Oikeustapauskokoelma

UNIONIN TUOMIOISTUIMEN TUOMIO (suuri jaosto)

6 päivänä lokakuuta 2020 *

[Teksti oikaistu 16.11.2020 annetulla määräyksellä]

Sisällys

Asiaa koskevat oikeussäännöt 6

Unionin oikeus 6

Direktiivi 95/46 6

Direktiivi 97/66 7

Direktiivi 2000/31 7

Direktiivi 2002/21 9

Direktiivi 2002/58 9

Asetus 2016/679 13

Ranskan oikeus 17

Sisäisestä turvallisuudesta annettu koodeksi 17

CPCE 21

Luottamuksesta digitaalisessa taloudessa 21.6.2004 annettu laki nro 2004-575 23

Asetus nro 2011-219 24

Belgian oikeus 26

Pääasiat ja ennakkoratkaisukysymykset 27

Asia C-511/18 27

Asia C-512/18 30

* Oikeudenkäyntikieli: ranska.

Asia C-520/18 31

Asioiden käsittelyn vaiheet unionin tuomioistuimessa 33

Ennakkoratkaisukysymysten tarkastelu 33

Ensimmäiset kysymykset asioissa C-511/18 ja C-512/18 sekä ensimmäinen ja toinen kysymys asiassa C-520/18 33

Alustavat toteamukset 33

Direktiivin 2002/58 soveltamisala 34

Direktiivin 2002/58 15 artiklan 1 kohdan tulkinta 37

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen ennakoivasta säilyttämisestä kansallisen turvallisuuden takaamiseksi 42

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen ennakoivasta säilyttämisestä rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi 43

– Lainsäädännölliset toimenpiteet, joissa säädetään IP-osoitteiden ja henkilöllisyyttä koskevien tietojen ennakoivasta säilyttämisestä rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi 45

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen säilyttämisen nopeasta varmistamisesta vakavan rikollisuuden torjumiseksi 47

Asiassa C-511/18 esitetyt toinen ja kolmas kysymys 49

Liikenne- ja paikkatietojen automaattinen analysointi 50

Liikenne- ja paikkatietojen kerääminen reaaliajassa 52

Tiedon antaminen henkilöille, joiden tiedot on kerätty tai analysoitu 53

Toinen kysymys asiassa C-666/18 56

Kolmas kysymys asiassa C-520/18 57

Oikeudenkäyntikulut 59

Ennakkoratkaisupyyntö – Henkilötietojen käsittely sähköisen viestinnän alalla – Sähköisten viestintäpalvelujen tarjoajat – Hosting-palvelujen tarjoajat ja internetyhteyden tarjoajat – Liikenne- ja paikkatietojen säilyttäminen yleisesti ja erotuksetta – Tietojen automaattinen analysointi – Tietojen saaminen reaaliajassa – Kansallisen turvallisuuden takaaminen ja terrorismin torjunta – Rikollisuuden torjunta – Direktiivi 2002/58/EY – Soveltamisala – 1 artiklan 3 kohta ja 3 artikla – Sähköisen viestinnän luottamuksellisuus – Suojaaminen – 5 artikla ja 15 artiklan 1 kohta – Direktiivi 2000/31/EY – Soveltamisala – Euroopan unionin perusoikeuskirja – 4, 6–8 ja 11 artikla sekä 52 artiklan 1 kohta – SEU 4 artiklan 2 kohta

Yhdistetyissä asioissa C-511/18, C-512/18 ja C-520/18,

joissa on kyse SEUT 267 artiklaan perustuvista ennakkoratkaisupyynnöistä, jotka Conseil d'État (ylin hallintotuomioistuin, Ranska) on esittänyt 26.7.2018 tekemillään päätöksillä, jotka ovat saapuneet unionin tuomioistuimeen 3.8.2018 (C-511/18 ja C-512/18), ja Cour constitutionnelle (perustuslakituomioistuin, Belgia) 19.7.2018 tekemällään päätöksellä, joka on saapunut unionin tuomioistuimeen 2.8.2018 (C-520/18), saadakseen ennakkoratkaisun asioissa

La Quadrature du Net (C-511/18 ja C-512/18),

French Data Network (C-511/18 ja C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 ja C-512/18) ja

Igwan.net (C-511/18)

vastaan

Premier ministre (C-511/18 ja C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 ja C-512/18),

Ministre de l'Intérieur (C-511/18) ja

Ministre des Armées (C-511/18),

Privacy Internationalin (C-512/18) ja

Center for Democracy and Technologyn (C-512/18) osallistuessa asian käsittelyyn

ja

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,

Child Focusin (C-520/18) osallistuessa asian käsittelyyn,

UNIONIN TUOMIOISTUIN (suuri jaosto),

toimien kokoonpanossa: presidentti K. Lenaerts, varapresidentti R. Silva de Lapuerta, jaostojen puheenjohtajat J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb ja L. S. Rossi sekä tuomarit J. Malenovský, L. Bay Larsen, T. von Danwitz (esittelevä tuomari), C. Toader, K. Jürimäe, C. Lycourgos ja N. Piçarra,

julkisasiamies: M. Campos Sánchez-Bordona,

kirjaaja: hallintovirkamies C. Strömholm,

ottaen huomioon kirjallisessa käsittelyssä ja 9. ja 10.9.2019 pidetyssä istunnossa esitetyn,

ottaen huomioon huomautukset, jotka sille ovat esittäneet

– Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net ja Center for Democracy and Technology, edustajanaan A. Fitzjean Ò Cobhthaigh, avocat,

– French Data Network, edustajanaan Y. Padova, avocat,

– Privacy International, edustajanaan H. Roy, avocat,

– Ordre des barreaux francophones et germanophone, edustajinaan E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart ja J.-F. Henrotte, avocats,

– Académie Fiscale ASBL ja UA, edustajanaan J.-P. Riquet,

– Liga voor Mensenrechten ASBL, edustajanaan J. Vander Velpen, avocat,

– Ligue des Droits de l'Homme ASBL, edustajinaan R. Jespers ja J. Fermon, avocats,

– VZ, WY ja XX, edustajanaan D. Pattyn, avocat,

– Child Focus, edustajinaan N. Buisseret, K. De Meester ja J. Van Cauter, avocats,

– Ranskan hallitus, asiamiehinään aluksi D. Dubois, F. Alabrune, D. Colas, E. de Moustier ja A.-L. Desjonquères, sittemmin D. Dubois, F. Alabrune, E. de Moustier ja A.-L. Desjonquères,

– Belgian hallitus, asiamiehinään J.-C. Halleux, P. Cottin ja C. Pochet, avustajinaan J. Vanpraet, Y. Peeters, S. Depré ja E. de Lophem, avocats,

– Tšekin hallitus, asiamiehinään M. Smolek, J. Vláčil ja O. Serdula,

– Tanskan hallitus, asiamiehinään aluksi J. Nymann-Lindegren, M. Wolff ja P. Ngo, sittemmin J. Nymann-Lindegren ja M. Wolff,

– Saksan hallitus, asiamiehinään aluksi J. Möller, M. Hellmann, E. Lankenau, R. Kanitz ja T. Henze, sittemmin J. Möller, M. Hellmann, E. Lankenau ja R. Kanitz,

– Viron hallitus, asiamiehinään N. Grünberg ja A. Kalbus,

– Irlannin hallitus, asiamiehinään A. Joyce, M. Browne ja G. Hodge, avustajanaan D. Fennelly, BL,

– Espanjan hallitus, asiamiehinään aluksi L. Aguilera Ruiz ja A. Rubio González, sittemmin L. Aguilera Ruiz,

– Kyproksen hallitus, asiamiehenään E. Neofytou,

– Latvian hallitus, asiamiehenään V. Soņeca,

– Unkarin hallitus, asiamiehinään aluksi M. Z. Fehér ja Z. Wagner, sittemmin M. Z. Fehér,

– Alankomaiden hallitus, asiamiehinään M. K. Bulterman ja M. A. M. de Ree,

– Puolan hallitus, asiamiehinään B. Majczyna, J. Sawicka ja M. Pawlicka,

– Ruotsin hallitus, asiamiehinään aluksi H. Shev, H. Eklinder, C. Meyer-Seitz ja A. Falk, sittemmin H. Shev, H. Eklinder, C. Meyer-Seitz ja J. Lundberg,

– Yhdistyneen kuningaskunnan hallitus, asiamiehenään S. Brandon, avustajinaan G. Facenna, QC, ja de C. Knight, barrister,

– [luetelmakohta poistettu 16.11.2020 annetulla määräyksellä],

– Euroopan komissio, asiamiehinään aluksi H. Kranenborg, M. Wasmeier ja P. Costa de Oliveira, sittemmin H. Kranenborg ja M. Wasmeier,

– Euroopan tietosuojavaltuutettu, asiamiehinään T. Zerdick ja A. Buchta,

kuultuaan julkisasiamiehen 15.1.2020 pidetyssä istunnossa esittämät ratkaisuehdotukset,

on antanut seuraavan

tuomion

1 Ennakkoratkaisupyynnöt koskevat yhtäältä henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12.7.2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) (EYVL 2002, L 201, s. 37), sellaisena kuin se on muutettuna 25.11.2009 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY (EUVL 2009, L 337, s. 11) (jäljempänä direktiivi 2002/58), 15 artiklan 1 kohdan ja toisaalta tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista 8.6.2000 annetun Euroopan parlamentin ja neuvoston direktiivin 2000/31/EY (”Direktiivi sähköisestä kaupankäynnistä”) (EYVL 2000, L 178, s. 1) 12–15 artiklan, luettuina Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 4, 6–8 ja 11 artiklan sekä 52 artiklan 1 kohdan ja SEU 4 artiklan 2 kohdan valossa, tulkintaa.

2 Pyyntö asiassa C-511/18 on esitetty oikeusriidoissa, joissa asianosaisina ovat yhtäältä Quadrature du Net, French Data Network, Fédération des fournisseurs d’accès à Internet associatifs ja Igwan.net sekä toisaalta Premier ministre (pääministeri, Ranska), Garde des Sceaux, ministre de la Justice (oikeusministeri, Ranska), ministre de l’Intérieur (sisäministeri, Ranska) ja ministre des Armées (puolustusministeri, Ranska) ja joissa on kyse erikoistuneiden tiedusteluyksiköiden nimeämisestä 28.9.2015 annetun asetuksen nro 2015-1185 (décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement) (JORF 29.9.2015, teksti 1/97; jäljempänä asetus nro 2015-1185), luvanvaraisten tiedustelumenetelmien soveltamiseen ja valtion turvallisuuteen vaikuttaviin tiedostoihin liittyvistä oikeudenkäyntiasioista 1.10.2015 annetun asetuksen nro 2015-1211 (décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en oeuvre des techniques

de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État) (JORF 2.10.2015, teksti 7/108; jäljempänä asetus nro 2015-1211), sellaisten muiden yksiköiden, joilla on erikoistuneiden tiedusteluyksiköiden lisäksi lupa käyttää sisäisestä turvallisuudesta annetun koodeksin VIII osan V luvussa mainittuja menetelmiä, nimeämisestä sisäisestä turvallisuudesta annetun koodeksin L. 811-4 §:n mukaisesti 11.12.2015 annetun asetuksen nro 2015-1639 (décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure) (JORF 12.12.2015, teksti 28/127; jäljempänä asetus nro 2015-1639) ja tiedonhankintamenetelmistä 29.1.2016 annetun asetuksen nro 2016-67 (décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement) (JORF 31.1.2016, teksti 2/113; jäljempänä asetus nro 2016-67) lainmukaisuudesta.

3 Pyyntö asiassa C-512/18 on esitetty oikeusriidoissa, joissa asianosaisina ovat yhtäältä French Data Network, Quadrature du Net ja Fédération des fournisseurs d'accès à Internet associatifs sekä toisaalta pääministeri ja oikeusministeri ja joissa on kyse postista ja sähköisestä viestinnästä annetun koodeksin (code des postes et des communications électroniques) (jäljempänä CPCE) R. 10-13 §:n ja sellaisten tietojen säilyttämisestä ja toimittamisesta, joiden perusteella voidaan tunnistaa kaikki verkkoon ladatun sisällön luomiseen osallistuneet henkilöt, 25.2.2011 annetun asetuksen nro 2011-219 (décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne) (JORF 1.3.2011, teksti 32/170; jäljempänä asetus nro 2011-219), lainmukaisuudesta.

4 Pyyntö asiassa C-520/18 on esitetty oikeusriidoissa, joissa asianosaisina ovat yhtäältä 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 sekä toisaalta Conseil des ministres (ministerineuvosto, Belgia) ja joissa on kyse tietojen keräämisestä ja säilyttämisestä sähköisen viestinnän alalla 29.5.2016 annetun lain (loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques) (Moniteur belge 18.7.2016, s. 44717; jäljempänä 29.5.2016 annettu laki) lainmukaisuudesta.

Asiaa koskevat oikeussäännöt

Unionin oikeus

Direktiivi 95/46

5 Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY (EYVL 1995, L 281, s. 31) on kumottu 25.5.2018 alkaen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetulla Euroopan parlamentin ja neuvoston asetuksella (EU) 2016/679 (EUVL 2016, L 119, s. 1). Direktiivin 95/46 3 artiklan 2 kohdassa säädettiin seuraavaa:

”Tätä direktiiviä ei sovelleta henkilötietojen käsittelyyn,

– joka suoritetaan sellaisessa toiminnassa, joka ei kuulu [unionin] oikeuden soveltamisalaan, kuten toiminta, josta on määrätty Euroopan unionista tehdyn sopimuksen V ja VI osastossa, ja kaikissa tapauksissa käsittely, joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta (myös valtion taloudellista hyvinvointia, kun käsittelyoperaatio on sidoksissa valtion turvallisuutta koskeviin kysymyksiin) ja rikosoikeuden alalla tapahtuvaa valtion toimintaa,

– jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa."

6 Direktiivin 95/46 III lukuun, jonka otsikko on "Oikeuskeinot, vastuu ja sanktiot", sisältyvässä kyseisen direktiivin 22 artiklassa, säädettiin seuraavaa:

"Jäsenvaltioiden on säädettävä siitä, että kenellä tahansa henkilöllä on mahdollisuus käyttää oikeussuojakeinoa, jos kyseessä olevaan käsittelyyn sovellettavien kansallisten säännösten mukaisesti hänelle kuuluvia oikeuksia loukataan, sanotun kuitenkaan rajoittamatta sellaisen hallinnollisen keinon soveltamista, johon voidaan turvautua, muun muassa 28 artiklassa tarkoitetun valvontaviranomaisen avulla ennen asian vireillepanoa oikeudessa."

Direktiivi 97/66

7 Henkilötietojen käsittelystä ja yksityisyyden suojasta televiestinnän alalla 15.12.1997 annetun Euroopan parlamentin ja neuvoston direktiivin 97/66/EY (EYVL 1997, L 24, s. 1) 5 artiklassa, jonka otsikko on "Viestinnän luottamuksellisuus", säädetään seuraavaa:

"1. Jäsenvaltioiden on kansallisilla säännöksillä taattava yleisen televerkon ja yleisesti saatavilla olevien telepalvelujen välityksellä tapahtuvan viestinnän luottamuksellisuus. Niiden on erityisesti kiellettävä se, että muut kuin käyttäjät voisivat ilman kyseisten käyttäjien suostumusta kuunnella, salakuunnella, tallentaa tai muulla tavalla siepata tai valvoa viestejä, jollei se ole laillisesti sallittua 14 artiklan 1 kohdan mukaisesti.

2. Mitä 1 kohdassa säädetään, ei koske laillisesti sallittua viestinnän nauhoittamista normaalin liiketoiminnan piirissä todisteeksi liiketapahtumasta tai mistä tahansa muusta liiketoimintaan liittyvästä viestinnästä."

Direktiivi 2000/31

8 Direktiivin 2000/31 johdanto-osan 14 ja 15 perustelukappaleessa todetaan seuraavaa:

"(14) Yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä säännellään yksinomaan [direktiivillä 95/46] sekä [direktiivillä 97/66], joita sovelletaan täysimääräisesti tietoyhteiskunnan palveluihin. Näillä direktiiveillä on jo luotu henkilötietoja koskevat [unionin] oikeudelliset puitteet, eikä tässä direktiivissä ole näin ollen tarpeen käsitellä tätä kysymystä sisämarkkinoiden moitteettoman toiminnan ja erityisesti jäsenvaltioiden välisen henkilötietojen vapaan liikkuvuuden varmistamiseksi. Tämän direktiivin täytäntöönpanossa ja soveltamisessa olisi noudatettava kaikilta osin henkilötietojen suojaa koskevia periaatteita erityisesti ei-toivotun kaupallisen viestinnän ja välittäjien vastuun osalta. Tällä direktiivillä ei voida estää avointen verkkojen kuten Internetin anonyymiä käyttöä.

(15) Sähköisen viestinnän luottamuksellisuus taataan [direktiivin 97/66] 5 artiklassa. Mainitun direktiivin perusteella jäsenvaltioiden on kiellettävä kaikenlainen muu kuin lähettäjien tai vastaanottajien suorittama sähköisen viestinnän kuuntelu tai valvonta, jollei tämä ole laillisesti sallittua."

9 Direktiivin 2000/31 1 artiklan sanamuoto on seuraava:

"1. Tämän direktiivin tavoitteena on edistää sisämarkkinoiden moitteetonta toimintaa varmistamalla tietoyhteiskunnan palvelujen vapaa liikkuvuus jäsenvaltioiden välillä.

2. Tällä direktiivillä lähennetään siinä määrin, kuin se on tarpeen 1 kohdassa tarkoitetun tavoitteen toteuttamiseksi, tiettyjä tietoyhteiskunnan palveluihin sovellettavia kansallisia säännöksiä, jotka koskevat sisämarkkinoita, palvelun tarjoajien sijoittautumista, kaupallista viestintää, sähköisessä muodossa tehtäviä sopimuksia, välittäjien vastuuta, käytännesääntöjä, tuomioistuinten ulkopuolella tapahtuvaa riitojen ratkaisemista, oikeussuojakeinoja ja jäsenvaltioiden välistä yhteistyötä.

3. Tämä direktiivi täydentää tietoyhteiskunnan palveluihin sovellettavaa [unionin] lainsäädäntöä, heikentämättä kuitenkaan [unionin] säädöksillä ja niiden täytäntöönpanemiseksi annetulla kansallisella lainsäädännöllä vahvistettua suojelun tasoa erityisesti kansanterveyden ja kuluttajien suojelun osalta, sikäli kuin tämä ei rajoita tietoyhteiskunnan palvelujen tarjoamisen vapautta.

– –

5. Tätä direktiiviä ei sovelleta:

– –

b) direktiivien [95/46] ja [97/66] soveltamisalaan kuuluviin tietoyhteiskunnan palveluihin liittyviin kysymyksiin;

– –”

10 Direktiivin 2000/31 2 artiklassa säädetään seuraavaa:

”Tässä direktiivissä tarkoitetaan:

a) ’tietoyhteiskunnan palveluilla’ [teknisiä standardeja ja määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 22.6.1998 annetun Euroopan parlamentin ja neuvoston] direktiivin 98/34/EY [(EYVL 1998, L 204, s. 37)], muutettuna [20.7.1998 annetulla Euroopan parlamentin ja neuvoston] direktiivillä 98/48/EY [(EYVL 1998, L 217, s. 18)], 1 artiklan 2 kohdassa tarkoitettuja palveluja;

– –”

11 Direktiivin 2000/31 15 artiklassa säädetään seuraavaa:

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

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

Direktiivi 2002/21

12 Sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä 7.3.2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/21/EY (puitedirektiivi) (EYVL 2002, L 108, s. 33) johdanto-osan kymmenennessä perustelukappaleessa todetaan seuraavaa:

”Direktiivin [98/34], sellaisena kuin se on muutettuna direktiivillä [98/48], 1 artiklassa oleva ’tietoyhteiskunnan palvelun’ määritelmä koskee useita verkossa toteutettavia taloudellisia toimintoja; suurin osa näistä toiminnoista ei kuulu tämän direktiivin soveltamisalaan, koska ne eivät koostu kokonaan tai pääosin signaalien siirtämisestä sähköisissä viestintäverkoissa; tämä direktiivi kattaa puhelinpalvelut ja sähköpostipalvelut. Sama yritys, esimerkiksi Internet-palveluntarjoaja, voi tarjota sekä sähköisen viestintäpalvelun, kuten Internet-yhteyden, että tämän direktiivin soveltamisalaan kuulumattomia palveluja, kuten Internet-sisältöjen toimittamisen.”

13 Direktiivin 2002/21 2 artiklassa säädetään seuraavaa:

”Tässä direktiivissä tarkoitetaan:

– –

c) ’sähköisellä viestintäpalvelulla’ tavallisesti korvausta vastaan suoritettuja palveluja, jotka muodostuvat kokonaan tai pääosin signaalien siirtämisestä sähköisissä viestintäverkoissa, mukaan lukien televiestintäpalvelut ja siirtopalvelut radio- ja televisiotoiminnassa käytetyissä verkoissa, mutta jättäen ulkopuolelle sähköisten viestintäverkkojen ja -palvelujen avulla siirretyt sisältöpalvelut tai sisältöä toimituksellisessa valvonnassaan pitävät palvelut; kyseinen palvelu ei käsitä myöskään direktiivin [98/34] ensimmäisessä artiklassa määriteltyjä tietoyhteiskunnan palveluja, jotka eivät muodostu kokonaan tai pääosin signaalien siirtämisestä sähköisissä viestintäverkoissa;

– –”

Direktiivi 2002/58

14 Direktiivin 2002/58 johdanto-osan 2, 6, 7, 11, 22, 26 ja 30 perustelukappaleessa todetaan seuraavaa:

”(2) Tässä direktiivissä pyritään kunnioittamaan perusoikeuksia ja siinä noudatetaan erityisesti [perusoikeuskirjassa] tunnustettuja periaatteita. Tässä direktiivissä pyritään erityisesti varmistamaan [perusoikeuskirjan] 7 ja 8 artiklassa vahvistettujen oikeuksien täysimääräinen kunnioittaminen.

– –

(6) Internet mullistaa markkinoiden perinteisiä rakenteita tarjoamalla käyttöön yhteisen ja maailmanlaajuisen infrastruktuurin, jossa voidaan jakaa laajaa valikoimaa sähköisiä viestintäpalveluja. Internetissä yleisesti saatavilla olevat sähköiset viestintäpalvelut avaavat käyttäjille uusia mahdollisuuksia, mutta aiheuttavat samalla heidän henkilötietoihinsa ja yksityisyyteensä liittyviä uusia riskejä.

(7) Yleisten viestintäverkkojen osalta olisi annettava erityiset lait, asetukset ja tekniset määräykset, jotta luonnollisten henkilöiden perusoikeudet ja -vapaudet sekä oikeushenkilöiden oikeutetut edut voidaan suojata ottaen erityisesti huomioon tilaajia ja käyttäjiä koskevien tietojen automaattisen tallennus- ja käsittelykapasiteetin lisääntyminen.

– –

(11) Tämä direktiivi, samoin kuin direktiivi [95/46], ei koske perusoikeuksien ja -vapauksien turvaamista sellaisessa toiminnassa, joka ei kuulu [unionin] oikeuden soveltamisalaan. Tästä syystä se ei vaikuta tasapainoon, joka tällä hetkellä vallitsee yksittäisten henkilöiden yksityisyyden suojan ja niiden tämän direktiivin 15 artiklan 1 kohdassa tarkoitettujen toimenpiteiden välillä, joita jäsenvaltiot voivat toteuttaa yleisen turvallisuuden, maanpuolustuksen tai valtion turvallisuuden (valtion taloudellinen hyvinvointi mukaan lukien, kun toimet liittyvät valtion turvallisuuteen) suojelemiseksi sekä rikosoikeuden täytäntöönpanemiseksi. Näin ollen tämä direktiivi ei vaikuta jäsenvaltioiden mahdollisuuteen harjoittaa sähköisen viestinnän laillista telekuuntelua tai toteuttaa muita toimenpiteitä, jos ne ovat välttämättömiä edellä mainittuja tarkoituksia varten ja jos noudatetaan [Roomassa 4.11.1950 allekirjoitettua] ihmisoikeuksien ja perusvapauksien suojaamiseksi tehtyä eurooppalaista yleissopimusta sellaisena kuin sitä on Euroopan ihmisoikeustuomioistuimen päätöksissä tulkittu. Näiden toimenpiteiden on oltava asianmukaisia, niiden on ehdottomasti oltava oikeassa suhteessa niiden tarkoitukseen nähden sekä välttämättömiä demokraattisessa yhteiskunnassa ja ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn eurooppalaisen yleissopimuksen mukaisia asianmukaisia suojamääräyksiä olisi sovellettava niihin.

– –

(22) Muiden kuin käyttäjien toimesta tai ilman käyttäjän suostumusta tapahtuvan viestinnän ja siihen liittyvien liikennetietojen tallentamisen kiellolla ei ole tarkoitus kieltää näiden tietojen automaatti-, väli- tai väliaikaistallennusta, jos sen ainoana tarkoituksena on välittää viestintää sähköisessä viestintäverkossa, edellyttäen, että tietoja ei tallenneta pidempään kuin on tarpeen niiden välittämistä ja liikenteen hallintaa varten ja että niiden luottamuksellisuus voidaan taata myös niiden ollessa tallennettuina. – –

– –

(26) Tilaajiin liittyvät tiedot, joita käsitellään sähköisissä viestintäverkoissa liittymien luomiseksi ja tietojen välittämiseksi, sisältävät tietoja luonnollisten henkilöiden yksityiselämästä ja koskevat heidän oikeuttaan viestintänsä suojaan tai oikeushenkilöiden oikeutettuja etuja. Tällaista tietoa voidaan tallentaa vain siinä määrin, kuin se on palvelun tarjoamisen kannalta välttämätöntä laskutuksen tai yhteenliittämismaksujen vuoksi ja vain rajoitetun ajan. Kaikki muu tällaisen tiedon jatkokäsittely – – sallitaan ainoastaan, jos tilaaja on tähän suostunut yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajan hänelle antamien täsmällisten ja täydellisten tietojen perusteella, jotka koskevat näitä suunniteltuja jatkokäsittelymuotoja ja tilaajan oikeutta olla antamatta suostumustaan tai peruuttaa suostumuksensa tällaiseen käsittelyyn. Viestintäpalvelujen markkinointiin – – käytettävät liikennetiedot olisi myös poistettava tai tehtävä nimettömiksi – –.

– –

(30) Sähköisiä viestintäverkkoja ja -palveluita tarjoavat järjestelmät olisi suunniteltava niin, että tarvittavien henkilötietojen määrä rajoitetaan mahdollisimman pieneksi. – –”

15 Direktiivin 2002/58 1 artiklassa, jonka otsikko on ”Soveltamisala ja tavoite”, säädetään seuraavaa:

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

2. Tämän direktiivin säännöksillä täsmennetään ja täydennetään direktiiviä [95/46] edellä 1 kohdassa mainittuja tarkoituksia varten. Niissä säädetään lisäksi tilaajien, jotka ovat oikeushenkilöitä, oikeutettujen etujen suojelemisesta.

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

16 Direktiivin 2002/58 2 artiklassa, jonka otsikko on "Määritelmät", säädetään seuraavaa:

"Jollei toisin ole säädetty, tässä direktiivissä sovelletaan direktiivin [95/46] ja direktiivin [2002/21] sisältämiä määritelmiä.

Lisäksi tässä direktiivissä tarkoitetaan

a) 'käyttäjällä' luonnollisia henkilöitä, jotka käyttävät yleisesti saatavilla olevaa sähköistä viestintäpalvelua yksityis- tai liikeasioihin olematta välttämättä tämän palvelun tilaajia;

b) 'liikennetiedoilla' tietoja, joita käsitellään sähköisessä viestintäverkossa välitettävää viestintää tai sen laskutusta varten;

c) 'paikkatiedoilla' sähköisessä viestintäverkossa tai sähköisen viestintäpalvelun avulla käsiteltäviä tietoja, jotka ilmaisevat yleisesti saatavilla olevan sähköisen viestintäpalvelun käyttäjän päätelaitteen maantieteellisen sijainnin;

d) 'viestinnällä' tietoa, jota vaihdetaan tai jota siirretään tiettyjen osapuolten kesken yleisesti saatavilla olevan sähköisen viestintäpalvelun avulla. Määritelmään ei sisälly tieto, joka välitetään yleisradiotoiminnan yhteydessä yleisölle sähköisessä viestintäverkossa, paitsi siltä osin kuin tieto voidaan yhdistää tietoa vastaanottavaan tunnistettavissa olevaan tilaajaan tai käyttäjään;

_ _"

17 Direktiivin 2002/58 3 artiklassa, jonka otsikko on "Palvelut", säädetään seuraavaa:

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

18 Direktiivin 2002/58 5 artiklassa, jonka otsikko on "Viestinnän luottamuksellisuus", säädetään seuraavaa:

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

_ _

3. Jäsenvaltioiden on varmistettava, että tietojen tallentaminen tai tilaajan tai käyttäjän päätelaitteelle tallennettujen tietojen käyttäminen sallitaan ainoastaan sillä edellytyksellä, että kyseinen tilaaja tai käyttäjä on antanut suostumuksensa saatuaan selkeät ja kattavat tiedot muun muassa käsittelyn tarkoituksesta direktiivin [95/46] mukaisesti. Tämä ei estä teknistä tallentamista tai käyttöä, jonka ainoana tarkoituksena on toteuttaa viestinnän välittäminen sähköisissä viestintäverkoissa tai joka on ehdottoman välttämätöntä tietoyhteiskuntapalvelun tarjoajalle sellaisen palvelun tarjoamiseksi, jota tilaaja tai käyttäjä on erityisesti pyytänyt."

19 Direktiivin 2002/58 6 artiklassa, jonka otsikko on "Liikennetiedot", säädetään seuraavaa:

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

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

3. Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja voi sähköisten viestintäpalvelujen markkinoimiseksi tai lisäarvopalvelujen tarjoamiseksi käsitellä 1 kohdassa tarkoitettuja tietoja siinä määrin ja niin kauan kuin tällainen palvelu tai markkinointi sitä edellyttää, jos tilaaja tai käyttäjä, jota tiedot koskevat, on antanut siihen ennakolta suostumuksensa. Käyttäjille tai tilaajille on annettava mahdollisuus perua liikennetietojen käsittelyä koskeva suostumuksensa milloin tahansa.

– –

5. Liikennetietojen käsittely 1, 2, 3 ja 4 kohdan mukaisesti on rajoitettava yleisten viestintäverkkojen ja yleisesti saatavilla olevien palvelujen tarjoajien vastuulla toimiviin henkilöihin, jotka käsittelevät laskutusta tai liikenteenhallintaa, asiakastiedusteluja, petosten paljastamista, sähköisten viestintäpalvelujen markkinoimista tai lisäarvopalvelujen tarjoamista, ja sitä voidaan suorittaa ainoastaan kyseisten toimien vaatimassa laajuudessa."

20 Kyseisen direktiivin 9 artiklan, jonka otsikko on "Muut paikkatiedot kuin liikennetiedot", 1 kohdassa säädetään seuraavaa:

"Jos yleisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen käyttäjien tai tilaajien muita paikkatietoja kuin liikennetietoja voidaan käsitellä, näitä tietoja saa käsitellä vain silloin, kun ne on tehty nimettömiksi tai jos käyttäjät tai tilaajat ovat antaneet siihen suostumuksensa, ja tietoja saa käsitellä ainoastaan siinä määrin ja niin kauan kuin lisäarvopalvelujen tarjoaminen edellyttää. Ennen kuin käyttäjät tai tilaajat antavat suostumuksensa, palvelun tarjoajan on ilmoitettava heille, minkä tyyppisiä muita paikkatietoja kuin liikennetietoja käsitellään, mikä on käsittelyn tarkoitus ja kuinka kauan se kestää sekä siirretäänkö tiedot kolmannelle osapuolelle lisäarvopalvelun tarjoamista varten. – –"

21 Mainitun direktiivin 15 artiklassa, jonka otsikko on "Direktiivin [95/46] tiettyjen säännösten soveltaminen", säädetään seuraavaa:

"1. Jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan tämän direktiivin 5 artiklassa, 6 artiklassa, 8 artiklan 1, 2, 3 ja 4 kohdassa sekä 9 artiklassa säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos tällaiset rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi direktiivin

[95/46] 13 artiklan 1 kohdan mukaisesti. Tätä varten jäsenvaltiot voivat muun muassa hyväksyä lainsäädännöllisiä toimenpiteitä, joissa säädetään tietojen säilyttämisestä sellaiseksi rajoitetuksi ajaksi, joka on perusteltua tässä kohdassa säädetyistä syistä. Kaikkien tässä kohdassa tarkoitettujen toimenpiteiden on oltava [unionin] oikeuden yleisten periaatteiden mukaisia, mukaan lukien Euroopan unionista tehdyn sopimuksen 6 artiklan 1 ja 2 kohdassa tarkoitetut periaatteet.

– –

2. Direktiivin [95/46] III jakson säännöksiä oikeuskeinoista, vastuista ja seuraamuksista sovelletaan ottaen huomioon tämän direktiivin mukaisesti annetut kansalliset säännökset ja tästä direktiivistä johtuvat henkilökohtaiset oikeudet.

– –”

Asetus 2016/679

22 Asetuksen N:o 2016/679 johdanto-osan kymmenennessä perustelukappaleessa todetaan seuraavaa:

”Jotta voitaisiin varmistaa yhdenmukainen ja korkeatasoinen luonnollisten henkilöiden suojelu ja poistaa henkilötietojen liikkuvuuden esteet unionissa, luonnollisten henkilöiden oikeuksien ja vapauksien suojelun tason näiden tietojen käsittelyssä olisi oltava vastaava kaikissa jäsenvaltioissa. Luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojelua henkilötietojen käsittelyssä koskevien sääntöjen johdonmukainen ja yhtenäinen soveltaminen olisi varmistettava kaikkialla unionissa. – –”

23 Kyseisen asetuksen 2 artiklassa säädetään seuraavaa:

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

2. Tätä asetusta ei sovelleta henkilötietojen käsittelyyn,

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

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

– –

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

– –

4. Tällä asetuksella ei rajoiteta direktiivin [2000/31] soveltamista etenkään niiltä osin kuin on kyse tuon direktiivin 12–15 artiklassa säädetyistä välittäjinä toimivien palveluntarjoajien vastuuta koskevista säännöistä.”

24 Mainitun asetuksen 4 artiklassa säädetään seuraavaa:

”Tässä asetuksessa tarkoitetaan

1) ’henkilötiedoilla’ kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella,

2) ’käsittelyllä’ toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista,

_ _”

25 Asetuksen 2016/679 5 artiklassa säädetään seuraavaa:

”1. Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia:

a) niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (’lainmukaisuus, kohtuullisuus ja läpinäkyvyys’);

b) ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa (’käyttötarkoitussidonnaisuus’);

c) henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (’tietojen minimointi’);

d) henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (’täsmällisyys’);

e) ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi (’säilytyksen rajoittaminen’);

f) niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (’eheys ja luottamuksellisuus’).

_ _”

26 Kyseisen asetuksen 6 artiklassa säädetään seuraavaa:

”1. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

– –

c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;

– –

3. Edellä olevan 1 kohdan c ja e alakohdassa tarkoitetun käsittelyn perustasta on säädettävä joko

a) unionin oikeudessa; tai

b) rekisterinpitäjään sovellettavassa jäsenvaltion lainsäädännössä.

Käsittelyn tarkoitus määritellään kyseisessä käsittelyn oikeusperusteessa – – Kyseinen käsittelyn oikeusperuste voi sisältää erityisiä säännöksiä, joilla mukautetaan tämän asetuksen sääntöjen soveltamista, muun muassa: yleisiä edellytyksiä, jotka koskevat rekisterinpitäjän suorittaman tietojenkäsittelyn lainmukaisuutta; käsiteltävien tietojen tyyppiä; asianomaisia rekisteröityjä, yhteisöjä joille ja tarkoituksia joihin henkilötietoja voidaan luovuttaa; käyttötarkoitussidonnaisuutta; säilytysaikoja; sekä käsittelytoimia ja -menettelyjä, mukaan lukien laillisen ja asianmukaisen tietojenkäsittelyn varmistamiseen tarkoitetut toimenpiteet, kuten toimenpiteet muita IX luvussa esitettyjä erityisiä tietojenkäsittelytilanteita varten. Unionin oikeuden tai jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden.

– –”

27 Mainitun asetuksen 23 artiklassa säädetään seuraavaa:

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

a) kansallinen turvallisuus;

b) puolustus;

c) yleinen turvallisuus;

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

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

f) oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen suojelu;

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

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

i) rekisteröidyn suojelu tai muille kuuluvat oikeudet ja vapaudet;

j) yksityisoikeudellisten kanteiden täytäntöönpano.

2. Edellä 1 kohdassa tarkoitettujen lainsäädäntötoimenpiteiden on sisällettävä tarpeen mukaan erityisiä säännöksiä, jotka koskevat ainakin

a) käsittelytarkoitusta tai käsittelyn ryhmiä;

b) henkilötietoryhmiä;

c) käyttöön otettujen rajoitusten soveltamisalaa;

d) suojatoimia, joilla estetään väärinkäyttö tai lainvastainen pääsy tietoihin tai niiden siirtäminen;

e) rekisterinpitäjän tai rekisterinpitäjien ryhmien määrittämistä;

f) tietojen säilytysaikoja ja sovellettavia suojatoimia ottaen huomioon käsittelyn tai käsittelyryhmien luonne, laajuus ja tarkoitukset;

g) rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä; ja

h) rekisteröityjen oikeutta saada tietoa rajoituksesta, paitsi jos tämä voisi vaarantaa rajoituksen tarkoituksen.”

28 Mainitun asetuksen 79 artiklan 1 kohdassa säädetään seuraavaa:

”Jokaisella rekisteröidyllä on oikeus tehokkaisiin oikeussuojakeinoihin, jos hän katsoo, että hänen tähän asetukseen perustuvia oikeuksiaan on loukattu sen takia, ettei hänen henkilötietojensa käsittelyssä ole noudatettu tätä asetusta, sanotun kuitenkaan rajoittamatta käytettävissä olevien hallinnollisten muutoksenhakukeinojen tai muiden kuin oikeudellisten oikeussuojakeinojen käyttöä, mukaan lukien 77 artiklaan perustuva oikeus tehdä valitus valvontaviranomaiselle.”

29 Asetuksen 2016/679 94 artiklassa säädetään seuraavaa:

”1. Kumotaan direktiivi [95/46] 25 päivästä toukokuuta 2018.

2. Viittauksia kumottuun direktiiviin pidetään viittauksina tähän asetukseen. Viittauksia direktiivin [95/46] 29 artiklalla perustettuun tietosuojatyöryhmään pidetään viittauksina tällä asetuksella perustettuun Euroopan tietosuojaneuvostoon.”

30 Kyseisen asetuksen 95 artiklassa säädetään seuraavaa:

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

Ranskan oikeus

Sisäisestä turvallisuudesta annettu koodeksi

31 Sisäisestä turvallisuudesta annetun koodeksin (code de la sécurité intérieure, jäljempänä CSI) lainsäädäntöosan VIII osassa olevissa L. 801-1–L. 898-1 §:ssä säädetään tiedustelua koskevista säännöistä.

32 CSI:n L. 811-3 §:ssä säädetään seuraavaa:

”Erikoistuneet tiedusteluyksiköt voivat pelkästään tehtäviensä hoitamiseksi käyttää tämän osan V osastossa mainittuja menetelmiä kerätäkseen tietoja, jotka koskevat kansakunnan seuraavien perustavanlaatuisten etujen puolustamista ja edistämistä:

1° kansallinen riippumattomuus, alueellinen koskemattomuus ja maanpuolustus

2° ulkopolitiikan tärkeimmät edut, Ranskan eurooppalaisten ja kansainvälisten sitoumusten täyttäminen ja kaiken ulkomaisen puuttumisen estäminen

3° Ranskan tärkeimmät taloudelliset, teolliset ja tieteelliset edut

4° terrorismin torjunta

5° seuraavien toimien estäminen:
   a) toimielinten tasavaltaiseen valtiomuotoon kohdistuvat loukkaukset
   b) toimet, joilla pyritään säilyttämään tai perustamaan uudelleen L. 212-1 §:n nojalla hajotetut ryhmittymät
   c) kollektiivinen väkivalta, joka on omiaan vahingoittamaan vakavasti yleistä rauhaa

6° järjestäytyneen rikollisuuden torjunta

7° joukkotuhoaseiden leviämisen estäminen.”

33 CSI:n L. 811-4 §:ssä säädetään seuraavaa:

”Commission nationale de contrôle des techniques de renseignementin [(kansallinen tiedustelumenetelmien valvontakomitea, Ranska)] lausunnon perusteella Conseil d’État’n [(ylin hallintotuomioistuin, Ranska)] kuulemisen jälkeen annetulla asetuksella nimetään puolustus-, sisä- ja oikeusministerien sekä taloudesta, talousarviosta tai tulliasioista vastaavien ministerien alaisuuteen kuuluvat muut yksiköt, joille voidaan erikoistuneiden tiedusteluyksikköjen lisäksi antaa lupa käyttää tämän osan V osastossa mainittuja menetelmiä samassa osassa säädetyin edellytyksin. Siinä täsmennetään kunkin yksikön osalta L. 811-3 §:ssä mainitut tarkoitukset ja menetelmät, joihin lupa voidaan antaa.”

34 CSI:n L. 821-1 §:n 1 momentissa täsmennetään seuraavaa:

”Tämän osan V osaston I–IV luvussa mainittujen tiedonhankintamenetelmien soveltaminen kansallisella alueella edellyttää pääministerin ennakkolupaa, joka myönnetään kansallisen tiedustelumenetelmien valvontakomitean annettua lausuntonsa.”

35 CSI:n L. 821-2 §:ssä säädetään seuraavaa:

”L. 821-1 §:ssä mainittu lupa myönnetään puolustusministerin, sisäministerin, oikeusministerin taikka taloudesta, talousarviosta tai tulliasioista vastaavien ministerien kirjallisesta ja perustellusta pyynnöstä. Kukin ministeri voi delegoida kyseisen toimivallan erikseen vain työntekijöille, joita sitoo suoraan kansallista puolustusta koskeva vaitiolovelvollisuus.

Pyynnössä on mainittava

1° sovellettava menetelmä tai sovellettavat menetelmät

2° yksikkö, jota varten pyyntö on esitetty

3° tarkoitus tai tarkoitukset

4° toimenpiteiden perustelu tai perustelut

5° luvan voimassaoloaika

6° kyseessä oleva henkilö tai kyseessä olevat henkilöt, kyseessä oleva paikka tai kyseessä olevat paikat taikka kyseessä olevat ajoneuvot.

Edellä olevaa 6 kohtaa sovellettaessa henkilöt, joiden henkilöllisyys ei ole tiedossa, voidaan nimetä heidän tunnisteidensa tai heidän asemansa perusteella, ja paikat tai ajoneuvot voidaan nimetä pyynnön kohteena oleviin henkilöihin viittaamalla.

– –”

36 CSI:n L. 821-3 §:n 1 momentissa säädetään seuraavaa:

”Pyyntö toimitetaan kansallisen tiedustelumenetelmien valvontakomitean puheenjohtajalle tai, jos tämä ei ole mahdollista, jollekin kyseisen komitean L. 831-1 §:n 2 ja 3 kohdassa mainitulle jäsenelle, joka antaa pääministerille lausunnon 24 tunnin kuluessa. Jos pyynnön käsittelee komitean rajattu kokoonpano tai täysistunto, pääministerille on ilmoitettava asiasta viipymättä, ja lausunto annetaan 72 tunnin kuluessa.”

37 CSI:n L. 821-4 §:ssä säädetään seuraavaa:

”Pääministeri myöntää luvan tämän osan V osaston I–IV luvussa mainittujen menetelmien soveltamiseen enintään neljäksi kuukaudeksi. – – Lupaan on sisällyttävä L. 821–2 §:n 1–6 kohdassa säädetyt perustelut ja maininnat. Lupa voidaan uusia samoin, tässä luvussa säädetyin edellytyksin.

Jos lupa myönnetään kansallisen tiedustelumenetelmien valvontakomitean annettua kielteisen lausunnon, siinä on ilmoitettava syyt, joiden vuoksi kyseistä lausuntoa ei ole noudatettu.

– –”

38 CSI:n kyseisen osaston III luvussa olevassa L. 833-4 §:ssä säädetään seuraavaa:

”Komitea valvoo omasta aloitteestaan tai kun sen käsiteltäväksi on saatettu valitus henkilöltä, joka haluaa tarkastaa, ettei häneen ole sovellettu mitään tiedustelumenetelmää sääntöjenvastaisesti, esiin tuodun menetelmän tai menetelmät tarkastaakseen, onko niitä sovellettu tai sovelletaanko niitä tätä osaa noudattaen. Se ilmoittaa valituksen tekijälle, että tarvittavat tarkastukset on suoritettu, vahvistamatta tai kieltämättä tällaisen menetelmän soveltamista.”

39 CSI:n L. 841-1 §:n 1 ja 2 momentissa säädetään seuraavaa:

”Jollei tämän lain L. 854-9 §:ssä säädetyistä erityissäännöksistä muuta johdu, Conseil d’État on toimivaltainen ratkaisemaan hallintolainkäyttölain [(code de justice administrative)] VII osan VII osaston III bis luvussa säädetyin edellytyksin hakemukset, jotka koskevat tämän osan V osastossa mainittujen tiedustelumenetelmien soveltamista.

Asian voi saattaa sen käsiteltäväksi

1° jokainen henkilö, joka haluaa tarkastaa, ettei häneen ole sovellettu mitään tiedustelumenetelmää sääntöjenvastaisesti ja joka osoittaa, että ensin on sovellettu L. 833-4 §:ssä säädettyä menettelyä,

2° kansallinen tiedustelumenetelmien valvontakomitea L. 833-8 §:ssä säädetyin edellytyksin.”

40 CSI:n lainsäädäntöosan VIII osan V osastossa, joka koskee ”luvanvaraisia tiedonhankintamenetelmiä”, on muun muassa I luku, jonka otsikko on ”Hallinnon oikeus saada yhteystietoja” ja joka sisältää CSI:n L. 851-1–L. 851-7 §:n.

41 CSI:n L. 851-1 §:ssä säädetään seuraavaa:

”Tämän osan II osaston I luvussa säädetyin edellytyksin on mahdollista antaa lupa siihen, että sähköisen viestinnän operaattoreilta ja [CPCE:n] L. 34-1 §:ssä mainituilta henkilöiltä sekä luottamuksesta digitaalisessa taloudessa 21.6.2004 annetun lain nro 2004-575 [loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique] [(JORF 22.6.2004, s. 11168)] 6 §:n I momentin 1 ja 2 kohdassa mainituilta henkilöiltä kerätään niiden verkoissa tai sähköisissä viestintäpalveluissa käsiteltyjä tai säilytettyjä tietoja tai asiakirjoja, mukaan lukien tekniset tiedot, jotka liittyvät sähköisten viestintäpalvelujen tilaaja- tai yhteysnumeroiden tunnistamiseen, nimetyn henkilön tilaaja- tai yhteysnumeroiden kartoittamiseen, käytettyjen päätelaitteiden paikantamiseen sekä jonkun tilaajan viestintään eli valittujen numeroiden ja soittajan numeroiden luetteloon sekä viestinnän kestoon ja päivämäärään.

Poiketen siitä, mitä L. 821-2 §:ssä säädetään, L. 811-2 ja L. 811-4 §:ssä mainitut tiedusteluyksikköjen erikseen nimetyt ja valtuutetut työntekijät toimittavat kirjalliset ja perustellut pyynnöt, jotka koskevat teknisiä tietoja, jotka liittyvät sähköisten viestintäpalvelujen tilaaja- tai yhteysnumeroiden tunnistamiseen taikka nimetyn henkilön kaikkien tilaaja- tai yhteysnumeroiden kartoittamiseen, suoraan kansalliselle tiedustelumenetelmien valvontakomitealle. Komitea antaa lausuntonsa L. 821-3 §:ssä säädetyin edellytyksin.

Pääministerin yksikön tehtävänä on kerätä tiedot tai asiakirjat tämän pykälän 1 momentissa mainituilta operaattoreilta ja henkilöiltä. Kansallinen tiedustelumenetelmien valvontakomitea voi jatkuvasti, täysimääräisesti, suoraan ja välittömästi tutustua kerättyihin tietoihin tai asiakirjoihin.

Tämän pykälän soveltamista koskevat yksityiskohtaiset säännöt vahvistetaan Commission nationale de l’informatique et des libertés’n ([kansallinen tietojenkäsittelyn ja vapauksien komitea, Ranska)] ja kansallisen tiedustelumenetelmien valvontakomitean lausunnon perusteella Conseil d’État’n kuulemisen jälkeen annetulla asetuksella.”

42 CSI:n L. 851-2 §:ssä säädetään seuraavaa:

”I. – Tämän osan II osaston I luvussa säädetyin edellytyksin ja ainoastaan terrorismin torjumiseksi voidaan erikseen antaa lupa L. 851-1 §:ssä mainittujen operaattorien ja henkilöiden verkoissa reaaliajassa tapahtuvaan samassa L. 851-1 §:ssä mainittujen sellaisten tietojen tai asiakirjojen keräämiseen, jotka koskevat etukäteen tunnistettua henkilöä, joka saattaa liittyä tiettyyn uhkaan. Jos on

vakavaa aihetta epäillä, että yksi tai useampi luvassa kyseessä olevan henkilön lähipiiriin kuuluva henkilö voi antaa tietoja luvan perusteena olevan tarkoituksen osalta, lupa voidaan myöntää erikseen myös kaikkien näiden henkilöiden osalta.

I bis. Pääministeri päättää tämän pykälän nojalla myönnettyjen samanaikaisesti voimassa olevien lupien enimmäismäärästä saatuaan kansallisen tiedustelumenetelmien valvontakomitean lausunnon. Päätös kyseisen kiintiön vahvistamisesta ja sen jakamisesta L. 821-2 §:n 1 momentissa mainittujen ministerien kesken sekä myönnettyjen kuuntelulupien määrä saatetaan komitean tietoon.

_ _”

43 CSI:n L. 851-3 §:ssä säädetään seuraavaa:

”I. – Tämän osan II osaston I luvussa säädetyin edellytyksin ja ainoastaan terrorismin torjumiseksi L. 851-1 §:ssä mainitut operaattorit ja henkilöt voidaan velvoittaa toteuttamaan verkoissaan automaattista käsittelyä, jolla pyritään luvassa määriteltyjen parametrien perusteella havaitsemaan yhteyksiä, jotka voivat paljastaa terroriuhan.

Tässä automaattisessa käsittelyssä käytetään yksinomaan L. 851-1 §:ssä mainittuja tietoja tai asiakirjoja eikä siinä kerätä muita kuin kyseisen käsittelyn suunnitteluparametrejä vastaavia tietoja eikä sen perusteella voida tunnistaa henkilöitä, joita tiedot tai asiakirjat koskevat.

Pääministerin luvassa täsmennetään suhteellisuusperiaatteen mukaisesti tämän käsittelyn toteuttamisen tekninen ulottuvuus.

II. – Kansallinen tiedustelumenetelmien valvontakomitea antaa lausunnon automaattista käsittelyä koskevasta lupapyynnöstä ja huomioon otettavista havaintaparametreistä. Se voi jatkuvasti, täysimääräisesti, suoraan ja välittömästi tutustua tähän käsittelyyn ja kerättyihin tietoihin. Sille ilmoitetaan kaikista käsittelyyn ja parametreihin tehtävistä muutoksista, ja se voi antaa suosituksia.

Tämän pykälän I momentissa säädettyä automaattisen käsittelyn toteuttamista koskeva ensimmäinen lupa myönnetään kahdeksi kuukaudeksi. Lupa voidaan uusia tämän osan II osaston I luvussa säädetyin voimassaoloaikaa koskevin edellytyksin. Uudistamishakemuksessa on oltava ote automaattisella käsittelyllä havaittujen tunnisteiden määrästä sekä analyysi näiden havaintojen merkityksellisyydestä.

III. – L. 871-6 §:ssä säädettyjä edellytyksiä sovelletaan niihin konkreettisiin toimiin, joita L. 851-1 §:ssä mainitut operaattorit ja henkilöt suorittavat tällaisen käsittelyn toteuttamista varten.

IV. – Jos tämän pykälän I momentissa mainitussa käsittelyssä tulee ilmi tietoja, jotka voivat osoittaa terroriuhan olemassaolon, pääministeri tai joku hänen valtuuttamistaan henkilöistä voi antaa luvan asianomaisen henkilön tai asianomaisten henkilöiden tunnistamiseen ja häneen tai heihin liittyvien tietojen keräämiseen sen jälkeen, kun kansallinen tiedustelumenetelmien valvontakomitea on antanut lausuntonsa tämän osan II osaston I luvussa säädetyin edellytyksin. Näitä tietoja on hyödynnettävä 60 päivän kuluessa tästä keräämisestä, ja ne hävitetään tämän määräajan päättyessä, jollei ole olemassa painavia seikkoja, jotka vahvistavat, että yhteen tai useampaan asianomaiseen henkilöön liittyy terroriuhka.

_ _”

44 CSI:n 851-4 §:ssä säädetään seuraavaa:

”Tämän osan II osaston I luvussa säädetyin edellytyksin L. 851-1 §:ssä mainittujen käytettyjen päätelaitteiden sijaintia koskevat tekniset tiedot voidaan kerätä verkosta pyydettäessä, ja operaattorit toimittavat ne reaaliajassa pääministerin yksikölle.”

45 CSI:n asetusosassa olevassa CSI:n R. 851-5 §:ssä säädetään seuraavaa:

”I. – L. 851-1 §:ssä mainittuja tietoja tai asiakirjoja ovat yhteydenpidon tai haettujen tietojen sisältöä lukuun ottamatta:

1° [CPCE:n] R. 10-13 §:ssä ja R. 10-14 §:ssä sekä asetuksen [nro 2011-219] 1 §:ssä luetellut tiedot ja asiakirjat

2° muut kuin 1 kohdassa mainitut tekniset tiedot, jotka

a) mahdollistavat päätelaitteiden paikantamisen

b) koskevat päätelaitteilta tapahtuvaa pääsyä verkkoihin tai yleisölle tarkoitettuihin verkkoviestintäpalveluihin

c) koskevat sähköisen viestinnän välittämistä verkoissa

d) koskevat käyttäjän, yhteyden, verkon tai yleisölle tarkoitetun verkkoviestintäpalvelun tunnistamista ja varmentamista

e) koskevat päätelaitteiden ominaisuuksia ja niiden ohjelmistojen konfigurointitietoja.

II. – L. 851-1 §:n nojalla voidaan kerätä pelkästään I momentin 1 kohdassa mainitut tiedot ja asiakirjat. Tämä kerääminen tapahtuu viiveellä.

I momentin 2 kohdassa luetellut tiedot voidaan kerätä ainoastaan L. 851-2 §:n ja L. 851-3 §:n nojalla näissä pykälissä säädetyin edellytyksin ja rajoituksin ja jollei R. 851-9 §:n soveltamisesta muuta johdu.”

CPCE

46 CPCE:n L. 34-1 §:ssä säädetään seuraavaa:

”I. – Tätä pykälää sovelletaan henkilötietojen käsittelyyn, jota suoritetaan tarjottaessa sähköisiä viestintäpalveluja yleisölle; sitä sovelletaan erityisesti verkkoihin, joissa voidaan käyttää tiedonkeruu- ja tunnistuslaitteita.

II. – Sähköisen viestinnän operaattorien ja erityisesti henkilöiden, joiden toimintaan kuuluu tarjota yhteys yleisölle tarkoitettuihin verkkoviestintäpalveluihin, on poistettava tai tehtävä nimettömiksi kaikki liikennetiedot, jollei III, IV, V ja VI momentin säännöksistä muuta johdu.

Henkilöiden, jotka tarjoavat yleisölle tarkoitettuja sähköisiä viestintäpalveluja, on edellä olevan kohdan säännöksiä noudattaen otettava käyttöön sisäisiä menettelyjä, joilla voidaan vastata toimivaltaisten viranomaisten pyyntöihin.

Henkilöiden, joiden pää- tai sivutoimialana on tarjota, myös ilmaiseksi, yleisölle liittymää, joka mahdollistaa verkkoviestinnän internetyhteyden kautta, on noudatettava sähköisen viestinnän operaattoreihin tämän pykälän nojalla sovellettavia säännöksiä.

III. – Toimenpiteitä, joiden tarkoituksena on poistaa tai tehdä nimettömiksi tietyt teknisten tietojen ryhmät, voidaan lykätä enintään vuoden ajaksi, jos se on tarpeen rikosten tai henkisestä omaisuudesta annetun koodeksin [(code de la propriété intellectuelle)] L. 336-3 §:ssä määritellyn velvoitteen laiminlyönnin tutkintaan, toteamiseen ja syytteeseenpanoon liittyvistä syistä taikka siinä tarkoituksessa, että estetään rikoskoodeksin [(code pénal)] 323-1–323-3-1 §:ssä tarkoitetut rangaistaviksi säädetyt

hyökkäykset tietojen automaattisiin käsittelyjärjestelmiin, ja yksinomaan sen mahdollistamiseksi, että nämä tiedot asetetaan tarvittaessa lainkäyttöviranomaisen tai henkisestä omaisuudesta annetun lain L. 331-12 §:ssä mainitun korkean viranomaisen taikka maanpuolustuskoodeksin [(code de la défense)] L. 2321-1 §:ssä mainitun tietojärjestelmien turvallisuudesta vastaavan kansallisen viranomaisen saataville. Nämä tietoryhmät ja tietojen säilyttämisen kesto määritetään kansallinen tietojenkäsittelyn ja vapauksien komitean lausunnon perusteella Conseil d'État'n kuulemisen jälkeen annetulla asetuksella VI momentissa vahvistetuin rajoituksin operaattoreiden toiminnan ja viestinnän luonteen mukaan sekä mahdollisesti niiden yksityiskohtaisten sääntöjen mukaan, jotka koskevat hyvityksiä yksilöitävissä olevista erityisistä lisäkustannuksista, joita operaattoreille syntyy niiden tällä perusteella valtion pyynnöstä suorittamista palveluista.

– –

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

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

Tietojen säilytyksessä ja käsittelyssä on noudatettava tietojenkäsittelystä, tiedostoista ja vapauksista 6.1.1978 annetun lain nro 78-17 [(loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)] säännöksiä.

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

47 CPCE:n R. 10-13 §:ssä säädetään seuraavaa:

"I. – L. 34-1 §:n III momentin mukaisesti sähköisen viestinnän operaattorien on säilytettävä rikosten tutkintaa, toteamista ja syytteeseenpanoa varten seuraavat tiedot:

a) tiedot, joiden perusteella käyttäjä voidaan tunnistaa

b) sähköisessä viestinnässä käytettyjä päätelaitteita koskevat tiedot

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

d) tilattuja tai käytettyjä lisäpalveluja ja niiden tarjoajia koskevat tiedot

e) tiedot, joiden perusteella viestinnän vastaanottaja tai vastaanottajat voidaan tunnistaa.

II. – Puhelintoiminnan osalta operaattori säilyttää II momentissa mainitut tiedot ja lisäksi tiedot, joiden perusteella viestinnän alkuperä voidaan määrittää ja viestintä voidaan paikantaa.

III. – Tässä pykälässä mainittuja tietoja säilytetään vuoden ajan niiden tallennuspäivästä.

IV. – Yksilöitävissä olevista erityisistä lisäkustannuksista, joita operaattoreille aiheutuu niiden lainkäyttöviranomaisten pyynnöstä suorittamasta tässä pykälässä mainittuihin ryhmiin kuuluvien tietojen toimittamisesta, hyvitetään rikosprosessilain [(code de procédure pénale)] R. 213-1 §:ssä säädettyjen yksityiskohtaisten sääntöjen mukaisesti."

48 CPCE:n R. 10-14 §:ssä säädetään seuraavaa:

”I. – L. 34-1 §:n IV momentin mukaan sähköisen viestinnän operaattoreilla on oikeus säilyttää laskutusta ja maksamista varten tekniset tiedot, joiden perusteella käyttäjä voidaan tunnistaa, sekä R. 10-13 §:n I momentin b, c ja d kohdassa mainitut tiedot.

II. – Puhelintoiminnan osalta operaattorit voivat säilyttää I momentissa mainittujen tietojen lisäksi viestinnän paikantamista ja viestinnän vastaanottajaa tai vastaanottajia koskevat tekniset tiedot sekä laskutuksen laatimisen mahdollistavat tiedot.

III. – Tämän pykälän I ja II momentissa mainitut tiedot voidaan säilyttää ainoastaan, jos ne ovat tarpeen suoritettujen palvelujen laskuttamiseksi ja maksamiseksi. Niitä ei saa säilyttää pidempään kuin on täysin välttämätöntä tämän tavoitteen saavuttamiseksi, kuitenkin siten, ettei niitä säilytetä yli yhden vuoden ajan.

IV. – Operaattorit voivat säilyttää verkkojen ja laitteiden turvallisuuden vuoksi enintään kolmen kuukauden ajan

a) tiedot, joiden perusteella viestinnän alkuperä voidaan tunnistaa

b) kunkin viestin tekniset ominaisuudet sekä päivämäärä, kellonaika ja kesto

c) tekniset tiedot, joiden perusteella viestinnän vastaanottaja tai vastaanottajat voidaan tunnistaa

d) tilattuja tai käytettyjä lisäpalveluja ja niiden tarjoajia koskevat tiedot.”

Luottamuksesta digitaalisessa taloudessa 21.6.2004 annettu laki nro 2004-575

49 Luottamuksesta digitaalisessa taloudessa 21.6.2004 annetun lain nro 2004-575 (loi n° 2004-575, du 21 juin 2004, pour la confiance dans l’économie numérique) (JORF 22.6.2004, s. 11168; jäljempänä LCEN) 6 §:ssä säädetään seuraavaa:

”I. – 1. Henkilöiden, joiden toimintaan kuuluu tarjota yhteys yleisölle tarkoitettuihin verkkoviestintäpalveluihin, on ilmoitettava tilaajilleen teknisistä keinoista, joilla voidaan rajoittaa tiettyjen palvelujen saatavuutta tai valita niitä, ja tarjottava heille ainakin yhtä näistä keinoista.

– –

2. Luonnolliset henkilöt tai oikeushenkilöt, jotka tallentavat, myös ilmaiseksi, yleisön saataviin saattamiseksi verkkoviestintäpalvelujen kautta kaikenlaiset näiden palvelujen vastaanottajien toimittamat merkit, kirjoitukset, kuvat, äänet tai viestit, eivät voi joutua siviilioikeudelliseen vastuuseen kyseisten palvelujen vastaanottajan toiminnan tai tämän pyynnöstä tallennettujen tietojen perusteella, jos he eivät tosiasiallisesti olleet tietoisia niiden laittomuudesta tai sellaisista tosiseikoista ja olosuhteista, joista tällainen laittomuus ilmenee, tai jos he ovat heti silloin, kun he ovat saaneet asiasta tiedon, ryhtyneet viipymättä toimenpiteisiin poistaakseen kyseiset tiedot tai tehdäkseen niiden saamisen mahdottomaksi.

– –

II. – I momentin 1 ja 2 kohdassa mainittujen henkilöiden on pidettävä hallussaan ja säilytettävä tiedot, joiden perusteella voidaan tunnistaa kuka tahansa henkilö, joka on ollut omalta osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä.

Kyseisten henkilöiden on tarjottava yleisölle tarkoitettua verkkoviestintäpalvelua editoiville henkilöille tekniset välineet, joiden avulla nämä voivat täyttää III momentissa säädetyt tunnistamisedellytykset.

Lainkäyttöviranomainen voi vaatia I momentin 1 ja 2 kohdassa mainittuja palveluntarjoajia toimittamaan 1 kohdassa mainitut tiedot.

Näiden tietojen käsittelyyn sovelletaan rikoslain 226-17 §:n, 226-21 §:n ja 226-22 §:n säännöksiä.

Edellä 1 kohdassa mainitut tiedot määritellään ja niiden säilytysaika ja säilyttämistavat vahvistetaan tietojenkäsittelyn ja vapauksien kansallisen komitean lausunnon perusteella Conseil d'État'n kuulemisen jälkeen annetulla asetuksella.

_ _"

Asetus nro 2011-219

50 Asetuksen nro 2011-219, joka on annettu LCEN:n 6 §:n II momentin viimeisen kohdan nojalla, I luku sisältää kyseisen asetuksen 1–4 §:n.

51 Asetuksen nro 2011-219 1 §:ssä säädetään seuraavaa:

"[LCEN:n] 6 §:n II momentissa mainitut tiedot, jotka henkilöiden on säilytettävä tämän säännöksen nojalla, ovat seuraavat:

1° saman pykälän I momentin 1 kohdassa mainittujen henkilöiden ja niiden tilaajien kunkin yhteyden osalta

a) yhteyden tunnistenumero

b) näiden henkilöiden tilaajalle osoittama tunnistenumero

c) yhteyden muodostukseen käytettävän päätelaitteen tunnistenumero, jos he voivat saada sen

d) yhteyden alkamisen ja päättymisen päivämäärä ja kellonaika

e) tilaajayhteyden ominaisuudet;

2° saman pykälän I momentin 2 kohdassa mainittujen henkilöiden ja kunkin luomisoperaation osalta

a) viestinnän taustalla olevan yhteyden tunnistenumero

b) tietojärjestelmän avulla annettu tunnistenumero sisällölle eli operaation kohteelle

c) ne protokollatyypit, joita käytetään palveluun liittymisessä ja sisältöjen siirtämisessä

d) operaation luonne

e) operaation päivämäärä ja kellonaika;

f) operaation suorittajan käyttämä tunnistenumero silloin, kun se on antanut tämän.

3° Saman pykälän I momentin 1 ja 2 kohdassa mainittujen henkilöiden osalta tiedot, jotka käyttäjä antaa sopimusta tehtäessä tai tiliä perustettaessa:

a) kyseisen yhteyden tunnistenumero tilin perustamisajankohtana

b) sukunimi ja etunimi tai toiminimi

c) niihin liittyvät postiosoitteet

d) käytetyt pseudonyymit

e) niihin liittyvät sähköpostiosoitteet tai tilit

f) puhelinnumerot

g) salasana sekä tiedot, joiden perusteella se voidaan todentaa tai sitä voidaan muuttaa, sellaisina kuin ne ovat viimeisimmässä muodossaan

4° Saman pykälän I momentin 1 ja 2 kohdassa mainittujen henkilöiden osalta silloin, kun sopimus tai tili on maksullinen, kunkin maksutapahtuman osalta seuraavat tiedot maksusta

a) käytetty maksutyyppi

b) maksun viitenumero

c) määrä

d) maksutapahtuman päivämäärä ja kellonaika.

Edellä 3 ja 4 kohdassa mainitut tiedot on säilytettävä vain siltä osin kuin henkilöt tavallisesti keräävät ne.”

52 Kyseisen asetuksen 2 §:ssä säädetään seuraavaa:

”Sisällön luomiseen myötävaikuttaminen kattaa toimet, jotka koskevat

a) sisältöjen alkuperäistä luomista

b) sisältöjen ja sisältöihin liittyvien tietojen muuttamista

c) sisältöjen poistamista.”

53 Mainitun asetuksen 3 §:ssä säädetään seuraavaa:

”Edellä 1 pykälässä mainittujen tietojen säilytysaika on yksi vuosi

a) siltä osin kuin on kyse 1 ja 2 kohdassa mainituista tiedoista sisältöjen luomispäivästä alkaen kunkin 2 §:ssä määritellyn, sisällön luomiseen myötävaikuttaneen toimen osalta

b) siltä osin kuin on kyse 3 kohdassa mainituista tiedoista sopimuksen irtisanomispäivästä tai tilin sulkemispäivästä alkaen

c) siltä osin kuin on kyse 4 kohdassa mainituista tiedoista laskun antamispäivästä tai maksutapahtumasta alkaen kunkin laskun tai maksutapahtuman osalta.”

Belgian oikeus

54 Muun muassa sähköisestä viestinnästä 13.6.2005 annettua lakia (loi du 13 juin 2005 relative aux communications électroniques; Moniteur belge 20.6.2005, s. 28070; jäljempänä 13.6.2005 annettu laki), rikostutkintalakia (code d'instruction criminelle) ja tiedustelu- ja turvallisuusyksiköistä 30.11.1998 annettua orgaanista lakia (loi du 30 novembre 1998 organique des services de renseignement et de sécurité; Moniteur belge 18.12.1998; s. 40312, jäljempänä 30.11.1998 annettu laki) on muutettu 29.5.2016 annetulla lailla.

55 Mainitun 13.6.2005 annetun lain, sellaisena kuin se perustuu 29.5.2016 annettuun lakiin, 126 §:ssä säädetään seuraavaa:

"1. Toimijoiden, jotka tarjoavat yleisölle puhelinpalveluja, myös internetin välityksellä, internetyhteyttä tai internetin sähköpostipalveluja, operaattorien, jotka tarjoavat yleisiä sähköisiä viestintäverkkoja, sekä operaattorien, jotka tarjoavat jotain näistä palveluista, on säilytettävä 3 momentissa tarkoitetut tiedot, joita ne tuottavat tai käsittelevät asianomaisten viestintäpalvelujen tarjoamisen yhteydessä, jollei yksityiselämän suojelusta henkilötietojen käsittelyssä 8.12.1992 annetusta laista [loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel] muuta johdu.

Tämä pykälä ei koske viestinnän sisältöä.

Jäljempänä 3 momentissa tarkoitettujen tietojen säilyttämistä koskevaa velvollisuutta sovelletaan myös epäonnistuneisiin puheluihin, jos kyseiset tiedot ovat kyseessä olevien viestintäpalvelujen tarjoamisen yhteydessä

1° yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoavien operaattorien tai yleisen sähköisen viestintäverkon operaattorien tuottamia tai käsittelemiä puhelutietoja taikka

2° näiden tarjoajien kirjaamia internetyhteystietoja.

2. Vain seuraavat viranomaiset voivat saada pelkästä pyynnöstä 1 momentin 1 kohdassa tarkoitetuilta tarjoajilta ja operaattoreilta tämän pykälän nojalla säilytettyjä tietoja jäljempänä mainittuihin tarkoituksiin ja jäljempänä säädetyin edellytyksin:

1° lainkäyttöviranomaiset rikosten tutkintaa, selvittämistä ja syyteharkintaa varten, rikostutkintalain 46bis §:ssä ja 88bis §:ssä tarkoitettujen toimenpiteiden toteuttamista varten ja kyseisissä pykälissä vahvistetuin edellytyksin

2° tiedustelu- ja turvallisuusyksiköt hoitaakseen tiedustelutehtäviä tiedustelu- ja turvallisuusyksiköistä 30.11.1998 annetun orgaanisen lain 16/2 §:ssä, 18/7 §:ssä ja 18/8 §:ssä tarkoitettujen tiedonkeruumenetelmien avulla ja tässä laissa säädetyin edellytyksin

3° kuka tahansa [Institut belge des services postaux et des télécommunicationsin (Belgian posti- ja televiestintälaitos)] poliisivirkamies 114 §:n ja 124 §:n ja tämän pykälän rikkomisten tutkintaa, selvittämistä ja syyteharkintaa varten

4° pelastusyksiköt, jotka tarjoavat ensiapua, jos ne eivät saa hätäpuhelun jälkeen kyseiseltä tarjoajalta tai operaattorilta soittajan tunnistustietoja 107 §:n 2 momentin 3 kohdassa tarkoitetun tietokannan avulla 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 välittömässä vaarassa. Asianomaiselta operaattorilta tai tarjoajalta 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 sovitteluyksikkö, Belgia) sellaisen henkilön tunnistamiseksi, joka on käyttänyt vilpillisesti verkkoa tai sähköistä viestintäpalvelua, eräiden taloudellisten julkisten yritysten uudistamisesta 21.3.1991 annetun lain (loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques) 43bis §:n 3 momentin 7 kohdassa tarkoitetuin edellytyksin. Pyynnön kohteena voivat olla vain tunnistustiedot.

Edellä 1 momentin 1 kohdassa tarkoitettujen tarjoajien ja operaattorien on meneteltävä siten, että 3 momentissa tarkoitetut tiedot ovat rajattomasti saatavilla Belgiasta ja että nämä tiedot ja kaikki muut näihin tietoihin liittyvät tarvittavat seikat voidaan välittää viipymättä ja yksinomaan tässä momentissa tarkoitetuille viranomaisille.

Edellä 1 momentin 1 kohdassa tarkoitetut tarjoajat ja operaattorit eivät voi käyttää 3 momentin nojalla säilytettyjä tietoja muihin tarkoituksiin, jollei muista lainsäännöksistä muuta johdu.

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

Tiedot, jotka liittyvät päätelaitteelta tapahtuvaan verkkoyhteyteen tai palveluun liittymiseen ja kyseisen laitteen sijaintiin, mukaan lukien verkon liityntäpiste, on säilytettävä 12 kuukauden ajan viestintäpäivästä.

Viestintätiedot, sisältöä lukuun ottamatta, mukaan lukien viestinnän alkuperä ja määränpää, on säilytettävä 12 kuukauden ajan viestintäpäivästä.

Kuningas vahvistaa ministerineuvostossa tehdyllä päätöksellä oikeusministerin ja [sähköistä viestintää koskevien kysymysten osalta toimivaltaisen] ministerin ehdotuksesta ja saatuaan Commission de la protection de la vie privéen [(yksityisyyden suojasta vastaava komitea, Belgia)] ja laitoksen lausunnon tiedot, jotka on säilytettävä 1–3 kohdassa tarkoitettujen ryhmien mukaisesti, sekä vaatimukset, jotka näiden tietojen on täytettävä.

_ _”

Pääasiat ja ennakkoratkaisukysymykset

Asia C-511/18

56 Quadrature du Net, French Data Network ja Fédération des fournisseurs d’accès à Internet associatifs sekä Igwan.net nostivat 30.11.2015 ja 16.3.2016 toimitetuilla kannekirjelmillä, jotka on yhdistetty pääasiassa, Conseil d’État’ssa kanteet, joissa vaaditaan kumoamaan asetukset nro 2015-1185, 2015-1211, 2015-1639 ja 2016-67 muun muassa sillä perusteella, että ne ovat vastoin Ranskan perustuslakia, ihmisoikeuksien ja perusvapauksien suojaamiseksi tehtyä eurooppalaista yleissopimusta (jäljempänä Euroopan ihmisoikeussopimus) sekä direktiivejä 2000/31 ja 2002/58, luettuina perusoikeuskirjan 7, 8 ja 47 artiklan valossa.

57 Ennakkoratkaisua pyytänyt tuomioistuin huomauttaa erityisesti direktiivin 2000/31 rikkomista koskevista kanneperusteista, että CSI:n L. 851-3 §:n säännösten mukaan sähköisen viestinnän operaattorit ja teknisten palvelujen tarjoajat velvoitetaan ”toteuttamaan verkoissaan automaattista käsittelyä, jolla pyritään luvassa määriteltyjen parametrien perusteella havaitsemaan yhteyksiä, jotka voivat paljastaa terroriuhan”. Tällä menetelmällä pyritään keräämään yksinomaan rajoitetun ajan kaikista näiden operaattorien ja palveluntarjoajien käsittelemistä yhteystiedoista sellaiset yhteystiedot, jotka saattavat liittyä tällaiseen vakavaan rikokseen. Mainituilla säännöksillä, joissa ei aseteta aktiivista valvontaa koskevaa yleistä velvollisuutta, ei näin ollen rikota direktiivin 2000/31 15 artiklaa.

58 Ennakkoratkaisua pyytänyt tuomioistuin katsoo direktiivin 2002/58 rikkomista koskevien kanneperusteiden osalta, että kyseisen direktiivin säännöksistä ja 21.12.2016 annetusta tuomiosta Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, EU:C:2016:970; jäljempänä tuomio Tele2) ilmenee muun muassa, että kansalliset säännökset, joissa sähköisten viestintäpalvelujen tarjoajille asetetaan velvollisuuksia, kuten velvollisuus säilyttää käyttäjiensä ja tilaajiensa liikenne- ja paikkatietoja yleisesti ja erotuksetta, mainitun direktiivin 15 artiklan 1 kohdassa mainittuihin tarkoituksiin, joihin kuuluu kansallisen turvallisuuden, puolustuksen ja yleisen turvallisuuden takaaminen, kuuluvat saman direktiivin soveltamisalaan siltä osin kuin näillä säännöstöillä säännellään mainittujen palveluntarjoajien toimintaa. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan sama koskee säännöstöjä, joilla säännellään kansallisten viranomaisten oikeutta saada tietoja ja käyttää niitä.

59 Ennakkoratkaisua pyytänyt tuomioistuin päättelee tästä, että direktiivin 2002/58 soveltamisalaan kuuluvat sekä CSI:n L. 851-1 §:ään perustuva säilyttämisvelvollisuus että mainitun lain L. 851-1 §:ssä, L. 851-2 §:ssä ja L. 851-4 §:ssä säädetty hallinnon oikeus saada mainitut tiedot myös reaaliajassa. Sama pätee kyseisen tuomioistuimen mukaan saman lain L. 851-3 §:n säännöksiin, joilla asianomaiset operaattorit velvoitetaan toteuttamaan verkoissaan automaattista tietojenkäsittelyä, jolla pyritään havaitsemaan yhteyksiä, jotka voivat paljastaa terroriuhan, vaikka siinä ei asetetakaan niille yleistä säilyttämisvelvollisuutta.

60 Kyseinen tuomioistuin katsoo sitä vastoin, että direktiivin 2002/58 soveltamisalaan eivät kuulu ne kumoamisvaatimuksissa mainitut CSI:n säännökset, jotka koskevat tiedonhankintamenetelmiä, jotka valtio on ottanut käyttöön suoraan ilman, että se olisi säännellyt sähköisten viestintäpalvelujen tarjoajien toimintaa asettamalla niille erityisiä velvollisuuksia. Ei siis voida katsoa, että kyseisillä säännöksillä sovelletaan unionin oikeutta, joten kanneperusteisiin, jotka perustuvat siihen, että ne ovat vastoin direktiiviä 2002/58, ei voida vedota tehokkaasti.

61 Jotta voidaan ratkaista oikeusriidat, jotka koskevat asetusten nro 2015-1185, 2015-1211, 2015-1639 ja 2016–67 lainmukaisuutta direktiiviin 2002/58 nähden, esiin tulee – siltä osin kuin kyseiset asetukset on annettu CSI:n L. 851-1 §–L. 851-4 §:n täytäntöönpanemiseksi – kolme unionin oikeuden tulkintaa koskevaa kysymystä.

62 Ennakkoratkaisua pyytänyt tuomioistuin pohtii direktiivin 2002/58 15 artiklan 1 kohdan tulkinnan osalta ensinnäkin sitä, onko sähköisten viestintäpalvelujen tarjoajille CSI:n L. 851-1 §:n ja R. 851-5 §:n nojalla asetettua yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevaa velvollisuutta pidettävä etenkin niiden takeiden ja tarkastusten kannalta, jotka liittyvät hallinnon oikeuteen saada yhteystietoja ja käyttää niitä, sellaisena puuttumisena, joka on perusteltavissa perusoikeuskirjan 6 artiklassa taatulla oikeudella turvallisuuteen ja kansallista turvallisuutta koskevilla vaatimuksilla, joita koskeva vastuu kuuluu yksinomaan jäsenvaltioille SEU 4 artiklan nojalla.

63 Ennakkoratkaisua pyytänyt tuomioistuin toteaa toiseksi sähköisten viestintäpalvelujen tarjoajille mahdollisesti asetettavista muista velvollisuuksista, että CSI:n L. 851-2 §:n säännöksissä sallitaan pelkästään terrorismin torjuntaa varten kyseisen lain L. 851-1 §:ssä säädettyjen tietojen tai asiakirjojen kerääminen samoilta henkilöiltä. Tämä kerääminen, joka koskee vain yhtä tai useampaa sellaista henkilöä, jonka on etukäteen todettu olevan mahdollisesti yhteydessä terroriuhkaan, tapahtuu reaaliajassa. Sama pätee mainitun lain L. 851-4 §:n säännöksiin, joissa sallitaan se, että operaattorit

siirtävät reaaliajassa vain teknisiä tietoja, jotka liittyvät päätelaitteiden paikallistamiseen. Näillä menetelmillä säännellään eri tarkoituksia varten ja erilaisten yksityiskohtaisten sääntöjen mukaan hallinnon oikeutta saada reaaliajassa CPCE:n ja LCEN:n nojalla säilytettyjä tietoja, mutta niissä ei kuitenkaan aseteta kyseisille palveluntarjoajille ylimääräistä säilyttämisvaatimusta suhteessa siihen, mikä on tarpeen niiden palvelujen laskuttamiseksi ja tarjoamiseksi. CSI:n L. 851-3 §:n säännökset, joissa säädetään palveluntarjoajille asetetusta velvollisuudesta toteuttaa verkoissaan yhteyksien automaattinen analysointi, eivät myöskään merkitse yleistä ja erotuksetta tapahtuvaa säilyttämistä.

64 Ennakkoratkaisua pyytänyt tuomioistuin katsoo kuitenkin yhtäältä, että sekä yleisestä ja erotuksetta tapahtuvasta säilyttämisestä että oikeudesta saada yhteystietoja reaaliajassa koituu asiayhteydessä, jolle ovat ominaisia vakavat ja jatkuvat uhat kansalliselle turvallisuudelle erityisesti terrorismin vaaran vuoksi, verratonta käytännön hyötyä. Yleinen ja erotuksetta tapahtuva säilyttäminen näet mahdollistaa sen, että tiedusteluyksiköt voivat saada viestintätietoja ennen kuin tunnistetaan syyt, joiden vuoksi asianomaisen henkilön katsotaan uhkaavan yleistä turvallisuutta, puolustusta tai valtion turvallisuutta. Oikeus saada yhteystietoja reaaliajassa antaa lisäksi mahdollisuuden seurata vahvasti reagoiden sellaisten henkilöiden toimintaan, jotka saattavat muodostaa välittömän uhan yleiselle järjestykselle.

65 Toisaalta CSI:n L. 851-3 §:ssä säädetty menetelmä antaa mahdollisuuden paljastaa tätä tarkoitusta varten täsmällisesti määriteltyjen kriteerien perusteella henkilöt, joiden toiminta saattaa, kun otetaan huomioon heidän viestintämuotonsa, muodostaa terrorismin uhkan.

66 Ennakkoratkaisua pyytänyt tuomioistuin pohtii kolmanneksi siltä osin kuin on kyse toimivaltaisten viranomaisten oikeudesta saada säilytettyjä tietoja, onko direktiiviä 2002/58, luettuna perusoikeuskirjan valossa, tulkittava siten, että yhteystietojen keräämismenettelyjen sääntöjenmukaisuus edellyttää sen mukaan kaikissa tapauksissa sitä, että asianomaisille henkilöille ilmoitetaan asiasta, kun tällainen ilmoittaminen ei voi enää vaarantaa toimivaltaisten viranomaisten tutkimuksia, vai voidaanko tällaisia menettelyjä pitää sääntöjenmukaisina, kun otetaan huomioon kaikki muut kansallisessa oikeudessa säädetyt menettelylliset takeet, kun niillä varmistetaan oikeussuojakeinojen tehokkuus.

67 Ennakkoratkaisua pyytänyt tuomioistuin täsmentää näistä muista menettelyllisistä takeista muun muassa, että jokainen henkilö, joka haluaa tarkastaa, ettei häneen sovelleta sääntöjenvastaisesti mitään tiedustelumenetelmää, voi saattaa asian sellaisen Conseil d'État'n erikoiskokoonpanon käsiteltäväksi, jonka on tarkastettava sille toimitettujen tietojen perusteella ilman kontradiktorista asian käsittelyä, onko hakijaan sovellettu jotain menetelmää, ja onko kyseistä menetelmää sovellettu CSI:n VIII osan mukaisesti. Kyseiselle kokoonpanolle annetulla valtuudella tutkia hakemukset taataan sen harjoittaman tuomioistuinvalvonnan tehokkuus. Sillä on siis toimivalta tutkia hakemukset, tuoda viran puolesta esiin kaikki sen toteamat lainvastaisuudet ja määrätä hallinto toteuttamaan kaikki hyödylliset toimenpiteet todettujen lainvastaisuuksien korjaamiseksi. Kansallisen tiedustelumenetelmien valvontakomitean tehtävänä on lisäksi tarkastaa, että tiedonhankintamenetelmiä sovelletaan Ranskan alueella CSI:stä johtuvien vaatimusten mukaisesti. Näin ollen se, että pääasiassa kyseessä olevissa säännöksissä ei säädetä siitä, että asianomaisille henkilöille on ilmoitettava heihin kohdistetuista valvontatoimenpiteistä, ei sinänsä loukkaa suhteettomasti oikeutta nauttia yksityiselämän kunnioitusta.

68 Tässä tilanteessa Conseil d'État päätti lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

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

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

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

Asia C-512/18

69 French Data Network, Quadrature du Net ja Fédération des fournisseurs d’accès à Internet associatifs nostivat 1.9.2015 toimitetulla kannekirjelmällä Conseil d’État’ssa kumoamiskanteen implisiittisestä hylkäyspäätöksestä, joka perustuu pääministerin vaikenemiseen niiden vaatimuksesta CPCE:n R. 10-13 §:n ja asetuksen nro 2011-219 kumoamiseksi erityisesti sillä perusteella, että kyseiset säädökset ovat vastoin direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan valossa. Privacy International ja Center for Democracy and Technology on hyväksytty väliintulijoiksi pääasian oikeudenkäyntiin.

70 Siltä osin kuin on kyse CPCE:n R. 10-13 §:stä ja siinä säädetystä viestintätietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevasta velvollisuudesta ennakkoratkaisua pyytänyt tuomioistuin, joka kiinnittää huomiota samankaltaisiin näkökohtiin kuin asiassa C-511/18, huomauttaa, että tällainen säilyttäminen mahdollistaa sen, että lainkäyttöviranomainen saa tietoja viestinnästä, jota yksityishenkilö on käynyt ennen kuin hänen on epäilty syyllistyneen rikokseen, joten tästä säilyttämisestä on verratonta hyötyä rikosten tutkintaa, toteamista ja syytteeseenpanoa varten.

71 Ennakkoratkaisua pyytänyt tuomioistuin katsoo asetuksen nro 2011-219 osalta, ettei LCEN:n 6 §:n II momentti, jossa asetetaan velvollisuus pitää hallussa ja säilyttää pelkästään sisällön luomiseen liittyvät tiedot, kuulu direktiivin 2002/58 soveltamisalaan, koska kyseistä direktiiviä sovelletaan sen 3 artiklan 1 kohdan mukaan vain yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa unionissa, vaan mainittu momentti kuuluu direktiivin 2000/31 soveltamisalaan.

72 Kyseinen tuomioistuin katsoo kuitenkin, että direktiivin 2000/31 15 artiklan 1 ja 2 kohdasta ilmenee, ettei kyseisellä direktiivillä oteta käyttöön sisällön luomiseen liittyvien tietojen säilyttämistä koskevaa periaatteellista kieltoa, josta voitaisiin poiketa ainoastaan poikkeuksellisesti. Esiin tulee siis kysymys siitä, onko mainitun direktiivin 12, 14 ja 15 artiklaa, luettuina perusoikeuskirjan 6–8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, tulkittava siten, että jäsenvaltio voi niiden mukaan antaa LCEN:n 6 §:n II momentin kaltaista kansallista lainsäädäntöä, jolla velvoitetaan asianomaiset henkilöt säilyttämään tiedot, joiden perusteella voidaan tunnistaa kuka tahansa henkilö, joka on ollut omalta osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä, jotta lainkäyttöviranomainen voisi tarvittaessa pyytää kyseisten tietojen toimittamista siviili- tai rikosvastuuta koskevien sääntöjen noudattamisen varmistamiseksi.

73 Tässä tilanteessa Conseil d'État päätti lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

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

2) Onko [direktiivin 2000/31] säännöksiä, luettuina yhdessä [perusoikeuskirjan] 6, 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan kanssa, tulkittava siten, että niissä sallitaan se, että valtio antaa kansallista lainsäädäntöä, jolla velvoitetaan henkilöt, joiden toimintaan kuuluu tarjota yhteys yleisölle tarkoitettuihin verkkoviestintäpalveluihin, ja luonnolliset henkilöt tai oikeushenkilöt, jotka tallentavat, myös ilmaiseksi, yleisön saataviin saattamiseksi verkkoviestintäpalvelujen kautta kaikenlaiset näiden palvelujen vastaanottajien toimittamat merkit, kirjoitukset, kuvat, äänet tai viestit, säilyttämään tiedot, joiden perusteella voidaan tunnistaa kuka tahansa henkilö, joka on ollut omalta osaltaan luomassa niiden tarjoamien palvelujen sisältöä tai osaa tästä sisällöstä, jotta lainkäyttöviranomainen voi tarvittaessa pyytää niiden toimittamista siviili- tai rikosvastuuta koskevien sääntöjen noudattamisen varmistamiseksi?”

Asia C-520/18

74 Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL ja UA, Liga voor Mensenrechten ASBL ja Ligue des Droits de l'Homme ASBL sekä VZ, WY ja XX nostivat 10.1., 16.1., 17.1. ja 18.1.2017 toimitetuilla kannekirjelmillä, jotka on yhdistetty pääasiassa, Cour constitutionnellessa (perustuslakituomioistuin, Belgia) kanteet, joissa vaaditaan 29.5.2016 annetun lain kumoamista sillä perusteella, että se on vastoin Belgian perustuslain (Constitution), luettuna yhdessä Euroopan ihmisoikeussopimuksen 5, 6–11, 14, 15, 17 ja 18 artiklan kanssa, 10 §:ää ja 11 §:ää, perusoikeuskirjan 7, 8, 11 ja 47 artiklaa sekä 52 artiklan 1 kohtaa, kansalaisoikeuksia ja poliittisia oikeuksia koskevaa kansainvälistä yleissopimusta, joka on hyväksytty Yhdistyneiden Kansakuntien yleiskokouksessa 16.12.1966 ja joka on tullut voimaan 23.3.1976, oikeusvarmuuteen, oikeasuhteisuuteen ja tietoja koskevaan itsemääräämisoikeuteen liittyviä yleisiä periaatteita sekä SEU 5 artiklan 4 kohtaa.

75 Pääasian kantajat vetoavat kanteidensa tueksi lähinnä siihen, että 29.5.2016 annettu laki on lainvastainen muun muassa sen vuoksi, että sillä ylitetään täysin välttämättömän rajat eikä siinä säädetä riittävistä suojan takeista. Ne väittävät erityisesti, että kyseisen lain säännökset, jotka koskevat tietojen säilyttämistä, ja säännökset, joilla säännellään viranomaisten oikeutta saada säilytettyjä tietoja, eivät täytä 8.4.2014 annetusta tuomiosta Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238; jäljempänä tuomio Digital Rights) eivätkä 21.12.2016 annetusta tuomiosta Tele2 (C-203/15 ja C-698/15, EU:C:2016:970) johtuvia vaatimuksia. Näihin säännöksiin sisältyy näet riski siitä, että toimivaltaiset viranomaiset laativat henkilöprofiileja, joihin liittyy mahdollisia väärinkäytöksiä, eikä niissä myöskään säädetä säilytettyjen tietojen turvaamisen ja suojan asianmukaisesta tasosta. Kyseinen laki kattaa myös salassapitovelvollisuuden alaiset henkilöt sekä henkilöt, joita sitoo velvollisuus säilyttää luottamuksellisuus, ja se koskee arkaluonteisia henkilökohtaisia viestintätietoja ilman erityisiä takeita viimeksi mainittujen tietojen suojaamiseksi.

76 Ennakkoratkaisua pyytänyt tuomioistuin toteaa, että tiedot, jotka puhelinpalveluja, myös internetin välityksellä, internetyhteyttä ja internetin sähköpostipalveluja tarjoavien toimijoiden sekä yleisiä sähköisiä viestintäverkkoja tarjoavien operaattorien on säilytettävä 29.5.2016 annetun lain nojalla, ovat samoja kuin tiedot, jotka on lueteltu yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin

2002/58/EY muuttamisesta 29.5.2006 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2006/24/EY (EUVL 2006, L 105, s. 54), eikä kyseisessä direktiivissä tehdä eroa asianomaisten henkilöiden osalta tai tavoitellun päämäärän perusteella. Ennakkoratkaisua pyytänyt tuomioistuin täsmentää viimeksi mainitusta seikasta, että lainsäätäjän kyseisellä lailla tavoittelemana päämääränä ei ole pelkästään terrorismin ja lapsipornon torjuminen vaan myös se, että säilytettyjä tietoja voidaan käyttää monissa eri tilanteissa rikostutkinnan yhteydessä. Ennakkoratkaisua pyytänyt tuomioistuin toteaa lisäksi, että mainitun lain perusteluista ilmenee, että kansallinen lainsäätäjä on katsonut, että tavoitellun päämäärän valossa oli mahdotonta ottaa käyttöön kohdennettua ja eriytettyä säilyttämisvelvollisuutta, ja päättänyt liittää yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevaan velvollisuuteen tiukat takeet sekä säilytettyjen tietojen että näiden tietojen saamisen osalta, jotta oikeuteen nauttia yksityiselämän kunnioitusta puututtaisiin mahdollisimman vähän.

77 Ennakkoratkaisua pyytänyt tuomioistuin toteaa vielä, että 13.6.2005 annetun lain, sellaisena kuin se perustuu 29.5.2016 annettuun lakiin, 126 §:n 2 momentin 1 ja 2 kohdassa säädetään edellytyksistä, joiden täyttyessä lainkäyttöviranomaiset sekä tiedustelu- ja turvallisuusyksiköt voivat saada säilytettyjä tietoja, joten kyseisen lain lainmukaisuuden tutkimista unionin oikeuden vaatimusten kannalta on lykättävä siihen saakka, kunnes unionin tuomioistuin antaa ratkaisunsa kahdessa siinä vireillä olevassa ennakkoratkaisumenettelyssä, jotka koskevat tällaista tiedonsaantia.

78 Ennakkoratkaisua pyytänyt tuomioistuin huomauttaa lopuksi, että 29.5.2016 annetun lain tarkoituksena on mahdollistaa tehokas rikostutkinta ja tehokkaat seuraamukset alaikäisiin kohdistuvasta seksuaalisesta hyväksikäytöstä sekä tällaisen rikoksen tekijän tunnistaminen myös silloin, kun tekijä käyttää sähköisiä viestintävälineitä. Ennakkoratkaisua pyytäneessä tuomioistuimessa vireillä olevassa oikeudenkäyntimenettelyssä on kiinnitetty tältä osin huomiota Euroopan ihmisoikeussopimuksen 3 ja 8 artiklasta johtuviin toimintavelvollisuuksiin. Nämä velvollisuudet voisivat myös ilmetä perusoikeuskirjan vastaavista määräyksistä, joilla voi olla seurauksia direktiivin 2002/58 15 artiklan 1 kohdan tulkinnalle.

79 Tässä tilanteessa Cour constitutionnelle päätti lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”1) Onko [direktiivin 2002/58] 15 artiklan 1 kohtaa, kun sitä luetaan yhdessä [perusoikeuskirjan] 6 artiklassa taatun turvallisuutta koskevan oikeuden ja [perusoikeuskirjan] 7 ja 8 artiklassa sekä 52 artiklan 1 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] tarkoitetut, niiden kyseisten palvelujen suorittamisen yhteydessä tuottamat tai käsittelemät liikenne- ja paikkatiedot ja jonka tavoitteena ei ole ainoastaan vakavien rikosten tutkinta, selvittäminen ja syyteharkinta vaan myös kansallisen turvallisuuden, maanpuolustuksen ja yleisen turvallisuuden takaaminen, muiden tekojen kuin vakavan rikollisuuden tutkinta, selvittäminen ja syyteharkinta tai sähköisten viestintäjärjestelmien kielletyn käytön estäminen taikka jonkin muun [asetuksen 2016/679] 23 artiklan 1 kohdassa yksilöidyn tavoitteen toteuttaminen ja jota lisäksi koskevat kyseisessä säännöstössä tietojen säilyttämisen ja tietojen saamisen osalta asetetut täsmälliset takeet?

2) Onko [direktiivin 2002/58] 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] tarkoitetut, niiden kyseisten palvelujen suorittamisen yhteydessä tuottamat tai käsittelemät liikenne- ja paikkatiedot, jos kyseisellä säännöstöllä on tarkoitus muun muassa toteuttaa viranomaisille perusoikeuskirjan 4 ja [7] artiklan perusteella kuuluvat toimintavelvollisuudet 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 [29.5.2016 annetun] lain vaikutukset, jotta vältetään oikeudellinen epävarmuus ja mahdollistetaan aikaisemmin kerättyjen ja säilytettyjen tietojen käyttäminen lakisääteisiin tarkoituksiin?”

Asioiden käsittelyn vaiheet unionin tuomioistuimessa

80 Unionin tuomioistuimen presidentin 25.9.2018 tekemällä päätöksellä asiat C-511/18 ja C-512/18 yhdistettiin kirjallista ja suullista käsittelyä sekä tuomion antamista varten. Asia C-520/18 yhdistettiin kyseisiin asioihin tuomion antamista varten unionin tuomioistuimen presidentin 9.7.2020 tekemällä päätöksellä.

Ennakkoratkaisukysymysten tarkastelu

Ensimmäiset kysymykset asioissa C-511/18 ja C-512/18 sekä ensimmäinen ja toinen kysymys asiassa C-520/18

81 Ennakkoratkaisua pyytäneet tuomioistuimet pyrkivät asioissa C-511/18 ja C-512/18 esitetyillä ensimmäisillä kysymyksillä ja asiassa C-520/18 esitetyllä ensimmäisellä ja toisella kysymyksellä, joita on tarkasteltava yhdessä, selvittämään lähinnä, onko direktiivin 2002/58 15 artiklan 1 kohtaa tulkittava siten, että se on esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot yleisesti ja erotuksetta kyseisessä 15 artiklan 1 kohdassa säädettyjä tarkoituksia varten.

Alustavat toteamukset

82 Unionin tuomioistuimen käytössä olevista asiakirja-aineistoista ilmenee, että pääasioissa kyseessä olevat säännöstöt kattavat kaikki sähköiset viestintävälineet ja niiden piiriin kuuluvat kaikki näiden välineiden käyttäjät ilman, että niissä tehtäisiin tältä osin mitään eroa tai poikkeusta. Tiedot, jotka sähköisten viestintäpalvelujen tarjoajien on kyseisten säännöstöjen mukaan säilytettävä, ovat lisäksi erityisesti tietoja, jotka ovat tarpeen viestinnän lähteen ja vastaanottajan jäljittämiseksi, viestinnän päivämäärän, kellonajan, keston ja tyypin määrittämiseksi, käytetyn viestintälaitteen tunnistamiseksi sekä päätelaitteiden ja viestinnän paikallistamiseksi; näihin tietoihin kuuluvat muun muassa käyttäjän nimi ja osoite, puhelun soittajan puhelinnumero ja valittu numero sekä internetpalvelujen osalta IP-osoite. Mainitut tiedot eivät sitä vastoin kata kyseessä olevan viestinnän sisältöä.

83 Niiden tietojen perusteella, joita on pääasioissa kyseessä olevien kansallisten säännöstöjen mukaan säilytettävä vuoden ajan, on siis mahdollista muun muassa selvittää, kenen henkilön kanssa sähköisen viestintävälineen käyttäjä on viestinyt ja millä välineellä tämä viestiminen on tapahtunut, määrittää viestinnän ja internetyhteyksien päivämäärä, kellonaika ja kesto sekä paikka, josta käsin viestintä on tapahtunut, sekä paikantaa päätelaitteet, vaikkei mitään viestintää ole välttämättä välitetty. Ne tarjoavat lisäksi mahdollisuuden määrittää käyttäjän ja tiettyjen henkilöiden välisen viestinnän määrän tiettynä ajanjaksona. Asioissa C-511/18 ja C-512/18 kyseessä olevan kansallisen säännöstön osalta vaikuttaa lopuksi siltä, että koska se kattaa myös tiedot, jotka koskevat sähköisen viestinnän välittämistä verkoissa, sen avulla voidaan myös yksilöidä verkossa haettujen tietojen luonne.

84 Tavoitelluista päämääristä on huomautettava, että asioissa C-511/18 ja C-512/18 kyseessä olevat säännöstöt koskevat muiden tavoitteiden ohella yleisesti rikosten tutkintaa, toteamista ja syyteharkintaa, kansallista riippumattomuutta, alueellista koskemattomuutta ja maanpuolustusta, ulkopolitiikan tärkeimpiä etuja, Ranskan eurooppalaisten ja kansainvälisten sitoumusten täyttämistä, Ranskan tärkeimpiä taloudellisia, teollisia ja tieteellisiä etuja sekä terrorismin torjuntaa ja toimielinten tasavaltaiseen valtiomuotoon kohdistuvien loukkauksien ja sellaisen kollektiivisen väkivallan estämistä, joka on omiaan vahingoittamaan vakavasti yleistä rauhaa. Asiassa C-520/18 kyseessä olevasta säännöstöstä on todettava, että sen tavoitteisiin kuuluvat muun muassa rikosten tutkinta, selvittäminen ja syyteharkinta sekä kansallisen turvallisuuden, maanpuolustuksen ja yleisen turvallisuuden takaaminen.

85 Ennakkoratkaisua pyytäneet tuomioistuimet tiedustelevat erityisesti perusoikeuskirjan 6 artiklassa vahvistetun turvallisuutta koskevan oikeuden mahdollisia vaikutuksia direktiivin 2002/58 15 artiklan 1 kohdan tulkintaan. Ne pohtivat myös, voidaanko pääasioissa kyseessä olevissa säännöstöissä säädetystä tietojen säilyttämisestä aiheutuvaa puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin pitää perusteltuna, kun otetaan huomioon säännöt, joilla rajoitetaan kansallisten viranomaisten oikeutta saada säilytettyjä tietoja. Conseil d'État'n mukaan on lisäksi niin, että koska tämä kysymys on esitetty asiayhteydessä, jolle ovat ominaisia vakava ja jatkuva uhka kansalliselle turvallisuudelle, sitä on arvioitava myös SEU 4 artiklan 2 kohdan kannalta. Cour constitutionnelle puolestaan korostaa, että asiassa C-520/18 kyseessä olevalla kansallisella säännöstöllä toteutetaan myös perusoikeuskirjan 4 ja 7 artiklasta johtuvat toimintavelvollisuudet eli säädetään lainsäädännöllisestä kehyksestä, jolla mahdollistetaan tehokas seuraamusten määrääminen alaikäisiin kohdistuvasta seksuaalisesta hyväksikäytöstä.

86 Vaikka sekä Conseil d'État että Cour constitutionnelle olettavat, että pääasioissa kyseessä olevat kansalliset säännöstöt, joilla säännellään liikenne- ja paikkatietojen säilyttämistä sekä kansallisten viranomaisten oikeutta saada näitä tietoja kansallisen turvallisuuden takaamisen kaltaisia direktiivin 2002/58 15 artiklan 1 kohdassa säädettyjä tarkoituksia varten, kuuluvat kyseisen direktiivin soveltamisalaan, eräät pääasioiden asianosaiset ja eräät unionin tuomioistuimelle kirjallisia huomautuksia esittäneet jäsenvaltiot ovat tältä osin eri mieltä erityisesti mainitun direktiivin 1 artiklan 3 kohdan tulkinnasta. Aluksi on siis tutkittava, kuuluvatko mainitut säännöstöt tämän saman direktiivin soveltamisalaan.

Direktiivin 2002/58 soveltamisala

87 Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International ja Center for Democracy and Technology vetoavat tältä osin direktiivin 2002/58 soveltamisalaa koskevaan unionin tuomioistuimen oikeuskäytäntöön ja väittävät lähinnä, että sekä tietojen säilyttäminen että oikeus saada säilytettyjä tietoja kuuluvat kyseiseen soveltamisalaan riippumatta siitä, saadaanko tiedot viiveellä vai reaaliajassa. Koska kansallisen turvallisuuden takaamista koskeva tavoite mainitaan nimenomaisesti kyseisen direktiivin 15 artiklan 1 kohdassa, tähän tavoitteeseen pyrkiminen ei johda siihen, ettei kyseistä direktiiviä voida soveltaa. SEU 4 artiklan 2 kohta, johon ennakkoratkaisua pyytäneet tuomioistuimet viittaavat, ei vaikuta tähän arviointiin.

88 Niistä tiedustelutoimenpiteistä, joita toimivaltaiset Ranskan viranomaiset toteuttavat suoraan ilman, että ne sääntelisivät sähköisten viestintäpalvelujen tarjoajien toimintaa asettamalla näille erityisiä velvollisuuksia, Center for Democracy and Technology huomauttaa, että kyseiset toimenpiteet kuuluvat välttämättä direktiivin 2002/58 ja perusoikeuskirjan soveltamisalaan, koska ne ovat poikkeuksia kyseisen direktiivin 5 artiklassa taatusta luottamuksellisuuden periaatteesta. Mainittujen toimenpiteiden on siis oltava kyseisen direktiivin 15 artiklan 1 kohdasta johtuvien vaatimusten mukaisia.

89 Ranskan, Tšekin ja Viron hallitukset, Irlanti sekä Kyproksen, Unkarin, Puolan, Ruotsin ja Yhdistyneen kuningaskunnan hallitukset väittävät sitä vastoin lähinnä, että direktiiviä 2002/58 ei sovelleta pääasiassa kyseessä olevan kaltaisiin kansallisiin säännöstöihin, koska niiden tarkoituksena on kansallisen turvallisuuden takaaminen. Tiedusteluyksikköjen toiminta kuuluu – siltä osin kuin se liittyy yleisen järjestyksen ylläpitämiseen sekä sisäisen turvallisuuden ja alueellisen koskemattomuuden takaamiseen – jäsenvaltioiden keskeisiin tehtäviin, ja yksin jäsenvaltioilla on sitä koskeva toimivalta, kuten erityisesti SEU 4 artiklan 2 kohdan kolmas virke osoittaa.

90 Nämä hallitukset ja Irlanti viittaavat lisäksi direktiivin 2002/58 1 artiklan 3 kohtaan, jossa direktiivin soveltamisalan ulkopuolelle jätetään, kuten jo direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa säädettiin, toimet, jotka koskevat yleistä turvallisuutta, puolustusta ja valtion turvallisuutta. Ne tukeutuvat tältä osin 30.5.2006 annettuun tuomioon parlamentti v. neuvosto ja komissio (C-317/04 ja C-318/04, EU:C:2006:346) sisältyvään viimeksi mainitun säännöksen tulkintaan.

91 Tältä osin on todettava, että direktiivin 2002/58 1 artiklan 1 kohdan mukaan direktiivissä säädetään sellaisten kansallisten säännösten yhdenmukaistamisesta, joita tarvitaan samantasoisen perusoikeuksien ja -vapauksien, erityisesti yksityisyyttä ja luottamuksellisuutta koskevan oikeuden, suojan varmistamiseksi henkilötietojen käsittelyssä sähköisen viestinnän alalla.

92 Kyseisen direktiivin 1 artiklan 3 kohdassa suljetaan direktiivin soveltamisalan ulkopuolelle ”valtion toimet” siinä tarkoitetuilla aloilla, joihin kuuluvat valtion toimet rikosoikeuden alalla ja yleistä turvallisuutta, puolustusta ja valtion turvallisuutta – mukaan lukien valtion taloudellinen hyvinvointi, kun toimet liittyvät valtion turvallisuuteen – koskevat toimet. Esimerkkeinä mainitut toimet ovat kussakin tapauksessa valtiolle tai valtion viranomaisille tyypillisiä toimintoja, jotka eivät liity yksityisten henkilöiden toiminta-aloihin (tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 32 kohta oikeuskäytäntöviittauksineen).

93 Direktiivin 2002/58 3 artiklassa säädetään lisäksi, että kyseistä direktiiviä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa unionissa, mukaan luettuina tiedonkeruu- ja tunnistuslaitteita tukevat yleiset viestintäverkot (jäljempänä sähköiset viestintäpalvelut). Mainitun direktiivin on siis katsottava sääntelevän tällaisten palvelujen tarjoajien toimia (tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 33 kohta oikeuskäytäntöviittauksineen).

94 Tässä yhteydessä on todettava, että direktiivin 2002/58 15 artiklan 1 kohdan nojalla jäsenvaltiot voivat siinä säädetyin edellytyksin 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” (tuomio 21.12.2016, Tele2, C-203/15, EU:C:2016:970, 71 kohta).

95 Direktiivin 2002/58 15 artiklan 1 kohta edellyttää kuitenkin väistämättä, että siinä tarkoitetut kansalliset lainsäädännölliset toimenpiteet kuuluvat kyseisen direktiivin soveltamisalaan, koska siinä nimenomaisesti sallitaan jäsenvaltioiden toteuttavan niitä vain siinä säädettyjä edellytyksiä noudattaen. Tällaisilla toimenpiteillä säännellään lisäksi kyseisessä säännöksessä mainituissa tarkoituksissa sähköisten viestintäpalvelujen tarjoajien toimintaa (tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 34 kohta oikeuskäytäntöviittauksineen).

96 Unionin tuomioistuin on todennut muun muassa näiden seikkojen perusteella, että direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna yhdessä sen 3 artiklan kanssa, on tulkittava siten, että sen soveltamisalaan kuuluu paitsi lainsäädännöllinen toimenpide, jossa sähköisten viestintäpalvelujen tarjoajat velvoitetaan säilyttämään liikenne- ja paikkatiedot, myös lainsäädännöllinen toimenpide, jossa ne velvoitetaan antamaan toimivaltaisille kansallisille viranomaisille oikeus saada näitä tietoja. Tällaiset lainsäädännölliset toimenpiteet merkitsevät näet välttämättä sitä, että kyseiset palveluntarjoajat käsittelevät mainittuja tietoja, eikä niitä voida – siltä osin kuin niillä säännellään näiden samojen

palveluntarjoajien toimintaa – rinnastaa mainitun direktiivin 1 artiklan 3 kohdassa tarkoitettuihin valtiolle tyypillisiin toimiin (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 35 ja 37 kohta oikeuskäytäntöviittauksineen).

97 Kun lisäksi otetaan huomioon tämän tuomion 95 kohdassa esitetyt seikat ja direktiivin 2002/58 yleinen rakenne, kyseisen direktiivin sellaisella tulkinnalla, jonka mukaan sen 15 artiklan 1 kohdassa tarkoitetut lainsäädännölliset toimenpiteet on suljettu mainitun direktiivin soveltamisalan ulkopuolelle sen vuoksi, että tavoitteet, joihin tällaisilla toimenpiteillä on vastattava, käyvät pääasiallisesti yksiin saman direktiivin 1 artiklan 3 kohdassa tarkoitettujen toimien tavoitteiden kanssa, kyseiseltä 15 artiklan 1 kohdalta riistettäisiin täysin sen tehokas vaikutus (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 72 ja 73 kohta).

98 Direktiivin 2002/58 1 artiklan 3 kohdassa olevaa toimien käsitettä ei siis voida, kuten julkisasiamies on pääosin huomauttanut antamansa ratkaisuehdotuksen La Quadrature du Net ym. (C-511/18 ja C-512/18, EU:C:2020:6) 75 kohdassa, tulkita siten, että se kattaa kyseisen direktiivin 15 artiklan 1 kohdassa tarkoitetut lainsäädännölliset toimenpiteet.

99 SEU 4 artiklan 2 kohdan määräykset, joihin tämän tuomion 89 kohdassa mainitut hallitukset ovat viitanneet, eivät voi horjuttaa tätä päätelmää. Unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan näet on niin, että vaikka jäsenvaltioiden asiana on määritellä keskeiset turvallisuusetunsa ja toteuttaa niiden sisäisen ja ulkoisen turvallisuuden varmistamiseen soveltuvat toimenpiteet, pelkästään se, että kansallinen toimenpide on annettu kansallisen turvallisuuden suojaamiseksi, ei voi johtaa siihen, ettei unionin oikeutta sovelleta, ja vapauttaa jäsenvaltioita velvollisuudesta noudattaa unionin oikeutta (ks. vastaavasti tuomio 4.6.2013, ZZ, C-300/11, EU:C:2013:363, 38 kohta; tuomio 20.3.2018, komissio v. Itävalta (Valtion painatuskeskus), C-187/16, EU:C:2018:194, 75 ja 76 kohta sekä tuomio 2.4.2020, komissio v. Puola, Unkari ja Tšekki (Tilapäinen mekanismi kansainvälisen suojelun hakijoiden siirtämiseksi), C-715/17, C-718/17 ja C-719/17, EU:C:2020:257, 143 ja 170 kohta).

100 On totta, että unionin tuomioistuin on 30.5.2006 antamassaan tuomiossa parlamentti v. neuvosto ja komissio (C-317/04 ja C-318/04, EU:C:2006:346, 56–59 kohta) todennut, että se, että lentoyhtiöt siirtävät henkilötietoja kolmannen valtion viranomaisille terrorismin ja muiden vakavien rikosten ehkäisemiseksi ja torjumiseksi, ei kuulu direktiivin 95/46 3 artiklan 2 kohdan ensimmäisen luetelmakohdan nojalla kyseisen direktiivin soveltamisalaan, koska tällainen siirto tapahtuu julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen.

101 Tämän tuomion 93, 95 ja 96 kohtaan sisältyvien seikkojen nojalla kyseistä oikeuskäytäntöä ei kuitenkaan voida soveltaa direktiivin 2002/58 1 artiklan 3 kohdan tulkintaan. Kuten julkisasiamies on antamansa ratkaisuehdotuksen La Quadrature du Net ym. (C-511/18 ja C-512/18, EU:C:2020:6) 70–72 kohdassa pääosin huomauttanut, direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa, johon mainittu oikeuskäytäntö liittyy, suljetaan näet viimeksi mainitun direktiivin soveltamisalan ulkopuolelle yleisesti ”käsittely, – – joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta”, tekemättä eroa sen perusteella, kuka asianomaisia tietoja on käsitellyt. Tällainen eron tekeminen on sitä vastoin tarpeen direktiivin 2002/58 1 artiklan 3 kohtaa tulkittaessa. Kuten tämän tuomion 94–97 kohdasta ilmenee, kaikki sähköisten viestintäpalvelujen tarjoajien suorittama henkilötietojen käsittely kuuluu mainitun direktiivin soveltamisalaan, mukaan lukien käsittely, joka seuraa viranomaisten niille asettamista velvollisuuksista, vaikka tämä viimeksi mainittu käsittely saattaisi mahdollisesti kuulua direktiivin 95/46 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa säädetyn poikkeuksen soveltamisalaan, kun otetaan huomioon kyseisen säännöksen laajempi sanamuoto, jossa mainitaan kaikki käsittely, joka käsittelijästä riippumatta koskee yleistä turvallisuutta, puolustusta tai valtion turvallisuutta.

102 Lisäksi on todettava, että 30.5.2006 annettuun tuomioon parlamentti v. neuvosto ja komissio (C-317/04 ja C-318/04, EU:C:2006:346) johtaneessa asiassa kyseessä ollut direktiivi 95/46 on asetuksen 2016/679 94 artiklan 1 kohdan mukaan kumottu ja korvattu kyseisellä asetuksella 25.5.2018 alkaen.

Vaikka mainitun asetuksen 2 artiklan 2 kohdan d alakohdassa täsmennetään, ettei sitä sovelleta käsittelyyn, jota ”toimivaltaiset viranomaiset” suorittavat muun muassa rikosten ennalta estämistä ja paljastamista varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten, saman asetuksen 23 artiklan 1 kohdan d ja h alakohdasta ilmenee, että yksityisten näihin samoihin tarkoituksiin suorittama henkilötietojen käsittely kuuluu kyseisen asetuksen soveltamisalaan. Tästä seuraa, että edellä esitetty direktiivin 2002/58 1 artiklan 3 kohdan, 3 artiklan ja 15 artiklan 1 kohdan tulkinta on johdonmukainen asetuksen 2016/679, jota kyseisellä direktiivillä täydennetään ja täsmennetään, soveltamisalan rajauksen kanssa.

103 Kun jäsenvaltiot panevat sitä vastoin suoraan täytäntöön sähköisen viestinnän luottamuksellisuudesta poikkeavia toimenpiteitä asettamatta tällaisen viestinnän palveluntarjoajille käsittelyä koskevia velvollisuuksia, asianomaisten henkilöiden tietosuojaan ei sovelleta direktiiviä 2002/58 vaan ainoastaan kansallista oikeutta, jollei luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 (EUVL 2016, L 119, s. 89) soveltamisesta muuta johdu, joten kyseessä olevien toimenpiteiden on oltava muun muassa perustuslain tasoisen kansallisen oikeuden ja Euroopan ihmisoikeussopimuksen vaatimusten mukaisia.

104 Edellä esitetystä seuraa, että pääasiassa kyseessä olevien kaltainen kansallinen säännöstö, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot kansallisen turvallisuuden suojaamiseksi ja rikollisuuden torjumiseksi, kuuluu direktiivin 2002/58 soveltamisalaan.

Direktiivin 2002/58 15 artiklan 1 kohdan tulkinta

105 Aluksi on muistutettava, että vakiintuneen oikeuskäytännön mukaan unionin oikeuden säännöksen tai määräyksen tulkitsemisessa on otettava huomioon sen sanamuodon lisäksi sen asiayhteys sekä sillä säännöstöllä tavoitellut päämäärät, jonka osa se on, ja erityisesti tämän säännöstön syntyhistoria (ks. vastaavasti tuomio 17.4.2018, Egenberger, C-414/16, EU:C:2018:257, 44 kohta).

106 Direktiivin 2002/58 tavoitteena on, kuten etenkin sen johdanto-osan kuudennesta ja seitsemännestä perustelukappaleesta ilmenee, suojata sähköisten viestintäpalvelujen käyttäjiä uusista teknologioista ja muun muassa tietojen automaattisen tallennus- ja käsittelykapasiteetin lisääntymisestä aiheutuvilta heidän henkilötietoihinsa ja yksityisyyteensä liittyviltä riskeiltä. Mainitulla direktiivillä pyritään erityisesti, kuten sen johdanto-osan toisessa perustelukappaleessa todetaan, varmistamaan perusoikeuskirjan 7 ja 8 artiklassa vahvistettujen oikeuksien täysimääräinen kunnioittaminen. Direktiivin 2002/58 taustalla olevan ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (KOM(2000) 385 lopullinen) perusteluista ilmenee tältä osin, että unionin lainsäätäjän tarkoituksena on ollut ”varmistaa, että henkilötietojen ja yksityisyyden suojan korkean tason säilyminen taataan kaikissa sähköisen viestinnän palveluissa käytetystä tekniikasta riippumatta”.

107 Direktiivin 2002/58 5 artiklan 1 kohdassa vahvistetaan tässä tarkoituksessa sekä sähköisen viestinnän että siihen liittyvien liikennetietojen luottamuksellisuuden periaate, ja se merkitsee muun muassa sitä, että muita henkilöitä kuin käyttäjiä on lähtökohtaisesti kielletty tallentamasta kyseistä viestintää ja kyseisiä tietoja ilman käyttäjien suostumusta.

108 Siltä osin kuin on kyse erityisesti siitä, miten sähköisten viestintäpalvelujen tarjoajat käsittelevät ja säilyttävät liikennetietoja, direktiivin 2002/58 6 artiklasta ja sen johdanto-osan 22 ja 26 perustelukappaleesta ilmenee, että tällainen käsittely on sallittua ainoastaan siinä määrin ja niin kauan kuin palvelujen markkinoiminen, palvelujen laskuttaminen ja lisäarvopalvelujen tarjoaminen sitä edellyttää. Tämän ajan päätyttyä käsitellyt ja tallennetut tiedot on poistettava tai tehtävä nimettömiksi.

Mainitun direktiivin 9 artiklan 1 kohdassa säädetään muiden paikkatietojen kuin liikennetietojen osalta, että kyseisiä tietoja saa käsitellä vain tietyin edellytyksin ja sen jälkeen, kun ne on tehty nimettömiksi, tai jos käyttäjät tai tilaajat ovat antaneet siihen suostumuksensa (tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 86 kohta oikeuskäytäntöviittauksineen).

109 Unionin lainsäätäjä on siis kyseisen direktiivin antaessaan konkretisoinut perusoikeuskirjan 7 ja 8 artiklassa vahvistetut oikeudet, joten sähköisten viestintävälineiden käyttäjillä on oikeus odottaa lähtökohtaisesti, että heidän viestintänsä ja siihen liittyvät tiedot säilyvät nimettöminä eikä niitä voida tallentaa, jos he eivät ole antaneet siihen suostumustaan.

110 Direktiivin 2002/58 15 artiklan 1 kohdan mukaan jäsenvaltiot voivat kuitenkin säätää poikkeuksista kyseisen direktiivin 5 artiklan 1 kohdassa vahvistetusta periaatteellisesta velvollisuudesta taata henkilötietojen luottamuksellisuus ja muun muassa saman direktiivin 6 ja 9 artiklassa mainituista vastaavista velvollisuuksista, jos tällainen rajoitus on välttämätön, asianmukainen ja oikeasuhteinen demokraattisen yhteiskunnan toimenpide kansallisen turvallisuuden sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. Tätä varten jäsenvaltiot voivat muun muassa hyväksyä lainsäädännöllisiä toimenpiteitä, joissa säädetään tietojen säilyttämisestä rajoitetuksi ajaksi, kun tämä on perusteltua jostakin näistä syistä.

111 Mahdollisuus poiketa direktiivin 2002/58 5, 6 ja 9 artiklassa säädetyistä oikeuksista ja velvollisuuksista ei kuitenkaan voi olla perusteena sille, että sähköisen viestinnän ja siihen liittyvien tietojen luottamuksellisuuden takaamista koskevasta periaatteellisesta velvollisuudesta ja erityisesti kyseisen direktiivin 5 artiklassa nimenomaisesti säädetystä näiden tietojen tallentamista koskevasta kiellosta poikkeamisesta tulisi sääntö (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 89 ja 104 kohta).

112 Unionin tuomioistuin on jo todennut tavoitteista, joilla voidaan oikeuttaa muun muassa direktiivin 2002/58 5, 6 ja 9 artiklassa säädettyjen oikeuksien ja velvollisuuksien rajoittaminen, että kyseisen direktiivin 15 artiklan 1 kohdan ensimmäisessä virkkeessä oleva tavoitteiden luettelo on tyhjentävä, joten kyseisen säännöksen nojalla toteutetun lainsäädännöllisen toimenpiteen on oltava tosiasiallisesti ja ehdottomasti näistä tavoitteista jonkin mukainen (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 52 kohta oikeuskäytäntöviittauksineen).

113 Direktiivin 2002/58 15 artiklan 1 kohdan kolmannesta virkkeestä ilmenee lisäksi, että jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan kyseisen direktiivin 5, 6 ja 9 artiklassa tarkoitettujen oikeuksien ja velvollisuuksien ulottuvuutta, ainoastaan, jos kyseiset toimenpiteet ovat unionin oikeuden yleisten periaatteiden, joihin kuuluu suhteellisuusperiaate, ja perusoikeuskirjassa taattujen perusoikeuksien mukaisia. Unionin tuomioistuin on tältä osin jo katsonut, että jäsenvaltion sähköisten viestintäpalvelujen tarjoajille kansallisella säännöstöllä asettama velvollisuus säilyttää liikennetiedot, jotta toimivaltaiset kansalliset viranomaiset voivat tarvittaessa saada niitä, herättää kysymyksiä paitsi perusoikeuskirjan 7 ja 8 artiklaan, jotka koskevat yksityisyyden suojaa ja henkilötietojen suojaa, myös sananvapautta koskevaan perusoikeuskirjan 11 artiklaan nähden (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 25 ja 70 kohta ja tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 91 ja 92 kohta oikeuskäytäntöviittauksineen).

114 Direktiivin 2002/58 15 artiklan 1 kohdan tulkinnassa on siten otettava huomioon sekä perusoikeuskirjan 7 artiklassa taatun yksityiselämän kunnioittamista koskevan oikeuden ja perusoikeuskirjan 8 artiklassa taatun henkilötietojen suojaa koskevan oikeuden tärkeys, sellaisena kuin se ilmenee unionin tuomioistuimen oikeuskäytännöstä, sekä sananvapautta koskevan oikeuden tärkeys; tämä perusoikeuskirjan 11 artiklassa taattu perusoikeus on eräs demokraattiseen ja moniarvoiseen yhteiskuntaan liittyvä olennainen perusta ja kuuluu arvoihin, joille unioni SEU 2 artiklan mukaisesti

perustuu (ks. vastaavasti tuomio 6.3.2001, Connolly v. komissio, C-274/99 P, EU:C:2001:127, 39 kohta ja tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 93 kohta oikeuskäytäntöviittauksineen).

115 Tältä osin on täsmennettävä, että liikenne- ja paikkatietojen säilyttäminen merkitsee sinänsä yhtäältä poikkeusta direktiivin 2002/58 5 artiklan 1 kohdassa säädetystä kiellosta, jonka mukaan muut henkilöt kuin käyttäjät eivät saa tallentaa näitä tietoja, ja toisaalta puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin, eikä merkitystä ole sillä, ovatko kyseessä olevat yksityiselämään liittyvät tiedot arkaluonteisia, tai onko asianomaisille mahdollisesti aiheutunut haittaa tästä puuttumisesta (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 124 ja 126 kohta oikeuskäytäntöviittauksineen; ks. analogisesti Euroopan ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomio 30.1.2020, Breyer v. Saksa, CE:ECHR:2020:0130JUD005000112, 81 kohta).

116 Merkitystä ei ole myöskään sillä, käytetäänkö säilytettyjä tietoja myöhemmin (ks. analogisesti Euroopan ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomio 16.2.2000, Amann v. Sveitsi, CE:ECHR:2000:0216JUD002779895, 69 kohta ja Euroopan ihmisoikeustuomioistuimen tuomio 13.2.2020, Trjakovski ja Chipovski v. Pohjois-Makedonia, CE:ECHR:2020:0213JUD005320513, 51 kohta), koska oikeus saada tällaisia tietoja merkitsee siitä riippumatta, miten niitä käytetään myöhemmin, erillistä puuttumista edellä olevassa kohdassa tarkoitettuihin perusoikeuksiin (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 124 ja 126 kohta).

117 Tämä päätelmä on sitäkin perustellumpi, koska liikenne- ja paikkatiedot voivat paljastaa tietoja huomattavasta määrästä asianomaisten henkilöiden yksityiselämään liittyviä seikkoja, ja myös arkaluonteisia tietoja, kuten seksuaalista suuntautumista, poliittisia mielipiteitä, uskonnollista, filosofista, yhteiskunnallista tai muuta vakaumusta sekä terveydentilaa koskevia tietoja, vaikka tällaiset tiedot saavat unionin oikeudessa lisäksi erityistä suojaa. 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, toiminnasta sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään. Niiden perusteella voidaan erityisesti laatia rekisteröityjen profiili, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 27 kohta ja tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 99 kohta).

118 Näin ollen yhtäältä liikenne- ja paikkatietojen säilyttäminen poliisikäyttöön on yksistään omiaan loukkaamaan perusoikeuskirjan 7 artiklassa vahvistettua oikeutta viestinnän kunnioittamiseen ja vaikuttamaan ennalta ehkäisevästi siihen, miten sähköisten viestintävälineiden käyttäjät käyttävät perusoikeuskirjan 11 artiklassa taattua sananvapauttaan (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 28 kohta ja tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 101 kohta). Tällaiset ehkäisevät vaikutukset voivat kohdistua erityisesti henkilöihin, joiden viestintä kuuluu kansallisten sääntöjen mukaan salassapitovelvollisuuden piiriin, sekä väärinkäytösten ilmoittajiin, joiden toimintaa suojataan unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta 23.10.2019 annetulla Euroopan parlamentin ja neuvoston direktiivillä (EU) 2019/1937 (EUVL 2019, L 305, s. 17). Nämä vaikutukset ovat lisäksi sitä vakavampia, mitä enemmän tietoja säilytetään ja mitä moninaisempia ne ovat.

119 Kun toisaalta otetaan huomioon niiden liikenne- ja paikkatietojen huomattava määrä, jotka voidaan säilyttää jatkuvasti yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevalla toimenpiteellä, sekä sen tiedon arkaluonteisuus, jotka tällaisista tiedoista voidaan saada, pelkästään siihen, että sähköisten viestintäpalvelujen tarjoajat säilyttävät mainitut tiedot, liittyy väärinkäyttöä ja lainvastaista saantia koskevia vaaroja.

120 Siltä osin kuin jäsenvaltioilla on direktiivin 2002/58 15 artiklan 1 kohdan mukaan mahdollisuus ottaa käyttöön tämän tuomion 110 kohdassa tarkoitettuja poikkeuksia, kyseinen säännös kuvastaa kuitenkin sitä, etteivät perusoikeuskirjan 7, 8 ja 11 artiklassa vahvistetut oikeudet ole ehdottomia, vaan ne on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa (ks. vastaavasti tuomio 16.7.2020, Facebook Ireland ja Schrems, C-311/18, EU:C:2020:559, 172 kohta oikeuskäytäntöviittauksineen).

121 Kuten perusoikeuskirjan 52 artiklan 1 kohdasta ilmenee, siinä sallitaan näet näiden oikeuksien käyttämisen rajoittaminen, kunhan näistä rajoituksista säädetään lailla mainittujen oikeuksien keskeistä sisältöä kunnioittaen ja kunhan ne suhteellisuusperiaatteen mukaisesti ovat tarpeellisia ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

122 Kun direktiivin 2002/58 15 artiklan 1 kohtaa tulkitaan perusoikeuskirjan valossa, siinä on siten otettava huomioon myös perusoikeuskirjan 3, 4, 6 ja 7 artiklassa vahvistettujen oikeuksien tärkeys sekä kansallisen turvallisuuden suojelua ja vakavan rikollisuuden torjuntaa koskevien tavoitteiden tärkeys, millä myötävaikutetaan muiden henkilöiden oikeuksien ja vapauksien suojeluun.

123 Perusoikeuskirjan 6 artiklassa, johon Conseil d'État ja Cour constitutionnelle viittaavat, vahvistetaan tältä osin jokaisen oikeus paitsi vapauteen myös turvallisuuteen ja taataan Euroopan ihmisoikeussopimuksen 5 artiklassa taattuja oikeuksia vastaavat oikeudet (ks. vastaavasti tuomio 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, 47 kohta; tuomio 28.7.2016, JZ, C-294/16 PPU, EU:C:2016:610, 48 kohta ja tuomio 19.9.2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, 42 kohta oikeuskäytäntöviittauksineen).

124 Lisäksi on huomautettava, että perusoikeuskirjan 52 artiklan 3 kohdan tarkoituksena on varmistaa tarvittava johdonmukaisuus perusoikeuskirjaan sisältyvien oikeuksien ja Euroopan ihmisoikeussopimuksessa taattujen vastaavien oikeuksien välillä, sanotun kuitenkaan vaikuttamatta unionin oikeuden itsenäisyyteen ja Euroopan unionin tuomioistuimen riippumattomuuteen. Euroopan ihmisoikeussopimuksen vastaavat oikeudet on siis otettava huomioon perusoikeuskirjaa tulkittaessa vähimmäissuojan tasona (ks. vastaavasti tuomio 12.2.2019, TC, C-492/18 PPU, EU:C:2019:108, 57 kohta ja tuomio 21.5.2019, komissio v. Unkari (Maatalousmaan käyttö- ja tuotto-oikeudet), C-235/17, EU:C:2019:432, 72 kohta oikeuskäytäntöviittauksineen).

125 Euroopan ihmisoikeussopimuksen 5 artiklasta, jossa vahvistetaan ”oikeus vapauteen” ja ”oikeus turvallisuuteen”, on todettava, että sillä pyritään Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan suojelemaan henkilöitä mielivaltaiselta tai perusteettomalta vapaudenmenetykseltä (ks. vastaavasti Euroopan ihmisoikeustuomioistuimen tuomio 18.3.2008, Ladent v. Puola, CE:ECHR:2008:0318JUD001103603, 45 ja 46 kohta; Euroopan ihmisoikeustuomioistuimen tuomio 29.3.2010, Medvedyev ym. v. Ranska, CE:ECHR:2010:0329JUD000339403, 76 ja 77 kohta sekä Euroopan ihmisoikeustuomioistuimen tuomio 13.12.2012, El-Masri v. ”The former Yugoslav Republic of Macedonia”, CE:ECHR:2012:1213JUD003963009, 239 kohta). Siltä osin kuin kyseinen määräys koskee viranomaisen toteuttamaa vapaudenmenetystä, perusoikeuskirjan 6 artiklaa ei kuitenkaan voida tulkita siten, että siinä asetettaisiin viranomaisille velvollisuus ryhtyä erityisiin toimenpiteisiin tietyistä rikoksista rankaisemiseksi.

126 Siltä osin kuin on kyse erityisesti sellaisten rikosten, joiden uhreja ovat etenkin alaikäiset ja muut heikossa asemassa olevat henkilöt, tehokkaasta torjunnasta, johon Cour constitutionnelle on viitannut, on sitä vastoin huomautettava, että perusoikeuskirjan 7 artiklasta voi seurata viranomaisia koskevia

toimintavelvollisuuksia sellaisten oikeudellisten toimenpiteiden toteuttamiseksi, joilla suojataan yksityis- ja perhe-elämää (ks. vastaavasti tuomio 18.6.2020, komissio v. Unkari (Järjestöjen avoimuus), C-78/18, EU:C:2020:476, 123 kohta Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöä koskevine viittauksineen). Tällaiset velvollisuudet voivat perustua myös mainittuun 7 artiklaan kodin ja viestien suojaamisen osalta sekä 3 ja 4 artiklaan jokaisen ruumiillisen ja henkisen koskemattomuuden suojaamisen osalta sekä kidutuksen sekä epäinhimillisen tai halventavan kohtelun kiellon osalta.

127 Kun otetaan huomioon nämä erilaiset toimintavelvollisuudet, kyseessä olevat eri intressit ja oikeudet on välttämättä sovitettava yhteen.

128 Euroopan ihmisoikeustuomioistuin on näet katsonut, että Euroopan ihmisoikeussopimuksen 3 ja 8 artiklasta johtuvat toimintavelvollisuudet, joita vastaavat takeet sisältyvät perusoikeuskirjan 4 ja 7 artiklaan, edellyttävät muun muassa sellaisten aineellisten ja menettelyllisten säännösten antamista sekä sellaisten käytännön toimenpiteiden toteuttamista, joilla voidaan tehokkaasti torjua henkilöihin kohdistuvia rikoksia tehokkaalla tutkinnalla ja syytteeseenpanolla, ja tämä velvollisuus on sitäkin tärkeämpi, kun lapsen fyysinen ja henkinen hyvinvointi ovat uhattuina. Niiden toimenpiteiden osalta, jotka toimivaltaisten viranomaisten on toteutettava, on kuitenkin noudatettava täysimääräisesti lain määräämää järjestystä ja muita takeita, joilla voidaan rajoittaa rikostutkintavaltuuksien laajuutta, sekä muita vapauksia ja oikeuksia. Kyseisen tuomioistuimen mukaan on erityisesti luotava sellainen lainsäädännöllinen kehys, jolla voidaan sovittaa yhteen eri intressit ja suojeltavat oikeudet (Euroopan ihmisoikeustuomioistuimen tuomio 28.10.1998, Osman v. Yhdistynyt kuningaskunta, CE:ECHR:1998:1028JUD002345294, 115 ja 116 kohta; Euroopan ihmisoikeustuomioistuimen tuomio 4.3.2004, M.C. v. Bulgaria, CE:ECHR:2003:1204JUD003927298, 151 kohta; Euroopan ihmisoikeustuomioistuimen tuomio 24.6.2004, Von Hannover v. Saksa, CE:ECHR:2004:0624JUD005932000, 57 ja 58 kohta sekä Euroopan ihmisoikeustuomioistuimen tuomio 2.12.2008, K.U. v. Suomi, CE:ECHR:2008:1202JUD000287202, 46, 48 ja 49 kohta).

129 Suhteellisuusperiaatteen noudattamisesta on todettava, että direktiivin 2002/58 15 artiklan 1 kohdan ensimmäisessä virkkeessä säädetään, että jäsenvaltiot voivat toteuttaa viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuuden periaatteesta poikkeavan toimenpiteen, jos tällainen toimenpide on ”välttämät[ön], asianmukai[nen] ja oikeasuhtei[nen] demokraattisen yhteiskunnan toimenpi[de]” kyseisessä säännöksessä mainittujen tavoitteiden kannalta. Kyseisen direktiivin johdanto-osan 11 perustelukappaleessa täsmennetään, että tällaisen toimenpiteen on ”ehdottomasti” oltava oikeassa suhteessa sen tarkoitukseen nähden.

130 Tältä osin on huomautettava, että yksityiselämän kunnioittamista koskevan perusoikeuden suoja edellyttää unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan, että poikkeukset henkilötietojen suojaan ja sitä koskevat rajoitukset toteutetaan täysin välttämättömän rajoissa. Yleisen edun mukaiseen tavoitteeseen ei myöskään voida pyrkiä ottamatta huomioon sitä, että se on sovitettava yhteen niiden perusoikeuksien kanssa, joita toimenpide koskee, saattamalla yleisen edun mukainen tavoite ja toisaalta kyseessä olevat oikeudet keskenään harmoniseen tasapainoon (ks. vastaavasti tuomio 16.12.2008, Satakunnan Markkinapörssi ja Satamedia, C-73/07, EU:C:2008:727, 56 kohta; tuomio 9.11.2010, Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, EU:C:2010:662, 76, 77 ja 86 kohta sekä tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 52 kohta; lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 140 kohta).

131 Unionin tuomioistuimen oikeuskäytännöstä ilmenee erityisesti, että jäsenvaltioiden mahdollisuutta oikeuttaa muun muassa direktiivin 2002/58 5, 6 ja 9 artiklassa säädettyjen oikeuksien ja velvollisuuksien rajoittaminen on arvioitava mittaamalla tällaiseen rajoittamiseen sisältyvän puuttumisen vakavuus ja tarkastamalla, että kyseisen rajoituksen yleisen edun mukaisen tavoitteen tärkeys on suhteessa tähän vakavuuteen (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 55 kohta oikeuskäytäntöviittauksineen).

132 Oikeasuhteisuutta koskevan edellytyksen täyttämiseksi säännöstössä on säädettävä selvistä ja täsmällisistä kyseessä olevan toimenpiteen laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden henkilötiedoista on kyse, on riittävät takeet, joiden avulla heidän henkilötietojaan voidaan tehokkaasti suojata väärinkäytön vaaroilta. Kyseisen säännöstön on oltava kansallisen oikeuden mukaan laillisesti sitova, ja siinä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksin tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa, jotta taataan, että puuttuminen rajoittuu täysin välttämättömään. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti, etenkin, kun on olemassa huomattava näiden tietojen lainvastaista saantia koskeva vaara. Nämä näkökohdat pätevät erityisesti silloin, kun on suojattava kyseistä henkilötietojen erityisryhmää eli arkaluonteisia tietoja (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 54 ja 55 kohta; tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 117 kohta ja lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 141 kohta).

133 Säännöstön, jossa säädetään henkilötietojen säilyttämisestä, on siis aina täytettävä objektiiviset kriteerit, joilla luodaan yhteys säilytettävien tietojen ja tavoitellun päämäärän välille (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 191 kohta oikeuskäytäntöviittauksineen ja tuomio 3.10.2019, A ym., C-70/18, EU:C:2019:823, 63 kohta).

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen ennakoivasta säilyttämisestä kansallisen turvallisuuden takaamiseksi

134 On huomautettava, ettei unionin tuomioistuin ole vielä tutkinut direktiiviä 2002/58 tulkitsevissa tuomioissaan erityisesti tavoitetta taata kansallinen turvallisuus, johon ennakkoratkaisua pyytäneet tuomioistuimet ja huomautuksia esittäneet hallitukset ovat vedonneet.

135 Tässä yhteydessä on todettava heti alkuun, että SEU 4 artiklan 2 kohdassa määrätään, että kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Tämä vastuu vastaa ensisijaisen tärkeää intressiä suojella valtion keskeisiä tehtäviä ja yhteiskunnan perustavanlaatuisia etuja, ja siihen kuuluu sellaisten etenkin terrorismin kaltaisten toimien torjuminen ja niistä rankaiseminen, jotka ovat omiaan horjuttamaan vakavasti tietyn maan perustavanlaatuisia perustuslaillisia, poliittisia, taloudellisia tai yhteiskunnallisia rakenteita ja erityisesti uhkaamaan suoraan yhteiskuntaa, väestöä tai valtiota sellaisenaan.

136 Kansallisen turvallisuuden takaamista koskeva tavoite, luettuna SEU 4 artiklan 2 kohdan valossa, on kuitenkin tärkeämpi kuin direktiivin 2002/58 15 artiklan 1 kohdassa tarkoitetut muut tavoitteet, ja etenkin rikollisuuden, jopa vakavan rikollisuuden, torjumista yleensä ja yleisen turvallisuuden suojaamista koskevat tavoitteet. Edellä olevassa kohdassa tarkoitetun kaltaiset uhat eroavat näet luonteeltaan ja erityiseltä vakavuudeltaan yleisestä vaarasta, joka koskee jopa vakavien jännitteiden tai häiriöiden aiheutumista yleiselle turvallisuudelle. Jollei perusoikeuskirjan 52 artiklan 1 kohdassa määrättyjen muiden vaatimusten noudattamisesta muuta johdu, kansallisen turvallisuuden takaamista koskevalla tavoitteella voidaan näin ollen oikeuttaa toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin toimenpiteillä, jotka voitaisiin oikeuttaa näillä muilla tavoitteilla.

137 Tämän tuomion 135 ja 136 kohdassa kuvaillun kaltaisissa tilanteissa direktiivin 2002/58 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei siis lähtökohtaisesti ole esteenä lainsäädännölliselle toimenpiteelle, jonka mukaan toimivaltaiset viranomaiset voivat määrätä sähköisten viestintäpalvelujen tarjoajat säilyttämään kaikkien sähköisten viestintävälineiden käyttäjien liikenne- ja paikkatiedot rajoitetun ajanjakson ajan, kun on olemassa riittävän konkreettisia seikkoja, joiden perusteella voidaan katsoa, että asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu tämän tuomion 135 ja 136 kohdassa tarkoitetun kaltainen vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi. Vaikka tällaista toimenpidettä sovelletaan erotuksetta kaikkiin sähköisten viestintävälineiden käyttäjiin

ilman, että ensi näkemältä vaikuttaisi siltä, että niillä on tämän tuomion 133 kohdassa mainitussa oikeuskäytännössä tarkoitettu yhteys kyseisen jäsenvaltion kansalliselle turvallisuudelle aiheutuvaan uhkaan, on kuitenkin katsottava, että tällaisen uhan olemassaolo on sellaisenaan omiaan osoittamaan tämän yhteyden.

138 Määräys, jonka mukaan kaikkien sähköisten viestintävälineiden käyttäjien tiedot on säilytettävä ennakoivasti, on kuitenkin rajoitettava ajallisesti täysin välttämättömään. Vaikka on mahdollista, että sähköisten viestintäpalvelujen tarjoajille annettu tietojen säilyttämistä koskeva määräys saatetaan uusia tällaisen uhan jatkumisen vuoksi, kulloisenkin määräyksen voimassaoloaika ei saa ylittää ennakoitavissa olevaa ajanjaksoa. Tällaiselle tietojen säilyttämiselle on asetettava rajoituksia ja siihen on sovellettava tiukkoja takeita, joilla voidaan tehokkaasti suojata asianomaisten henkilöiden henkilötietoja väärinkäytön vaaroilta. Tämä säilyttäminen ei siis voi olla järjestelmällistä.

139 Kun otetaan huomioon se, että tällaisesta tietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä koskevasta toimenpiteestä johtuva puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin on vakavaa, on varmistettava, että kyseiseen toimenpiteeseen turvaudutaan tosiasiallisesti vain tämän tuomion 135 ja 136 kohdassa tarkoitettujen kaltaisissa tilanteissa, joissa kansalliseen turvallisuuteen kohdistuu vakava uhka. Tässä tarkoituksessa on olennaista, että joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa päätökseen, jolla sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään tiedot tällä tavalla, tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan.

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen ennakoivasta säilyttämisestä rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi

140 Siltä osin kuin on kyse rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa koskevasta tavoitteesta on todettava, että ainoastaan vakavan rikollisuuden torjuminen ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen voivat suhteellisuusperiaatteen mukaisesti oikeuttaa liikenne- ja paikkatietojen säilyttämisestä johtuvan kaltaiset vakavat puuttumiset perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin. Yleensä siis vain sellaiset puuttumiset mainittuihin perusoikeuksiin, jotka eivät ole vakavia, voidaan oikeuttaa rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 102 kohta; tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 56 ja 57 kohta sekä lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 149 kohta).

141 Kansallinen säännöstö, jossa säädetään liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä vakavan rikollisuuden torjumiseksi, ylittää täysin välttämättömän rajat, eikä sitä voida pitää perusteltuna demokraattisessa yhteiskunnassa siten kuin sitä edellytetään direktiivin 2002/58 15 artiklan 1 kohdassa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 107 kohta).

142 Kun otetaan huomioon liikenne- ja paikkatiedoista mahdollisesti saatavan tiedon arkaluonteisuus, liikenne- ja paikkatietojen luottamuksellisuus on yksityiselämän kunnioittamista koskevan oikeuden kannalta olennaista. Koska yhtäältä näiden tietojen säilyttäminen voi tämän tuomion 118 kohdassa tarkoitetulla tavalla vaikuttaa ehkäisevästi perusoikeuskirjan 7 ja 11 artiklassa vahvistettujen perusoikeuksien käyttöön ja toisaalta tällaisesta säilyttämisestä johtuva puuttuminen on vakavaa, demokraattisessa yhteiskunnassa on siten tärkeää, että säilyttäminen on – kuten direktiivillä 2002/58 käyttöön otetussa järjestelmässä säädetään – poikkeus eikä sääntö ja että näitä tietoja ei voida säilyttää

järjestelmällisesti ja jatkuvasti. Tämä päätelmä on tehtävä myös vakavan rikollisuuden torjuntaa ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemistä koskevien tavoitteiden ja näille tavoitteille annettavan merkityksen kannalta.

143 Unionin tuomioistuin on lisäksi korostanut, että säännöstö, jossa säädetään liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä, kattaa lähes koko väestön sähköisen viestinnän ilman, että tehtäisiin mitään erottelua, rajoituksia tai poikkeuksia tavoitteen perusteella. Tällainen säännöstö koskee tämän tuomion 133 kohdassa mainitusta vaatimuksesta poiketen yleisellä tavalla kaikkia sähköisiä viestintäpalveluja käyttäviä henkilöitä, vaikka kyseiset henkilöt eivät ole edes välillisesti tilanteessa, joka voisi johtaa rikosoikeudellisiin toimiin. Sitä sovelletaan siis myös henkilöihin, joiden osalta ei ole mitään seikkaa, jonka perusteella voitaisiin olettaa, että heidän toimintansa voisi liittyä edes välillisesti tai kaukaisesti kyseiseen vakavan rikollisuuden torjumisen tavoitteeseen, ja erityisesti ilman, että säilytettävien tietojen ja yleiselle turvallisuudelle aiheutuvan uhan välillä olisi mitään yhteyttä (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 57 ja 58 kohta sekä tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 105 kohta).

144 Tällaista säännöstöä ei ole varsinkaan, kuten unionin tuomioistuin on jo todennut, rajattu säilyttämiseen, joka koskee joko tiettyyn ajanjaksoon ja/tai maantieteellisesti määriteltyyn alueeseen ja/tai sellaisten henkilöiden piiriin, jotka voisivat olla sekaantuneita tavalla tai toisella vakavaan rikokseen, liittyviä tietoja taikka henkilöitä, joiden tietojen säilyttäminen voisi muilla perusteilla myötävaikuttaa vakavan rikollisuuden torjumiseen (ks. vastaavasti tuomio 8.4.2014, Digital Rights, C-293/12 ja C-594/12, EU:C:2014:238, 59 kohta ja tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 106 kohta).

145 Edes jäsenvaltioiden toimintavelvollisuudet, jotka voivat perustua tapauksen mukaan perusoikeuskirjan 3, 4 ja 7 artiklaan ja jotka – kuten tämän tuomion 126 ja 128 kohdassa on todettu – koskevat sellaisten sääntöjen käyttöönottamista, joilla voidaan torjua tehokkaasti rikoksia, eivät kuitenkaan voi oikeuttaa yhtä vakavia puuttumisia kuin ne, joita säännöstöstä, jossa säädetään liikenne- ja paikkatietojen säilyttämisestä, aiheutuu lähes koko väestön perusoikeuskirjan 7 ja 8 artiklassa vahvistetuille perusoikeuksille ilman, että asianomaisten henkilöiden tiedot olisivat omiaan tuomaan esiin ainakin välillisen yhteyden tavoiteltuun päämäärään.

146 Tämän tuomion 142–144 kohdassa todetun mukaisesti ja kun otetaan huomioon kyseessä olevien oikeuksien ja intressien välttämätön yhteensovittaminen, vakavan rikollisuuden torjuntaa, yleiselle turvallisuudelle aiheutuvan vakavan vahingon ehkäisemistä ja varsinkin kansallisen turvallisuuden takaamista koskevat tavoitteet voivat sitä vastoin oikeuttaa – kun otetaan huomioon niiden tärkeys – edellä olevassa kohdassa mainittujen ja etenkin Cour constitutionnellen viittaamien toimintavelvollisuuksien kannalta sellaisen erityisen vakavan puuttumisen, jota liikenne- ja paikkatietojen kohdennettu säilyttäminen merkitsee.

147 Kuten unionin tuomioistuin on jo todennut, direktiivin 2002/58 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei siten ole esteenä sille, että jäsenvaltio antaa säännöstön, jossa sallitaan ennakoivasti liikenne- ja paikkatietojen kohdennettu säilyttäminen vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi kuten myös kansallisen turvallisuuden takaamiseksi, sillä edellytyksellä, että tällainen säilyttäminen on säilytettävien tietoryhmien, kyseessä olevien viestintävälineiden, asianomaisten henkilöiden ja aiotun säilytyksen keston osalta rajoitettu täysin välttämättömään (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 108 kohta).

148 Siltä osin kuin kyse on siitä, että tällainen tietojen säilyttämistä koskeva toimenpide on rajattava, on todettava, että rajaaminen voidaan toteuttaa muun muassa asianomaisten henkilöiden ryhmien perusteella, koska direktiivin 2002/58 15 artiklan 1 kohta ei ole esteenä säännöstölle, joka perustuu objektiivisiin seikkoihin, joiden perusteella kohteeksi voidaan valikoida henkilöt, joiden liikenne- ja paikkatiedot voivat paljastaa ainakin välillisen yhteyden vakaviin rikoksiin, myötävaikuttaa tavalla tai

toisella vakavan rikollisuuden torjumiseen tai ehkäistä yleistä turvallisuutta koskevan vakavan uhan taikka kansallista turvallisuutta koskevan uhan (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 111 kohta).

149 Tältä osin on täsmennettävä, että näin kohteeksi valitut henkilöt voivat olla muun muassa henkilöitä, jotka on etukäteen tunnistettu sovellettavien kansallisten menettelyjen yhteydessä objektiivisten seikkojen perusteella henkilöiksi, jotka aiheuttavat uhkan asianomaisen jäsenvaltion yleiselle turvallisuudelle tai kansalliselle turvallisuudelle.

150 Liikenne- ja paikkatietojen säilyttämistä koskevan toimenpiteen rajaaminen voi perustua myös maantieteelliseen kriteeriin, jos toimivaltaiset kansalliset viranomaiset katsovat objektiivisten ja syrjimättömien seikkojen perusteella, että yhdellä tai useammalla maantieteellisellä alueella vallitsee tilanne, jossa on kohonnut riski vakavien rikosten valmisteluun tai toteuttamiseen (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 111 kohta). Näillä alueilla voi olla muun muassa paikkoja, joilla tehdään lukuisia vakavia rikoksia, paikkoja, jotka ovat erityisen alttiita vakavien rikosten tekemiselle, kuten paikkoja tai infrastruktuureja, joissa käy säännöllisesti hyvin suuri määrä henkilöitä, taikka lentoasemien, rautatieasemien tai tietullialueiden kaltaisia strategisia paikkoja.

151 Sen varmistamiseksi, että tämän tuomion 147–150 kohdassa kuvatuista kohdennetuista säilyttämistä koskevista toimenpiteistä aiheutuva puuttuminen on suhteellisuusperiaatteen mukaista, kyseisten toimenpiteiden kesto ei saa ylittää sitä, mikä on täysin välttämätöntä tavoitellun päämäärän ja toimenpiteiden perusteena olevien olosuhteiden kannalta, sanotun kuitenkaan rajoittamatta toimenpiteen mahdollista uudistamista sen vuoksi, että tällaisen säilyttämisen tarve on edelleen olemassa.

– Lainsäädännölliset toimenpiteet, joissa säädetään IP-osoitteiden ja henkilöllisyyttä koskevien tietojen ennakoivasta säilyttämisestä rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi

152 On huomautettava, että vaikka IP-osoitteet kuuluvat liikennetietoihin, ne luodaan ilman, että ne liittyvät tiettyyn viestintään, ja niiden ensisijaisena tarkoituksena on tunnistaa sähköisten viestintäpalvelujen tarjoajien välityksellä luonnollinen henkilö, joka omistaa päätelaitteen, jonka kautta viestintä internetin välityksellä tapahtuu. Sähköpostin ja internetin välityksellä tarjottavien puhelinpalvelujen osalta on siis todettava, että siltä osin kuin pelkästään viestinnän lähteen eikä viestinnän vastaanottajan IP-osoitteet säilytetään, nämä osoitteet eivät paljasta sellaisinaan mitään tietoa niistä kolmansista henkilöistä, jotka ovat olleet yhteydessä viestinnän alullepanijana olevaan henkilöön. Tähän ryhmään kuuluvat tiedot eivät ole siis yhtä arkaluonteisia kuin muut liikennetiedot.

153 Koska IP-osoitteita voidaan kuitenkin käyttää muun muassa internetin käyttäjän selailupolun ja siten hänen verkkotoimintansa kattavaan jäljittämiseen, näiden tietojen perusteella voidaan selvittää internetin käyttäjän yksityiskohtainen profiili. Mainittujen IP-osoitteiden säilyttäminen ja analysointi, jota tällainen jäljittäminen edellyttää, merkitsee siten sellaista vakavaa puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin internetin käyttäjän perusoikeuksiin, jolla voi olla tämän tuomion 118 kohdassa tarkoitetun kaltainen ennalta ehkäisevä vaikutus.

154 Tämän tuomion 130 kohdassa mainitussa oikeuskäytännössä edellytetyn kyseessä olevien oikeuksien ja intressien välttämättömän yhteensovittamisen kannalta on kuitenkin otettava huomioon se, että verkkorikoksen tapauksessa IP-osoite voi olla ainoa tutkintakeino, jolla voidaan yksilöidä henkilö, jolle kyseinen osoite oli annettu kyseisen rikoksen tekohetkellä. Tämän lisäksi se, että sähköisten viestintäpalvelujen tarjoajat säilyttävät IP-osoitteet sitä ajanjaksoa pidemmän ajan, jota varten kyseiset tiedot on annettu, ei lähtökohtaisesti ole tarpeen kyseessä olevien palvelujen laskuttamiseksi, joten verkkorikosten paljastaminen voi tästä syystä, kuten useat hallitukset ovat unionin tuomioistuimelle esitetyissä huomautuksissaan todenneet, osoittautua mahdottomaksi, jollei ole mahdollista turvautua direktiivin 2002/58 15 artiklan 1 kohtaan perustuvaan lainsäädännölliseen toimenpiteeseen. Tästä voi

olla kyse muun muassa – kuten kyseiset hallitukset ovat väittäneet – lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja neuvoston puitepäätöksen 2004/68/YOS korvaamisesta 13.12.2011 annetun Euroopan parlamentin ja neuvoston direktiivin 2011/93/EU (EUVL 2011, L 335, s. 1) 2 artiklan c alakohdassa tarkoitetun lapsipornografian hankkimisen, levittämisen, välittämisen tai verkkoon lähettämisen kaltaisten lapsipornografiaan liittyvien erityisen vakavien rikosten osalta.

155 Vaikka siis on totta, että lainsäädännöllinen toimenpide, jossa säädetään kaikkien sellaisten luonnollisten henkilöiden IP-osoitteiden säilyttämisestä, jotka omistavat päätelaitteen, jonka kautta internetyhteys voidaan muodostaa, koskisi henkilöitä, joilla ei ensi arviolta ole tämän tuomion 133 kohdassa mainitussa oikeuskäytännössä tarkoitettua liittymää tavoiteltuihin päämääriin, ja vaikka internetin käyttäjillä on tämän tuomion 109 kohdassa todetun mukaisesti oikeus odottaa perusoikeuskirjan 7 ja 8 artiklan nojalla, ettei heidän henkilöllisyyttään lähtökohtaisesti paljasteta, lainsäädännöllinen toimenpide, jossa säädetään pelkästään jonkin liittymän lähteelle annettujen IP-osoitteiden yleisesti ja erotuksetta tapahtuvasta säilyttämisestä, ei lähtökohtaisesti ole vastoin direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, kunhan kyseisen mahdollisuuden osalta noudatetaan tiukasti sellaisia aineellisia ja menettelyllisiä edellytyksiä, joita kyseisten tietojen käyttöön on sovellettava.

156 Kun otetaan huomioon se, että kyseisestä säilyttämisestä johtuva puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin on vakavaa, ainoastaan vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen voivat kansallisen turvallisuuden takaamisen tavoin oikeuttaa kyseisen puuttumisen. Säilyttämisen kesto ei myöskään saa ylittää sitä, mikä on täysin välttämätöntä tavoitellun päämäärän kannalta. Lopuksi on todettava, että tällaisessa toimenpiteessä on säädettävä tiukoista edellytyksistä ja takeista asianomaisten henkilöiden verkossa suorittaman viestinnän ja toteuttamien toimien osalta siltä osin kuin on kyse näiden tietojen hyödyntämisestä muun muassa jäljittämällä.

157 Siltä osin kuin lopuksi on kyse sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevista tiedoista, on todettava, että pelkästään näiden tietojen perusteella ei voida selvittää suoritetun viestinnän päivämäärää, kellonaikaa, kestoa ja vastaanottajia eikä myöskään paikkoja, joissa viestintä on tapahtunut, tai viestinnän määrää tiettyjen henkilöiden kanssa tiettynä ajanjaksona, joten niistä ei saada näiden käyttäjien osoitteiden kaltaisia yhteystietoja lukuun ottamatta mitään tietoa tietystä viestinnästä eikä siis heidän yksityiselämästään. Näiden tietojen säilyttämisestä aiheutuvaa puuttumista ei siten lähtökohtaisesti voida pitää vakavana (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 59 ja 60 kohta).

158 Tästä seuraa, että tämän tuomion 140 kohdassa todetun mukaisesti lainsäädännölliset toimenpiteet, jotka koskevat näiden tietojen käsittelyä sellaisinaan ja etenkin tietojen säilyttämistä ja niiden saamista pelkästään asianomaisen käyttäjän tunnistamista varten ilman, että mainittuja tietoja voidaan yhdistää suoritettua viestintää koskeviin tietoihin, voidaan oikeuttaa rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella, johon direktiivin 2002/58 15 artiklan 1 kohdan ensimmäisessä virkkeessä viitataan (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 62 kohta).

159 Kun otetaan huomioon kyseessä olevien oikeuksien ja intressien välttämätön yhteensovittaminen, tämän tuomion 131 ja 158 kohdassa mainituista syistä on näin ollen katsottava, että vaikka kaikkien sähköisten viestintävälineiden käyttäjien ja tavoiteltujen päämäärien välillä ei ole liittymää, direktiivin 2002/58 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei ole esteenä lainsäädännölliselle toimenpiteelle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on ilman erityistä määräaikaa säilytettävä kaikkien sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevat tiedot rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa sekä yleisen turvallisuuden takaamista varten, ilman että on tarpeen, että rikokset tai yleiseen turvallisuuteen kohdistuvat uhat ovat vakavia.

– Lainsäädännölliset toimenpiteet, joissa säädetään liikenne- ja paikkatietojen säilyttämisen nopeasta varmistamisesta vakavan rikollisuuden torjumiseksi

160 Sähköisten viestintäpalvelujen tarjoajien direktiivin 2002/58 5, 6 ja 9 artiklan tai sen 15 artiklan 1 kohdan nojalla toteutettujen lainsäädännöllisten toimenpiteiden, sellaisina kuin ne ovat kuvattuina tämän tuomion 134–159 kohdassa, perusteella käsittelemien ja tallentamien liikenne- ja paikkatietojen osalta on todettava, että kyseiset tiedot on lähtökohtaisesti tapauksen mukaan poistettava tai tehtävä nimettömiksi niiden lakisääteisten määräaikojen päätyttyä, jotka kyseisen direktiivin täytäntöönpanemiseksi annetuissa kansallisissa säännöksissä on asetettu niiden käsittelylle ja tallentamiselle.

161 Tämän käsittelyn ja tallentamisen aikana voi kuitenkin syntyä tilanteita, joissa on välttämätöntä säilyttää mainitut tiedot näiden määräaikojen jälkeen vakavien rikosten tai kansalliseen turvallisuuteen kohdistuvien loukkausten selvittämiseksi, ja näin on sekä tilanteessa, jossa nämä rikokset tai loukkaukset on jo voitu todeta, että tilanteessa, jossa voidaan kaikkien merkityksellisten seikkojen objektiivisen tarkastelun päätteeksi kohtuudella epäillä, että kyseinen rikos tai loukkaus on tapahtunut.

162 Tältä osin on todettava, että 23.11.2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen (Euroopan sopimussarja – nro 185), jonka 27 jäsenvaltiota ovat allekirjoittaneet ja 25 jäsenvaltiota ratifioineet ja jonka tavoitteena on helpottaa tietoverkkoja käyttäen tehtyjen rikosten torjuntaa, 14 artiklassa määrätään, että sopimuspuolet ryhtyvät yksittäistä rikostutkintaa tai rikosoikeudenkäyntiä varten jo tallennettujen liikennetietojen osalta tiettyihin säilyttämisen nopean varmistamisen kaltaisiin toimenpiteisiin. Kyseisen yleissopimuksen 16 artiklan 1 kappaleessa määrätään erityisesti, että sopimuspuolet ryhtyvät tarvittaviin lainsäädännöllisiin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä tai muutoin varmistaa nopeasti sellaisten liikennetietojen säilyttäminen, jotka on tallennettu tietojärjestelmän avulla, erityisesti silloin kun on syytä uskoa, että näiden tietojen häviäminen tai muuttaminen on erityisen todennäköistä.

163 Tämän tuomion 161 kohdassa tarkoitetun kaltaisessa tilanteessa jäsenvaltiot voivat – kun otetaan huomioon tämän tuomion 130 kohdassa tarkoitettu kyseessä olevien oikeuksien ja intressien välttämätön yhteensovittaminen – säätää direktiivin 2002/58 15 artiklan 1 kohdan nojalla annetussa lainsäädännössä mahdollisuudesta velvoittaa sähköisten viestintäpalvelujen tarjoajat sellaisen toimivaltaisen viranomaisen päätöksellä, joka voi olla tehokkaan tuomioistuinvalvonnan kohteena, varmistamaan nopeasti niiden käytössä olevien liikenne- ja paikkatietojen säilyttäminen tietyn ajan.

164 Siltä osin kuin tällaisen säilyttämisen nopean varmistamisen tavoite ei enää vastaa niitä tavoitteita, joita varten tiedot on alun perin kerätty ja säilytetty, ja siltä osin kuin kaiken tietojenkäsittelyn on perusoikeuskirjan 8 artiklan 2 kohdan mukaan tapahduttava tiettyä tarkoitusta varten, jäsenvaltioiden on lainsäädännössään täsmennettävä tavoite, jota varten tietojen säilyttämisen nopea varmistaminen on mahdollista. Kun otetaan huomioon se, että tällaisesta säilyttämisestä todennäköisesti aiheutuva puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin on vakavaa, ainoastaan vakavan rikollisuuden torjunta ja varsinkin kansallisen turvallisuuteen takaaminen voivat oikeuttaa kyseisen puuttumisen. Lisäksi sen varmistamiseksi, että tämäntyyppisestä toimenpiteestä johtuva puuttuminen rajoittuu täysin välttämättömään, yhtäältä säilyttämisvelvollisuuden on koskettava ainoastaan liikenne- ja paikkatietoja, joilla voidaan myötävaikuttaa kyseessä olevan vakavan rikoksen tai kansalliseen turvallisuuteen kohdistuvan loukkauksen selvittämiseen. Toisaalta tietojen säilyttämisen kesto on rajoitettava täysin välttämättömään, mutta sitä voidaan kuitenkin jatkaa, kun olosuhteet ja mainitulla toimenpiteellä tavoiteltu päämäärä sen oikeuttavat.

165 Tältä osin on täsmennettävä, että tällaista säilyttämisen nopeaa varmistamista ei pidä rajoittaa sellaisten henkilöiden tietoihin, joiden konkreettisesti epäillään syyllistyneen rikokseen tai loukanneen kansallista turvallisuutta. Koska tällaisen toimenpiteen osalta on noudatettava direktiivin 2002/58 15 artiklan 1 kohdassa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan ja 52 artiklan 1 kohdan valossa, vahvistettuja puitteita ja kun otetaan huomioon tämän tuomion 133 kohdassa esitetyt seikat,

se voidaan lainsäätäjän valinnan mukaan ja täysin välttämättömän rajoissa ulottaa koskemaan muihin kuin sellaisiin henkilöihin liittyviä liikenne- ja paikkatietoja, joiden epäillään suunnitelleen vakavaa rikosta ja kansalliseen turvallisuuteen kohdistuvaa loukkausta taikka syyllistyneen tällaiseen rikokseen tai loukkaukseen, siltä osin kuin kyseisillä tiedoilla voidaan objektiivisten ja syrjimättömien seikkojen perusteella myötävaikuttaa tällaisen rikoksen tai tällaisen kansalliseen turvallisuuteen kohdistuvan loukkauksen selvittämiseen; tällaisia tietoja ovat esimerkiksi rikoksen uhria ja hänen sosiaalista tai ammatillista lähipiiriään koskevat tiedot taikka tiettyjä maantieteellisiä alueita, kuten kyseessä olevan rikoksen teko- tai valmistelupaikkaa tai kyseessä olevaan kansalliseen turvallisuuteen kohdistuvan loukkauksen tapahtuma- tai valmistelupaikkaa, koskevat tiedot. Toimivaltaisten viranomaisten oikeus saada näin säilytettyjä tietoja on toteutettava noudattamalla edellytyksiä, jotka perustuvat siihen oikeuskäytäntöön, jossa direktiiviä 2002/58 on tulkittu (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 118–121 kohta oikeuskäytäntöviittauksineen).

166 On vielä todettava, että – kuten erityisesti tämän tuomion 115 ja 133 kohdasta ilmenee – oikeus saada palveluntarjoajien direktiivin 2002/58 15 artiklan 1 kohdan nojalla toteutetun toimenpiteen nojalla säilyttämiä liikenne- ja paikkatietoja voidaan lähtökohtaisesti oikeuttaa ainoastaan sillä yleisen edun mukaisella tavoitteella, jonka tähden kyseisille palveluntarjoajille on asetettu tämä säilyttämisvelvollisuus. Tästä seuraa erityisesti, että oikeutta saada tällaisia tietoja tavanomaisen rikoksen syyteharkintaa ja siitä määrättävää seuraamusta varten ei voida missään tapauksessa myöntää, jos tietojen säilyttämistä on perusteltu vakavan rikollisuuden torjuntaa tai varsinkin kansallisen turvallisuuden takaamista koskevalla tavoitteella. Suhteellisuusperiaatteen, sellaisena kuin sitä on täsmennetty tämän tuomion 131 kohdassa, mukaan oikeus saada säilytettyjä tietoja vakavan rikollisuuden torjumiseksi voi sitä vastoin olla perusteltavissa – siltä osin kuin edellä olevassa kohdassa mainittuja tällaiseen tietojen saantiin liittyviä aineellisia ja menettelyllisiä edellytyksiä noudatetaan – kansallisen turvallisuuden takaamista koskevalla tavoitteella.

167 Jäsenvaltiot voivat tältä osin säätää lainsäädännössään, että liikenne- ja paikkatietoja voidaan saada näitä samoja aineellisia ja menettelyllisiä edellytyksiä noudattaen vakavan rikollisuuden torjumiseksi tai kansallisen turvallisuuden takaamiseksi silloin, kun palveluntarjoaja säilyttää mainitut tiedot direktiivin 2002/58 5, 6 ja 9 artiklan tai 15 artiklan 1 kohdan mukaisesti.

168 Kaiken edellä esitetyn perusteella asioissa C-511/18 ja C-512/18 esitettyihin ensimmäisiin kysymyksiin ja asiassa C-520/18 esitettyyn ensimmäiseen ja toiseen kysymykseen on vastattava, että direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se on esteenä lainsäädännöllisille toimenpiteille, joissa säädetään kyseisessä 15 artiklan 1 kohdassa säädettyjä tarkoituksia varten ennakoivasti liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä. Mainittu 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei sitä vastoin ole esteenä lainsäädännöllisille toimenpiteille, joissa

– sallitaan kansallisen turvallisuuden takaamiseksi se, että sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään liikenne- ja paikkatiedot yleisesti ja erotuksetta tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa päätökseen, jolla tällainen määräys annetaan, tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan; mainittu määräys voidaan antaa ainoastaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa, jos kyseinen uhka on edelleen olemassa

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi liikenne- ja paikkatietojen kohdennetusta säilyttämisestä, joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä ajanjaksoksi, joka on rajattu täysin välttämättömään

– säädetään kansallisen turvallisuuden takaamiseksi, rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä ja

– sallitaan vakavan rikollisuuden torjumiseksi ja varsinkin kansallisen turvallisuuden takaamiseksi se, että sähköisten viestintäpalvelujen tarjoajat määrätään toimivaltaisen viranomaisen päätöksellä, johon kohdistuu tehokas tuomioistuinvalvonta, varmistamaan nopeasti kyseisten palveluntarjoajien käytössä olevien liikenne- ja paikkatietojen säilyttäminen tietyn ajan,

jos näillä toimenpiteillä varmistetaan selvin ja täsmällisin säännöin, että kyseessä olevien tietojen säilyttämisen ehtona on, että näihin toimenpiteisiin liittyviä aineellisia ja menettelyllisiä edellytyksiä noudatetaan, ja että asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja vastaan.

Asiassa C-511/18 esitetyt toinen ja kolmas kysymys

169 Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee asiassa C-511/18 esittämillään toisella ja kolmannella kysymyksellä lähinnä, onko direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, tulkittava siten, että se on esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on toteutettava verkoissaan toimenpiteet, jotka mahdollistavat yhtäältä liikenne- ja paikkatietojen automaattisen analysoinnin ja keräämisen reaaliajassa ja toisaalta käytettyjen päätelaitteiden sijaintipaikkaa koskevien teknisten tietojen keräämisen reaaliajassa ilman, että rekisteröidyille on ilmoitettava tästä käsittelystä ja keräämisestä.

170 Ennakkoratkaisua pyytänyt tuomioistuin täsmentää, että CSI:n L. 851-2–L. 851-4 §:ssä säädetyt tiedonhankintamenetelmät eivät merkitse sähköisten viestintäpalvelujen tarjoajille erityistä liikenne- ja paikkatietojen säilyttämistä koskevaa vaatimusta. Kyseinen tuomioistuin toteaa erityisesti CSI:n L. 851-3 §:ssä tarkoitetusta automaattisesta analysoinnista, että kyseisen käsittelyn tarkoituksena on selvittää tätä varten määriteltyjen kriteerien perusteella yhteydet, jotka saattavat paljastaa terroriuhan. Ennakkoratkaisua pyytänyt tuomioistuin toteaa CSI:n L. 851-2 §:ssä tarkoitetusta reaaliaikaisesta keräämisestä, että se koskee vain yhtä tai useampaa henkilöä, jonka on etukäteen todettu voivan liittyä terroriuhkaan. Saman tuomioistuimen mukaan näitä kumpaakin menetelmää voidaan käyttää vain terrorismin torjumiseksi, ja ne koskevat CSI:n L. 851-1 ja R. 851-5 §:ssä tarkoitettuja tietoja.

171 Aluksi on täsmennettävä, että se, että CSI:n L. 851-3 §:n mukaan siinä säädetyn automaattisen analysoinnin avulla ei sellaisenaan ole mahdollista tunnistaa käyttäjiä, joiden tiedot kuuluvat tämän analysoinnin piiriin, ei ole esteenä tällaisten tietojen luonnehtimiselle ”henkilötiedoiksi”. Koska tämän saman säännöksen IV momentissa säädetty menettely mahdollistaa myöhemmässä vaiheessa sen henkilön tai niiden henkilöiden tunnistamisen, joita ne tiedot koskevat, joiden automaattinen analysointi on paljastanut, että terroriuhka saattaa olla olemassa, kaikki henkilöt, joiden tietoja

analysoidaan automaattisesti, ovat edelleen tunnistettavissa näiden tietojen perusteella. Asetuksen 2016/679 4 artiklan 1 alakohtaan sisältyvän henkilötietojen määritelmän mukaan tällaisia tietoja ovat muun muassa tunnistettavissa olevaan henkilöön liittyvät tiedot.

Liikenne- ja paikkatietojen automaattinen analysointi

172 CSI:n L. 851-3 §:stä ilmenee, että siinä säädetty automaattinen analysointi merkitsee lähinnä kaikkien sähköisten viestintäpalvelujen tarjoajien säilyttämien liikenne- ja paikkatietojen suodatusta, jonka kyseiset palvelujentarjoajat suorittavat toimivaltaisten kansallisten viranomaisten pyynnöstä näiden määrittämien parametrien mukaisesti. Tästä seuraa, että kaikki sähköisten viestintävälineiden käyttäjien tiedot tarkastetaan, jos ne vastaavat näitä parametrejä. Tällaisen automaattisen analysoinnin on siis katsottava merkitsevän sitä, että asianomaiset sähköisten viestintäpalvelujen tarjoajat suorittavat toimivaltaisen viranomaisen lukuun yleisesti ja erotuksetta tapahtuvaa käsittelyä asetuksen 2016/679 4 artiklan 2 alakohdassa tarkoitettuna automaattisen tietojenkäsittelyn avulla tapahtuvana käyttönä, joka kattaa kaikkien sähköisten viestintävälineiden käyttäjien liikenne- ja paikkatiedot kokonaisuudessaan. Tämä käsittely tapahtuu erillään CSI:n L. 851-3 §:n IV momentin nojalla sallitusta, automaattisen analysoinnin avulla tunnistettuihin henkilöiden liittyvien tietojen myöhemmästä keräämisestä.

173 Kansallisella säännöstöllä, jossa sallitaan tällainen liikenne- ja paikkatietojen automaattinen analysointi, poiketaan kuitenkin direktiivin 2002/58 5 artiklassa asetetusta periaatteellisesta velvollisuudesta taata sähköisen viestinnän ja siihen liittyvien tietojen luottamuksellisuus. Tällainen säännöstö merkitsee myös puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin riippumatta siitä, miten näitä tietoja käytetään myöhemmin. Lopuksi on todettava, että mainittu säännöstö on tämän tuomion 118 kohdassa mainitun oikeuskäytännön perusteella omiaan vaikuttamaan ennalta ehkäisevästi perusoikeuskirjan 11 artiklassa vahvistetun sananvapauden käyttämiseen.

174 Pääasiassa kyseessä olevan kaltaisesta liikenne- ja paikkatietojen automaattisesta analysoinnista seuraava puuttuminen on lisäksi erityisen vakavaa, koska analysointi kattaa yleisesti ja erotuksetta sähköisiä viestintävälineitä käyttävien henkilöiden tiedot. Tämä toteamus pätee varsinkin, kun – kuten pääasiassa kyseessä olevasta kansallisesta säännöstöstä ilmenee – automaattisen analysoinnin kohteena olevat tiedot voivat paljastaa verkossa haettujen tietojen luonteen. Tällaista automaattista analysointia sovelletaan lisäksi kokonaisvaltaisesti kaikkiin henkilöihin, jotka käyttävät sähköisiä viestintävälineitä, ja tämän johdosta myös henkilöihin, joiden osalta ei ole mitään seikkaa, jonka perusteella voidaan olettaa, että heidän toimintansa voisi liittyä edes välillisesti tai kaukaisesti terrorismiin.

175 Tällaisen puuttumisen oikeuttamisesta on täsmennettävä, että perusoikeuskirjan 52 artiklan 1 kohdassa asetettu edellytys, jonka mukaan perusoikeuksien käyttämistä voidaan rajoittaa ainoastaan lailla, tarkoittaa sitä, että itse siinä oikeusperustassa, joka mahdollistaa rajoittamisen, on määritettävä asianomaisen oikeuden käyttämiselle asetettavien rajoitusten laajuus (ks. vastaavasti tuomio 16.7.2020, Facebook Ireland ja Schrems, C-311/18, EU:C:2020:559, 175 kohta oikeuskäytäntöviittauksineen).

176 Jotta täytettäisiin tämän tuomion 130 ja 131 kohdassa mieleen palautettu oikeasuhteisuuden vaatimus, jonka mukaan poikkeukset henkilötietojen suojaan ja sitä koskevat rajoitukset on toteutettava täysin välttämättömän rajoissa, kansallisessa säännöstössä, jossa säännellään toimivaltaisten viranomaisten oikeutta saada säilytettyjä liikenne- ja paikkatietoja, on lisäksi noudatettava tämän tuomion 132 kohdassa mainitusta oikeuskäytännöstä seuraavia vaatimuksia. Tällaisessa säännöstössä ei etenkään voida tyytyä vaatimaan, että viranomaisten oikeus saada tietoja vastaa kyseisen säännöstön tarkoitusta, vaan siinä on myös säädettävä aineellisista ja menettelyllisistä kyseistä käyttöä koskevista edellytyksistä (ks. analogisesti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 192 kohta oikeuskäytäntöviittauksineen).

177 Tässä yhteydessä on muistutettava, että erityisen vakava puuttuminen, jota liikenne- ja paikkatietojen yleinen ja erotuksetta tapahtuva säilyttäminen merkitsee ja johon tämän tuomion 134–139 kohdassa esitetyissä toteamuksissa viitataan, sekä kyseisten tietojen automaattisesta analysoinnista muodostuva erityisen vakava puuttuminen voivat täyttää oikeasuhteisuutta koskevan vaatimuksen vain tilanteissa, joissa jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja sillä edellytyksellä, että kyseisen säilyttämisen kesto on rajoitettu täysin välttämättömään.

178 Edellä olevassa kohdassa tarkoitettujen kaltaisissa tilanteissa kaikkien sähköisten viestintävälineiden käyttäjien liikenne- ja paikkatietojen automaattista analysointia tiukasti rajoitetun ajanjakson ajan voidaan pitää oikeutettuna direktiivin 2002/58 15 artiklan 1 kohdasta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, johtuvien vaatimusten kannalta.

179 Jotta voidaan taata, että tällaiseen toimenpiteeseen turvautuminen rajoittuu tosiasiallisesti siihen, mikä on kansallisen turvallisuuden suojaamisen ja erityisesti terrorismin ehkäisemisen kannalta ehdottoman välttämätöntä, on tämän tuomion 139 kohdassa todetun mukaisesti olennaista, että joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa siihen päätökseen, jolla automaattinen analysointi sallitaan, tahokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on tilanne, joka oikeuttaa mainitun toimenpiteen, ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan.

180 Tältä osin on täsmennettävä, että ennalta vahvistettujen mallien ja kriteerien, joihin tämäntyyppinen tietojenkäsittely perustuu, on oltava yhtäältä erityisiä ja luotettavia, jotta niiden avulla voidaan saavuttaa tulokset, joilla tunnistetaan henkilöt, joihin voisi kohdistua kohtuullinen epäily osallistumisesta terrorismirikoksiin, ja toisaalta syrjimättömiä (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 172 kohta).

181 Lisäksi on muistutettava, että millä tahansa automaattisella analyysillä, joka tehdään siihen lähtökohtaan perustuvien mallien ja kriteerien nojalla, jonka mukaan jonkin henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliittoon kuuluminen, terveydentila tai seksuaalinen käyttäytyminen voisivat itsessään ja kyseisen henkilön omasta käyttäytymisestä riippumatta olla merkityksellisiä terrorismin torjunnan kannalta, loukattaisiin perusoikeuskirjan 7 ja 8 artiklassa, luettuina yhdessä sen 21 artiklan kanssa, taattuja oikeuksia. Automaattista analyysiä varten ennalta vahvistettuja malleja ja kriteereitä, joilla pyritään ehkäisemään kansallista turvallisuutta vakavasti uhkaava terrorismi, ei siten voida perustaa pelkästään näihin arkaluonteisiin tietoihin (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 165 kohta).

182 Koska liikenne- ja paikkatietojen automaattiset analyysit sisältävät lisäksi välttämättä tietyn virhemarginaalin, kukin automaattisen käsittelyn johdosta saatu positiivinen tulos on tutkittava uudelleen erikseen muilla kuin automaattisilla välineillä ennen sellaisen yksittäistoimenpiteen toteuttamista, jolla on kielteisiä vaikutuksia asianomaisiin henkilöihin ja jossa on kyse esimerkiksi liikenne- ja paikkatietojen myöhemmästä keräämisestä reaaliajassa, sillä tällainen toimenpide ei voi perustua ratkaisevasti pelkkään automaattisen käsittelyn tulokseen. Samoin sen takaamiseksi käytännössä, että ennalta vahvistetut mallit ja kriteerit, niiden käyttö sekä käytettävät tietokannat eivät ole syrjiviä ja että ne rajoittuvat täysin välttämättömään kansallista turvallisuutta vakavasti uhkaavan terrorismin ehkäisemistä koskevan tavoitteen kannalta, näiden ennalta vahvistettujen mallien ja kriteerien sekä käytettävien tietokantojen luotettavuus ja ajankohtaisuus on tutkittava säännöllisesti uudelleen (ks. vastaavasti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 173 ja 174 kohta).

Liikenne- ja paikkatietojen kerääminen reaaliajassa

183 CSI:n L. 851-2 §:ssä tarkoitetusta liikenne- ja paikkatietojen keräämisestä reaaliajassa on todettava, että siihen voidaan erikseen antaa lupa siltä osin kuin on kyse ”etukäteen tunnistet[usta] henkilö[stä], joka saattaa liittyä [terrori]uhkaan”. Tässä säännöksessä säädetään myös, että ”jos on vakavaa aihetta epäillä, että yksi tai useampi luvassa kyseessä olevan henkilön lähipiiriin kuuluva henkilö voi antaa tietoja luvan perusteena olevan tarkoituksen osalta, lupa voidaan myöntää erikseen myös kaikkien näiden henkilöiden osalta”.

184 Tämän luonteisen toimenpiteen kohteena olevat tiedot mahdollistavat sen, että toimivaltaiset kansalliset viranomaiset voivat luvan voimassaoloaikana jatkuvasti ja reaaliajassa valvoa niitä henkilöitä, joiden kanssa asianomaiset henkilöt viestivät, niitä välineitä, joita he käyttävät, heidän käymänsä viestinnän kestoa sekä heidän oleskelupaikkojaan ja liikkumistaan. Ne näyttävät myös paljastavan verkosta haettujen tietojen luonteen. Kun näitä tietoja tarkastellaan kokonaisuutena, ne mahdollistavat – kuten tämän tuomion 117 kohdasta ilmenee – hyvin tarkkojen päätelmien tekemisen asianomaisten henkilöiden yksityiselämästä, ja niiden perusteella voidaan laatia heidän profiilinsa, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö.

185 CSI:n L. 851-4 §:ssä tarkoitetusta reaaliajassa tapahtuvasta tietojen keräämisestä on huomautettava, että kyseisessä säännöksessä sallitaan päätelaitteiden sijaintipaikkaa koskevien teknisten tietojen kerääminen ja niiden välittäminen reaaliajassa pääministerin yksikölle. On ilmeistä, että tällaisten tietojen perusteella toimivaltainen yksikkö voi milloin tahansa luvan voimassaoloaikana määrittää jatkuvasti ja reaaliajassa matkapuhelinten kaltaisten käytettyjen päätelaitteiden sijaintipaikan.

186 Kansallisella säännöstöllä, jossa sallitaan tällainen reaaliajassa tapahtuva kerääminen, poiketaan kuitenkin sen säännöstön tavoin, jossa sallitaan tietojen automaattinen analysointi, direktiivin 2002/58 5 artiklassa asetetusta periaatteellisesta velvollisuudesta taata sähköisen viestinnän ja siihen liittyvien tietojen luottamuksellisuus. Myös se merkitsee siis puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin ja on omiaan vaikuttamaan ennalta ehkäisevästi perusoikeuskirjan 11 artiklassa taatun sananvapauden harjoittamiseen.

187 On korostettava, että päätelaitteen sijaintipaikan määrittämisen mahdollistavasta reaaliajassa tapahtuvasta tietojen keräämisestä aiheutuva puuttuminen on erityisen vakavaa, koska nämä tiedot tarjoavat toimivaltaisille kansallisille viranomaisille keinon seurata täsmällisesti ja jatkuvasti matkapuhelinten käyttäjien liikkumista. Koska näitä tietoja on siis pidettävä erityisen arkaluonteisina, toimivaltaisten viranomaisten oikeus saada tällaisia tietoja reaaliajassa on erotettava kyseisten tietojen saamisesta viiveellä, sillä tietojen saaminen reaaliajassa on rajoittavampaa siltä osin kuin se mahdollistaa näiden käyttäjien lähes täydellisen valvonnan (ks. analogisesti Euroopan ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomio 8.2.2018, Ben Faiza v. Ranska, CE:ECHR:2018:0208JUD003144612, 74 kohta). Tämän puuttumisen intensiteetti on lisäksi vielä merkittävämpää silloin, kun reaaliaikainen kerääminen ulottuu myös asianomaisten henkilöiden liikennetietoihin.

188 Vaikka pääasiassa kyseessä olevan kansallisen säännöstön tavoitteena oleva terrorismin torjunta voi tärkeytensä perusteella oikeuttaa puuttumisen, jota reaaliajassa tapahtuva liikenne- ja paikkatietojen kerääminen merkitsee, tällainen toimenpide voidaan erityisen rajoittavuutensa vuoksi kohdistaa vain sellaisiin henkilöihin, joiden osalta on olemassa pätevä syy epäillä, että he osallistuvat tavalla tai toisella terrorismiin. Tähän ryhmään kuulumattomien henkilöiden tietojen osalta on todettava, että niiden saaminen on mahdollista vain viiveellä, koska tietoja voidaan unionin tuomioistuimen oikeuskäytännön mukaan saada vain erityisissä tilanteissa, kuten tilanteissa, joissa on kyse terrorismista, ja jos olemassa on objektiivisia seikkoja, joiden perusteella voidaan katsoa, että näillä

tiedoilla voitaisiin konkreettisessa tapauksessa tosiasiallisesti myötävaikuttaa terrorismin torjumiseen (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 119 kohta oikeuskäytäntöviittauksineen).

189 Lisäksi päätöksen, jolla annetaan lupa liikenne- ja paikkatietojen keräämiseen reaaliajassa, on perustuttava kansallisessa lainsäädännössä säädettyihin objektiivisiin kriteereihin. Tässä lainsäädännössä on erityisesti määriteltävä tämän tuomion 176 kohdassa mainitun oikeuskäytännön mukaisesti ne olosuhteet ja edellytykset, joiden täyttyessä tällaiseen keräämisen voidaan myöntää lupa, ja säädettävä, että – kuten edellä olevassa kohdassa on täsmennetty – kyse voi olla pelkästään henkilöistä, jotka liittyvät terrorismin ehkäisemistä koskevaan tavoitteeseen. Lisäksi päätöksen, jolla annetaan lupa liikenne- ja paikkatietojen keräämiseen reaaliajassa, on perustuttava kansallisessa lainsäädännössä säädettyihin objektiivisiin ja syrjimättömiin kriteereihin. Sen takaamiseksi, että näitä edellytyksiä noudatetaan käytännössä, on olennaista, että keräämisen reaaliajassa sallivan toimenpiteen toteuttaminen saatetaan joko tuomioistuimen tai sellaisen riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, etukäteisvalvontaan, ja kyseisen tuomioistuimen tai elimen on muun muassa varmistauduttava siitä, että tällainen tietojen kerääminen reaaliajassa sallitaan ainoastaan täysin välttämättömän rajoissa (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 120 kohta). Asianmukaisesti perustellussa kiireellisessä tapauksessa valvonta on suoritettava viipymättä.

Tiedon antaminen henkilöille, joiden tiedot on kerätty tai analysoitu

190 On tärkeää, että toimivaltaiset kansalliset viranomaiset, jotka keräävät reaaliajassa liikenne- ja paikkatietoja, antavat siitä tiedon asianomaisille henkilöille sovellettavien kansallisten menettelyjen yhteydessä siltä osin kuin ja heti kun kyseinen ilmoittaminen ei ole omiaan vaarantamaan kyseisille virnaomaisille kuuluvia tehtäviä. Tämä tiedon antaminen on näet välttämätöntä, jotta kyseiset henkilöt voivat käyttää perusoikeuskirjan 7 ja 8 artiklaan perustuvia oikeuksiaan pyytää oikeutta saada tutustua kyseisten toimenpiteiden kohteena oleviin henkilötietoihin ja mahdollisesti pyytää niiden oikaisemista tai poistamista sekä hakea perusoikeuskirjan 47 artiklan ensimmäisen kohdan mukaisesti tehokasta oikeussuojaa tuomioistuimessa; viimeksi mainittu oikeus taataan lisäksi nimenomaisesti asetuksen 2002/58 15 artiklan 2 kohdassa, luettuna yhdessä direktiivin 2016/679 79 artiklan 1 kohdan kanssa (ks. vastaavasti tuomio 21.12.2016, Tele2, C-203/15 ja C-698/15, EU:C:2016:970, 121 kohta oikeuskäytäntöviittauksineen ja lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 219 ja 220 kohta).

191 Tiedon antamisesta liikenne- ja paikkatietojen automaattisen analysoinnin yhteydessä on todettava, että toimivaltaisen kansallisen viranomaisen on julkaistava tätä analyysiä koskevia yleisluonteisia tietoja tarvitsematta antaa asianomaisille henkilöille tietoa erikseen. Sitä vastoin tilanteessa, jossa tiedot vastaavat siinä toimenpiteessä täsmennettyjä parametrejä, jolla annetaan lupa automaattiseen analyysiin, ja jossa kyseinen viranomainen tunnistaa asianomaisen henkilön analysoidakseen häntä koskevia tietoja yksityiskohtaisemmin, tiedon antaminen kyseiselle henkilölle erikseen on tarpeen. Tieto on kuitenkin annettava vain siltä osin kuin ja vasta siitä lähtien kun se ei ole omiaan vaarantamaan mainitulle viranomaiselle kuuluvia tehtäviä (ks. analogisesti lausunto 1/15 (EU:n ja Kanadan välinen PNR-sopimus), 26.7.2017, EU:C:2017:592, 222–224 kohta).

192 Edellä esitettyjen seikkojen perusteella asiassa C-511/18 esitettyihin toiseen ja kolmanteen kysymykseen on vastattava, että direktiivin 2002/58 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se ei ole esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on yhtäältä analysoitava automaattisesti ja kerättävä reaaliajassa muun muassa liikenne- ja paikkatietoja ja toisaalta kerättävä reaaliajassa käytettyjen päätelaitteiden sijaintipaikkaa koskevia teknisiä tietoja, kun

– automaattinen analysointi rajoittuu tilanteisiin, joissa jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa tähän analysointiin tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on tilanne, joka oikeuttaa mainitun toimenpiteen, ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan, ja

– liikenne- ja paikkatietojen kerääminen reaaliajassa on rajattu henkilöihin, joiden osalta on olemassa pätevä syy epäillä, että he osallistuvat tavalla tai toisella terrorismiin, ja keräämistä valvotaan etukäteen joko tuomioistuimessa tai riippumattomassa hallinnollisessa elimessä, jonka ratkaisu on sitova, sen varmistamiseksi, että tällainen reaaliajassa tapahtuva tietojen kerääminen sallitaan ainoastaan täysin välttämättömän rajoissa. Asianmukaisesti perustellussa kiireellisessä tapauksessa valvonta on suoritettava viipymättä.

Toinen kysymys asiassa C-512/18

193 Asiassa C-512/18 esittämällään toisella kysymyksellä ennakkoratkaisua pyytänyt tuomioistuin pyrkii lähinnä selvittämään, onko direktiivin 2000/31 säännöksiä, luettuina perusoikeuskirjan 6–8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, tulkittava siten, että ne ovat esteenä kansalliselle säännöstölle, jonka mukaan yhteyttä yleisölle tarkoitettuihin verkkoviestintäpalveluihin tarjoavien toimijoiden ja hosting-palvelujen tarjoajien on säilytettävä yleisesti ja erotuksetta muun muassa kyseisiin palveluihin liittyvät henkilötiedot.

194 Vaikka ennakkoratkaisua pyytänyt tuomioistuin katsoo, että tällaiset palvelut kuuluvat direktiivin 2000/31 eivätkä direktiivin 2002/58 soveltamisalaan, se on sitä mieltä, että direktiivin 2000/31 15 artiklan 1 ja 2 kohdalla, luettuna yhdessä sen 12 ja 14 artiklan kanssa, ei sellaisenaan oteta käyttöön sisällön luomiseen liittyvien tietojen säilyttämistä koskevaa periaatteellista kieltoa, josta voitaisiin poiketa ainoastaan poikkeuksellisesti. Kyseinen tuomioistuin pohtii kuitenkin, onko tämä arviointi hyväksyttävissä, kun otetaan huomioon perusoikeuskirjan 6–8 ja 11 artiklassa vahvistettujen perusoikeuksien välttämätön noudattaminen.

195 Ennakkoratkaisua pyytänyt tuomioistuin täsmentää lisäksi, että sen kysymys koskee LCEN:n 6 §:ssä, luettuna yhdessä asetuksen nro 2011-219 kanssa, säädettyä säilyttämisvelvollisuutta. Tiedot, jotka asianomaisten palveluntarjoajien on säilytettävä tällä perusteella, sisältävät muun muassa näitä palveluja käyttäneiden henkilöiden henkilöllisyyttä koskevat tiedot, kuten heidän nimensä, etunimensä, heidän niihin liittyvät postiosoitteensa, heidän niihin liittyvät sähköpostiosoitteensa tai tilinsä, heidän salasanansa ja, jos sopimus tai tili on maksullinen, käytetty maksutyyppi, maksun viitenumero, määrä sekä maksutapahtuman päivämäärä ja kellonaika.

196 Säilyttämisvelvollisuuden piiriin kuuluvat tiedot kattavat myös tilaajien, yhteyksien ja käytettyjen päätelaitteiden tunnistenumerot, sisällöille annetut tunnistenumerot, yhteyksien ja tapahtumien alkamisen ja päättymisen päivämäärät ja kellonajat sekä protokollatyypit, joita käytetään palveluun liittymisessä ja sisältöjen siirtämisessä. Näiden tietojen, joita säilytetään vuoden ajan, saantia voidaan pyytää rikos- ja siviiliprosesseissa siviili- tai rikosoikeudellista vastuuta koskevien sääntöjen noudattamisen varmistamiseksi sekä sellaisten tiedonhankintatoimenpiteiden yhteydessä, joihin sovelletaan CSI:n L. 851-1 §:ää.

197 Tältä osin on huomautettava, että direktiivin 2000/31 1 artiklan 2 kohdan mukaan kyseisellä direktiivillä lähennetään tiettyjä sen 2 artiklan a alakohdassa tarkoitettuihin tietoyhteiskunnan palveluihin sovellettavia kansallisia säännöksiä.

198 Tietoyhteiskunnan palvelut kattavat tosin etäpalveluina tietoja elektronisesti käsittelevien ja säilyttävien laitteiden avulla palvelun vastaanottajan henkilökohtaisesta pyynnöstä tarjottavat palvelut, joista tavallisesti maksetaan korvaus, kuten internet- tai viestintäverkkoyhteyspalvelut tai hosting-palvelut (ks. vastaavasti tuomio 24.11.2011, Scarlet Extended, C-70/10, EU:C:2011:771, 40 kohta; tuomio 16.12.2012, SABAM, C-360/10, EU:C:2012:85, 34 kohta; tuomio 15.9.2016, Mc Fadden, C-484/14, EU:C:2016:689, 55 kohta ja tuomio 7.8.2018, SNB-REACT, C-521/17, EU:C:2018:639, 42 kohta oikeuskäytäntöviittauksineen).

199 Direktiivin 2000/31 1 artiklan 5 kohdassa säädetään kuitenkin, ettei kyseistä direktiiviä sovelleta direktiivien 95/46 ja 97/66 soveltamisalaan kuuluviin tietoyhteiskunnan palveluihin liittyviin kysymyksiin. Direktiivin 2000/31 johdanto-osan 14 ja 15 perustelukappaleesta ilmenee tältä osin, että viestinnän luottamuksellisuuden suojaa ja yksilöiden suojelua henkilötietojen käsittelyssä tietoyhteiskunnan palvelujen yhteydessä säännellään yksinomaan direktiiveillä 95/46 ja 97/66, ja viimeksi mainitun direktiivin 5 artiklassa kielletään viestinnän luottamuksellisuuden suojaamiseksi kaikenlainen viestinnän kuuntelu tai valvonta.

200 Viestinnän luottamuksellisuuden ja henkilötietojen suojaan liittyviä kysymyksiä on siten arvioitava direktiivin 97/66 korvanneen direktiivin 2002/58 ja direktiivin 95/46 korvanneen asetuksen 2016/679 perusteella, ja suojalla, joka direktiivillä 2000/31 pyritään varmistamaan, ei saada missään tapauksessa rajoittaa direktiivistä 2002/58 ja asetuksesta 2016/679 johtuvia vaatimuksia (ks. vastaavasti tuomio 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, 57 kohta).

201 Tämän tuomion 195 kohdassa tarkoitetussa kansallisessa säännöstössä yhteyttä yleisölle tarkoitettuihin viestintäpalveluihin tarjoaville toimijoille ja hosting-palvelujen tarjoajille asetettua velvollisuutta säilyttää näihin palveluihin liittyviä henkilötietoja on siis – kuten julkisasiamies on antamansa ratkaisuehdotuksen La Quadrature du Net ym. (C-511/18 ja C-512/18, EU:C:2020:6) 141 kohdassa todennut – arvioitava direktiivin 2002/58 tai asetuksen 2016/679 valossa.

202 Siitä riippuen, sovelletaanko tämän kansallisen säännöstön piiriin kuuluvien palvelujen tarjoamiseen direktiiviä 2002/58, sitä säännellään joko viimeksi mainitulla direktiivillä ja erityisesti sen 15 artiklan 1 kohdalla, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, tai asetuksella 2016/679 ja erityisesti mainitun asetuksen 23 artiklan 1 kohdalla, luettuna näiden perusoikeuskirjan samojen määräysten valossa.

203 Nyt käsiteltävässä asiassa ei voida pitää mahdottomana, että – kuten Euroopan komissio on kirjallisissa huomautuksissaan todennut – tietyt palvelut, joihin sovelletaan tämän tuomion 195 kohdassa tarkoitettua kansallista säännöstöä, ovat direktiivissä 2002/58 tarkoitettuja sähköisiä viestintäpalveluja, mikä ennakkoratkaisua pyytäneen tuomioistuimen on tarkastettava.

204 Tältä osin on huomautettava, että direktiivi 2002/58 kattaa sähköiset viestintäpalvelut, jotka täyttävät edellytykset, jotka on asetettu direktiivin 2002/21 2 artiklan c alakohdassa, johon direktiivin 2002/58 2 artiklassa viitataan ja jossa määritellään sähköinen viestintäpalvelu siten, että sillä tarkoitetaan ”tavallisesti korvausta vastaan suoritettuja palveluja, jotka muodostuvat kokonaan tai pääosin signaalien siirtämisestä sähköisissä viestintäverkoissa, mukaan lukien televiestintäpalvelut ja siirtopalvelut radio- ja televisiotoiminnassa käytetyissä verkoissa”. Tämän tuomion 197 ja 198 kohdassa tarkoitettujen kaltaisten ja direktiivin 2000/31 soveltamisalaan kuuluvien tietoyhteiskunnan palvelujen osalta on todettava, että ne ovat sähköisiä viestintäpalveluja, jos ne muodostuvat kokonaan tai pääosin signaalien siirtämisestä sähköisissä viestintäverkoissa (ks. vastaavasti tuomio 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, 47 ja 48 kohta).

205 Internetyhteyspalvelut, jotka ilmeisesti kuuluvat tämän tuomion 195 kohdassa tarkoitetun kansallisen säännöstön soveltamisalaan, ovat, kuten direktiivin 2002/21 johdanto-osan kymmenennessä perustelukappaleessa vahvistetaan, kyseisessä direktiivissä tarkoitettuja sähköisiä viestintäpalveluja (ks. vastaavasti tuomio 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, 37 kohta). Tämä pätee

myös internetpohjaisiin sähköpostipalveluihin, joiden osalta ei näytä olevan poissuljettua, että myös ne kuuluvat kyseisen kansallisen säännöstön soveltamisalaan, jos ne tekniseltä kannalta edellyttävät kokonaan tai pääosin signaalien siirtämistä sähköisissä viestintäverkoissa (ks. vastaavasti tuomio 13.6.2019, Google, C-193/18, EU:C:2019:498, 35 ja 38 kohta).

206 Direktiivin 2002/58 15 artiklan 1 kohdasta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, johtuvien vaatimusten osalta on viitattava kaikkiin toteamuksiin ja arviointeihin, jotka on esitetty asioissa C-511/18 ja C-512/18 esitettyihin ensimmäisiin kysymyksiin sekä asiassa C-520/18 esitettyihin ensimmäiseen ja toiseen kysymykseen annetun vastauksen yhteydessä.

207 Asetuksesta 2016/679 johtuvista vaatimuksista on muistutettava, että kyseisellä asetuksella pyritään, kuten sen johdanto-osan kymmenennestä perustelukappaleesta ilmenee, muun muassa varmistamaan luonnollisten henkilöiden korkeatasoinen suojelu unionissa ja tätä varten varmistamaan näiden henkilöiden perusoikeuksien ja -vapauksien suojelua henkilötietojen käsittelyssä koskevien sääntöjen johdonmukainen ja yhtenäinen soveltaminen kaikkialla unionissa (ks. vastaavasti tuomio 16.7.2020, Facebook Ireland ja Schrems, C-311/18, EU:C:2020:559, 101 kohta).

208 Tätä varten henkilötietojen käsittelyssä on noudatettava asetuksen 2016/679 II luvussa mainittuja henkilötietojen käsittelyä koskevia periaatteita ja sen III luvussa vahvistettuja rekisteröidyn oikeuksia, jollei kyseisen asetuksen 23 artiklassa säädetyistä poikkeuksista muuta johdu. Erityisesti on todettava, että henkilötietojen käsittelyn on yhtäältä oltava mainitun asetuksen 5 artiklassa ilmaistujen periaatteiden mukaista ja toisaalta täytettävä saman asetuksen 6 artiklassa luetellut lainmukaisuuden edellytykset (ks. analogisesti direktiivin 95/46 osalta tuomio 30.5.2013, Worten, C-342/12, EU:C:2013:355, 33 kohta oikeuskäytäntöviittauksineen).

209 Erityisesti asetuksen 2016/679 23 artiklan 1 kohdasta on todettava, että – samalla tavalla kuin direktiivin 2002/58 15 artiklan 1 kohdassa säädetään – siinä annetaan jäsenvaltioille mahdollisuus rajoittaa siinä säädettyjen tavoitteiden kannalta lainsäädäntötoimenpiteillä siinä mainittujen velvollisuuksien ja oikeuksien ulottuvuutta, ”jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide, jotta voidaan taata” asetettu tavoite. Kaikkien tämän perusteella toteutettujen lainsäädäntötoimenpiteiden on erityisesti oltava kyseisen asetuksen 23 artiklan 2 kohdassa asetettujen erityisvaatimusten mukaisia.

210 Asetuksen 2016/679 23 artiklan 1 ja 2 kohtaa ei siten voida tulkita siten, että niissä voitaisiin antaa jäsenvaltioille valta puuttua yksityiselämän kunnioittamiseen perusoikeuskirjan 7 artiklan vastaisesti tai muihin perusoikeuskirjassa määrättyihin takeisiin (ks. analogisesti direktiivin 95/46 osalta tuomio 20.5.2003, Österreichischer Rundfunk ym., C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, 91 kohta). Kuten tilanne on direktiivin 2002/58 15 artiklan 1 kohdan osalta, asetuksen 2016/679 23 artiklan 1 kohdassa jäsenvaltioille annettua valtaa voidaan erityisesti käyttää vain noudattamalla oikeasuhteisuutta koskevaa vaatimusta, jonka mukaan poikkeukset henkilötietojen suojaan ja sitä koskevat rajoitukset on toteutettava täysin välttämättömän rajoissa (ks. analogisesti direktiivin 95/46 osalta tuomio 7.11.2013, IPI, C-473/12, EU:C:2013:715, 39 kohta oikeuskäytäntöviittauksineen).

211 Tästä seuraa, että asioissa C-511/18 ja C-512/18 esitettyihin ensimmäisiin kysymyksiin sekä asiassa C-520/18 esitettyihin ensimmäiseen ja toiseen kysymykseen annetun vastauksen yhteydessä esitettyjä toteamuksia ja arviointeja sovelletaan soveltuvin osin asetuksen 2016/679 23 artiklaan.

212 Edellä esitetyn perusteella asiassa C-512/18 esitettyyn toiseen kysymykseen on vastattava, että direktiiviä 2000/31 on tulkittava siten, että sitä ei sovelleta viestinnän luottamuksellisuuden suojaan ja yksilöiden suojeluun henkilötietojen käsittelyssä tietoyhteiskunnan palvelujen yhteydessä, koska tätä suojaa säännellään tapauksen mukaan direktiivillä 2002/58 tai asetuksella 2016/679. Asetuksen

2016/679 23 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se on esteenä kansalliselle säännöstölle, jonka mukaan yhteyttä yleisölle tarkoitettuihin viestintäpalveluihin tarjoavien toimijoiden ja hosting-palvelujen tarjoajien on säilytettävä yleisesti ja erotuksetta muun muassa kyseisiin palveluihin liittyvät henkilötiedot.

Kolmas kysymys asiassa C-520/18

213 Asiassa C-520/18 esittämällään kolmannella kysymyksellä ennakkoratkaisua pyytänyt tuomioistuin pyrkii selvittämään, voiko kansallinen tuomioistuin soveltaa kansallisen oikeutensa säännöstä, jossa sille annetaan toimivalta rajoittaa ajallisesti sellaisen lainvastaisuutta koskevan toteamuksen vaikutuksia, joka sen on kyseisen oikeuden nojalla tehtävä kansallisesta lainsäädännöstä, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on muun muassa kansallisen turvallisuuden takaamista ja rikollisuuden torjuntaa koskeviin tavoitteisiin pyrittäessä säilytettävä yleisesti ja erotuksetta liikenne- ja paikkatietoja, ja joka perustuu siihen, että kyseinen lainsäädäntö on ristiriidassa direktiivin 2002/58 15 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, kanssa.

214 Unionin oikeuden ensisijaisuuden periaatteella vahvistetaan unionin oikeuden etusija jäsenvaltioiden oikeuteen nähden. Kyseinen periaate velvoittaa siis kaikki jäsenvaltioiden elimet huolehtimaan unionin eri oikeussääntöjen täyden vaikutuksen toteutumisesta, eikä jäsenvaltioiden oikeudella voida puuttua siihen vaikutukseen, joka näillä eri oikeussäännöillä katsotaan olevan mainittujen valtioiden alueella (tuomio 15.7.1964, Costa, 6/64, EU:C:1964:66, s. 1159 ja s. 1160 ja tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus), C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 157 ja 158 kohta oikeuskäytäntöviittauksineen).

215 Ensisijaisuusperiaatteen mukaan on niin, että jos kansallinen tuomioistuin, jonka tehtävänä on toimivaltansa puitteissa soveltaa unionin oikeuden säännöksiä ja määräyksiä, ei voi tulkita kansallista säännöstöä unionin oikeuden vaatimusten mukaisesti, sillä on velvollisuus varmistaa kyseisten säännösten ja määräysten täysi vaikutus ja jättää tarvittaessa omasta aloitteestaan soveltamatta kaikkia unionin oikeuden kanssa ristiriidassa olevia, myös myöhemmin annettuja kansallisen lainsäädännön säännöksiä ilman, että sen olisi pyydettävä tai odotettava, että tällainen säännös ensin poistetaan lainsäädäntöteitse tai jollakin muulla perustuslain mukaisella keinolla (tuomio 22.6.2010, Melki ja Abdeli, C-188/10 ja C-189/10, EU:C:2010:363, 43 kohta oikeuskäytäntöviittauksineen ja tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus), C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 160 kohta).

216 Ainoastaan unionin tuomioistuin voi poikkeustapauksissa ja oikeusvarmuutta koskevista pakottavista syistä lykätä tilapäisesti unionin oikeuden säännön syrjäyttävää vaikutusta sen kanssa ristiriidassa olevaan kansallisen oikeuden sääntöön nähden. Unionin tuomioistuimen unionin oikeudesta esittämän tulkinnan vaikutuksia voidaan rajoittaa tällä tavalla ajallisesti ainoastaan siinä samassa tuomiossa, jossa annetaan pyydetty tulkintaratkaisu (ks. vastaavasti tuomio 23.10.2012, Nelson ym., C-581/10 ja C-629/10, EU:C:2012:657, 89 ja 91 kohta; tuomio 23.4.2020, Herst, C-401/18, EU:C:2020:295, 56 ja 57 kohta ja tuomio 25.6.2020, A ym. (Tuulivoimalat – Aalter ja Nevele), C-24/19, EU:C:2020:503, 84 kohta oikeuskäytäntöviittauksineen).

217 Unionin oikeuden ensisijaisuutta ja yhtenäistä soveltamista näet heikennettäisiin, jos kansallisilla tuomioistuimilla olisi toimivalta antaa kansallisille säännöksille etusija, vaikka vain väliaikaisesti, siihen unionin oikeuteen nähden, jota niillä rikotaan (ks. vastaavasti tuomio 29.7.2019, Inter-Environnement Wallonie ja Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, 177 kohta oikeuskäytäntöviittauksineen).

218 Unionin tuomioistuin on kuitenkin katsonut asiassa, jossa oli kyse sellaisten toimenpiteiden lainmukaisuudesta, jotka oli toteutettu noudattamatta unionin oikeudessa asetettua velvollisuutta arvioida etukäteen hankkeen ympäristövaikutukset suojeltuun alueeseen, että kansallinen tuomioistuin voi kansallisen lainsäädännön sen salliessa poikkeuksellisesti pysyttää tällaisten toimenpiteiden vaikutukset, jos vaikutusten pysyttäminen on perusteltua sellaisten pakottavien syiden vuoksi, jotka liittyvät tarpeeseen estää sellainen todellinen ja vakava vaara, että sähköntoimitus kyseisessä jäsenvaltiossa keskeytyy, kun tätä vaaraa ei voida torjua muilla keinoilla ja vaihtoehdoilla erityisesti sisämarkkinoilla, mutta tällainen vaikutusten pysyttäminen voi kestää vain ajan, joka on täysin välttämätön kyseisen lainvastaisuuden korjaamiseksi (ks. vastaavasti tuomio 29.7.2019, Inter-Environnement Wallonie ja Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, 175, 176, 179 ja 181 kohta).

219 Ympäristönsuojelun erityisalalla suoritettavan hankkeen vaikutusten ennakkoarvioinnin kaltaisen menettelyllisen velvollisuuden noudattamatta jättämisestä poiketen direktiivin 2002/58 15 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, rikkomista ei voida kuitenkaan korjata menettelyllä, joka on verrattavissa edellä olevassa kohdassa mainittuun menettelyyn. Pääasiassa kyseessä olevan kaltaisen kansallisen lainsäädännön vaikutusten pysyttäminen merkitsisi nimittäin sitä, että tässä lainsäädännössä asetetaan edelleen sähköisten viestintäpalvelujen tarjoajille velvollisuuksia, jotka ovat unionin oikeuden vastaisia ja joilla puututaan vakavasti niiden henkilöiden perusoikeuksiin, joiden tietoja on säilytetty.

220 Ennakkoratkaisua pyytänyt tuomioistuin ei siis voi soveltaa kansallisen oikeutensa säännöstä, jossa sille annetaan toimivalta rajoittaa ajallisesti sellaisen lainvastaisuutta koskevan toteamuksen vaikutuksia, joka sen on tehtävä kyseisen oikeuden nojalla pääasiassa kyseessä olevan kansallisen lainsäädännön osalta.

221 VZ, WY ja XX väittävät unionin tuomioistuimelle toimittamissaan huomautuksissa kuitenkin, että kolmannessa kysymyksessä tuodaan esiin implisiittisesti mutta väistämättä kysymys siitä, onko unionin oikeus esteenä sille, että rikosprosessissa hyödynnetään tietoja ja todisteita, jotka on hankittu unionin oikeuden vastaisella liikenne- ja paikkatietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä.

222 Hyödyllisen vastauksen antamiseksi ennakkoratkaisua pyytäneelle tuomioistuimelle on tältä osin muistutettava, että unionin oikeuden nykytilassa lähtökohtaisesti yksinomaan kansallisessa oikeudessa on määritettävä säännöt, jotka koskevat sellaisten tietojen ja todisteiden, jotka on hankittu tällaisella unionin oikeuden vastaisella tietojen säilyttämisellä, hyväksyttävyyttä ja arviointia rikosprosessissa, joka on pantu vireille vakavista rikoksista epäiltyjä henkilöitä vastaan.

223 Vakiintuneen oikeuskäytännön mukaan on näet niin, että silloin, kun unioni ei ole antanut asiaa koskevia sääntöjä, kunkin jäsenvaltion asiana on menettelyllisen autonomian periaatteen nojalla antaa sisäisessä oikeusjärjestyksessään menettelysäännöt sellaisia oikeussuojakeinoja varten, joilla pyritään turvaamaan unionin oikeuteen perustuvat yksityisten oikeudet, sillä edellytyksellä kuitenkin, että kyseiset säännöt eivät ole epäedullisempia kuin säännöt, jotka koskevat samankaltaisia jäsenvaltion kansallisen oikeuden soveltamisalaan kuuluvia tilanteita (vastaavuusperiaate), eivätkä ne ole sellaisia, että unionin oikeudessa vahvistettujen oikeuksien käyttäminen on käytännössä mahdotonta tai suhteettoman vaikeaa (tehokkuusperiaate) (ks. vastaavasti tuomio 6.10.2015, Târşia, C-69/14, EU:C:2015:662, 26 ja 27 kohta; tuomio 24.10.2018, XC ym., C-234/17, EU:C:2018:853, 21 ja 22 kohta oikeuskäytäntöviittauksineen ja tuomio 19.12.2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, 33 kohta).

224 Vastaavuusperiaatteesta on todettava, että kansallisen tuomioistuimen, jossa on vireillä rikosprosessi, joka perustuu direktiiviin 2002/58 perustuvien vaatimusten vastaisesti hankittuihin tietoihin tai todisteisiin, on tarkastettava, säädetäänkö kyseistä prosessia sääntelevässä kansallisessa oikeudessa

säännöistä, jotka ovat tällaisten tietojen ja todisteiden hyväksyttävyyden ja hyödyntämisen osalta epäedullisempia kuin säännöt, jotka koskevat tietoja ja todisteita, jotka on hankittu kansallisen oikeuden vastaisesti.

225 Tehokkuusperiaatteesta on todettava, että tietojen ja todisteiden hyväksyttävyyttä ja hyödyntämistä koskevien kansallisten sääntöjen tavoitteena on kansallisessa oikeudessa tehtyjen valintojen perusteella välttää se, että lainvastaisesti hankituilla tiedoilla ja todisteilla vahingoitetaan perusteettomasti henkilöä, jonka epäillään tehneen rikoksia. Tämä tavoite voidaan kuitenkin kansallisen oikeuden mukaan saavuttaa paitsi kiellolla hyödyntää tällaisia tietoja ja todisteita myös kansallisilla säännöillä ja käytännöillä, joilla säännellään tietojen ja todisteiden arviointia ja punnintaa, tai ottamalla huomioon niiden lainvastaisuus rangaistusta määritettäessä.

226 Unionin tuomioistuimen oikeuskäytännöstä ilmenee kuitenkin, että tarvetta sulkea pois tiedot ja todisteet, jotka on hankittu unionin oikeuden vaatimusten vastaisesti, on arvioitava muun muassa ottamalla huomioon se vaara, joka tällaisten tietojen ja todisteiden hyväksyttävyydestä aiheutuu kontradiktorisen periaatteen ja näin ollen oikeudenmukaista oikeudenkäyntiä koskevan oikeuden noudattamiselle (ks. vastaavasti tuomio 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, 76 ja 77 kohta). Tuomioistuimen, joka katsoo, ettei asianosainen voi tehokkaasti ilmaista käsitystään todistuskeinosta, joka kuuluu alalle, jota tuomarit eivät tunne, ja joka voi vaikuttaa ratkaisevalla tavalla tosiseikkojen arviointiin, on kuitenkin todettava oikeudenmukaista oikeudenkäyntiä koskevan oikeuden loukkaaminen ja suljettava pois tämä todistuskeino tällaisen loukkaamisen välttämiseksi (ks. vastaavasti tuomio 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, 78 ja 79 kohta).

227 Tehokkuusperiaate velvoittaa näin ollen kansallisen rikostuomioistuimen jättämään huomiotta tiedot ja todisteet, jotka on hankittu unionin oikeuden vastaisella liikenne- ja paikkatietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä, rikosprosessissa, joka on pantu vireille sellaisia henkilöitä vastaan, joiden epäillään syyllistyneen rikoksiin, jos kyseiset henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä tiedoista ja todisteista, jotka ovat peräisin alalta, jota tuomarit eivät tunne, ja jotka voivat vaikuttaa ratkaisevalla tavalla tosiseikkojen arviointiin.

228 Edellä esitetyn perusteella asiassa C-520/18 esitettyyn kolmanteen kysymykseen on vastattava, että kansallinen tuomioistuin ei voi soveltaa kansallisen oikeutensa säännöstä, jossa sille annetaan toimivalta rajoittaa ajallisesti sellaisen lainvastaisuutta koskevan toteamuksen vaikutuksia, joka sen on kyseisen oikeuden nojalla tehtävä kansallisesta lainsäädännöstä, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on muun muassa kansallisen turvallisuuden takaamista ja rikollisuuden torjuntaa koskeviin tavoitteisiin pyrittäessä säilytettävä direktiivin 2002/58 15 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, vastaisesti liikenne- ja paikkatietoja yleisesti ja erotuksetta. Kun kyseistä 15 artiklan 1 kohtaa tulkitaan tehokkuusperiaatteen valossa, siinä edellytetään, että kansallinen rikostuomioistuin jättää huomiotta tiedot ja todisteet, jotka on hankittu unionin oikeuden vastaisella liikenne- ja paikkatietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä, rikosprosessissa, joka on pantu vireille sellaisia henkilöitä vastaan, joiden epäillään syyllistyneen rikoksiin, jos kyseiset henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä tiedoista ja todisteista, jotka ovat peräisin alalta, jota tuomarit eivät tunne, ja jotka voivat vaikuttaa ratkaisevalla tavalla tosiseikkojen arviointiin.

Oikeudenkäyntikulut

229 Pääasioiden asianosaisten osalta asioiden käsittely unionin tuomioistuimessa on välivaihe kansallisissa tuomioistuimissa vireillä olevien asioiden käsittelyssä, minkä vuoksi kansallisten tuomioistuinten asiana on päättää oikeudenkäyntikulujen korvaamisesta. Oikeudenkäyntikuluja, jotka ovat aiheutuneet muille kuin näille asianosaisille huomautusten esittämisestä unionin tuomioistuimelle, ei voida määrätä korvattaviksi.

Näillä perusteilla unionin tuomioistuin (suuri jaosto) on ratkaissut asiat 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), sellaisena kuin se on muutettuna 25.11.2009 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY, 15 artiklan 1 kohtaa, luettuna Euroopan unionin perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se on esteenä lainsäädännöllisille toimenpiteille, joissa säädetään kyseisessä 15 artiklan 1 kohdassa säädettyjä tarkoituksia varten ennakoivasti liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä. Direktiivin 2002/58, sellaisena kuin se on muutettuna direktiivillä 2009/136, 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei sitä vastoin ole esteenä lainsäädännöllisille toimenpiteille, joissa**

   – **sallitaan kansallisen turvallisuuden takaamiseksi se, että sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään liikenne- ja paikkatiedot yleisesti ja erotuksetta tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa päätökseen, jolla tällainen määräys annetaan, tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan; mainittu määräys voidaan antaa ainoastaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa, jos kyseinen uhka on edelleen olemassa**

   – **säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi liikenne- ja paikkatietojen kohdennetusta säilyttämisestä, joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa**

   – **säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä ajanjaksoksi, joka on rajoitettu täysin välttämättömään**

   – **säädetään kansallisen turvallisuuden suojaamiseksi, rikollisuuden torjumiseksi ja yleisen turvallisuuden suojaamiseksi sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä ja**

   – **sallitaan vakavan rikollisuuden torjumiseksi ja varsinkin kansallisen turvallisuuden takaamiseksi se, että sähköisten viestintäpalvelujen tarjoajat määrätään toimivaltaisen viranomaisen päätöksellä, johon kohdistuu tehokas tuomioistuinvalvonta, varmistamaan nopeasti kyseisten palveluntarjoajien käytössä olevien liikenne- ja paikkatietojen säilyttäminen tietyn ajan,**

   jos näillä toimenpiteillä varmistetaan selvin ja täsmällisin säännöin, että kyseessä olevien tietojen säilyttämisen ehtona on, että näihin toimenpiteisiin liittyviä aineellisia ja menettelyllisiä edellytyksiä noudatetaan, ja että asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja vastaan.

2) **Direktiivin 2002/58, sellaisena kuin se on muutettuna direktiivillä 2009/136, 15 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se ei ole esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on yhtäältä analysoitava automaattisesti ja kerättävä reaaliajassa muun muassa liikenne- ja paikkatietoja ja toisaalta kerättävä reaaliajassa käytettyjen päätelaitteiden sijaintipaikkaa koskevia teknisiä tietoja, kun**

   – **automaattinen analysointi rajoittuu tilanteisiin, joissa jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa tähän analysointiin tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on tilanne, joka oikeuttaa mainitun toimenpiteen, ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan, ja**

   – **liikenne- ja paikkatietojen kerääminen reaaliajassa on rajattu henkilöihin, joiden osalta on olemassa pätevä syy epäillä, että he osallistuvat tavalla tai toisella terrorismiin, ja keräämistä valvotaan etukäteen joko tuomioistuimessa tai riippumattomassa hallinnollisessa elimessä, jonka ratkaisu on sitova, sen varmistamiseksi, että tällainen reaaliajassa tapahtuva tietojen kerääminen sallitaan ainoastaan täysin välttämättömän rajoissa. Asianmukaisesti perustellussa kiireellisessä tapauksessa valvonta on suoritettava viipymättä.**

3) **Tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista 8.6.2000 annettua Euroopan parlamentin ja neuvoston direktiiviä 2000/31/EY (”Direktiivi sähköisestä kaupankäynnistä”) on tulkittava siten, että sitä ei sovelleta viestinnän luottamuksellisuuden suojaan ja yksilöiden suojeluun henkilötietojen käsittelyssä tietoyhteiskunnan palvelujen yhteydessä, koska tätä suojaa säännellään tapauksen mukaan direktiivillä 2002/58, sellaisena kuin se on muutettuna direktiivillä 2009/136, tai luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetulla Euroopan parlamentin ja neuvoston asetuksella (EU) 2016/679. Asetuksen 2016/679 23 artiklan 1 kohtaa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se on esteenä kansalliselle säännöstölle, jonka mukaan yhteyttä yleisölle tarkoitettuihin viestintäpalveluihin tarjoavien toimijoiden ja hosting-palvelujen tarjoajien on säilytettävä yleisesti ja erotuksetta muun muassa kyseisiin palveluihin liittyvät henkilötiedot.**

4) **Kansallinen tuomioistuin ei voi soveltaa kansallisen oikeutensa säännöstä, jossa sille annetaan toimivalta rajoittaa ajallisesti sellaisen lainvastaisuutta koskevan toteamuksen vaikutuksia, joka sen on kyseisen oikeuden nojalla tehtävä kansallisesta lainsäädännöstä, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on muun muassa kansallisen turvallisuuden takaamista ja rikollisuuden torjuntaa koskeviin tavoitteisiin pyrittäessä säilytettävä direktiivin 2002/58, sellaisena kuin se on muutettuna direktiivillä 2009/136, 15 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, vastaisesti liikenne- ja paikkatietoja yleisesti ja erotuksetta. Kun kyseistä 15 artiklan 1 kohtaa tulkitaan tehokkuusperiaatteen valossa, siinä edellytetään, että kansallinen rikostuomioistuin jättää huomiotta tiedot ja todisteet, jotka on hankittu unionin oikeuden vastaisella liikenne- ja paikkatietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä, rikosprosessissa, joka on pantu vireille sellaisia henkilöitä vastaan, joiden epäillään syyllistyneen rikoksiin, jos kyseiset henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä tiedoista ja todisteista, jotka ovat peräisin alalta, jota tuomarit eivät tunne, ja jotka voivat vaikuttaa ratkaisevalla tavalla tosiseikkojen arviointiin.**

Allekirjoitukset