehokas seuraamusten määrääminen alaikäisiin kohdistuvasta seksuaalisesta hyväksikäytöstä sekä tällaisen rikoksentekijän tunnistaminen tehokkaasti myös silloin, kun tekijä käyttää sähköisiä viestintävälineitä”. [81]

115. Mielestäni tämä konkreettinen *positiivinen velvollisuus* ei eroa kovin paljon niistä erityistehtävistä, joita perusoikeuksien luettelon antaminen valtiolle käytännössä asettaa. Oikeus elämään (perusoikeuskirjan 2 artikla), oikeus henkilökohtaiseen koskemattomuuteen (perusoikeuskirjan 3 artikla) tai tietosuojaan (perusoikeuskirjan 8 artikla) samoin kuin sananvapaus (perusoikeuskirjan 11 artikla) tai ajatuksen, omantunnon ja uskonnon vapaus (perusoikeuskirjan 10 artikla) velvoittavat valtiot laatimaan lainsäädäntökehyksen, jossa taataan tosiasiallinen mahdollisuus näiden oikeuksien käyttöön tarvittaessa turvautumalla valtiolle yksinoikeudella kuuluvaan voimankäyttöön sitä kohtaan, joka yrittää estää niiden käytön tai vaikeuttaa sitä. [82]

116. Euroopan ihmisoikeustuomioistuin katsoo lasten seksuaalisen hyväksikäytön osalta, että lapsilla ja muilla haavoittuvassa asemassa olevilla henkilöillä on kvalifioitu oikeus valtion suojeluun, joka turvataan rikosoikeudellisin säännöksin, joilla määrätään tehokkaita seuraamuksia näistä rikoksista ja ehkäistään niitä. [83]

117. Tämä laillinen oikeus suojeluun ei kuulu vain perusoikeuskirjan 4 artiklan soveltamisalaan, sillä luonnollisesti voidaan vedota myös 1 artiklaan (ihmisarvo) tai 3 artiklaan (oikeus ruumiilliseen ja henkiseen koskemattomuuteen).

118. Vaikka viranomaisten positiivista velvollisuutta taata lasten ja muiden haavoittuvassa asemassa olevien henkilöiden suojelu ei voida sivuuttaa pohdittaessa oikeushyviä, joihin kansallinen lainsäädäntö vaikuttaa, [84] sen ei myöskään voida katsoa tarkoittavan ”kohtuuttomia rasitteita” viranomaisille, [85] eikä sitä voida täyttää muuten kuin lainsäädännöllisin keinoin tai kunnioittamatta muita perusoikeuksia. [86]

81 Toisen kysymyksen loppuosan sanamuoto. Tässä viittauksessa sähköisiin viestintävälineisiin selitetään, että kysymyksessä mainitaan valtioille kuuluva toinen positiivinen velvollisuus, joka asetetaan perusoikeuskirjan 8 artiklassa henkilötietojen suojan osalta. Kaksinkertaisesta viittauksesta perusoikeuskirjan 8 artiklaan ilmenee, että ennakkoratkaisua pyytänyt tuomioistuin antaa perusoikeuskirjassa taatuille oikeuksille niiden luonteen perusteella kaksiosaisen tehtävän: niillä sekä *rajoitetaan* riidanalaista velvollisuutta että *oikeutetaan* se.

82 Tämä tehokkuutta koskeva velvollisuus merkitsee käytännössä sitä, että hyvinvointivaltiossa, jossa oikeuksien muodollisen tunnustamisen lisäksi on tärkeää niiden aineellisen sisällön toteutuminen käytännössä, viranomaisilla on tulosvelvoite.

83 Euroopan ihmisoikeustuomioistuimen tuomio 2.12.2008, K.U. v. Suomi (ECHR:2008:1202JUD000287202, 46 kohta).

84 Katson tässä yhteydessä, että oikeuksiin, joihin ennakkoratkaisua pyytänyt tuomioistuin vetoaa (kyseessä olevan velvollisuuden *rajoituksina*, ei sen *oikeutuksena*), voitaisiin lisätä oikeus tehokkaisiin oikeussuojakeinoihin (perusoikeuskirjan 47 artikla) tai oikeus puolustukseen (perusoikeuskirjan 48 artikla), joiden mahdollista loukkaamista on myös käsitelty pääasioissa. Ennakkoratkaisupyynnön määräysosassa viitataan kuitenkin vain perusoikeuskirjan 7, 8 ja 11 artiklaan ja 52 artiklan 1 kohtaan.

85 Euroopan ihmisoikeustuomioistuimen tuomio 28.10.1998, Osman v. Yhdistynyt kuningaskunta (CE:ECHR:1998:1028JUD002345294, 116 kohta).

86 Ibidem, 116 kohdan loppuosa: ”[on tarpeen] varmistaa, että poliisi rikollisuuden torjuntaa ja ehkäisemistä koskevia valtuuksiaan käyttäessään noudattaa täysimääräisesti lakisääteisiä keinoja ja muita takeita, joilla rajoitetaan oikeutetusti sen rikostutkintatoimien ulottuvuutta”. Ks. myös Euroopan ihmisoikeustuomioistuimen tuomio 2.12.2008, K.U. v. Suomi (CE:ECHR:2008:1202JUD000287202, 48 kohta). Unionin tuomioistuin on vastaavasti todennut 29.7.2019 antamansa tuomion Gambino ja Hyka (C-38/18, EU:C:2019:628) 49 kohdassa, että rikoksen uhrille tunnustetut oikeudet eivät voi vaikuttaa syytetylle tunnustettujen oikeuksien tosiasialliseen käyttämiseen.

3. Ensimmäinen ennakkoratkaisukysymys

119. Ennakkoratkaisua pyytänyt tuomioistuin haluaa lähinnä tietää, onko kansallinen laki, josta sen on lausuttava perustuslainmukaisuutta koskevan kanteen yhteydessä, ristiriidassa unionin oikeuden kanssa.

120. Koska unionin tuomioistuin on jo esittänyt direktiivistä 2002/58 tulkinnan, joka on perusoikeuskirjan vastaavien määräysten mukainen, ennakkoratkaisukysymykseen annettavassa vastauksessa on otettava huomioon tuomiossa Tele2 Sverige ja Watson vahvistettu oikeuskäytäntö, tarvittaessa nyt tehtävin täsmennyksin.

121. Tämän lähtökohdan perusteella tulkintaohjeissa, jotka Cour constitutionnellelle voidaan antaa sitä varten, että se vertailee itse, onko kansallinen lainsäädäntö unionin oikeuden mukainen, on käsiteltävä erikseen tietojen säilyttämistä ja tietojen saantia sellaisina kuin niistä säädetään kyseisessä kansallisessa lainsäädännössä.

a) Tietojen säilyttämisen edellytykset

122. Belgian hallitus korostaa halunneensa laatia selvän lainsäädännöllisen kehyksen, joka sisältää yksityiselämän suojaamista varten tarvittavat takeet, sen sijaan, että se vetoaisi sähköisten viestintäpalvelujen tarjoajien käytäntöön, joka koskee tietojen säilyttämistä laskutusta tai asiakastiedustelujen käsittelyä varten.

123. Belgian hallituksen näkemyksen mukaan tietojen säilyttämistä koskevan yleisen ja ehkäisevän velvollisuuden tavoitteeksi on asetettu vakavien rikosten tutkinnan, selvittämisen ja syyteharkinnan lisäksi valtion turvallisuuden suojaaminen, maanpuolustuksen ja yleisen turvallisuuden takaaminen, muiden tekojen kuin vakavan rikollisuuden tutkinta, selvittäminen ja syyteharkinta tai sähköisten viestintäjärjestelmien kielletyn käytön torjuminen [87] taikka jokin muu asetuksen N:o 2016/679 23 artiklan 1 kohdassa määritellyistä tavoitteista.

124. Belgian hallitus toteaa seuraavaa:

– Pelkän tietojen säilyttämisen perusteella ei voida tehdä kovin tarkkoja päätelmiä asianomaisten henkilöiden yksityiselämästä: tällaisia päätelmiä on mahdollista tehdä vain siltä osin kuin säilytettyjä tietoja annetaan saataville.

– Lakiin sisältyy yksityisyyden suojaamiseen tarkoitettuja varaumia; muun muassa, että tietojen säilyttäminen ei koske viestinnän sisältöä; säilyttämisen perusteltavuuteen, tietojen saantia koskevaan oikeuteen, tietojen oikaisemista koskevaan oikeuteen ja muihin oikeuksiin liittyviä takeita sovelletaan täysimääräisesti; palveluntarjoajien ja operaattoreiden on noudatettava säilytettyjen tietojen osalta samoja velvoitteita ja samaa tietoturvaa ja -suojaa kuin verkossa olevien tietojen osalta ja estettävä kyseisten tietojen vahingossa tapahtuva tai laiton tuhoaminen sekä vahingossa tapahtuva häviäminen tai muuttaminen.

– Tietoja voidaan säilyttää 12 kuukauden ajan (minkä jälkeen ne on tuhottava) ja ainoastaan unionin alueella.

[87] Se on perusteltua myös pelastusyksiköille soitettuihin hätäpuheluihin vastaamiseksi tai sellaisen kadonneen henkilön löytämiseksi, jonka fyysinen koskemattomuus on välittömässä vaarassa.

– Palveluntarjoajien ja operaattoreiden on toteutettava teknisiä suojatoimenpiteitä, joilla varmistetaan, että säilytettävät tiedot eivät ole niiden rekisteröinnin jälkeen sellaisten henkilöiden luettavissa eivätkä käytettävissä, joilla ei ole lupaa tutustua niihin.

– Nämä toimet toteutetaan joka tapauksessa Belgian posti- ja televiestintäalan sääntelyelimen ja tietosuojaviranomaisen valvonnassa.

125. Näistä takeista huolimatta on selvää, että Belgian lainsäädännössä asetetaan operaattoreille ja sähköisten viestintäpalvelujen tarjoajille direktiivissä 2002/58 tarkoitettu velvollisuus, joka koskee näiden palvelujen tarjoamisen yhteydessä käsiteltyjen liikenne- ja paikkatietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä. Säilytysaika on, kuten jo todettiin, yleisesti 12 kuukautta: aikaa ei ole rajoitettu säilytettävien tietojen luokkien perusteella.

126. Tämä yleistä ja erotuksetta tapahtuvaa säilyttämistä koskeva velvollisuus on voimassa pysyvästi ja jatkuvasti. Vaikka tällaisen velvollisuuden tavoitteena on kaikentyyppisten rikosten torjunta, tutkiminen ja syyteharkinta (valtion turvallisuuteen ja puolustukseen liittyvistä tai erityisen vakavista rikoksista sellaisiin rikoksiin, joista säädetty rangaistus on alle vuosi vankeutta), se ei ole unionin tuomioistuimen oikeuskäytännön mukainen, joten sitä ei voida pitää yhteensopivana perusoikeuskirjan kanssa.

127. Kyseisen oikeuskäytännön noudattamiseksi Belgian lainsäätäjän on tutkittava muita keinoja (kuten niitä, jotka olen edempänä maininnut), joilla otetaan käyttöön rajoitettuja säilyttämistapoja. Nämä säilytystavat vaihtelevat tietoluokkien mukaan, ja niissä on noudatettava periaatetta siitä, että säilytetään riskiin tai uhkaan perustuva välttämätön *vähimmäismäärä* tietoja rajoitetun ajan, joka määräytyy tallennettujen tietojen luonteen mukaan. Säilyttäminen ei kuitenkaan voi antaa mahdollisuutta asianomaisten henkilöiden yksityiselämän, tottumusten, käyttäytymisen tai sosiaalisten suhteiden tarkkaan *kartoittamiseen*.

b) Viranomaisten edellytykset saada säilytettäviä tietoja

128. Mielestäni tuomiossa Tele2 Sverige ja Watson asetetut edellytykset[88] ovat edelleen merkityksellisiä myös tietojen saannin kannalta: kansallisessa lainsäädännössä on säädettävä aineellisista ja menettelyllisistä edellytyksistä, joiden nojalla toimivaltaiset kansalliset viranomaiset voivat saada säilytettyjä tietoja.[89]

129. Belgian hallitus täsmentää, että (sähköisestä viestinnästä) vuonna 2005 annetun lain 126 §:n 2 momentissa[90] säädetään rajoitetusti ne kansalliset viranomaiset, jotka voivat saada säilytettyjä tietoja saman artiklan 1 kohdan mukaisesti.

130. Näihin viranomaisiin kuuluvat varsinaiset oikeusviranomaiset ja syyttäjäviranomainen, valtion turvallisuudesta vastaavat viranomaiset, valtion tiedustelu- ja turvallisuuspalvelu, kukin niistä riippumattomien komiteoidensa valvonnassa, Belgian posti- ja televiestintälaitoksen poliisivirkamiehet, pelastusyksiköt, liittovaltion kadonneiden henkilöiden yksikön poliisivirkamiehet, televiestinnän välitysyksikkö ja rahoitusalan valvontaelin.

88 Ks. edellä tämän ratkaisuehdotuksen 60 kohta.

89 Tuomio Tele2 Sverige ja Watson, 118 kohta.

90 Lain 126 §, sellaisena kuin se on muutettuna 29.5.2016 annetulla lailla.

131. Belgian hallitus toteaa yleisesti, että eri viranomaisilla ei ole kansallisen lainsäädännön perusteella lupaa saada tietoja sellaisiin yksilöimättömiin uhkiin, joista ei ole konkreettisia tietoja, liittyvää aktiivista selvittämistä varten. Kansalliset viranomaiset eivät siis voi perusteitta saada viestintää koskevaa raakadataa ja käsitellä sitä automaattisesti saadakseen tietoja ja ehkäistäkseen aktiivisesti turvallisuuteen kohdistuvia vaaroja.

132. Saman hallituksen mukaan tietojen saantiin on sovellettava tiukkoja edellytyksiä kunkin toimivaltaisen kansallisen viranomaisen aseman mukaan.

133. Ensimmäiseen ennakkoratkaisukysymykseen annettava vastaus ei mielestäni edellytä, että unionin tuomioistuin analysoi tyhjentävästi edellytykset, joiden on täytyttävä, jotta kukin näistä viranomaisista voi saada säilytetyt tiedot. Tämä tehtävä kuuluu pikemminkin ennakkoratkaisua pyytäneelle tuomioistuimelle, jonka on suoritettava se tuomiossa Tele2 Sverige ja Watson ja tuomiossa Ministerio Fiscal esitetyn tulkinnan perusteella.

134. Belgian hallituksen toimittamien tietojen mukaan oikeusviranomaisiin tai syyttäjäviranomaiseen [91] sovellettavat edellytykset, jotka koskevat tietojen saantia rikostutkintalain 46bis [92] ja 88bis [93] §:ssä tarkoitettua rikosten tutkintaa, selvittämistä ja syyteharkintaa varten, ja muihin viranomaisiin sovellettavat vastaavat edellytykset poikkeavat toisistaan huomattavasti.

135. Vuonna 1998 annetussa laissa todetaan turvallisuus- ja tiedustelupalvelujen osalta, että operaattoreiden hallussa olevien liikenne- ja paikkatietojen saantia koskevan pyynnön on perustuttava objektiivisiin kriteereihin, jotta taataan tietojen saannin rajoittuminen täysin välttämättömään ennalta tunnistetun uhkan perusteella. [94] Erilaisia saatavuutta koskevia määräaikoja (kuusi, yhdeksän tai kaksitoista kuukautta) säädetään mahdollisen uhkan perusteella, ja vaatimuksen on oltava suhteellisuus- ja toissijaisuusperiaatteen mukainen. On myös otettu käyttöön riippumattoman viranomaisen vastuulle kuuluva itsenäinen valvontajärjestelmä. [95]

136. Belgian posti- ja televiestintälaitoksen (BIPT) poliisivirkamiesten on mahdollista saada televiestintäoperaattoreiden hallussa olevia tietoja syyttäjäviranomaisen valvonnassa vain hyvin harvoissa erityistapauksissa, [96] mutta Belgian hallituksen mukaan sen toiminta ei kuitenkaan ulotu niihin henkilöihin, joiden tietoja säilytetään.

[91] Syyttäjäviranomaisen pätevyyttä määrätä tämäntyyppisistä toimenpiteistä käsitellään ennakkoratkaisupyynnössä C-746/18, HK v. Prokuratur, joka on edelleen vireillä.

[92] Syyttäjäviranomaisella on toimivalta vaatia operaattoreilta tunnistetietoja perustellulla kirjallisella päätöksellä (kiireellisessä tapauksessa suullisesti), jossa vahvistetaan toimenpiteen oikeasuhteisuus yksityiselämän kunnioittamiseen nähden ja sen toissijaisuus mihin tahansa muuhun selvittämisvelvoitteeseen nähden. Niiden rikosten osalta, joista ei seuraa vähintään yhden vuoden vankeusrangaistus tai sitä ankarampi rangaistus, syyttäjäviranomainen voi pyytää tietoja vain päätöstään edeltäneiden kuuden kuukauden ajalta.

[93] Tutkintatuomarilla on toimivalta vaatia operaattoreilta sähköisen viestinnän tai säilytettyjen liikenne- ja paikkatietojen jäljittämistä, ja se voi määrätä tästä toimenpiteestä, jos on olemassa vahvoja viitteitä rikoksesta, josta määrätään tiettyjä rangaistuksia, perustellulla kirjallisella määräyksellä (kiireellisessä tapauksessa suullisesti), johon sovelletaan samoja oikeasuhteisuutta ja toissijaisuutta koskevia vaatimuksia kuin syyttäjäviranomaisen päätökseen. Eräitä poikkeuksia sovelletaan silloin, kun toimenpide kohdistuu tiettyihin suojattuihin ammattiryhmiin (esimerkiksi asianajajiin tai lääkäreihin).

[94] Päätöksessä täsmennetään tapauskohtaisesti luonnolliset henkilöt tai oikeushenkilöt, rekisteröimättömät yhdistykset tai ryhmät, esineet, paikat, tapahtumat tai tiedot, joihin sovelletaan erityistä menetelmää. Siinä on myös mainittava pyydettyjen tietojen tarkoituksen ja mahdollisen uhkan välinen yhteys, jolla tätä erityistä menetelmää perustellaan.

[95] Tiedustelu- ja turvallisuuspalvelujen erityisten ja poikkeuksellisten tiedonkeruumenetelmien valvonnasta vastaava hallintokomitea (BIM-komitea) ja tiedustelupalvelujen valvonnasta vastaava pysyvä komitea (R-komitea). Belgian hallitus toteaa, että BIM-komitea vastaa tiedustelu- ja turvallisuuspalvelujen käyttämien hakumenetelmien seurannasta ja harjoittaa niiden osalta ensimmäisen asteen valvontaa. Tämä tuomareista koostuva komitea hoitaa tehtävänsä täysin riippumattomasti. Toisen asteen riippumattoman valvonnan järjestämisestä vastaa R-komitea.

[96] Se sallitaan vuonna 2005 annetun lain 114 (verkkoturvallisuus), 124 (sähköisen viestinnän luottamuksellisuus) ja 126 (tietojen säilyttäminen ja saanti) §:ssä tarkoitettujen rikosten tutkintaa, selvittämistä ja syyteharkintaa varten.

137. Ensiapua tarjoavat pelastusyksiköt voivat pyytää hätäpuhelun soittajan tietoja silloin, kun ne eivät hätäpuhelun jälkeen saa toimittajalta tai operaattorilta kyseisen soittajan tunnistustietoja tai saavat puutteellisia tai virheellisiä tietoja.

138. Liittovaltion poliisin kadonneiden henkilöiden yksikön poliisivirkamiehet voivat pyytää operaattorilta tarvittavat tiedot sellaisen kadonneen henkilön löytämiseksi, jonka fyysinen koskemattomuus on välittömässä vaarassa. Tietojen saantiin sovelletaan tiukkoja edellytyksiä, ja se rajoittuu käyttäjän tunnistamisen mahdollistaviin tietoihin ja tietoihin, jotka liittyvät verkkoyhteyteen ja päätelaitteen verkkoliittymään sekä näiden laitteiden sijaintiin ja 48 tunnin ajan ennen tietopyynnön esittämistä tallennettuihin tietoihin.

139. Televiestinnän välitysyksikkö voi pyytää vain sellaisen henkilön tunnistetietoja, joka on käyttänyt vilpillisesti sähköistä viestintäverkkoa tai -palvelua. Tässä tapauksessa (välitysyksiköstä erillinen) riippumaton oikeus- tai hallintoviranomainen ei harjoita ennakkovalvontaa.

140. Rahoitusalan valvontaelimelle voidaan finanssialan rikollisuuden torjumiseksi myöntää oikeus saada liikenne- ja paikkatietoja tutkintatuomarin etukäteisluvalla.

141. Näistä säilytettyjen tietojen saantiin sovellettavista yksityiskohtaisista säännöistä ja edellytyksistä, jotka jokaisen viranomaisen, jolla on oikeus saada näitä tietoja, on täytettävä, ilmenee monenlaisia tilanteita ja suojatoimia, joiden yksityiskohtainen mukauttaminen unionin tuomioistuimen oikeuskäytännössään [97] käyttämiin perusteisiin on ennakkoratkaisua pyytäneen tuomioistuimen tehtävä.

142. Huomautan esimerkiksi, että kyseessä olevan lainsäädännön asiayhteydestä ei ilmene, että toimivaltaisilla kansallisilla viranomaisilla olisi velvollisuus systemaattisesti ilmoittaa asianomaisille henkilöille (sillä edellytyksellä, että ilmoittaminen ei vaaranna meneillään olevaa tutkintaa) siitä, että heidän tietoihinsa on tutustuttu. Ei myöskään vaikuta siltä, että ainakaan tietyissä – esimerkiksi rahoitusalan rikoksiin liittyvissä – tapauksissa laadittaisiin ennalta niiden vakavuutta koskevia sääntöjä niitä koskevien tietojen saannin perustelemiseksi. Tuomiossa Ministerio Fiscal tarkoitettu oikeuksiin puuttumisen intensiteetin ja tutkitun rikoksen vakavuuden välinen yhteys ei käy ilmi kaikissa tapauksissa.

143. Näkökohdat, jotka liittyvät viranomaisten oikeuteen saada tietoja, jäävät mielestäni joka tapauksessa taka-alalle silloin, kun edellä esitetyn perusteella juuri kyseisten tietojen yleinen ja erotuksetta tapahtuva säilyttäminen on tärkein syy siihen, että tämän ennakkoratkaisupyynnön taustalla oleva kansallinen lainsäädäntö ei ole unionin oikeuden mukainen.

4. Kolmas ennakkoratkaisukysymys

144. Cour constitutionnelle haluaa tietää, voidaanko siinä tapauksessa, että kansallinen lainsäädäntö todetaan unionin tuomioistuimen vastauksen perusteella yhteensopimattomaksi unionin oikeuden kanssa, pitää väliaikaisesti voimassa kyseisen lainsäädännön vaikutukset. Näin vältettäisiin oikeudellinen epävarmuus ja mahdollistettaisiin aikaisemmin kerättyjen ja säilytettyjen tietojen käyttäminen asetettujen tavoitteiden saavuttamiseen.

[97] Viittaan tämän ratkaisuehdotuksen 60 kohtaan.

145. Vakiintuneen oikeuskäytännön mukaan ”ainoastaan unionin tuomioistuin voi poikkeustapauksissa ja oikeusvarmuutta koskevista pakottavista syistä lykätä tilapäisesti unionin oikeuden säännön syrjäyttävää vaikutusta sen kanssa ristiriidassa olevaan kansallisen oikeuden sääntöön”. Jos ”kansallisilla tuomioistuimilla olisi toimivalta antaa kansallisille säännöksille etusija, vaikkakin vain väliaikaisesti, siihen unionin oikeuteen nähden, jonka kanssa ne ovat ristiriidassa, heikennettäisiin unionin oikeuden yhtenäistä soveltamista”. [98]

146. Komissio katsoo, että koska unionin tuomioistuin ei ole rajoittanut direktiivin 2002/58 15 artiklan 1 kohdan tulkinnan ajallisia vaikutuksia, tähän ennakkoratkaisua pyytäneen tuomioistuimen kysymykseen on vastattava kieltävästi. [99]

147. Unionin tuomioistuin totesi kuitenkin 28.2.2012 antamassaan tuomiossa Inter-Environnement Wallonie ja Terre wallonne [100], että kansallisen tuomioistuimen voidaan ympäristönsuojeluun liittyvän pakottavan syyn olemassaolon vuoksi poikkeuksellisesti sallia soveltavan kansallista säännöstään, jossa sille annetaan mahdollisuus pitää voimassa eräitä kumotun kansallisen toimen vaikutuksia unionin oikeuden rikkomisen seurauksena. [101]

148. Tämä oikeuskäytännön linja on vahvistettu 29.7.2019 annetussa tuomiossa Inter-Environnement Wallonie ja Bond Beter Leefmilieu Vlaanderen. [102] Koska oikeuskäytäntö on syntynyt ympäristönsuojelun alalla tai sen taustalla on sähkön toimitusvarmuus, ei ole mielestäni syytä jättää sitä soveltamatta muilla unionin oikeuden aloilla, erityisesti käsiteltävässä asiassa kyseessä olevalla alalla.

149. Se, että kansallinen tuomioistuin voi poikkeuksellisesti ”ympäristönsuojeluun liittyvän pakottavan syyn” perusteella pitää voimassa unionin oikeuden kanssa yhteensopimattoman kansallisen säännöksen tietyt vaikutukset, johtuu siitä, että ympäristönsuojelu on eräs ”unionin päätavoitteista ja luonteeltaan läpäisevä ja perustavanlaatuinen”. [103]

150. Unionin päämääriin kuuluu myös turvallisuuden alueen perustaminen (SEU 3 artikla), mukaan lukien keskeisten valtion tehtävien kunnioittaminen, erityisesti niiden, joiden tarkoituksena on yleisen järjestyksen turvaaminen sekä kansallisen turvallisuuden takaaminen (SEU 4 artiklan 2 kohta). Kyseinen tavoite on yhtä ”läpäisevä ja perustavanlaatuinen” kuin ympäristön suojeleminen, sillä sen toteuttaminen on välttämätön edellytys sellaisen oikeudellisen kehyksen luomiselle, jolla voidaan taata perusoikeuksien ja -vapauksien tosiasiallinen käyttäminen.

151. Mielestäni kansallisen turvallisuuden suojeluun liittyvillä pakottavilla syillä voidaan tässä asiassa perustella se, että unionin tuomioistuin poikkeuksellisesti sallii ennakkoratkaisua pyytäneen tuomioistuimen pitää voimassa ainakin joitakin kyseessä olevan lain vaikutuksia.

98 Tuomio 28.7.2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, 33 kohta).

99 Komission kirjallisten huomautusten 100 kohta.

100 C-41/11, EU:C:2012:103.

101 Tuomio 28.2.2012, Inter-Environnement Wallonie ja Terre wallonne (C-41/11, EU:C:2012:103, 58 kohta). Unionin tuomioistuin päätteli 28.7.2016 antamansa tuomion Association France Nature Environnement (C-379/15, EU:C:2016:603) 34 kohdassa tästä toteamuksesta, että ”tarkoituksena on ollut tunnustaa kansallisen tuomioistuimen tapauskohtainen ja poikkeuksellinen toimivalta mukauttaa unionin oikeuden vastaiseksi katsotun kansallisen säännöksen kumoamisen vaikutuksia”.

102 C-411/17 (EU:C:2019:622, 178 kohta).

103 Tuomio 28.2.2012, Inter-Environnement Wallonie ja Terre wallonne (C-41/11, EU:C:2012:103, 57 kohta).

152. Tällainen voimassa pitäminen edellyttää, että ennakkoratkaisua pyytänyt tuomioistuin katsoo unionin tuomioistuimen ratkaisun perusteella, että kansallinen lainsäädäntö on yhteensopimaton unionin oikeuden kanssa, ja pitää erittäin häiritsevänä vaikutuksia, joita sen välittömällä kumoamisella (jos kumoaminen olisi kansallisessa oikeudessa seurausta kyseisestä yhteensopimattomuudesta) tai soveltamatta jättämisellä voisi olla yleiseen tai valtion turvallisuuteen.

153. Kansallisen lain (kaikkien tai joidenkin) vaikutusten tilapäinen jatkuminen edellyttää lisäksi seuraavaa:

– kyseisen pidentämisen tarkoituksena olisi välttää lainsäädäntötyhjiö, jonka vaikutukset ovat yhtä vahingolliset kuin kyseessä olevan lainsäädännön soveltamisesta johtuvat vaikutukset ja jota ei voida torjua muilla keinoilla ja joka merkitsisi sitä, että kansalliset viranomaiset menettäisivät valtion turvallisuuden takaamisen kannalta arvokkaan välineen; ja

– vaikutuksia jatkettaisiin ainoastaan sen ajan, joka on ehdottoman välttämätön niiden toimenpiteiden toteuttamiseksi, jotka ovat tarpeen todetun unionin oikeuden vastaisuuden korjaamiseksi. [104]

154. Tätä ratkaisua puoltaa lisäksi se, että kansallista lainsäädäntöä on vaikea yhdenmukaistaa tuomiossa Tele2 Sverige ja Watson [105] vahvistetun oikeuskäytännön kanssa ja että Belgian lainsäätäjän tahto noudattaa tuomiota Digital Rights ilmeni sen muuttaessa kansallista lainsäädäntöään. Tämä ennakkotapaus antaa aihetta ajatella, että se yhdenmukaistaa myös 29.5.2016 annetun lain (joka julkaistiin ennen tuomion Tele2 Sverige ja Watson antamista) viimeksi mainitussa tuomiossa vahvistetun oikeuskäytännön kanssa.

V Ratkaisuehdotus

155. Edellä esitetyn perusteella ehdotan, että unionin tuomioistuin vastaa Cour constitutionnellen ennakkoratkaisukysymyksiin seuraavasti:

1) 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, kun sitä luetaan yhdessä Euroopan unionin perusoikeuskirjan 7, 8 ja 11 artiklan ja 52 artiklan 1 kohdan kanssa, on tulkittava seuraavasti:

   – Se on esteenä kansalliselle säännöstölle, jossa säädetään operaattoreita ja sähköisten viestintäpalvelujen tarjoajia koskevasta yleisestä velvollisuudesta säilyttää erotuksetta kaikkien tilaajien ja käyttäjien liikenne- ja paikkatiedot kaikkien sähköisten viestintävälineiden osalta.

104 Tuomio 28.2.2012, Inter-Environnement Wallonie ja Terre wallonne (C-41/11, EU:C:2012:103, 62 kohta).

105 Tanskan hallituksen kirjallisten huomautusten 45 kohta.

– Edellä esitetylle ei ole esteenä se, että kyseisen kansallisen lainsäädännön tavoitteena ei ole ainoastaan vakavuudeltaan eriasteisten rikosten tutkinta, selvittäminen ja syyteharkinta vaan myös valtion turvallisuuden, maanpuolustuksen ja yleisen turvallisuuden takaaminen, sähköisten viestintäjärjestelmien kielletyn käytön torjuminen taikka jokin muu luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) 23 artiklan 1 kohdassa säädetyistä tavoitteista.

– Edellä esitetylle ei ole esteenä myöskään se, että säilytettyjen tietojen saantia koskevat täsmällisesti säännellyt takeet. Ennakkoratkaisua pyytäneen tuomioistuimen tehtävänä on tutkia, rajoitetaanko kansallisella lainsäädännöllä, jolla säännellään toimivaltaisten viranomaisten oikeutta saada kyseisiä tietoja, niiden saanti erityistapauksiin, joiden vakavuus tekee oikeuksiin puuttumisesta välttämätöntä; asetetaanko siinä näiden tietojen saannin edellytykseksi tuomioistuimen tai riippumattoman viranomaisen suorittama etukäteisvalvonta (kiireellisiä tapauksia lukuun ottamatta) ja säädetäänkö siinä, että henkilöille, joita asia koskee, ilmoitetaan tästä tietojen saannista edellyttäen, että ilmoittaminen ei vaaranna kyseisten viranomaisten toimintaa.

2) Euroopan unionin perusoikeuskirjan 4 ja 6 artiklalla ei ole direktiivin 2002/58 15 artiklan 1 kohdan, luettuna yhdessä muiden edellä mainittujen perusoikeuskirjan artiklojen kanssa, tulkintaan sellaista vaikutusta, että ne estäisivät määrittämästä, onko pääasiassa kyseessä olevan kaltainen kansallinen lainsäädäntö yhteensopimaton unionin oikeuden kanssa.

3) Kansallinen tuomioistuin voi kansallisen lainsäädännön sen salliessa poikkeuksellisesti ja tilapäisesti pitää voimassa pääasiassa kyseessä olevan kaltaisen lainsäädännön vaikutukset silloinkin, kun lainsäädäntö on yhteensopimaton unionin oikeuden kanssa, jos vaikutusten voimassa pitäminen on perusteltua sellaisten pakottavien syiden vuoksi, jotka liittyvät yleiseen tai kansalliseen turvallisuuteen kohdistuviin uhkiin, joita ei voida torjua muilla keinoilla tai vaihtoehdoilla. Vaikutusten voimassa pitämistä voidaan jatkaa vain niin kauan kuin on ehdottoman välttämätöntä, jotta mainittu yhteensopimattomuus unionin oikeuden kanssa saadaan oikaistuksi.