Samling af Afgørelser

DOMSTOLENS DOM (Store Afdeling)

6. oktober 2020*

[Tekst berigtiget ved kendelse af 16. november 2020]

Indhold

* Processprog: fransk.

»Præjudiciel forelæggelse – behandling af personoplysninger i den elektroniske kommunikationssektor – udbydere af elektroniske kommunikationstjenester – udbydere af hostingtjenester og udbydere af internetadgang – generel og udifferentieret lagring af trafikdata og lokaliseringsdata – automatiseret dataanalyse – adgang til data i realtid – beskyttelse af den nationale sikkerhed og bekæmpelse af terrorisme – bekæmpelse af kriminalitet – direktiv 2002/58/EF – anvendelsesområde – artikel 1, stk. 3, og artikel 3 – fortrolighed af elektronisk kommunikation – beskyttelse – artikel 5 og artikel 15, stk. 1 – direktiv 2000/31/EF – anvendelsesområde – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 4, 6-8 og 11 samt artikel 52, stk. 1 – artikel 4, stk. 2, TEU«

I de forenede sager C-511/18, C-512/18 og C-520/18,

angående anmodninger om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) ved afgørelser af 26. juli 2018, indgået til Domstolen den 3. august 2018 (sag C-511/18 og sag C-512/18), og af Cour constitutionnelle (forfatningsdomstol, Belgien) ved afgørelse af 19. juli 2018, indgået til Domstolen den 2. august 2018 (sag C-520/18), i sagerne

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

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

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

Igwan.net (sag C-511/18),

mod

Premier ministre (sag C-511/18 og sag C-512/18),

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

Ministre de l'Intérieur (sag C-511/18),

Ministre des Armées (sag C-511/18), procesdeltager:

Privacy International (sag C-512/18),

Center for Democracy and Technology (sag C-512/18),

og

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

mod

Conseil des ministres,

procesdeltager:

Child Focus (sag C-520/18),

har

DOMSTOLEN (Store Afdeling),

sammensat af præsidenten, K. Lenaerts, vicepræsidenten, R. Silva de Lapuerta, afdelingsformændene J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb og L.S. Rossi samt dommerne J. Malenovský, L. Bay Larsen, T. von Danwitz (refererende dommer), C. Toader, K. Jürimäe, C. Lycourgos og N. Piçarra,

generaladvokat: M. Campos Sánchez-Bordona,

justitssekretær: fuldmægtig C. Strömholm,

på grundlag af den skriftlige forhandling og efter retsmødet den 9. og den 10. september 2019,

efter at der er afgivet indlæg af:

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

– French Data Network ved avocat Y. Padova,

– Privacy International ved avocat H. Roy,

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

– Académie Fiscale ASBL og UA ved J.-P. Riquet,

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

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

– VZ, WY og XX ved avocat D. Pattyn,

– Child Focus ved avocats N. Buisseret, K. De Meester og J. Van Cauter,

– den franske regering først ved D. Dubois, F. Alabrune, D. Colas, E. de Moustier og A.-L. Desjonquères, derefter ved D. Dubois, F. Alabrune, E. de Moustier og A.-L. Desjonquères, som befuldmægtigede,

– den belgiske regering ved J.-C. Halleux, P. Cottin og C. Pochet, som befuldmægtigede, bistået af avocats J. Vanpraet, Y. Peeters, S. Depré og E. de Lophem,

– den tjekkiske regering ved M. Smolek, J. Vláčil og O. Serdula, som befuldmægtigede,

– den danske regering først ved J. Nymann-Lindegren, M. Wolff og P. Ngo, derefter ved J. Nymann-Lindegren og M. Wolff, som befuldmægtigede,

– den tyske regering, først ved J. Möller, M. Hellmann, E. Lankenau, R. Kanitz og T. Henze, derefter ved J. Möller, M. Hellmann, E. Lankenau og R. Kanitz, som befuldmægtigede,

– den estiske regering ved N. Grünberg og A. Kalbus, som befuldmægtigede,

– Irland ved A. Joyce, M. Browne og G. Hodge, som befuldmægtigede, bistået af D. Fennelly, BL,

– den spanske regering først ved L. Aguilera Ruiz og A. Rubio González, derefter ved L. Aguilera Ruiz, som befuldmægtigede,

– den cypriotiske regering ved E. Neofytou, som befuldmægtiget,

– den lettiske regering ved V. Soņeca, som befuldmægtiget,

– den ungarske regering først ved Z. Fehér og Z. Wagner, derefter ved Z. Fehér, som befuldmægtigede,

– den nederlandske regering ved M.K. Bulterman og M.A.M. de Ree, som befuldmægtigede,

– den polske regering ved B. Majczyna, J. Sawicka og M. Pawlicka, som befuldmægtigede,

– den svenske regering først ved H. Shev, H. Eklinder, C. Meyer-Seitz og A. Falk, derefter ved H. Shev, H. Eklinder, C. Meyer-Seitz et J. Lundberg, som befuldmægtigede,

– Det Forenede Kongeriges regering ved S. Brandon, som befuldmægtiget, bistået af G. Facenna, QC, og barrister C. Knight,

– [slettet ved kendelse af 16. november 2020],

– Europa-Kommissionen først ved H. Kranenborg, M. Wasmeier og P. Costa de Oliveira, derefter ved H. Kranenborg og M. Wasmeier, som befuldmægtigede,

– Den Europæiske Tilsynsførende for Databeskyttelse ved T. Zerdick og A. Buchta, som befuldmægtigede,

og efter at generaladvokaten har fremsat forslag til afgørelse i retsmødet den 15. januar 2020,

afsagt følgende

Dom

1 Anmodningerne om præjudiciel afgørelse vedrører fortolkningen af for det første artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT 2002, L 201, s. 37), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EUT 2009, L 337, s. 11) (herefter »direktiv 2002/58«), og for det andet artikel 12-15 i Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«) (EFT 2000, L 178, s. 1), sammenholdt med artikel 4, 6-8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«) og artikel 4, stk. 2, TEU.

2 Anmodningen i sag C-511/18 er blevet indgivet i forbindelse med tvister mellem på den ene side Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs (sammenslutning af udbydere af internetadgang) og Igwan.net og på den anden side Premier ministre (premierministeren, Frankrig), Garde des Sceaux, ministre de la Justice (justitsministeren, Frankrig), ministre de l'Intérieur (indenrigsministeren, Frankrig) og ministre des Armées (forsvarsministeren, Frankrig) vedrørende lovligheden af décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (dekret 2015-1185 af 28.9.2015 om udpegning af specialiserede efterretningstjenester, JORF af 29.9.2015, tekst 1 af 97, herefter »dekret 2015-1185«), af décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekret 2015-1211 af 1.10.2015 om retstvister vedrørende anvendelse af efterretningsteknikker, som kræver tilladelse, og vedrørende datasæt af betydning for statens sikkerhed, JORF af 2.10.2015, tekst 7 af 108, herefter »dekret 2015-1211«), af 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 (dekret 2015-1639 af 11.12.2015 om udpegning af andre tjenester end specialiserede efterretningstjenester, som er godkendt til at anvende de teknikker, der er nævnt i afsnit V i bog VIII i lov om indre sikkerhed, vedtaget i medfør af artikel L. 811-4 i lov om indre sikkerhed, JORF af 12.12.2015, tekst 28 af 127, herefter »dekret 2015-1639«), og af décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (dekret 2016-67 af 29.1.2016 om teknikker til indsamling af efterretninger, JORF af 31.1.2016, tekst 2 af 113, herefter »dekret 2016-67«).

3 Anmodningen i sag C-512/18 er blevet indgivet i forbindelse med tvister mellem på den ene side French Data Network, Quadrature du Net og Fédération des fournisseurs d'accès à Internet associatifs (sammenslutning af udbydere af internetadgang) og på den anden side Premier ministre (premierministeren, Frankrig) og Garde des Sceaux, ministre de la justice (justitsministeren, Frankrig) vedrørende lovligheden af artikel R. 10-13 i code des postes et des communications électroniques (lov om postvæsen og elektronisk kommunikation, herefter »CPCE«) og af décret nº 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 (dekret 2011-219 af 25.2.2011 om lagring og kommunikation af data, der gør det muligt at identificere enhver person, der har bidraget til at skabe onlineindhold, JORF af 1.3.2011, tekst 32 af 170, herefter »dekret 2011-219«).

4 Anmodningen i sag C-520/18 er blevet indgivet i forbindelse med tvister mellem på den ene side Ordre des barreaux francophones et germanophone (forening af fransktalende og tysktalende advokater), Académie Fiscale ASBL (akademi for skatteret), UA, Liga voor Mensenrechten ASBL (forening for menneskerettigheder), Ligue des Droits de l'Homme ASBL (forening for menneskerettigheder), VZ, WY og XX og på den anden side Conseil des ministres (ministerrådet, Belgien) vedrørende lovligheden af loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (lov om indsamling og lagring af data i den elektroniske kommunikationssektor, *Moniteur belge* af 18.7.2016, s. 44717, herefter »lov af 29. maj 2016«).

Retsforskrifter

EU-retten

Direktiv 95/46

5 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31) blev ophævet med virkning fra den 25. maj 2018 ved

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46 (EUT 2016, L 119, s. 1). Artikel 3, stk. 2, i direktiv 95/46 bestemte:

»Dette direktiv gælder ikke for sådan behandling af personoplysninger,

– som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f. eks. de aktiviteter, der er fastsat i afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område

– som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.«

6 Artikel 22 i direktiv 95/46, som var indeholdt i dette direktivs kapitel III med overskriften »Retsmidler, ansvar og sanktioner«, var affattet således:

»Uden at foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanser, fastsætter medlemsstaterne bestemmelser om, at enhver har ret til for en domstol at indbringe en klage over krænkelser af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling.«

Direktiv 97/66

7 Artikel 5 med overskriften »Telekommunikationshemmeligheden« i Europa-Parlamentets og Rådets direktiv 97/66/EF af 15. december 1997 om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (EFT 1997, L 24, s. 1) bestemte:

»1. Medlemsstaterne sikrer via nationale forskrifter telekommunikationshemmeligheden ved brug af offentlige telenet og offentligt tilgængelige teletjenester. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge loven, jf. artikel 14, stk. 1.

2. Stk. 1 vedrører ikke lovmedholdelig optagelse af samtaler, der foretages som led i lovlig forretningspraksis med henblik på at kunne forelægge bevis for en handelstransaktion eller enhver anden forretningsmæssig samtale.«

Direktiv 2000/31

8 14. og 15. betragtning til direktiv 2000/31 har følgende ordlyd:

»(14) For beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger gælder alene bestemmelserne i […] direktiv [95/46] og i […] direktiv [97/66], som fuldt ud finder anvendelse på informationssamfundstjenester; disse direktiver opstiller allerede en fællesskabsretlig ramme inden for personoplysninger, og det er derfor ikke nødvendigt at behandle dette spørgsmål i nærværende direktiv for at sikre, at det indre marked fungerer efter hensigten, især med hensyn til den frie bevægelighed for personoplysninger mellem medlemsstaterne; nærværende direktiv bør gennemføres og anvendes i fuld overensstemmelse

med principperne om beskyttelse af personoplysninger, især hvad angår uopfordret kommerciel kommunikation og reglerne om formidleransvar; direktivet kan ikke forhindre anonym brug af åbne netværk som f.eks. [i]nternettet.

(15) Fortrolig behandling af meddelelser er sikret ved artikel 5 i direktiv [97/66]; medlemsstaterne skal i medfør af nævnte direktiv forbyde enhver form for opfangning eller overvågning af sådanne meddelelser af andre end afsenderen og modtageren, bortset fra tilfælde, hvor det er tilladt ifølge loven.«

9 Artikel 1 i direktiv 2000/31 har følgende ordlyd:

»1. Dette direktiv har til formål at bidrage til et velfungerende indre marked ved at sikre fri bevægelighed for informationssamfundstjenester mellem medlemsstaterne.

2. Ved dette direktiv foretages der, i det omfang det er nødvendigt for at nå det i stk. 1 omhandlede mål, en tilnærmelse af visse nationale bestemmelser om informationssamfundstjenester, som vedrører det indre marked, tjenesteydernes etablering, kommerciel kommunikation, elektroniske kontrakter, formidleransvar, adfærdskodekser, udenretslig bilæggelse af tvister, klageadgang og samarbejde mellem medlemsstaterne.

3. Dette direktiv supplerer den fællesskabsret, der finder anvendelse på informationssamfundstjenester, uden at det berører det niveau for beskyttelse af især folkesundheden og forbrugernes interesser, der er fastlagt ved Fællesskabets retsakter og den nationale lovgivning til gennemførelse heraf, forudsat at det ikke begrænser adgangen til at levere informationssamfundstjenester.

[…]

5. Dette direktiv finder ikke anvendelse på:

[…]

b) spørgsmål, der vedrører informationssamfundstjenester omfattet af direktiv [95/46] og [97/66]

[…]«

10 Artikel 2 i direktiv 2000/31 er affattet således:

»I dette direktiv forstås ved:

a) »informationssamfundstjenester«: tjenester som defineret i artikel 1, nr. 2), i [Europa-Parlamentets og Rådets] direktiv 98/34/EF [af 22.6.1998 om en informationsprocedure med hensyn til tekniske standarder og forskrifter (EFT 1998, L 204, s. 37)], som ændret ved [Europa-Parlamentets og Rådets] direktiv 98/48/EF [af 20.7.1998 (EFT 1998, L 127, s. 18)]

[…]«

11 Artikel 15 i direktiv 2000/31 bestemmer:

»1. Med hensyn til levering af de i artikel 12, 13 og 14 omhandlede tjenester må medlemsstaterne ikke pålægge tjenesteyderne en generel forpligtelse til at overvåge den information, de fremsender eller oplagrer, eller en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed.

2. Medlemsstaterne kan kræve, at leverandører af informationssamfundstjenester straks underretter de kompetente offentlige myndigheder om påståede ulovlige aktiviteter, der udøves, eller information, der leveres af deres tjenestemodtagere, eller at de på anmodning giver de kompetente myndigheder oplysninger, som gør det muligt at identificere de tjenestemodtagere, de har oplagringsaftaler med.«

Direktiv 2002/21

12 Tiende betragtning til Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) (EFT 2002, L 108, s. 33) har følgende ordlyd:

»I definitionen af informationssamfundets tjenester i artikel 1 i […] direktiv [98/34, som ændret ved direktiv 98/48] indgår en bred vifte af økonomiske online-aktiviteter: De fleste af disse aktiviteter er ikke omfattet af nærværende direktiv, da de ikke udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet. Taletelefoni og elektroniske posttjenester er omfattet af nærværende direktiv. En og samme virksomhed, [f.eks.] en [i]nternet-udbyder, kan tilbyde både elektronisk kommunikation, som f.eks. adgang til Internettet, og tjenester, som ikke er omfattet af nærværende direktiv, f.eks. levering af webbaseret indhold.«

13 Artikel 2 i direktiv 2002/21 bestemmer:

»I dette direktiv forstås ved:

[…]

c) »elektronisk kommunikationstjeneste«: en tjeneste, som normalt ydes mod betaling, og som udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet, herunder telekommunikationstjenester og transmissionstjenester på net, der anvendes til radio- og tv-spredning, men ikke tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester; begrebet omfatter ikke informationssamfundets tjenester som defineret i artikel 1 i direktiv [98/34], og som ikke udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet

[…]«

Direktiv 2002/58

14 2., 6., 7., 11., 22., 26. og 30. betragtning til direktiv 2002/58 har følgende ordlyd:

»(2) Dette direktiv søger at overholde de grundlæggende rettigheder og respektere de principper, der anerkendes i især [chartret]. Direktivet søger især at sikre fuld overholdelse af rettighederne i [chartrets] artikel 7 og 8.

[…]

(6) Internettet vender op og ned på de traditionelle markedsstrukturer, idet det udgør en fælles, global infrastruktur for fremføring af en lang række elektroniske kommunikationstjenester. Offentligt tilgængelige elektroniske kommunikationstjenester via internettet giver brugerne nye muligheder, men medfører også nye risikomomenter for deres personoplysninger og privatliv.

(7) Med hensyn til offentlige kommunikationsnet bør der træffes særlige foranstaltninger af lovgivningsmæssig, administrativ og teknisk art for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder og juridiske personers legitime interesser, navnlig mod den voksende risiko, der er forbundet med automatiseret opbevaring og behandling af oplysninger om abonnenter og brugere.

[…]

(11) Ligesom direktiv [95/46] finder dette direktiv ikke anvendelse på beskyttelse af grundlæggende rettigheder og frihedsrettigheder, der er forbundet med aktiviteter, der ikke er omfattet af [EU-]retten. Det ændrer derfor ikke den nuværende balance mellem enkeltpersoners ret til privatlivets fred og medlemsstaternes mulighed for, jf. artikel 15, stk. 1, i dette direktiv, at træffe de foranstaltninger, der er nødvendige til beskyttelse af den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område. Dette direktiv berører derfor ikke medlemsstaternes mulighed for lovligt at opfange elektronisk kommunikation eller træffe andre foranstaltninger, hvis det er nødvendigt med et af disse formål for øje og i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder[, undertegnet i Rom den 4.11.1[9]50,] som fortolket i Den Europæiske Menneskerettighedsdomstols retspraksis. Sådanne foranstaltninger skal være passende, stå i åbenbart rimeligt forhold til det mål, der forfølges, og være nødvendige i et demokratisk samfund, og foranstaltningerne bør omfattes af passende beskyttelsesordninger i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

[…]

(22) Det er ikke tanken, at forbuddet mod, at der af andre end brugerne eller uden disses samtykke lagres oplysninger og de dertil hørende trafikdata, skal omfatte enhver automatisk, mellemliggende og kortvarig lagring af denne information, når blot lagringen udelukkende sker med henblik på gennemførelse af transmissionen i de elektroniske kommunikationsnet, og oplysningerne ikke lagres længere end det tidsrum, der er nødvendigt for transmissionen og af hensyn til trafikstyringen, forudsat at sikkerhedsbeskyttelsen af oplysningerne i lagringsperioden fortsat er garanteret. […]

[…]

(26) Abonnentoplysninger, som behandles i elektroniske kommunikationsnet ved etablering af en kommunikationsforbindelse og fremføring af information, indeholder oplysninger om fysiske personers privatliv og vedrører retten til respekt for deres korrespondance eller vedrører juridiske personers legitime interesser. Sådanne data må kun lagres i det omfang, det er nødvendigt for tjenestens gennemførelse med henblik på debitering og afregning for samtrafik, og kun i et begrænset tidsrum. [Yderligere behandling af sådanne data må] kun ske, hvis abonnenten har givet sit samtykke hertil på grundlag af en nøjagtig og fuldstændig orientering fra udbyderen af de offentligt tilgængelige elektroniske kommunikationstjenester om arten af den yderligere behandling, han agter at foretage, og om abonnentens ret til at nægte eller tilbagekalde sit samtykke til denne behandling. Trafikdata, som anvendes til markedsføring af udbyderens egne kommunikationstjenester […], bør ligeledes slettes eller anonymiseres […]

[…]

(30) Systemer til levering af elektroniske kommunikationsnet og kommunikationstjenester bør konstrueres, så de begrænser mængden af nødvendige personoplysninger til et absolut minimum. […]«

15 Artikel 1 i direktiv 2002/58 med overskriften »Anvendelsesområde og formål« bestemmer:

»1. Dette direktiv tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i [Den Europæiske Union].

2. Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser direktiv [95/46]. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer.

3. Dette direktiv gælder ikke for aktiviteter, der ikke er omfattet af [TEUF], som f.eks. de aktiviteter, der er omfattet af afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område.«

16 Artikel 2 i direktiv 2002/58 med overskriften »Definitioner« fastsætter:

»Medmindre andet angives, gælder i dette direktiv de definitioner, der er fastsat i direktiv [95/46] og […] direktiv [2002/21].

Følgende definitioner anvendes også:

a) »bruger«: en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste

b) »trafikdata«: data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf

c) »lokaliseringsdata«: data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender

d) »kommunikation«: oplysninger, som udveksles eller overføres mellem et begrænset antal parter via en offentligt tilgængelig elektronisk kommunikationstjeneste. Dette omfatter ikke oplysninger, der overføres som del af en radio- og fjernsynstransmissionstjeneste til offentligheden via et elektronisk kommunikationsnet, medmindre oplysningerne kan kædes sammen med en identificerbar abonnent eller bruger, der modtager oplysningerne

[…]«

17 Artikel 3 i direktiv 2002/58 med overskriften »Omfattede tjenester« bestemmer:

»Dette direktiv finder anvendelse på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr.«

18 Artikel 5 i direktiv 2002/58 med overskriften »Kommunikationshemmelighed« har følgende ordlyd:

»1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

[…]

3. Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv [95/46] at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.«

19 Artikel 6 i direktiv 2002/58 med overskriften »Trafikdata« bestemmer:

»1. Trafikdata vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste, skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3 og 5 samt artikel 15, stk. 1.

2. Med henblik på debitering af abonnenten og afregning for samtrafik er det tilladt at behandle trafikdata. En sådan behandling er tilladt indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger.

3. Med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af værdiforøgende tjenester er det tilladt udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste at behandle de i stk. 1 omtalte oplysninger i det omfang og tidsrum, som sådanne tjenester eller markedsføringen kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, forudgående har givet sit samtykke hertil. Brugeren eller abonnenten skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke til behandling af trafikdata tilbage.

[…]

5. Behandling af trafikdata i henhold til stk. 1, 2, 3 og 4 må kun foretages af personer, som handler efter bemyndigelse fra udbydere af de offentligt tilgængelige kommunikationsnet og -tjenester, og som er beskæftiget med debitering eller trafikstyring, kundeforespørgsler, afsløring af svig, markedsføring af elektroniske kommunikationstjenester eller levering af en tillægstjeneste, og skal begrænses til det for sådanne aktiviteter nødvendige.«

20 Dette direktivs artikel 9 med overskriften »Lokaliseringsdata, bortset fra trafikdata« bestemmer i stk. 1:

»Hvis lokaliseringsdata, bortset fra trafikdata, vedrørende brugere af eller abonnenter på de offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, kan behandles, må disse data kun behandles, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil, og da kun i det omfang og i det tidsrum, som er nødvendigt for levering af en

tillægstjeneste. Tjenesteudbyderen skal, inden brugernes eller abonnenternes samtykke indhentes, underrette dem om, hvilken type lokaliseringsdata, bortset fra trafikdata, der behandles, hvorfor og hvor længe de behandles, og om de videregives til en tredjemand med henblik på levering af tillægstjenesten. […]«

21 Det nævnte direktivs artikel 15 med overskriften »Anvendelsesområdet for visse bestemmelser i direktiv [95/46]« er affattet som følger:

»1. Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv [95/46]. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med [EU-]rettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.

[…]

2. Bestemmelserne i direktiv [95/46], kapitel III, »retsmidler, ansvar og sanktioner«, finder anvendelse på nationale bestemmelser, der vedtages til nærværende direktivs gennemførelse, og på individuelle rettigheder afledt af nærværende direktiv.

[…]«

Forordning 2016/679

22 Tiende betragtning til forordning 2016/679 har følgende ordlyd:

»For at sikre et ensartet og højt niveau for beskyttelse af fysiske personer og for at fjerne hindringerne for udveksling af personoplysninger inden for Unionen bør beskyttelsesniveauet for fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstater. Det bør sikres, at reglerne for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen. […]«

23 Denne forordnings artikel 2 bestemmer:

»1. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Denne forordning gælder ikke for behandling af personoplysninger:

a) under udøvelse af aktiviteter, der falder uden for EU-retten

b) som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i [EU-traktaten]

[…]

d) som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

[…]

4. Denne forordning berører ikke anvendelsen af direktiv [2000/31], navnlig reglerne om formidleransvar for tjenesteydere, der er fastsat i artikel 12-15 i nævnte direktiv.«

24 Den nævnte forordnings artikel 4 bestemmer:

»I denne forordning forstås ved:

1) »personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet

2) »behandling«: enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

[…]«

25 Artikel 5 i forordning 2016/679 bestemmer:

»1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)

d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)

e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål

eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

[…]«

26 Denne forordnings artikel 6 har følgende ordlyd:

»1. Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:

[…]

c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

[…]

3. Grundlaget for behandling i henhold til stk. 1, litra c) og e), skal fremgå af:

a) EU-retten, eller

b) medlemsstaternes nationale ret, som den dataansvarlige er underlagt.

Formålet med behandlingen skal være fastlagt i dette retsgrundlag […] Dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i denne forordning, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til, og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer som omhandlet i kapitel IX. EU-retten eller medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges.

[…]«

27 Den nævnte forordnings artikel 23 bestemmer:

»1. EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige eller databehandleren er underlagt, kan ved lovgivningsmæssige foranstaltninger begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22, når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til:

a) statens sikkerhed

b) forsvaret

c) den offentlige sikkerhed

d) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed

e) andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed

f) beskyttelse af retsvæsenets uafhængighed og retssager

g) forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv

h) kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i de tilfælde, der er omhandlet i litra a)-e) og g)

i) beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder

j) håndhævelse af civilretlige krav.

2. Navnlig skal enhver lovgivningsmæssig foranstaltning, der er omhandlet i stk. 1, som minimum, hvor det er relevant, indeholde specifikke bestemmelser vedrørende:

a) formålene med behandlingen eller kategorierne af behandling

b) kategorierne af personoplysninger

c) rækkevidden af de indførte begrænsninger

d) garantierne for at undgå misbrug eller ulovlig adgang eller overførsel

e) specifikation af den dataansvarlige eller kategorierne af dataansvarlige

f) opbevaringsperioder og de gældende garantier under hensyntagen til behandlingens karakter, omfang og formål eller kategorier af behandling

g) risiciene for de registreredes rettigheder og frihedsrettigheder, og

h) de registreredes ret til at blive underrettet om begrænsningen, medmindre dette kan skade formålet med begrænsningen.«

28 Den nævnte forordnings artikel 79, stk. 1, er affattet således:

»Uden at det berører andre tilgængelige administrative eller udenretslige klageadgange, herunder retten til at indgive klage til en tilsynsmyndighed i henhold til artikel 77, skal den enkelte registrerede have adgang til effektive retsmidler, hvis vedkommende finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling af vedkommendes personoplysninger i strid med denne forordning.«

29 Artikel 94 i forordning 2016/679 har følgende ordlyd:

»1. Direktiv [95/46] ophæves med virkning fra den 25. maj 2018.

2. Henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning. Henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv [95/46], gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved denne forordning.«

30 Denne forordnings artikel 95 bestemmer:

»Denne forordning indfører ikke yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv [2002/58].«

Fransk ret

Lov om indre sikkerhed

31 Bog VIII i den dispositive del af code de la sécurité intérieure (lov om indre sikkerhed, herefter »CSI«) indeholder i artikel L. 801-1 til L. 898-1 regler om efterretninger.

32 CSI's artikel L. 811-3 bestemmer:

»De specialiserede efterretningstjenester kan alene med henblik på udførelsen af deres respektive opgaver anvende de teknikker, der er nævnt i denne bogs afsnit V, med henblik på indsamling af følgende efterretninger om forsvar og om fremme af statens grundlæggende interesser:

1° statens uafhængighed, territoriale integritet og forsvar

2° væsentlige udenrigspolitiske interesser, opfyldelse af Frankrigs europæiske og internationale forpligtelser og forebyggelse af enhver form for udenlandsk indblanding

3° Frankrigs væsentlige økonomiske, industrielle og videnskabelige interesser

4° forebyggelse af terrorisme

5° forebyggelse af:
   a) angreb på institutioners republikanske grundlag
   b) handlinger, der har til formål at bevare eller videreføre grupper, der er blevet opløst i henhold til artikel L. 212-1
   c) kollektive voldshandlinger, der alvorligt påvirker opretholdelsen af lov og orden.

6° forebyggelse af kriminalitet, herunder organiseret kriminalitet

7° forebyggelse af spredning af masseødelæggelsesvåben.«

33 CSI's artikel L. 811-4 bestemmer:

»I et dekret, der vedtages efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager)], og efter indhentelse af en udtalelse fra Commission nationale de contrôle des techniques de renseignement [(den nationale tilsynskommission for efterretningsteknikker)], udpeges de tjenester, der ud over de specialiserede efterretningstjenester henhører under forsvars-, indenrigs- og justitsministeren samt ministrene med ansvar for økonomi-, finans- og toldområdet, og som kan gives

tilladelse til at anvende de teknikker, der er nævnt i denne bogs afsnit V, på de i denne bog fastsatte betingelser. I dette dekret angives for hver enkelt tjeneste de formål, der er nævnt i artikel L. 811-3, og de teknikker, der kan give anledning til tilladelse.«

34 CSI's artikel L. 821-1, stk. 1, er affattet som følger:

»Anvendelse på statens område af de teknikker til indsamling af efterretninger, der er nævnt kapitel I-IV i denne bogs afsnit V, er betinget af, at der fra premierministeren indhentes en forudgående tilladelse, som meddeles efter udtalelse fra den nationale tilsynskommission for efterretningsteknikker.«

35 CSI's artikel L. 821-2 fastsætter:

»Den i artikel L. 821-1 omhandlede tilladelse udstedes efter skriftlig og begrundet anmodning fra forsvarsministeren, indenrigsministeren, justitsministeren eller ministeren med ansvar for økonomi-, finans- eller toldområdet. Den enkelte minister kan individuelt kun delegere denne beføjelse til direkte underordnede medarbejdere, der er godkendt til at håndtere forsvarshemmeligheder.

Anmodningen skal indeholde oplysning om:

1° den eller de teknikker, der skal anvendes

2° den tjeneste, som anmodningen vedrører

3° det eller de forfulgte formål

4° den eller de grunde, hvorpå foranstaltningerne er baseret

5° tilladelsens gyldighedsperiode

6° den eller de personer samt det eller de steder eller køretøjer, som anmodningen vedrører.

Med henblik på anvendelsen af nr. 6° kan personer, hvis identitet ikke er kendt, udpeges med angivelse af en identifikator eller deres stilling, og steder eller køretøjer kan udpeges ved henvisning til de personer, der er omfattet af anmodningen.

[…]«

36 CSI's artikel L. 821-3, stk. 1, har følgende ordlyd:

»Anmodningen indgives til formanden, eller i dennes forfald til et af de medlemmer af den nationale tilsynskommission for efterretningsteknikker, der er nævnt i artikel L. 831-1, nr. 2° og 3°, som afgiver udtalelse til premierministeren inden for en frist på 24 timer. Hvis anmodningen behandles af tilsynskommissionen i dennes begrænsede eller fulde sammensætning, underrettes premierministeren straks, og udtalelsen afgives inden for en frist på 72 timer.«

37 CSI's artikel L. 821-4 bestemmer:

»Premierministeren meddeler tilladelse til at anvende de teknikker, der er nævnt i kapitel I-IV i denne bogs afsnit V, for en periode på højst fire måneder. […] I tilladelsen angives de grunde og oplysninger, der er nævnt i artikel L.821-2, nr. 1°-6°. Tilladelsen kan forlænges på samme betingelser som dem, der er fastsat i dette kapitel.

Når tilladelsen udstedes efter en negativ udtalelse fra den nationale tilsynskommission for efterretningsteknikker, skal den indeholde oplysning om grundene til, at denne udtalelse ikke er blevet fulgt.

[…]«

38 CSI's artikel L. 833-4, der er indeholdt i dette afsnits kapitel III, bestemmer:

»Kommissionen kan på eget initiativ eller på grundlag af en klage fra enhver, der ønsker en kontrol af, at den pågældende ikke er genstand for ulovlige efterretningsteknikker, gennemføre et tilsyn med den eller de angivne teknikker med henblik på at kontrollere, om denne eller disse teknikker er blevet anvendt i overensstemmelse med denne bog. Kommissionen underretter klageren om, at de nødvendige undersøgelser er foretaget, uden hverken at be- eller afkræfte, at sådanne efterretningsteknikker er blevet anvendt.«

39 CSI's artikel L. 841-1, stk. 1 og 2, har følgende ordlyd:

»Med forbehold af de særlige bestemmelser i denne lovs i artikel L. 854-9 har Conseil d'État [(øverste domstol i forvaltningsretlige sager)] kompetence til under de betingelser, der er fastsat i kapitel IIIa, afsnit VII, bog VII i code de justice administrative [(lov om administrativ retspleje)], at påkende søgsmål vedrørende anvendelse af de efterretningsteknikker, der er nævnt i denne bogs afsnit V.

Søgsmål kan anlægges ved Conseil d'État [(øverste domstol i forvaltningsretlige sager)] af:

1° Enhver, der ønsker en kontrol af, at den pågældende ikke er genstand for ulovlige efterretningsteknikker, og som kan godtgøre, at den i artikel L. 833-4 omhandlede procedure er blevet gennemført.

2° Den nationale tilsynskommission for efterretningsteknikker under de betingelser, der er fastsat i artikel L. 833-8.«

40 Afsnit V i bog VIII i den dispositive del af CSI, der vedrører »teknikker til indsamling af efterretninger, som kræver tilladelse«, indeholder bl.a. et kapitel I med overskriften »Administrativ adgang til forbindelsesdata«, som indeholder CSI's artikel L. 851-1 til L. 851-7.

41 CSI's artikel L. 851-1 bestemmer:

»Under de betingelser, som er fastsat i kapitel 1 i denne bogs afsnit II, kan indsamling tillades fra operatører inden for elektronisk kommunikation og de personer, der henvises til i [CPCE's] artikel L. 34-1, samt fra de personer, der henvises til i artikel 6, stk. I-1 og I-2, i loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(lov nr. 2004-575 af 21.6.2004 om tillid til den digitale økonomi, JORF af 22.6.2004, s. 11168)], af oplysninger eller dokumenter, der er behandlet eller lagret af deres elektroniske kommunikationsnet eller -tjenester, herunder tekniske data vedrørende identificering af abonnementsnumre eller forbindelsesnumre til elektroniske kommunikationstjenester, opgørelse af alle en bestemt persons abonnements- eller forbindelsesnumre, lokalisering af anvendt terminaludstyr samt en abonnents kommunikationer for så vidt angår oversigten over opkaldte og opkaldende numre, varigheden af og datoen for kommunikationerne.

Uanset artikel L. 821-2 indgiver de individuelt udpegede og bemyndigede agenter fra de i artikel L. 811-2 og L. 811-4 nævnte efterretningstjenester skriftlige og begrundede anmodninger om tekniske data vedrørende identificering af abonnementsnumre eller forbindelsesnumre til elektroniske kommunikationstjenester, eller om opgørelse af alle en bestemt persons abonnements- eller forbindelsesnumre, direkte til den nationale tilsynskommission for efterretningsteknikker. Kommissionen afgiver sin udtalelse på de betingelser, der er fastsat i artikel L. 821-3.

En tjenestegren under premierministeren har til opgave at indsamle oplysninger eller dokumenter fra de operatører og personer, der er nævnt i denne artikels stk. 1. Den nationale tilsynskommission for efterretningsteknikker har permanent, fuldstændig, direkte og umiddelbar adgang til de indsamlede oplysninger eller dokumenter.

Gennemførelsesbestemmelserne til denne artikel fastsættes ved dekret efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager)] og efter udtalelse fra Commission nationale de l'informatique et des libertés [(den nationale kommission for databehandling og frihedsrettigheder)] og den nationale tilsynskommission for efterretningsteknikker.«

42 CSI's artikel L. 851-2 bestemmer:

»I. – På de betingelser, der er fastsat i denne bogs afsnit II, kapitel I, og alene med henblik på at forebygge terrorisme, kan der gives individuel tilladelse til fra de netværksoperatører og de personer, der er nævnt i artikel L. 851-1, at foretage indsamling i realtid af de oplysninger eller dokumenter, der er nævnt i samme artikel L. 851-1, og som vedrører en person, som på forhånd er identificeret som en person, der kan have forbindelse til en trussel. Hvis der foreligger tungtvejende grunde til at antage, at en eller flere personer, der tilhører den personkreds, som den person, der er omfattet af tilladelsen, færdes i, er i stand til at tilvejebringe oplysninger, der vedrører det formål, som ligger til grund for tilladelsen, kan der desuden individuelt gives en sådan tilladelse med hensyn til hver enkelt af disse personer.

Ia. Det maksimale antal tilladelser med samtidig gyldighed, der kan udstedes i henhold til denne artikel, fastsættes af premierministeren efter udtalelse fra den nationale tilsynskommission for efterretningsteknikker. Kommissionen underrettes om afgørelsen om denne kvote og denne kvotes fordeling mellem de ministre, der er nævnt i artikel L. 821-2, stk. 1, og om antallet af udstedte tilladelser til opfangning.

[…]«

43 CSI's artikel L. 851-3 fastsætter:

»I. – Under de betingelser, der er fastsat i kapitel I i denne bogs afsnit II, og alene med henblik på at forebygge terrorisme, kan det pålægges de operatører og personer, der er nævnt i artikel L. 851-1, at anvende automatiserede behandlinger i deres netværk med henblik på i overensstemmelse med de parametre, som præciseres i tilladelsen, at opdage forbindelser, der vil kunne afsløre en terrortrussel.

Disse automatiserede behandlinger anvender udelukkende de oplysninger eller dokumenter, der er nævnt i artikel L. 851-1, uden at indsamle andre data end dem, der opfylder designparametrene, og uden at gøre det muligt at identificere de personer, som oplysningerne eller dokumenterne vedrører.

Premierministerens tilladelse skal under overholdelse af proportionalitetsprincippet indeholde en præcisering af det tekniske område, der er genstand for anvendelsen af disse behandlinger.

II. – Den nationale tilsynskommission for efterretningsteknikker afgiver en udtalelse om anmodningen om tilladelse til at foretage automatiserede behandlinger og om de anvendte overvågningsparametre. Kommissionen har permanent, fuldstændig og direkte adgang til disse behandlinger og til de indsamlede oplysninger og data. Kommissionen underrettes om enhver ændring af behandlingerne og parametrene og kan afgive anbefalinger.

Den første tilladelse til at anvende automatiserede behandlinger som omhandlet i denne artikels stk. I udstedes for en periode på to måneder. Tilladelsen kan forlænges under de betingelser for varighed, der er fastsat i kapitel I i denne bogs afsnit II. En anmodning om forlængelse skal indeholde en oversigt over antallet af identifikatorer, der er indberettet ved hjælp af automatiseret behandling, og en analyse af disse indberetningers relevans.

III. – De betingelser, der er fastsat i artikel L. 871-6, finder anvendelse på de fysiske operationer, som udføres af de operatører og personer, der er nævnt i artikel L. 851-1, med henblik på at gennemføre en sådan automatiseret behandling.

IV. – Når der som følge af de i stk. I nævnte behandlinger fremkommer data, der giver anledning til at antage, at der foreligger en terrortrussel, kan premierministeren eller en af denne bemyndiget person efter udtalelse fra den nationale tilsynskommission for efterretningsteknikker, der er afgivet i henhold til de betingelser, der er fastsat i kapitel I i denne bogs afsnit II, give tilladelse til, at der foretages identifikation af den eller de berørte personer og indsamling af oplysninger om pågældende. Disse data skal anvendes senest 60 dage efter, at de er blevet indsamlet, og tilintetgøres efter udløbet af denne frist, medmindre der foreligger alvorlige oplysninger, der bekræfter, at en eller flere af de berørte personer udgør en terrortrussel.

[…]«

44 CSI's artikel L. 851-4 er affattet således:

»Under de betingelser, der er fastsat i kapitel I i denne bogs afsnit II, kan de tekniske oplysninger vedrørende lokaliseringen af det i artikel L. 851-1 omhandlede terminaludstyr indsamles efter anmodning fra netværket og overføres i realtid af operatørerne til en tjeneste under premierministeren.«

45 CSI's artikel L. 851-5, der er indeholdt i denne lovs dispositive del, bestemmer:

»I. – Med undtagelse af indholdet af den udvekslede korrespondance og de oplysninger, hvorom der er forespurgt, udgør de oplysninger eller dokumenter, der er omhandlet i artikel L. 851-1, følgende:

1° de oplysninger, der er nævnt i [CPCE's] artikel R. 10-13 og R. 10-14 og artikel 1 i dekret [nr. 2011-219]

2° tekniske data, bortset fra de under nr. 1° nævnte:

a) der gør det muligt at lokalisere terminaludstyr

b) der vedrører terminaludstyrs adgang til netværk eller offentlige onlinekommunikationstjenester

c) der vedrører overførsel af elektronisk kommunikation via netværk

d) der vedrører identifikation og autentificering af en bruger, en forbindelse, et netværk eller en offentlig onlinekommunikationstjeneste

e) der vedrører terminaludstyrets egenskaber og konfigurationsdataene for dets software.

II. – Der kan i henhold til artikel L. 851-1 kun indsamles de oplysninger og dokumenter, der er nævnt i stk. 1, nr. 1°. Denne indsamling gennemføres ikke i realtid.

De oplysninger, der er nævnt i stk. I, nr. 2°, kan kun indsamles i henhold til artikel L. 851-2 og L. 851-3 på de betingelser og med de begrænsninger, der er fastsat i disse artikler og med forbehold af artikel R. 851-9.«

Lov om postvæsen og elektronisk kommunikation

46 CPCE's artikel L. 34-1 bestemmer:

»I. – Denne artikel finder anvendelse på behandling af personoplysninger i forbindelse med levering af elektroniske kommunikationstjenester til offentligheden, herunder navnlig i de netværk, der indeholder anordninger til indsamling af oplysninger og identifikation.

II. – Operatører inden for elektronisk kommunikation, og navnlig personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester, skal slette eller anonymisere samtlige trafikdata, med forbehold af stk. III, IV, V og VI.

Leverandører af elektroniske kommunikationstjenester til offentligheden skal under iagttagelse af bestemmelserne i foregående afsnit fastlægge interne procedurer med henblik på at efterkomme de kompetente myndigheders krav.

Personer, som gennem en erhvervsmæssig hoved- eller bibeskæftigelse offentligt udbyder en forbindelse, der giver mulighed for onlinekommunikation via netværksadgang, herunder også vederlagsfrit, har pligt til at overholde de gældende bestemmelser for operatører inden for elektronisk kommunikation, der er fastsat i denne artikel.

III. – Med henblik på at efterforske, fastslå og retsforfølge strafbare handlinger eller manglende opfyldelse af den i artikel L. 336-3 i code de la propriété intellectuelle [(lov om intellektuelle ejendomsrettigheder)] fastsatte forpligtelse, eller med henblik på at forebygge de angreb på automatiserede databehandlingssystemer, som er omhandlet og sanktioneret i artikel 323-1 til 323-3-1 i code pénal [(straffeloven)], og med det ene formål i givet fald at tillade en tilrådighedsstillelse for den retslige myndighed eller øverste myndighed, som er nævnt i artikel L. 331-12 i [lov om intellektuelle ejendomsrettigheder], eller for den nationale sikkerhedsmyndighed på området for informationssystemer, som er nævnt i artikel L. 2321-1 i code de la défense [(forsvarsloven)], kan de aktiviteter, der har til formål at slette eller anonymisere bestemte kategorier af tekniske data, udskydes i op til et år. Et dekret efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager)], som vedtages efter indhentelse af en udtalelse fra den nationale kommission for databehandling og frihedsrettigheder, fastlægger, inden for de grænser, som er fastsat i stk. VI, disse kategorier af data og varigheden af deres lagring, afhængigt af operatørernes virksomhed og kommunikationernes karakter, samt vilkårene for eventuel godtgørelse af identificerbare og specifikke meromkostninger forbundet med de tjenester, som i denne forbindelse leveres af operatørerne på statens anmodning.

[…]

VI. – De data, der lagres og behandles under de i stk. III, IV og V fastsatte betingelser, omfatter udelukkende identifikationen af brugerne af de af operatørerne leverede tjenester, de tekniske egenskaber for den kommunikation, der stilles til rådighed af sidstnævnte, og lokaliseringen af terminaludstyret.

De må i intet tilfælde omfatte indholdet af den udvekslede korrespondance eller de oplysninger, hvorom der er forespurgt – i en hvilken som helst form – i forbindelse med den pågældende kommunikation.

Lagringen og behandlingen af data skal ske under iagttagelse af bestemmelserne i loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(lov nr. 78-17 af 6.1.1978 om IT, registre og frihedsrettigheder)].

Operatørerne træffer alle de nødvendige foranstaltninger med henblik på at forebygge, at disse data anvendes til andre formål end de i denne artikel fastsatte.«

47 CPCE's artikel R. 10-13 er affattet således:

»I. – Operatører inden for elektronisk kommunikation har i henhold til artikel L. 34-1, stk. III, pligt til af hensyn til efterforskning, afsløring og retsforfølgning af strafbare handlinger at lagre:

a) oplysninger, der gør det muligt at fastslå brugerens identitet

b) oplysninger om det anvendte terminaludstyr

c) de tekniske kendetegn samt dato, tidspunkt og varighed af hver kommunikation

d) oplysninger vedrørende de supplerende tjenester, der er anmodet om eller anvendt, samt leverandørerne heraf

e) oplysninger, der gør det muligt at fastslå identiteten på den eller de modtagere, som kommunikationen er rettet til.

II. – I forbindelse med telefonitjenester skal operatøren lagre de i stk. II nævnte oplysninger og de oplysninger, der kan bidrage til at fastslå kommunikationens oprindelse og lokaliseringen heraf.

III. – De i denne artikel nævnte oplysninger skal lagres i et år, regnet fra den dato, hvor de er blevet registreret.

IV. – De identificerbare og specifikke meromkostninger, som er afholdt af de operatører, der af retslige myndigheder er blevet pålagt at udlevere data, som er omfattet af de i denne artikel nævnte kategorier, modtager kompensation i henhold til i artikel R. 213-1 i code de procédure pénale [(strafferetsplejeloven)].«

48 CPCE's artikel L. 10-14 bestemmer:

»I. – I henhold til artikel L. 34-1, stk. IV, har operatører inden for elektronisk kommunikation ret til i forbindelse med deres fakturerings- og betalingstransaktioner at lagre tekniske data, der gør det muligt at fastslå identiteten på brugeren, og de data, der er nævnt i artikel R. 10-13, stk. I, litra b), c) og d).

II. – I forbindelse med telefonitjenester kan operatørerne ud over de i stk. I nævnte data lagre tekniske data, der vedrører lokaliseringen af kommunikationen, identifikation af modtageren eller modtagerne af kommunikationen og de data, der gør det muligt at foretage fakturering.

III. – De i denne artikels stk. I og II nævnte data må kun lagres, hvis de er nødvendige for faktureringen af og betalingen for de leverede tjenester. Lagringen af disse data skal begrænses til det tidsrum, der er strengt nødvendigt for at nå dette formål, og må ikke overstige et år.

IV. – Operatører kan af hensyn til netværks- og udstyrssikkerheden i en periode på højst tre måneder lagre:

a) data, der gør det muligt at identificere kommunikationens oprindelse

b) de tekniske kendetegn samt dato, tidspunkt og varighed af hver kommunikation

c) tekniske data, der gør det muligt at fastslå identiteten på modtageren eller modtagerne af kommunikationen

d) data vedrørende de supplerende tjenester, der er anmodet om eller anvendt, samt leverandørerne heraf.«

Lov nr. 2004-575 af 21. juni 2004 om tillid til den digitale økonomi

49 Artikel 6 i loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (lov nr. 2004-575 af 21.6.2004 om tillid til den digitale økonomi, JORF af 22.6.2004, s. 11168, herefter »LCEN«) bestemmer:

»I. – 1. Personer, hvis virksomhed består i at tilbyde offentlige onlinekommunikationstjenester, informerer deres abonnenter om de tekniske funktioner, der gør det muligt at begrænse adgangen til visse tjenester eller at vælge mellem disse tjenester, og tilbyder dem mulighed for at anvende mindst en af disse funktioner.

[…]

2. Fysiske eller juridiske personer, der, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art, der leveres af modtagere af disse tjenester, ifalder ikke civilretligt ansvar som følge af, at de efter anmodning fra en modtager af disse tjenester har udført handlinger eller lagret oplysninger, hvis de ikke havde konkret kendskab til, at disse handlinger eller lagringen af disse oplysninger var ulovlig, eller til de faktiske forhold og omstændigheder, der gjorde det muligt at konstatere denne ulovlighed, eller hvis de på det tidspunkt, hvor de fik kendskab hertil, straks tog skridt til at fjerne eller hindre adgangen til disse data.

[…]

II. – De personer, der er nævnt i stk. I-1 og I-2, skal lagre og opbevare data på en sådan måde, at det er muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer.

De giver de personer, der leverer en offentlig onlinekommunikationstjeneste, adgang til tekniske funktioner, der gør det muligt for disse sidstnævnte personer, at opfylde de identifikationskrav, der er fastsat i stk. III.

En retslig myndighed kan kræve, at de i stk. I nævnte data videregives til de tjenesteudbydere, der er nævnt i stk. I-1 og I-2.

[Straffelovens] artikel 226-17, 226-21 og 226-22 finder anvendelse på behandlingen af disse data.

I et dekret, der vedtages efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager)], og efter indhentelse af en udtalelse fra den nationale databehandling og frihedsrettigheder, gives præcisering af de i stk. I nævnte data og af lagringens varighed og metode.

[…]«

Dekret 2011-219

50 Kapitel I i dekret 2011-219, der er vedtaget på grundlag af LCEN's artikel 6, stk. II, sidste stykke, indeholder dette dekrets artikel 1-4.

51 Artikel 1 i dekret 2011-219 bestemmer:

»De data, der er nævnt i [LCEN's] artikel 6, stk. II, i hvilken forbindelse der i henhold til denne bestemmelse består en lagringspligt, omfatter:

1° for personer, der er nævnt i samme artikels stk. I-1, og for hver enkelt abonnentforbindelse:
   a) forbindelsesidentifikatoren
   b) den identifikator, som disse personer har tildelt abonnenten
   c) identifikatoren for den terminal, der anvendes, når de tilgår forbindelsen
   d) dato og tidspunkt for forbindelsens opstart og afslutning
   e) kendetegnene på abonnentlinjen.

2° for de personer, der er nævnt i samme artikels stk. I-2, og for hver enkelt handling, hvorved der skabes indhold:
   a) identifikatoren for forbindelsen på kommunikationens oprindelsessted
   b) den identifikator, som af informationssystemet tildeles det indhold, der er genstand for aktiviteten
   c) de anvendte protokoltyper ved forbindelsen til tjenesten og ved overførsel af indhold
   d) aktivitetens art
   e) dato og tidspunkt for aktiviteten
   f) den identifikator, der er anvendt af den, der har foretaget aktiviteten, når den pågældende har tildelt identifikatoren

3° for de personer, der er nævnt i samme artikels stk. I-1 og I-2, de oplysninger, der er tilvejebragt af en bruger ved indgåelsen af en aftale eller oprettelsen af en konto:
   a) forbindelsesidentifikatoren ved oprettelsen af denne konto
   b) for- og efternavne eller virksomhedsnavn
   c) de tilknyttede postadresser
   d) de anvendte pseudonymer
   e) de tilknyttede e-mailadresser eller kontoadresser
   f) telefonnumre
   g) den opdaterede adgangskode samt de oplysninger, der gør det muligt at kontrollere eller ændre denne.

4° for de personer, der er nævnt i samme artikels stk. I-1 og I-2, når der i forbindelse med indgåelsen en aftale eller oprettelsen af en konto opkræves betaling, for hver enkelt betalingstransaktion:
   a) den anvendte betalingsform
   b) betalingsreferencen
   c) beløbet
   d) dato og tidspunkt for transaktionen.

De data, der er nævnt i nr. 3° og 4°, må kun lagres, for så vidt som disse personer sædvanligvis indsamler sådanne data.«

52 Dette dekrets artikel 2 har følgende ordlyd:

»Aktiviteter, der bidrager til indholdsskabelse, omfatter følgende:

a) den oprindelige indholdsskabelse

b) ændringer af indhold og de data, der er forbundet med dette indhold

c) fjernelse af indhold.«

53 Det nævnte dekrets artikel 3 bestemmer:

»Lagringsperioden for de i artikel 1 nævnte data, er:

a) med hensyn til de data, der er nævnt i nr. 1° og 2°, et år regnet fra den dag, hvor indholdet skabes, for hver enkelt aktivitet, der bidrager til at skabe indhold som defineret i artikel 2

b) med hensyn til de data, der er nævnt i nr. 3°, et år regnet fra den dag, hvor aftalen opsiges, eller hvor kontoen lukkes

c) med hensyn til de data, der er nævnt i nr. 4°, et år regnet fra datoen for udstedelsen af fakturaen eller for betalingstransaktionen, for hver enkelt faktura eller betalingstransaktion.«

Belgisk ret

54 Ved lov af 29. maj 2016 blev der bl.a. foretaget ændringer af loi du 13 juin 2005 relative aux communications électroniques (lov af 13.6.2005 om elektronisk kommunikation, *Moniteur belge* af 20.6.2005, s. 28070, herefter »lov af 13. juni 2005«), code d'instruction criminelle (strafferetsplejeloven) og loi du 30 novembre 1998 organique des services de renseignement et de sécurité (lov af 30.11.1998 om organiseringen af efterretnings- og sikkerhedstjenester, *Moniteur belge* af 18.12.1998, s. 40312, herefter »lov af 30. november 1998«).

55 Artikel 126, i lov af 13. juni 2005 i den affattelse, der følger af lov af 29. maj 2016, bestemmer:

»1. Uden at det berører loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [(lov af 8.12.1992 om beskyttelse af privatlivets fred i forbindelse med behandling af personoplysninger)] skal udbydere af telefontjenester til offentligheden, herunder IP-telefoni, internetadgang, e-mailtjenester, operatører, der udbyder offentlige elektroniske kommunikationsnet, samt operatører, der udbyder en af disse tjenester, lagre de data, der er omhandlet i stk. 3, og som genereres eller behandles af disse i forbindelse med leveringen af de pågældende elektroniske kommunikationstjenester.

Denne artikel omfatter ikke indholdet af kommunikationen.

Den i stk. 3 nævnte forpligtelse til lagring af data finder også anvendelse på forgæves opkaldsforsøg, når disse data i forbindelse med leveringen af de pågældende elektroniske kommunikationstjenester:

1° genereres eller behandles af operatører af offentligt tilgængelige elektroniske kommunikationstjenester eller et offentligt elektronisk kommunikationsnet, for så vidt angår telefonidata, eller

2° arkiveres af disse udbydere, for så vidt angår internetdata.

2. Det er alene følgende myndigheder, der har ret til efter anmodning at indhente de data, der lagres i henhold til denne artikel, fra de i stk. 1, første afsnit, nævnte udbydere og operatører til de formål og på de betingelser, der er opregnet nedenfor:

1° retslige myndigheder med henblik på undersøgelse, efterforskning og retsforfølgning af strafbare handlinger, med henblik på gennemførelse af de foranstaltninger, der er omhandlet i [strafferetsplejelovens] artikel 46a og 88a, og på de betingelser, der er fastsat i disse artikler

2° efterretnings- og sikkerhedstjenester med henblik på at udføre deres efterretningsopgaver under anvendelse af de metoder for indsamling af data, der er omhandlet i artikel 16/2, 18/7 og 18/8 i [lov af 30.11.1998 om organiseringen af efterretnings- og sikkerhedstjenester] og under overholdelse af de betingelser, der er fastsat i denne lov

3° retshåndhævelsespersonale ved [Institut belge des services postaux et des télécommunications (det belgiske institut for posttjenester og telekommunikation)] med henblik på undersøgelse, efterforskning og retsforfølgning af overtrædelser af artikel 114, 124 og nærværende artikel

4° beredskabstjenester, der yder hjælp på stedet, såfremt de efter et alarmopkald ikke fra den pågældende udbyder eller operatør kan få identifikationsoplysninger for den, der har foretaget opkaldet, på grundlag af oplysningerne i den database, der er nævnt i artikel 107, stk. 2, tredje afsnit, eller får ufuldstændige eller ukorrekte data. Der kan kun anmodes om identifikationsoplysninger for den, der foretager opkaldet, og anmodningen skal fremsættes senest 24 timer efter opkaldet.

5° retshåndhævelsespersonale ved Cellule des personnes disparues de la Police Fédérale [(forbundspolitiets enhed for savnede personer)] inden for rammerne af dennes opgave med at yde hjælp til personer i fare, eftersøgning af savnede personer og såfremt der foreligger formodning eller stærke indicier for, at den savnede persons fysiske integritet er i overhængende fare. Det er kun de data, der er omhandlet i stk. 3, første og andet afsnit, vedrørende den savnede person, som er blevet lagret i 48 timer inden anmodningen om adgang til oplysninger, der kan forlanges udleveret fra den berørte operatør eller udbyder, af en af kongen udnævnt bestemt polititjenestegren

6° Service de médiation pour les télécommunications [(ombudstjenesten for telekommunikation)], med henblik på identifikation af den person, der har foretaget en fejlagtig anvendelse af et net eller en elektronisk kommunikationstjeneste, i overensstemmelse med de betingelser, der er omhandlet i artikel 43a, stk. 3, nr. 7), i loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [(lov af 21.3.1991 om reform af visse offentlige virksomheder)]. Der kan kun anmodes om identifikationsdata.

De udbydere og operatører, der er omhandlet i stk. 1, første afsnit, skal sikre, at der er ubegrænset adgang til de data fra Belgien, der er omhandlet i stk. 3, og at disse data og alle øvrige oplysninger, der er nødvendige vedrørende disse data, kan overføres straks og kun til de myndigheder, der er omhandlet i dette stykke.

Med forbehold af andre lovbestemmelser kan de udbydere og operatører, der er omhandlet i stk. 1, første afsnit, ikke anvende de data, der er lagret i henhold til stk. 3 til andre formål.

3. Data til identifikation af brugeren eller abonnenten og kommunikationsmidlerne med undtagelse af de data, der er specifikt nævnt i andet og tredje afsnit, skal lagres i 12 måneder regnet fra datoen, hvor en meddelelse er mulig for sidste gang ved hjælp af den anvendte tjeneste.

Data vedrørende terminaludstyrets adgang og forbindelse til nettet og lokaliseringen af dette udstyr, herunder nettermineringspunktet, skal lagres i 12 måneder regnet fra datoen for meddelelsen.

Kommunikationsdata med undtagelse af indholdet, herunder deres oprindelse og destination, skal lagres i 12 måneder regnet fra datoen for meddelelsen.

Kongen fastsætter ved bekendtgørelse godkendt af Conseil des ministres [(ministerrådet)] og efter forslag fra justitsministeren og [den ansvarlige minister for området for elektronisk kommunikation] og efter udtalelse fra Commission de la protection de la vie privée [(kommissionen for beskyttelse af privatlivet)] og instituttet de data, der skal lagres efter type af de kategorier, der er omhandlet i første til tredje afsnit, samt de krav, som de pågældende data skal opfylde.

[…]«

Tvisterne i hovedsagerne og de præjudicielle spørgsmål

Sag C-511/18

56 Ved søgsmål anlagt den 30. november 2015 og den 16. marts 2016 ved Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig), og senere forenet i hovedsagen, har Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs og Igwan.net nedlagt påstand om annullation af dekret 2015-1185, 2015-1211, 2015-1639 og 2016-67, bl.a. med den begrundelse, at disse dekreter tilsidesætter den franske forfatning, den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (herefter »EMRK«) samt direktiv 2000/31 og 2002/58, sammenholdt med chartrets artikel 7, 8 og 47.

57 Hvad navnlig angår de anbringender, der vedrører tilsidesættelse af direktiv 2000/31, har den forelæggende ret anført, at CSI's artikel L. 851-3 pålægger operatører inden for elektronisk kommunikation og udbydere af tekniske tjenester »at anvende automatiseret behandling i deres netværk med henblik på i overensstemmelse med de parametre, som præciseres i tilladelsen, at opdage forbindelser, der vil kunne afsløre en terrortrussel«. Denne teknik tager udelukkende sigte på, i et begrænset tidsrum og blandt samtlige de forbindelsesdata, som disse operatører og disse udbydere behandler, at indsamle de data, der vil kunne have forbindelse til en sådan alvorlig strafbar handling. Under disse omstændigheder tilsidesætter de nævnte bestemmelser, der ikke pålægger en generel forpligtelse til aktiv overvågning, ikke artikel 15 i direktiv 2000/31.

58 Hvad angår de anbringender, der vedrører tilsidesættelse af direktiv 2002/58, er den forelæggende ret af den opfattelse, at det af bestemmelserne i dette direktiv og af dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, herefter »Tele2-dommen«, EU:C:2016:970), bl.a. følger, at de nationale bestemmelser, der pålægger udbydere af elektroniske kommunikationstjenester forpligtelser, såsom en forpligtelse til at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata vedrørende deres brugere og abonnenter, af de hensyn, der fremgår af det nævnte direktivs artikel 15, stk. 1, herunder hensynet til beskyttelse af den nationale sikkerhed, forsvaret og den offentlige sikkerhed, henhører under anvendelsesområdet for dette samme direktiv, for så vidt som disse bestemmelser regulerer de nævnte udbyderes virksomhed. Det samme gør sig gældende for de bestemmelser, der regulerer de nationale myndigheders adgang til og brug af disse data.

59 Den forelæggende ret har heraf udledt, at såvel den forpligtelse til lagring, der følger af CSI's artikel L. 851-1, som den administrative adgang til de nævnte data, herunder adgang i realtid, i henhold til den nævnte lovs artikel L. 851-1, L. 851-2 og L. 851-4, er omfattet af anvendelsesområdet for direktiv 2002/58. Dette gælder efter den forelæggende rets opfattelse også for den samme lovs artikel L. 851-3, der ganske vist ikke pålægger de pågældende operatører en generel lagringsforpligtelse, men dog pålægger dem i deres netværk at anvende automatiserede behandlinger, der er bestemt til at opdage forbindelser, som vil kunne afsløre en terrortrussel.

60 Denne ret er til gengæld af den opfattelse, at de bestemmelser i CSI, der er genstand for annullationspåstandene, og som vedrører de teknikker til indsamling af efterretninger, der anvendes direkte af staten, uden at regulere den virksomhed, der udøves af udbydere af elektroniske kommunikationstjenester, ved at pålægge dem specifikke forpligtelser, ikke er omfattet af anvendelsesområdet for direktiv 2002/58. Disse bestemmelser kan derfor ikke anses for at gennemføre EU-retten, hvilket indebærer, at de anbringender, der vedrører spørgsmålet om, hvorvidt disse bestemmelser tilsidesætter direktiv 2002/58, ikke med føje kan gøres gældende.

61 For at kunne tage stilling til de tvister, der vedrører lovligheden af dekret 2015-1185, 2015-1211, 2015-1639 og 2016-67 i lyset af direktiv 2002/58, for så vidt som disse dekreter er vedtaget til gennemførelse af CSI's artikel L. 851-1 til L. 851-4, er det således nødvendigt at besvare tre spørgsmål om fortolkning af EU-retten.

62 Hvad angår fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 ønsker den forelæggende ret for det første oplyst, om en forpligtelse til at foretage generel og udifferentieret lagring, som pålægges udbydere af elektroniske kommunikationstjenester på grundlag af CSI's artikel L. 851-1 og R. 851-5, navnlig henset til de garantier og den kontrol, der derefter er forbundet med den administrative adgang til forbindelsesdata og anvendelsen heraf, skal anses for at udgøre et indgreb, der er begrundet i retten til personlig sikkerhed, som er sikret ved chartrets artikel 6, og i hensyn til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 TEU.

63 Hvad for det andet angår de øvrige forpligtelser, der kan pålægges udbydere af elektroniske kommunikationstjenester, har den forelæggende ret anført, at CSI's artikel L. 851-2 alene med henblik på forebyggelse af terrorisme tillader indsamling af de oplysninger eller dokumenter, der er nævnt i denne lovs artikel L. 851-1, fra de samme personer. Denne indsamling, som kun vedrører en eller flere personer, der på forhånd er identificeret som personer, der kan have forbindelse til en terrortrussel, foretages i realtid. Det samme gælder den nævnte lovs artikel L. 851-4, hvorefter operatører i realtid kun kan overføre tekniske data, der vedrører lokaliseringen af terminaludstyr. Disse teknikker regulerer med henblik på andre formål og efter andre regler den administrative adgang i realtid til de data, der er lagret i henhold til CPCE og LCEN, uden at pålægge de pågældende udbydere et yderligere krav om lagring i forhold til, hvad der er nødvendigt for at foretage fakturering og levering af deres tjenester. Endvidere indebærer artikel L. 851-3, der foreskriver en forpligtelse for tjenesteudbyderne til at foretage en automatiseret analyse af forbindelserne i deres netværk, heller ikke en generel og udifferentieret lagring.

64 Den forelæggende ret er imidlertid for det første af den opfattelse, at den operationelle nytte af såvel generel og udifferentieret lagring som adgang i realtid til forbindelsesdata savner modstykke i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed, navnlig risikoen for terror. Generel og udifferentieret lagring gør det nemlig muligt for efterretningstjenesterne at få adgang til kommunikationsdata, før grundene til at antage, at en bestemt person udgør en trussel mod den offentlige sikkerhed, forsvaret eller statens sikkerhed, er identificeret. Endvidere gør adgang i realtid til forbindelsesdata det muligt med høj reaktionshastighed at følge den adfærd, som udvises af de personer, der kan udgøre en umiddelbar trussel mod den offentlige orden.

65 For det andet gør den teknik, der er fastsat i CSI's artikel L. 851-3, det muligt, på grundlag af præcist definerede kriterier herfor, at opdage personer, hvis adfærd, når deres kommunikationsmåder tages i betragtning, vil kunne afsløre en terrortrussel.

66 Hvad for det tredje angår de kompetente myndigheders adgang til de lagrede data ønsker den forelæggende ret oplyst, om direktiv 2002/58, sammenholdt med chartret, skal fortolkes således, at det i alle tilfælde gør lovligheden af procedurer til indsamling af forbindelsesdata betinget af opfyldelsen af et krav om underretning af de berørte personer, når en sådan underretning ikke længere kan skade de

kompetente myndigheders efterforskning, eller om sådanne procedurer kan anses for at være lovlige, henset til alle de andre proceduremæssige garantier, der er fastsat i national ret, når disse sikrer, at adgangen til retsmidler er effektiv.

67 Hvad angår disse andre proceduremæssige garantier har den forelæggende ret bl.a. præciseret, at enhver, der ønsker en kontrol af, at den pågældende ikke er genstand for ulovlige efterretningsteknikker, kan anlægge sag ved den specialiserede afdeling ved Conseil d'État (øverste domstol i forvaltningsretlige sager), som det derefter påhviler under hensyn til de oplysninger, som denne domstol har modtaget, og uden at gennemføre en kontradiktorisk procedure, at foretage en prøvelse af, om der har været anvendt en sådan teknik i forhold til sagsøgeren, og om anvendelsen af denne teknik er sket i overensstemmelse med bog VIII i CSI. De beføjelser, som denne afdeling er tillagt med hensyn til at oplyse sagerne, sikrer, at den retslige prøvelse, som den udøver, er effektiv. Denne afdeling har således kompetence til at oplyse sagerne, af egen drift at påpege alle de ulovligheder, som den konstaterer, og at pålægge forvaltningen at træffe alle relevante foranstaltninger med henblik på at afhjælpe de konstaterede ulovligheder. Endvidere tilkommer det den nationale tilsynskommission for efterretningsteknikker at kontrollere, at teknikkerne til indsamling af efterretninger på nationalt område bliver anvendt i overensstemmelse med de krav, der følger af CSI. Den omstændighed, at de i hovedsagen omhandlede lovbestemmelser ikke foreskriver, at de berørte personer skal underrettes om de overvågningsforanstaltninger, som de har været genstand for, udgør således ikke i sig selv et uforholdsmæssigt indgreb i retten til respekt for privatlivet.

68 Under disse omstændigheder har Conseil d'État (øverste domstol i forvaltningsretlige sager) besluttet at udsætte sagen og at forelægge Domstolen følgende præjudicielle spørgsmål:

»1) Skal den forpligtelse til generel og udifferentieret lagring, som pålægges udbyderne på grundlag af bestemmelserne i artikel 15, stk. 1, i direktiv [2002/58], i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror, anses for et indgreb, der er begrundet i retten til personlig sikkerhed, som er sikret ved [chartrets] artikel 6 […], og hensyn til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 [TEU]?

2) Skal direktiv [2002/58,] sammenholdt med [chartret,] fortolkes således, at det tillader lovgivningsmæssige foranstaltninger, såsom foranstaltninger med henblik på indsamling i realtid af trafik- og lokaliseringsdata vedrørende bestemte personer, som ganske vist påvirker rettigheder og forpligtelser for udbydere af en elektronisk kommunikationstjeneste, men dog ikke pålægger dem en specifik forpligtelse til lagring af deres data?

3) Skal direktiv [2002/58,] sammenholdt med [chartret,] fortolkes således, at det i alle tilfælde gør [lovligheden] af procedurer til indsamling af forbindelsesdata betinget af opfyldelsen af et krav om underretning af de berørte personer, når en sådan underretning ikke længere kan skade de kompetente myndigheders efterforskning, eller kan sådanne procedurer anses for at være [lovlige,] henset til samtlige øvrige eksisterende proceduremæssige garantier, idet disse sikrer, at adgangen til retsmidler er effektiv?«

Sag C-512/18

69 Ved et søgsmål anlagt den 1. september 2015 ved Conseil d'État (øverste domstol i forvaltningsretlige sager) har French Data Network, Quadrature du Net og Fédération des fournisseurs d'accès à Internet associatifs nedlagt påstand om annullation af den stiltiende afgørelse om afslag, der fulgte af premierministerens manglende reaktion på deres anmodning om ophævelse af CPCE's artikel R. 10-13 og af dekret 2011-219, bl.a. med den begrundelse, at disse tekster er i strid med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11. Privacy International og Center for Democracy and Technology har fået tilladelse til at intervenere i hovedsagen.

70 Hvad angår CPCE's artikel R. 10-13 og den deri fastsatte forpligtelse til at foretage generel og udifferentieret lagring af kommunikationsdata har den forelæggende ret, der har anført betragtninger svarende til dem, der er fremsat i forbindelse med sag C-511/18, nævnt, at en sådan lagring gør det muligt for den retslige myndighed at få adgang til data om kommunikation, som en person har taget del i, før vedkommende er blevet mistænkt for at have begået en strafbar handling, hvilket indebærer, at nytten af denne lagring med henblik på at efterforske, fastslå og retsforfølge strafbare handlinger savner modstykke.

71 Hvad angår dekret 2011-219 er den forelæggende ret af den opfattelse, at LCEN's artikel 6, stk. II, der udelukkende pålægger en forpligtelse til bevaring og lagring af data, der vedrører skabelse af indhold, ikke er omfattet af anvendelsesområdet for direktiv 2002/58, idet dette anvendelsesområde i overensstemmelse med dette direktivs artikel 3, stk. 1, er begrænset til at omfatte offentligt tilgængelige elektroniske kommunikationstjenester, der stilles til rådighed via offentlige kommunikationsnet i Unionen, men inden for anvendelsesområdet for direktiv 2000/31.

72 Den forelæggende ret er imidlertid af den opfattelse, at det af artikel 15, stk. 1 og 2, i direktiv 2000/31 følger, at dette direktiv ikke indfører et principielt forbud mod lagring af data, der vedrører skabelse af indhold, som kun kan fraviges undtagelsesvis. Dette rejser spørgsmålet om, hvorvidt det nævnte direktivs artikel 12, 14 og 15, sammenholdt med chartrets artikel 6-8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at disse bestemmelser tillader en medlemsstat at indføre en national lovgivning, såsom LCEN's artikel 6, stk. II, der pålægger de berørte personer at lagre data, som vil kunne gøre det muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer, for at den retslige myndighed i påkommende tilfælde kan kræve videregivelse heraf med henblik på at sikre overholdelsen af reglerne om civil- eller strafferetligt ansvar.

73 Under disse omstændigheder har Conseil d'État (øverste domstol i forvaltningsretlige sager) besluttet at udsætte sagen og at forelægge Domstolen følgende præjudicielle spørgsmål:

»1) Skal den forpligtelse til generel og udifferentieret lagring, som pålægges udbyderne på grundlag af bestemmelserne i artikel 15, stk. 1, i direktiv [2002/58], navnlig henset til de garantier og den kontrol, som derefter er knyttet til indsamlingen og anvendelsen af disse forbindelsesdata, anses for et indgreb, der er begrundet i retten til personlig sikkerhed, som er sikret ved [chartrets] artikel 6 […], og hensyn til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 [TEU]?

2) Skal bestemmelserne i direktiv [2000/31,] sammenholdt med [chartrets] artikel 6, 7, 8, 11 og artikel 52, stk. 1, […] fortolkes således, at de tillader en stat at indføre en national lovgivning, der pålægger personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester, og fysiske eller juridiske personer, der, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art, der leveres af modtagere af disse tjenester, at lagre data, som vil kunne gøre det muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer, for at den retslige myndighed i påkommende tilfælde kan kræve videregivelse heraf med henblik på at sikre overholdelsen af reglerne om civil- eller strafferetligt ansvar?«

Sag C-520/18

74 Ved søgsmål anlagt den 10. januar, den 16. januar, den 17. januar og den 18. januar 2017 ved Cour constitutionnelle (forfatningsdomstol, Belgien), og senere forenet i hovedsagen, har Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL og UA, Liga voor Mensenrechten ASBL og Ligue des Droits de l'Homme ASBL samt VZ, WY og XX nedlagt påstand om annullation af

lov af 29. maj 2016 med den begrundelse, at denne lov tilsidesætter artikel 10 og 11 i den belgiske forfatning, sammenholdt med EMRK's artikel 5, 6-11, 14, 15, 17 og 18, chartrets artikel 7, 8, 11 og 47 samt artikel 52, stk. 1, artikel 17 i den internationale konvention om borgerlige og politiske rettigheder, vedtaget af De Forenede Nationers Generalforsamling den 16. december 1966 og trådt i kraft den 23. marts 1976, generelle principper om retssikkerhed, proportionalitet og selvbestemmelse på informationsområdet samt artikel 5, stk. 4, TEU.

75 Sagsøgerne i hovedsagen har til støtte for deres søgsmål i det væsentlige gjort gældende, at lov af 29. maj 2016 navnlig som følge af den omstændighed, at denne lov overskrider grænserne for det strengt nødvendige og ikke fastsætter tilstrækkelige garantier for beskyttelse, er ulovlig. Hverken denne lovs bestemmelser om datalagring eller dens bestemmelser om myndighedernes adgang til lagrede data opfylder de krav, der følger af dom af 8. april 2014, Digital Rights Ireland m.fl. (C-293/12 og C-594/12, herefter »Digital Rights-dommen«, EU:C:2014:238), og af 21. december 2016, Tele2 (C-203/15 og C-698/15, EU:C:2016:970). Disse bestemmelser medfører nemlig en risiko for, at der udfærdiges personprofiler, som kan føre til misbrug fra de kompetente myndigheders side, og fastsætter heller ikke et passende sikkerheds- og beskyttelsesniveau for de lagrede data. Endelig omfatter denne lov de personer, der er underlagt tavshedspligt, og de personer, der er underlagt en fortrolighedsforpligtelse, og vedrører følsomme personoplysninger uden at indeholde særlige garantier med henblik på at beskytte disse sidstnævnte oplysninger.

76 Den forelæggende ret har anført, at de data, som udbyderne af telefontjenester, herunder IP-telefoni, internetadgang, e-mailtjenester, og de operatører, der udbyder offentlige elektroniske kommunikationsnet i henhold til lov af 29. maj 2016 er de samme som dem, der er nævnt i Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006, L 105, s. 54), uden at der er foretaget en sondring med hensyn til de berørte personer eller ud fra det forfulgte formål. I denne sidstnævnte henseende har den forelæggende ret præciseret, at det formål, som lovgiver forfølger med denne lov, ikke kun er at bekæmpe terrorisme og børnepornografi, men ligeledes at kunne anvende de lagrede oplysninger i en række forskellige situationer i forbindelse med strafferetlig efterforskning. Den forelæggende ret har endvidere anført, at det af begrundelsen for den nævnte lov fremgår, at den nationale lovgiver var af den opfattelse, at det i lyset af det forfulgte formål ikke var muligt at indføre en forpligtelse til at foretage målrettet og differentieret lagring, og at denne lovgiver valgte at lade forpligtelsen til at foretage generel og udifferentieret lagring ledsage af strenge garantier med hensyn til såvel de lagrede data som adgangen hertil, med henblik på at begrænse indgrebet i retten til respekt for privatlivet til et minimum.

77 Den forelæggende ret har tilføjet, at artikel 126, stk. 2, nr. 1° og 2°, i lov af 13. juni 2005 i den affattelse, der følger af lov af 29. maj 2016, fastsætter de betingelser, hvorunder henholdsvis de retslige myndigheder og efterretnings- og sikkerhedstjenesterne kan få adgang til de lagrede data, og undersøgelsen af, om denne lov i lyset af de krav, der følger af EU-retten, er lovlig, bør derfor udsættes, indtil Domstolen har truffet afgørelse i de to præjudicielle sager, der verserer for den, og som vedrører en sådan adgang.

78 Endelig har den forelæggende ret anført, at lov af 29. maj 2016 har til formål at gøre det muligt at sikre effektiv strafferetlig efterforskning af og effektive sanktioner over for seksuelt misbrug af mindreårige og at gøre det muligt at foretage identifikation af gerningsmanden bag en sådan overtrædelse, selv i de tilfælde, hvor der gøres brug af elektroniske kommunikationsmidler. Under sagen for den forelæggende ret er opmærksomheden i denne henseende blevet henledt på de positive forpligtelser, der følger af EMRK's artikel 3 og 8. Disse forpligtelser kan ligeledes følge af de tilsvarende bestemmelser i chartret, hvilket kan påvirke fortolkningen af artikel 15, stk. 1, i direktiv 2002/58.

79 Under disse omstændigheder har Cour constitutionnelle (forfatningsdomstol) besluttet at udsætte sagen og at forelægge Domstolen følgende præjudicielle spørgsmål:

»1) Skal artikel 15, stk. 1, i direktiv [2002/58], sammenholdt med den ret til sikkerhed, der er sikret ved [chartrets] artikel 6 […], og retten til respekt for personoplysninger, som er sikret ved [chartrets] artikel 7, 8 og artikel 52, stk. 1, […], fortolkes således, at bestemmelsen er til hinder for en national lovgivning – såsom den omhandlede, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata som omhandlet i direktiv [2002/58], der genereres og behandles af dem inden for rammerne af udbuddet af disse tjenester – som ikke kun har efterforskning, afsløring og retsforfølgning af grov kriminalitet som formål, men ligeledes sikring af den nationale sikkerhed, forsvar af territoriet, den offentlige sikkerhed, efterforskning, afsløring og retsforfølgning af andre grunde end grov kriminalitet eller forebyggelse af ulovlig brug af elektroniske kommunikationssystemer eller gennemførelse af et andet formål i henhold til artikel 23, stk. 1, i forordning [2016/679], og som endvidere er undergivet præcise garantier i denne lovgivning vedrørende lagring af data og adgangen dertil?

2) Skal artikel 15, stk. 1, i direktiv [2002/58], sammenholdt med [chartrets] artikel 4,7, 8, 11 og artikel 52, stk. 1, […] fortolkes således, at bestemmelsen er til hinder for en national lovgivning – såsom den omhandlede, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata som omhandlet i direktiv [2002/58], der genereres og behandles af dem inden for rammerne af udbuddet af disse tjenester – såfremt denne lovgivning bl.a. har til formål at opfylde de positive forpligtelser, der påhviler myndigheden i henhold til chartrets artikel 4 og [7], der består i at fastsætte en retlig ramme, der muliggør en effektiv strafferetlig efterforskning af og en effektiv retshåndhævelse over for seksuelt misbrug af mindreårige, og som rent faktisk gør det muligt at identificere gerningsmanden bag overtrædelsen, selv i tilfælde, hvor der gøres brug af elektroniske kommunikationsmidler?

3) Såfremt Cour constitutionnelle (forfatningsdomstol) på grundlag af besvarelserne af det første og det andet præjudicielle spørgsmål konkluderer, at den anfægtede lov er i strid med en eller flere af de forpligtelser, der følger af de i disse spørgsmål nævnte bestemmelser, kan Cour constitutionnelle (forfatningsdomstol) da midlertidigt opretholde virkningerne af lov af [29. maj 2016] med henblik på at undgå retsusikkerhed og muliggøre, at data, der forinden er blevet indsamlet og lagret, stadig kan anvendes til de formål, der er omhandlet i loven?«

Retsforhandlingerne for Domstolen

80 Ved afgørelse truffet af Domstolens præsident den 25. september 2018 er sag C-511/18 og sag C-512/18 blevet forenet med henblik på den skriftlige forhandling, den mundtlige forhandling og dommen. Ved afgørelse truffet af Domstolens præsident den 9. juli 2020 er sag C-520/18 blevet forenet med disse sager med henblik på dommen.

De præjudicielle spørgsmål

De første spørgsmål i sagerne C-511/18 og C-512/18 og det første og det andet spørgsmål i sag C-520/18

81 Med det første spørgsmål i sagerne C-511/18 og C-512/18 og det første og det andet spørgsmål i sag C-520/18, som skal behandles samlet, ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 15, stk. 1, i direktiv 2002/58 skal fortolkes således, at denne bestemmelse er til hinder for en

national lovgivning, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, pålægger udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata.

Indledende bemærkninger

82 Det fremgår af de sagsakter, som Domstolen råder over, at de i hovedsagerne omhandlede lovgivninger omfatter alle elektroniske kommunikationsmidler og alle de brugere, der anvender disse midler, uden i denne henseende at foreskrive nogen form for sondring eller undtagelse. De data, som udbyderne af elektroniske kommunikationstjenester i medfør af disse lovgivninger skal lagre, er endvidere navnlig de data, der er nødvendige for at spore kilden til en kommunikation og dens bestemmelsessted, fastslå en kommunikations dato, tidspunkt, varighed og type, identificere det anvendte kommunikationsudstyr og foretage lokalisering af terminaludstyret og kommunikationerne, dvs. data, der navnlig omfatter navn og adresse på brugeren, telefonnummer på den, der foretager opkaldet, og det kaldte nummer samt for internettjenester en IP-adresse. De nævnte data omfatter derimod ikke indholdet af den pågældende kommunikation.

83 De data, der i henhold til de i hovedsagerne omhandlede nationale lovgivninger skal lagres i et år, gør det således navnlig muligt at få kendskab til, med hvilken person brugeren af et elektronisk kommunikationsmiddel har kommunikeret, og ved hjælp af hvilket middel denne kommunikation har fundet sted, at fastslå datoen og tidspunktet for samt varigheden af kommunikationen og internetforbindelsen, og den lokalitet, hvorfra den har fundet sted, og at få kendskab til lokaliseringen af terminaludstyr, uden at der nødvendigvis er sket overføring af kommunikation. Desuden gør disse data det muligt at få kendskab til hyppigheden af brugerens kommunikation med bestemte personer i en given periode. Hvad endelig angår den i sagerne C-511/18 og C-512/18 omhandlede nationale lovgivning synes denne lovgivning, for så vidt som den også omfatter de data, der vedrører overføring af elektronisk kommunikation via netværk, at gøre det muligt at identificere arten af de oplysninger, der er tilgået online.

84 Hvad angår de forfulgte formål skal det bemærkes, at de i sagerne C-511/18 og C-512/18 omhandlede lovgivninger bl.a. har til formål at gøre det muligt at efterforske, fastslå og retsforfølge strafbare handlinger i almindelighed og at sikre hensynet til statens uafhængighed, den territoriale integritet og det nationale forsvar, væsentlige udenrigspolitiske interesser, opfyldelsen af Frankrigs europæiske og internationale forpligtelser, Frankrigs væsentlige økonomiske, industrielle og videnskabelige interesser samt hensynet til at forebygge terrorisme, angreb mod institutioners republikanske grundlag og kollektive voldshandlinger, der alvorligt påvirker opretholdelsen af lov og orden. Hvad angår den i sag C-520/18 omhandlede lovgivning har denne bl.a. til formål at gøre det muligt at efterforske, afsløre og retsforfølge strafbare handlinger samt at varetage hensynet til beskyttelsen af den nationale sikkerhed, forsvaret af territoriet og den offentlige sikkerhed.

85 De forelæggende retter ønsker nærmere bestemt oplyst, hvilken eventuel indvirkning retten til personlig sikkerhed, der er sikret ved chartrets artikel 6, har på fortolkningen af artikel 15, stk. 1, i direktiv 2002/58. De ønsker endvidere oplyst, om det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som den lagring af data, der er fastsat bestemmelse om i de i hovedsagerne omhandlede lovgivninger, medfører, kan anses for at være begrundet som følge af eksistensen af regler, der begrænser de nationale myndigheders adgang til de lagrede data. Conseil d'État (øverste domstol i forvaltningsretlige sager) er endvidere af den opfattelse, at eftersom dette spørgsmål er opstået i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed, skal det desuden vurderes i lyset af artikel 4, stk. 2, TEU. Cour constitutionnelle (forfatningsdomstol) har anført, at den i sag C-520/18 omhandlede nationale lovgivning endvidere gennemfører de positive forpligtelser, der følger af chartrets artikel 4 og 7, og som består i at fastsætte en retlig ramme, der gør det muligt at foretage effektiv retshåndhævelse over for seksuelt misbrug af mindreårige.

86 Mens såvel Conseil d'État (øverste domstol i forvaltningsretlige sager) som Cour constitutionnelle (forfatningsdomstol) har taget udgangspunkt i den forudsætning, at de i hovedsagerne omhandlede nationale lovgivninger, som regulerer lagring af trafikdata og lokaliseringsdata, samt de nationale myndigheders adgang til disse data med henblik på de formål, der er fastsat i artikel 15, stk. 1, i direktiv 2002/58, såsom beskyttelsen af den nationale sikkerhed, er omfattet af dette direktivs anvendelsesområde, har visse af parterne i hovedsagerne og visse af de medlemsstater, der har indgivet skriftlige indlæg til Domstolen, i denne forbindelse givet udtryk for en anden opfattelse, navnlig med hensyn til fortolkningen af det nævnte direktivs artikel 1, stk. 3. Det skal derfor først undersøges, om de nævnte lovgivninger er omfattet af anvendelsesområdet for dette samme direktiv.

Anvendelsesområdet for direktiv 2002/58

87 La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International og Center for Democracy and Technology har i denne henseende under henvisning til Domstolens praksis vedrørende anvendelsesområdet for direktiv 2002/58 i det væsentlige anført, at såvel lagringen af data som adgangen til de lagrede data er omfattet af dette anvendelsesområde, uanset om denne adgang finder sted med forsinkelse eller i realtid. Eftersom formålet om at beskytte den nationale sikkerhed udtrykkeligt er nævnt i dette direktivs artikel 15, stk. 1, kan forfølgelsen af dette formål ikke medføre, at det nævnte direktiv ikke finder anvendelse. Artikel 4, stk. 2, TEU, som de forelæggende retter har henvist til, påvirker ikke denne vurdering.

88 Hvad angår de efterretningsforanstaltninger, som de kompetente franske myndigheder anvender direkte, uden at regulere den virksomhed, der udøves af udbyderne af elektroniske kommunikationstjenester, ved at pålægge dem specifikke forpligtelser, har Center for Democracy and Technology anført, at disse foranstaltninger nødvendigvis er omfattet af anvendelsesområdet for direktiv 2002/58 og af anvendelsesområdet for chartret, eftersom de udgør undtagelser fra det fortrolighedsprincip, der er sikret ved dette direktivs artikel 5. De nævnte foranstaltninger skal således overholde de krav, der følger af dette direktivs artikel 15, stk. 1.

89 Den franske, den tjekkiske og den estiske regering, Irland, den cypriotiske, den ungarske, den polske og den svenske regering samt Det Forenede Kongeriges regering har derimod i det væsentlige gjort gældende, at direktiv 2002/58 ikke finder anvendelse på nationale lovgivninger som de i hovedsagerne omhandlede, for så vidt som disse lovgivninger har til formål at beskytte den nationale sikkerhed. For så vidt som efterretningstjenesternes aktiviteter vedrører opretholdelse af lov og orden samt beskyttelse af den interne sikkerhed og den territoriale integritet, henhører de under medlemsstaternes centrale funktioner og dermed under medlemsstaternes enekompetence, således som det bl.a. fremgår af artikel 4, stk. 2, tredje punktum, TEU.

90 Disse regeringer og Irland har endvidere henvist til artikel 1, stk. 3, i direktiv 2002/58, hvorefter dette direktivs anvendelsesområde i lighed med, hvad der allerede fremgik af artikel 3, stk. 2, første led, i direktiv 95/46, ikke omfatter de aktiviteter, der vedrører den offentlige sikkerhed, forsvaret og statens sikkerhed. Disse procesdeltagere har i denne henseende støttet sig på den fortolkning af denne sidstnævnte bestemmelse, der fremgår af dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346).

91 Det skal i denne henseende bemærkes, at det af artikel 1, stk. 1, i direktiv 2002/58 fremgår, at dette direktiv bl.a. tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor.

92 Dette direktivs artikel 1, stk. 3, udelukker fra sit anvendelsesområde »statens aktiviteter« på de områder, som er nævnt deri, herunder statens aktiviteter på det strafferetlige område og aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed, herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed. De aktiviteter, der er nævnt som eksempler heri, er under alle omstændigheder statens eller statslige myndigheders aktiviteter, der ikke har noget at gøre med området for den enkelte borgers aktiviteter (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 32 og den deri nævnte retspraksis).

93 Det fremgår endvidere af artikel 3 i direktiv 2002/58, at dette direktiv finder anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Unionen, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr (herefter »de elektroniske kommunikationstjenester«). Det nævnte direktiv skal derfor anses for at regulere den virksomhed, som udbydere af sådanne tjenester udøver (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 33 og den deri nævnte retspraksis).

94 I denne henseende gør artikel 15, stk. 1, i direktiv 2002/58 det muligt for medlemsstaterne under iagttagelse af de i direktivet fastsatte betingelser at vedtage »retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i [dette direktivs] artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9« (dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 71).

95 Artikel 15, stk. 1, i direktiv 2002/58 forudsætter imidlertid nødvendigvis, at de heri omhandlede nationale retsforskrifter er omfattet af det nævnte direktivs anvendelsesområde, idet det af direktivet udtrykkeligt fremgår, at medlemsstaterne kun må vedtage sådanne retsforskrifter under iagttagelse af de i direktivet fastsatte betingelser. Sådanne retsforskrifter regulerer desuden med de i bestemmelsen fastsatte formål for øje den virksomhed, som udøves af udbydere af elektroniske kommunikationstjenester (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 34 og den deri nævnte retspraksis).

96 Domstolen fastslog bl.a. ud fra disse betragtninger, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med dette direktivs artikel 3, skal fortolkes således, at det ikke kun er en retsforskrift, der pålægger udbyderne af elektroniske kommunikationstjenester at lagre trafikdata og lokaliseringsdata, der er omfattet af dette direktivs anvendelsesområde, men også en retsforskrift, der pålægger disse udbydere at give de kompetente nationale myndigheder adgang til disse data. Sådanne retsforskrifter indebærer nemlig nødvendigvis, at de nævnte udbydere behandler de nævnte oplysninger, og kan, for så vidt som de regulerer de nævnte udbyderes virksomhed, ikke sidestilles med statens aktiviteter, der er omfattet af det nævnte direktivs artikel 1, stk. 3 (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 35 og 37 og den deri nævnte retspraksis).

97 Henset til de betragtninger, der fremgår af denne doms præmis 95, og til den generelle opbygning af direktiv 2002/58 ville en fortolkning af dette direktiv, hvorefter de retsforskrifter, der er nævnt i dets artikel 15, stk. 1, er udelukket fra det nævnte direktivs anvendelsesområde som følge af, at de formål, som sådanne retsforskrifter skal opfylde, i det væsentlige kan sammenholdes med de formål, der forfølges med de i dette samme direktivs artikel 1, stk. 3, omhandlede aktiviteter, endvidere fratage denne artikel 15, stk. 1, enhver effektiv virkning (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 72 og 73).

98 Begrebet »aktiviteter«, der er anvendt i artikel 1, stk. 3, i direktiv 2002/58, kan, således som generaladvokaten i det væsentlige har anført i punkt 75 i forslaget til afgørelse i sagen La Quadrature du Net m.fl. (C-511/18 og C-512/18, EU:C:2020:6), derfor ikke fortolkes således, at det omfatter de retsforskrifter, der er omhandlet i dette direktivs artikel 15, stk. 1.

99 Artikel 4, stk. 2, TEU, som de regeringer, der er nævnt i denne doms præmis 89, har henvist til, kan ikke rejse tvivl om denne konklusion. Det fremgår nemlig af Domstolens faste praksis, at selv om det tilkommer medlemsstaterne at fastsætte deres væsentlige sikkerhedsinteresser og at træffe de nødvendige foranstaltninger til at opretholde deres indre og ydre sikkerhed, kan alene den omstændighed, at en national foranstaltning er blevet truffet med henblik på at beskytte den nationale sikkerhed, ikke medføre, at EU-retten ikke finder anvendelse, og fritage medlemsstaterne fra at sikre den nødvendige overholdelse af denne ret (jf. i denne retning dom af 4.6.2013, ZZ, C-300/11, EU:C:2013:363, præmis 38, af 20.3.2018, Kommissionen mod Østrig (Statstrykkeri), C-187/16, EU:C:2018:194, præmis 75 og 76, og af 2.4.2020, Kommissionen mod Polen, Ungarn og Den Tjekkiske Republik (Midlertidig flytningsordning for ansøgere om international beskyttelse), C-715/17, C-718/17 og C-719/17, EU:C:2020:257, præmis 143 og 170).

100 Det er korrekt, at Domstolen i dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346, præmis 56-59), fastslog, at luftfartsselskabers videregivelse af personoplysninger til offentlige myndigheder i et tredjeland med henblik på at forebygge og bekæmpe terrorisme og andre alvorlige forbrydelser i henhold til artikel 3, stk. 2, første led, i direktiv 95/46 ikke var omfattet af dette direktivs anvendelsesområde, eftersom denne videregivelse skete inden for rammer, der var indført af de offentlige myndigheder, og som vedrørte den offentlige sikkerhed.

101 Henset til de betragtninger, der fremgår af denne doms præmis 93, 95 og 96, kan denne retspraksis imidlertid ikke overføres på fortolkningen af artikel 1, stk. 3, i direktiv 2002/58. Således som generaladvokaten i det væsentlige har anført i punkt 70-72 i forslag til afgørelse La Quadrature du Net m.fl. (C-511/18 og C-512/18, EU:C:2020:6), udelukkede artikel 3, stk. 2, første led, i direktiv 95/46, som den nævnte retspraksis omhandlede, nemlig generelt »behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed«, fra dette sidstnævnte direktivs anvendelsesområdet, uden at foretage en sondring ud fra, hvem der havde behandlet de pågældende data. Det er i forbindelse med fortolkningen af artikel 1, stk. 3, i direktiv 2002/58, til gengæld nødvendigt at foretage en sådan sondring. Som det fremgår af denne doms præmis 94-97, henhører al behandling af personoplysninger, der foretages af udbydere af elektroniske kommunikationstjenester, nemlig under det nævnte direktivs anvendelsesområde, herunder de behandlinger, der følger af de forpligtelser, som disse udbydere er pålagt af de offentlige myndigheder, selv om disse sidstnævnte behandlinger i givet fald kunne være omfattet af den undtagelse, der er fastsat i artikel 3, stk. 2, første led, i direktiv 95/46, som følge af den bredere formulering af denne bestemmelse, der omhandler alle behandlinger, uanset hvem der foretager dem, og som vedrører den offentlige sikkerhed, forsvaret eller statens sikkerhed.

102 Det skal i øvrigt bemærkes, at direktiv 95/46, der var genstand for den sag, der gav anledning til dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346), i henhold til artikel 94, stk. 1, i forordning 2016/679 blev ophævet og erstattet af denne sidstnævnte forordning med virkning fra den 25. maj 2018. Selv om det af den nævnte forordnings artikel 2, stk. 2, litra d), fremgår, at denne forordning ikke gælder for behandlinger, som foretages af »kompetente myndigheder« med henblik på bl.a. at forebygge og afsløre strafbare handlinger, herunder beskytte og forebygge trusler mod den offentlige sikkerhed, fremgår det af samme forordnings artikel 23, stk. 1, litra d) og h), at behandling af personoplysninger, der af privatpersoner foretages med henblik på de samme formål, er omfattet af forordningens anvendelsesområde. Det følger heraf, at den ovenfor anførte fortolkning af artikel 1, stk. 3, artikel 3 og artikel 15, stk. 1, i direktiv 2002/58 er i overensstemmelse med den afgrænsning af anvendelsesområdet for forordning 2016/679, som dette direktiv supplerer og præciserer.

103 Når medlemsstaterne direkte vedtager foranstaltninger, der fraviger kravet om fortrolighed i forbindelse med elektronisk kommunikation, uden at pålægge de udbydere, der tilbyder denne form for kommunikation, behandlingsforpligtelser, henhører beskyttelsen af de pågældende personoplysninger til gengæld ikke under direktiv 2002/58, men udelukkende under national ret, dog med forbehold af anvendelsen af Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med

henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2006, L 119, s. 89), hvilket indebærer, at de omhandlede foranstaltninger skal overholde bl.a. de nationale regler, der har forfatningsrang, og de krav, der følger af EMRK.

104 Det følger af de ovenfor anførte betragtninger, at en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at lagre trafikdata og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed og bekæmpe kriminalitet, såsom de i hovedsagerne omhandlede lovgivninger, er omfattet af anvendelsesområdet for direktiv 2002/58.

Fortolkningen af artikel 15, stk. 1, i direktiv 2002/58

105 Det skal indledningsvis bemærkes, at det af fast retspraksis fremgår, at der ved fortolkningen af en EU-retlig bestemmelse ikke blot skal tages hensyn til dennes ordlyd, men også til den sammenhæng, hvori den indgår, og til de mål, der forfølges med den lovgivning, som den er en del af, og bl.a. til denne lovgivnings tilblivelse (jf. i denne retning dom af 17.4.2018, Egenberger, C-414/16, EU:C:2018:257, præmis 44).

106 Som det bl.a. fremgår af sjette og syvende betragtning til direktiv 2002/58, har dette direktiv til formål at beskytte brugerne af elektroniske kommunikationstjenester mod de risikomomenter for deres personoplysninger og privatliv, der følger af anvendelsen af ny teknologi, og navnlig den øgede mulighed for at foretage automatiseret opbevaring og behandling af oplysninger. Det nævnte direktiv søger, således som det fremgår af anden betragtning hertil, især at sikre fuld overholdelse af de rettigheder, der er nævnt i chartrets artikel 7 og 8. Det fremgår i denne henseende af begrundelsen til forslaget til Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000) 385 endelig), der lå til grund for direktiv 2002/58, at EU-lovgiver ønskede »at sikre, at der fortsat garanteres en høj grad af beskyttelse af personoplysninger og privatlivets fred i forbindelse med alle elektroniske kommunikationstjenester, uanset hvilken teknologi der anvendes«.

107 Artikel 5, stk. 1, i direktiv 2002/58 fastsætter i denne henseende princippet om fortrolighed i forbindelse med såvel elektronisk kommunikation som de dermed forbundne trafikdata, og indebærer navnlig, at det for andre end brugerne principielt er forbudt for enhver at lagre denne kommunikation og disse data, uden at disse brugere har givet samtykke hertil.

108 Hvad navnlig angår den behandling og lagring af trafikdata, der foretages af udbydere af elektroniske kommunikationstjenester, fremgår det af artikel 6 i samt af 22. og 26. betragtning til direktiv 2002/58, at en sådan behandling kun er tilladt i det omfang og tidsrum, der er nødvendigt af hensyn til markedsføringen og faktureringen af tjenesterne, samt leveringen af tillægstjenester. Når denne frist er udløbet, skal de behandlede eller lagrede data slettes eller gøres anonyme. Hvad angår andre lokaliseringsdata end trafikdata bestemmer det nævnte direktivs artikel 9, stk. 1, at disse data kun kan behandles under visse betingelser og kun, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil (dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 86 og den deri nævnte retspraksis).

109 EU-lovgiver har således med vedtagelsen af dette direktiv konkretiseret de rettigheder, der er sikret ved chartrets artikel 7 og 8, hvilket indebærer, at brugerne af elektroniske kommunikationsmidler principielt med rette kan forvente, at deres kommunikation og de dermed forbundne data forbliver anonyme, så længe de ikke har givet deres samtykke, og ikke kan gøres til genstand for registrering.

110 Artikel 15, stk. 1, i direktiv 2002/58 gør det imidlertid muligt for medlemsstaterne at indføre undtagelser til såvel den i dette direktivs artikel 5, stk. 1, fastsatte principielle forpligtelse til at sikre fortroligheden af personoplysninger som til de tilsvarende forpligtelser, der bl.a. er anført i det nævnte direktivs artikel 6 og 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed, forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af disse hensyn.

111 Når dette er sagt, kan den mulighed for at fravige de rettigheder og forpligtelser, der er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, ikke begrunde, at en fravigelse af den principielle pligt til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data, og navnlig af det forbud mod at lagre disse data, der udtrykkeligt er fastsat i dette direktivs artikel 5, bliver hovedreglen (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 89 og 104).

112 Hvad angår de formål, som kan begrunde en begrænsning af de rettigheder og forpligtelser, der er fastsat i navnlig artikel 5, 6 og 9 i direktiv 2002/58, har Domstolen allerede fastslået, at opregningen af de formål, der er fastsat i dette direktivs artikel 15, stk. 1, første punktum, er udtømmende, således at en retsforskrift, der er vedtaget i henhold til denne bestemmelse, faktisk og præcist skal opfylde et af disse formål (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 52 og den deri nævnte retspraksis).

113 Det fremgår endvidere af artikel 15, stk. 1, tredje punktum, i direktiv 2002/58, at medlemsstaterne kun har mulighed for at vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der er omhandlet i dette direktivs artikel 5, 6 og 9, såfremt dette sker i overensstemmelse med EU-rettens generelle principper, som bl.a. omfatter proportionalitetsprincippet, og de grundlæggende rettigheder, der er sikret ved chartret. Domstolen har i denne henseende allerede fastslået, at den pligt, som en medlemsstat i henhold til en national lovgivning har pålagt udbydere af elektroniske kommunikationstjenester, til at lagre trafikdata med henblik på i påkommende tilfælde at gøre dem tilgængelige for de kompetente nationale myndigheder, ikke blot rejser en række spørgsmål vedrørende overholdelsen af chartrets artikel 7 og 8, der vedrører henholdsvis respekten for privatlivet og beskyttelsen af personoplysninger, men ligeledes vedrørende artikel 11, der omhandler ytringsfriheden (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 25 og 70, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 91 og 92 og den deri nævnte retspraksis).

114 I forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 skal der således tages hensyn til betydningen af såvel retten til respekt for privatlivet, der er sikret ved chartrets artikel 7, som retten til beskyttelse af personoplysninger, der er sikret ved dette charters artikel 8, således som denne betydning fremgår af Domstolens praksis, og retten til ytringsfrihed, idet denne grundlæggende rettighed, der er sikret ved chartrets artikel 11, udgør et af de væsentlige grundlag for et demokratisk og pluralistisk samfund, og er en del af de værdier, som Unionen i overensstemmelse med artikel 2 TEU er støttet på (jf. i denne retning dom af 6.3.2001, Connolly mod Kommissionen, C-274/99 P, EU:C:2001:127, præmis 39, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 93 og den deri nævnte retspraksis).

115 Det skal i denne henseende præciseres, at lagring af trafikdata og lokaliseringsdata i sig selv udgør dels en undtagelse fra det forbud mod at lagre disse data, der er fastsat i artikel 5, stk. 1, i direktiv 2002/58, og som gælder for alle andre end brugerne, dels et indgreb i den grundlæggende ret til respekt for privatlivet og til beskyttelse af personoplysninger, der er sikret ved chartrets artikel 7 og 8, idet det ikke er afgørende, om de pågældende oplysninger vedrørende privatlivet er følsomme, eller om dette indgreb har medført eventuelle ubehageligheder for de berørte (jf. i denne retning udtalelse 1/15

(PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 124 og 126 og den deri nævnte retspraksis; jf. analogt om EMRK's artikel 8, Menneskerettighedsdomstolen, 30.1.2020, Breyer mod Tyskland, CE:ECHR:2020:0130JUD005000112, § 81).

116 Det er desuden ikke afgørende, om de lagrede data efterfølgende anvendes (jf. analogt om EMRK's artikel 8, Menneskerettighedsdomstolen, 16.2.2000, Amann mod Schweiz, CE:ECHR:2000:0216JUD002779895, § 69, og af 13.2.2020, Trjakovski og Chipovski mod Nordmakedonien, CE:ECHR:2020:0213JUD005320513, § 51), idet adgangen til sådanne data, uanset hvorledes disse data efterfølgende anvendes, udgør et særskilt indgreb i de grundlæggende rettigheder, der er nævnt i den foregående præmis (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 124 og 126).

117 Denne konklusion forekommer så meget desto mere begrundet, som trafikdata og lokaliseringsdata kan afsløre oplysninger om en lang række forhold, der vedrører de berørte personers privatliv, herunder følsomme oplysninger, såsom oplysninger om seksuel orientering, politiske anskuelser, samfundsmæssige, filosofiske, religiøse og andre overbevisninger samt oplysninger om helbredstilstand, mens sådanne oplysninger i øvrigt nyder en særlig beskyttelse i EU-retten. De nævnte data vil tilsammen kunne gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer. Særligt gør disse data det muligt at lave en profil af de berørte personer, hvilken oplysning, henset til retten for respekt af privatlivet, er lige så følsom som selve indholdet af kommunikationen (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 27, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 99).

118 For det første bemærkes, at lagring af trafikdata og lokaliseringsdata med henblik på politimæssige formål i sig selv kan medføre et indgreb i retten til respekt for kommunikation, der er sikret ved chartrets artikel 7, og have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved dette charters artikel 11 (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 28, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 101). Sådanne afskrækkende virkninger kan imidlertid navnlig påvirke de personer, hvis kommunikation i henhold til nationale bestemmelser er undergivet tavshedspligt, og de whistleblowere, hvis aktiviteter er beskyttet i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (EUT 2019, L 305, s. 17). Disse virkninger er desuden så meget desto mere alvorlige i betragtning af, at der er tale om store mængder af lagrede data af meget forskellig art.

119 For det andet bemærkes, at henset til den store mængde trafikdata og lokaliseringsdata, der løbende kan lagres ved hjælp af en generel og udifferentieret lagringsforanstaltning, og den følsomme karakter af de oplysninger, som disse data kan give adgang til, medfører alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, en risiko for misbrug og ulovlig adgang.

120 Når dette er sagt, afspejler artikel 15, stk. 1, i direktiv 2002/58, for så vidt som den giver medlemsstaterne mulighed for at indføre de undtagelser, der er nævnt i denne doms præmis 110, det forhold, at de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, ikke er absolutte rettigheder, men skal ses i sammenhæng med deres funktion i samfundet (jf. i denne retning dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 172 og den deri nævnte retspraksis).

121 Som det fremgår af chartrets artikel 52, stk. 1, tillader dette charter nemlig begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen og respekterer de nævnte rettigheders væsentligste indhold, og for så vidt som disse begrænsninger under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

122 I forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 i lyset af chartret skal der således også tages hensyn til betydningen af de rettigheder, der er sikret ved chartrets artikel 3, 4, 6 og 7, og den betydning, som formålene om beskyttelse af den nationale sikkerhed og om bekæmpelse af grov kriminalitet har som følge af, at de bidrager til beskyttelsen af andres rettigheder og friheder.

123 Chartrets artikel 6, som Conseil d'État (øverste domstol i forvaltningsretlige sager) og Cour constitutionnelle (forfatningsdomstol) har henvist til, fastsætter i denne henseende ikke blot retten for enhver til frihed, men også til personlig sikkerhed, og sikrer rettigheder, der svarer til dem, der er sikret ved EMRK's artikel 5 (jf. i denne retning dom af 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, præmis 47, af 28.7.2016, JZ, C-294/16 PPU, EU:C:2016:610, præmis 48, og af 19.9.2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, præmis 42 og den deri nævnte retspraksis).

124 Det skal endvidere bemærkes, at chartrets artikel 52, stk. 3, har til formål at sikre den nødvendige sammenhæng mellem de i chartret indeholdte rettigheder og de tilsvarende ved EMRK sikrede rettigheder, uden at dette berører EU-rettens og Den Europæiske Unions Domstols autonomi. Der skal derfor ved fortolkningen af chartret tages hensyn til de tilsvarende rettigheder i EMRK som tærskel for minimumsbeskyttelse (jf. i denne retning dom af 12.2.2019, TC, C-492/18 PPU, EU:C:2019:108, præmis 57, og af 21.5.2019, Kommissionen mod Ungarn (Brugsrettigheder over landbrugsarealer), C-235/17, EU:C:2019:432, præmis 72 og den deri nævnte retspraksis).

125 Hvad angår EMRK's artikel 5, der fastsætter »retten til frihed« og »retten til personlig sikkerhed«, har denne artikel ifølge Den Europæiske Menneskerettighedsdomstols praksis til formål at beskytte individet mod enhver form for vilkårlig eller ubegrundet frihedsberøvelse (jf. i denne retning Menneskerettighedsdomstolen, 18.3.2008, Ladent mod Polen, CE:ECHR:2008:0318JUD001103603, §§ 45 og 46, 29.3.2010, Medvedyev m.fl. mod Frankrig, CE:ECHR:2010:0329JUD000339403, §§ 76 og 77, og af 13.12.2012, El-Masri mod »The former Yugoslav Republic of Macedonia«, CE:ECHR:2012:1213JUD003963009, § 239). Eftersom denne bestemmelse omhandler frihedsberøvelse, der foretages af en offentlig myndighed, kan chartrets artikel 6 imidlertid ikke fortolkes således, at den pålægger de offentlige myndigheder en pligt til at vedtage specifikke foranstaltninger med henblik på at retsforfølge visse strafbare handlinger.

126 Hvad navnlig angår den effektive bekæmpelse af strafbare handlinger, som navnlig mindreårige og andre sårbare personer er ofre for, og som Cour constitutionnelle (forfatningsdomstol) har henvist til, skal det derimod fremhæves, at der i medfør af chartrets artikel 7 kan påhvile de offentlige myndigheder positive forpligtelser til at vedtage retlige foranstaltninger, der har til formål at beskytte privatlivet og familielivet (jf. i denne retning dom af 18.6.2020, Kommissionen mod Ungarn (Foreningers gennemsigtighed), C-78/18, EU:C:2020:476, præmis 123 og den deri nævnte praksis fra Menneskerettighedsdomstolen). Sådanne forpligtelser kan ligeledes følge af den nævnte artikel 7 med hensyn til den beskyttelse, der gælder for en persons hjem og kommunikation, af artikel 3 og 4 med hensyn til beskyttelsen af en persons fysiske og psykiske integritet og af forbuddet mod tortur og umenneskelig og nedværdigende behandling.

127 Som følge af eksistensen af disse forskellige positive forpligtelser, er det imidlertid nødvendigt, at der foretages en afvejning mellem de omhandlede forskellige interesser og rettigheder.

128 Den Europæiske Menneskerettighedsdomstol har således fastslået, at de positive forpligtelser, der følger af EMRK's artikel 3 og 8, idet chartrets artikel 4 og 7 indeholder de tilsvarende garantier, navnlig indebærer, at der skal vedtages materielle og proceduremæssige bestemmelser samt praktiske

foranstaltninger, der gør det muligt effektivt at bekæmpe lovovertrædelser mod personer gennem effektiv efterforskning og retsforfølgning, idet denne forpligtelse er så meget desto vigtigere, når et barns fysiske og psykiske velbefindende er truet. Når dette er sagt, skal de foranstaltninger, som det tilkommer de kompetente myndigheder at træffe, fuldt ud respektere adgangen til retsmidler og de andre garantier, der kan begrænse omfanget af de strafferetlige efterforskningsbeføjelser, og de andre rettigheder og frihedsrettigheder. Der skal efter denne domstols opfattelse navnlig indføres en retlig ramme, der gør det muligt at foretage en afvejning mellem de forskellige interesser og rettigheder, der skal beskyttes (Menneskerettighedsdomstolen, 28.10.1998, Osman mod Det Forenede Kongerige, CE:ECHR:1998:1028JUD002345294, §§ 115 og 116, 4.3.2004, M.C. mod Bulgarien, CE:ECHR:2003:1204JUD003927298, § 151, 24.6.2004, Von Hannover mod Tyskland, CE:ECHR:2004:0624JUD005932000, §§ 57 og 58, og 2.12.2008, K.U. mod Finland, CE:ECHR:2008:1202JUD000287202, §§ 46, 48 og 49).

129 Hvad angår overholdelsen af proportionalitetsprincippet bestemmer artikel 15, stk. 1, første punktum, i direktiv 2002/58, at medlemsstaterne kan vedtage en foranstaltning, der fraviger princippet om fortroligheden af kommunikation og de dermed forbundne trafikdata, når en sådan foranstaltning er »nødvendig, passende og forholdsmæssig i et demokratisk samfund« af hensyn til de formål, der er nævnt i denne bestemmelse. Det fremgår af 11. betragtning til dette direktiv, at en foranstaltning af denne art skal stå i »åbenbart« rimeligt forhold til det mål, der forfølges.

130 Det skal i denne henseende bemærkes, at det af Domstolens faste praksis fremgår, at beskyttelsen af den grundlæggende ret til respekt for privatlivet kræver, at undtagelserne til og begrænsningerne af beskyttelsen af personoplysninger holdes inden for det strengt nødvendige. Desuden kan et mål af almen interesse ikke forfølges uden hensyntagen til den omstændighed, at dette mål skal forenes med de grundlæggende rettigheder, der er berørt af foranstaltningen, ved at foretage en rimelig afvejning mellem målet af almen interesse og de pågældende rettigheder (jf. i denne retning dom af 16.12.2008, Satakunnan Markkinapörssi og Satamedia, C-73/07, EU:C:2008:727, præmis 56, af 9.11.2010, Volker und Markus Schecke og Eifert, C-92/09 og C-93/09, EU:C:2010:662, præmis 76, 77 og 86, og af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 52, samt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 140).

131 Det fremgår nærmere bestemt af Domstolens praksis, at medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der navnlig er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, skal vurderes ved at bedømme alvoren af det indgreb, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 55 og den deri nævnte retspraksis).

132 For at opfylde kravet om proportionalitet skal en lovgivning fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug. Denne lovgivning skal være retligt bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige. Nødvendigheden af at råde over sådanne garantier er så meget desto større, når personoplysningerne er undergivet en automatiseret behandling, navnlig når der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger. Disse betragtninger gør sig især gældende, når der er tale om beskyttelse af den særlige kategori af personoplysninger, som følsomme oplysninger udgør (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 54 og 55, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 117, samt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 141).

133 En lovgivning, der foreskriver lagring af personoplysninger, skal således altid opfylde objektive kriterier, som fastlægger et forhold mellem de oplysninger, der skal lagres, og det forfulgte mål (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 191 og den deri nævnte retspraksis, og dom af 3.10.2019, A m.fl., C-70/18, EU:C:2019:823, præmis 63).

– De lovgivningsmæssige foranstaltninger, der foreskriver forebyggende lagring af trafikdata og lokaliseringsdata med henblik på beskyttelse af den nationale sikkerhed

134 Det skal bemærkes, at Domstolen i de domme, hvori den har foretaget en fortolkning af direktiv 2002/58, endnu ikke konkret har taget stilling til det formål om beskyttelse af den nationale sikkerhed, som de forelæggende retter og de regeringer, der har afgivet indlæg, har henvist til.

135 Det skal i denne henseende indledningsvis bemærkes, at det af artikel 4, stk. 2, TEU fremgår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar. Dette ansvar svarer til den primære interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed.

136 Formålet om beskyttelse af den nationale sikkerhed, sammenholdt med artikel 4, stk. 2, TEU, vejere tungere end de andre formål, der er indeholdt i artikel 15, stk. 1, i direktiv 2002/58, bl.a. formålet om bekæmpelse af kriminalitet i almindelighed, herunder også grov kriminalitet, og om beskyttelse af den offentlige sikkerhed. Trusler som dem, der er nævnt i den foregående præmis, adskiller sig nemlig på grund af deres art og særligt alvorlige karakter fra den generelle risiko for, selv alvorlige, spændinger eller forstyrrelser, for den offentlige sikkerhed. Med forbehold for overholdelsen af de øvrige krav, der er fastsat i chartrets artikel 52, stk. 1, kan formålet om beskyttelse af den nationale sikkerhed derfor begrunde foranstaltninger, der indebærer indgreb i de grundlæggende rettigheder, som er mere alvorlige end dem, som disse andre formål kan begrunde.

137 I situationer som dem, der er beskrevet i denne doms præmis 135 og 136, er artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, således principielt ikke til hinder for en lovgivningsmæssig foranstaltning, der giver de kompetente myndigheder mulighed for at pålægge udbydere af elektroniske kommunikationstjenester at foretage lagring af trafikdata og lokaliseringsdata, der vedrører alle de brugere, som anvender elektroniske kommunikationsmidler i en begrænset periode, når der foreligger tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at den berørte medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed som den, der er nævnt i denne doms præmis 135 og 136, og som må anses for at være reel og aktuel eller forudsigelig. Selv om en sådan foranstaltning uden forskel omfatter alle brugere af elektroniske kommunikationsmidler, uden at disse umiddelbart synes at have en forbindelse som omhandlet i den retspraksis, der er nævnt i denne doms præmis 133, til en trussel mod denne medlemsstats nationale sikkerhed, skal det ikke desto mindre fastslås, at den omstændighed, at der foreligger en sådan trussel, i sig selv kan godtgøre, at der består en sådan forbindelse.

138 Et påbud om at foretage forebyggende lagring af data, der vedrører alle brugere af elektroniske kommunikationsmidler, skal ikke desto mindre tidsmæssigt begrænses til det strengt nødvendige. Selv om det ikke kan udelukkes, at et påbud, der udstedes til udbyderne af elektroniske kommunikationstjenester, om at foretage lagring af data, kan forlænges som følge af, at en sådan trussel fortsat består, må varigheden af hvert enkelt påbud ikke overstige et forudseeligt tidsrum. Desuden skal en sådan lagring af data være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug. Denne lagring må således ikke have en systematisk karakter.

139 Henset til alvoren af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som følger af en sådan generel og udifferentieret datalagringsforanstaltning, er det vigtigt at sikre, at anvendelsen af denne foranstaltning rent faktisk begrænses til de situationer, hvor der foreligger en alvorlig trussel mod den nationale sikkerhed, såsom de situationer, der er omhandlet i denne doms præmis 135 og 136. Det er i denne henseende væsentligt, at en afgørelse, hvorved udbyderne af elektroniske kommunikationstjenester pålægges at foretage en sådan lagring af data, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

– De lovgivningsmæssige foranstaltninger, der foreskriver forebyggende lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af kriminalitet og beskyttelse af den offentlige sikkerhed

140 Hvad angår formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger er det i overensstemmelse med proportionalitetsprincippet kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, såsom de indgreb, som lagring af trafikdata og lokaliseringsdata indebærer. Det er således kun de indgreb i de nævnte grundlæggende rettigheder, der ikke er alvorlige, som kan begrundes i formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 102, og af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 56 og 57, samt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 149).

141 En national lovgivning, der foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, overskrider det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 107).

142 Henset til den følsomme karakter af de oplysninger, som trafikdata og lokaliseringsdata kan give adgang til, er det nemlig af afgørende betydning for retten til respekt for privatlivet, at disse data behandles med fortrolighed. Når der henses til dels de afskrækkende virkninger for udøvelsen af de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 11, og som er nævnt i denne doms præmis 118, som lagringen af disse data kan have, dels alvoren af det indgreb, som en sådan lagring indebærer, er det i et demokratisk samfund således væsentligt, at dette indgreb, således som det er tilfældet for det system, der er indført ved direktiv 2002/58, udgør undtagelsen og ikke reglen, og at disse data ikke kan gøres til genstand for en systematisk og løbende lagring. Denne konklusion gælder selv med hensyn til formålene om bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed samt den betydning, som disse formål skal tillægges.

143 Domstolen har endvidere fastslået, at en lovgivning, der foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata, omfatter elektronisk kommunikation, der foretages af praktisk talt hele befolkningen, uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål. En sådan lovgivning omfatter i modsætning til det krav, der er nævnt i denne doms præmis 133, generelt alle personer, der gør brug af elektroniske kommunikationstjenester, uden at disse personer – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning. Den finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – sammenhæng med dette formål om at bekæmpe handlinger i form af grov kriminalitet, og navnlig uden at der er foreligger nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel

mod den offentlige sikkerhed (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 57 og 58, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 105).

144 Som Domstolen allerede har fastslået, er en sådan lovgivning navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af grov kriminalitet (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 59, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 106).

145 Selv de positive forpligtelser for medlemsstaterne, der alt efter omstændighederne kan følge af chartrets artikel 3, 4 og 7, og som, således som det er anført i denne doms præmis 126 og 128, vedrører indførelsen af regler, der gør det muligt effektivt at bekæmpe strafbare handlinger, kan imidlertid ikke begrunde indgreb, der er så alvorlige som de indgreb, som en lovgivning, der foreskriver lagring af trafikdata og lokaliseringsdata, indebærer i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, og som berører praktisk talt hele befolkningen, uden at de berørte personers data kan afsløre en forbindelse, endog ikke indirekte, til det forfulgte formål.

146 I overensstemmelse med det i denne doms præmis 142-144 anførte og henset til den afvejning, der nødvendigvis skal foretages mellem de omhandlede rettigheder og interesser, kan formålene om bekæmpelse af grov kriminalitet og om forebyggelse af alvorlige angreb mod den offentlige sikkerhed og a fortiori formålet om beskyttelse af den nationale sikkerhed i betragtning af deres betydning og under hensyn til de positive forpligtelser, der er nævnt i den foregående præmis, hvortil Cour constitutionnelle (forfatningsdomstol) bl.a. har henvist, til gengæld begrunde det særligt alvorlige indgreb, som en målrettet lagring af trafikdata og data indebærer.

147 Som Domstolen allerede har fastslået, er artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, således ikke til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt med henblik på beskyttelse af den nationale sikkerhed, forudsat at en sådan lagring begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 108).

148 Hvad angår den afgrænsning, der skal foretages med hensyn til en sådan datalagringsforanstaltning, kan denne foranstaltning navnlig fastsættes på grundlag af kategorier af berørte personer, idet artikel 15, stk. 1, i direktiv 2002/58 ikke er til hinder for en lovgivning, der er baseret på objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafikdata og lokaliseringsdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed eller endog en risiko for den nationale sikkerhed (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 111).

149 I denne henseende skal det præciseres, at de således omhandlede personer bl.a. kan være sådanne, som på forhånd inden for rammerne af de gældende nationale procedurer og på grundlag af objektive forhold er blevet identificeret som en trussel mod den pågældende medlemsstats offentlige sikkerhed eller nationale sikkerhed.

150 Afgrænsningen af en foranstaltning, der foreskriver lagring af trafikdata og lokaliseringsdata, kan endvidere baseres på et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive og ikke-diskriminerende forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at grov kriminalitet bliver planlagt eller begået (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 111). Disse områder kan navnlig være steder, der er kendetegnet ved et højt antal tilfælde af grov kriminalitet, steder, hvor der i særlig grad kan begås grov kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

151 For at sikre, at det indgreb, som de målrettede lagringsforanstaltninger, der er beskrevet i denne doms præmis 147-150, indebærer, er i overensstemmelse med proportionalitetsprincippet, må deres varighed ikke overstige, hvad der er strengt nødvendigt i forhold til det forfulgte formål og de omstændigheder, der begrunder dem, dog med forbehold af muligheden for at forlænge foranstaltningen som følge af, at det fortsat er nødvendigt at foretage en sådan lagring.

– De lovgivningsmæssige foranstaltninger, der foreskriver forebyggende lagring af IP-adresser og data vedrørende personers identitet med henblik på bekæmpelse af kriminalitet og beskyttelse af den offentlige sikkerhed

152 Det bemærkes, at selv om IP-adresser indgår blandt de forskellige former for trafikdata, genereres de uden at være knyttet til en bestemt kommunikation og tjener hovedsageligt til gennem udbydere af elektroniske kommunikationstjenester at identificere den fysiske person, der ejer det terminaludstyr, hvorfra en kommunikation via internettet foretages. Hvad angår e-mail og IP-telefoni afslører IP-adresser, for så vidt som det kun er IP-adresserne på kilden til kommunikationen og ikke IP-adresserne på modtageren af kommunikationen, der lagres, således ikke som sådan nogen oplysninger om de tredjemænd, der har været i kontakt med den person, som har foretaget kommunikationen. Denne kategori af data er derfor mindre følsomme end andre former for trafikdata.

153 Eftersom IP-adresser kan anvendes til bl.a. at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter, gør disse oplysninger det imidlertid muligt at skabe en detaljeret profil af denne internetbruger. Den lagring og analyse af de nævnte IP-adresser, som en sådan sporing kræver, udgør således alvorlige indgreb i internetbrugerens grundlæggende rettigheder, som er sikrede ved chartrets artikel 7 og 8, og som kan have afskrækkende virkninger som dem, der er nævnt i denne doms præmis 118.

154 Med henblik på at foretage den nødvendige afvejning af de omhandlede rettigheder og interesser, som kræves i henhold til den retspraksis, der er nævnt i denne doms præmis 130, skal der tages hensyn til den omstændighed, at IP-adressen i det tilfælde, hvor en lovovertrædelse er begået online, kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået. Hertil kommer den omstændighed, at den lagring af IP-adresser, som udbyderne af elektroniske kommunikationstjenester måtte foretage ud over den periode, for hvilken disse data er tildelt, principielt ikke forekommer at være nødvendig for faktureringen af de omhandlede tjenester, hvilket indebærer, at det af denne grund ikke vil være muligt at afsløre lovovertrædelser, der er begået online, således som flere regeringer har anført i deres indlæg for Domstolen, uden at anvende en lovgivningsmæssig foranstaltning i henhold til artikel 15, stk. 1, i direktiv 2002/58. Som disse regeringer har gjort gældende, kan dette bl.a. være tilfældet for særligt alvorlige lovovertrædelser på området for børnepornografi, såsom erhvervelse, udbredelse, transmission eller tilrådighedsstillelse online af børnepornografi som omhandlet i artikel 2, litra c), i Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT 2011, L 335, s. 1).

155 Under disse omstændigheder, og selv om det er korrekt, at en lovgivningsmæssig foranstaltning, der foreskriver lagring af IP-adresser på alle de fysiske personer, der ejer terminaludstyr, hvorfra det er muligt at tilgå internettet, vil omfatte personer, der ikke umiddelbart har en forbindelse som omhandlet i den retspraksis, der er nævnt i denne doms præmis 133, til de forfulgte formål, og at internetbrugere i overensstemmelse med, hvad der er fastslået i denne doms præmis 109, har ret til i henhold til chartrets artikel 7 og 8 at forvente, at deres identitet principielt ikke afsløres, forekommer en lovgivningsmæssig foranstaltning, der foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, principielt ikke at være i strid med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, under forudsætning af, at denne mulighed er betinget af en streng overholdelse af de materielle og proceduremæssige betingelser, der skal gælde for brugen af disse data.

156 Henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som denne lagring indebærer, er det kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der i lighed med beskyttelsen af den nationale sikkerhed kan begrunde dette indgreb. Lagringsperioden må endvidere ikke overstige, hvad der er strengt nødvendigt for at nå det forfulgte formål. Endelig skal en foranstaltning af denne art indeholde strenge betingelser og garantier for så vidt angår brugen af disse data, bl.a. ved hjælp af sporing, med hensyn til de kommunikationer og de aktiviteter, som de berørte personer foretager online.

157 Hvad endelig angår de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, gør disse data det ikke i sig selv muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode, hvilket indebærer, at disse data bortset fra de pågældendes kontaktoplysninger, såsom deres adresser, ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om disse personers privatliv. Det indgreb, som en lagring af disse data indebærer, kan således principielt ikke kvalificeres som alvorligt (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 59 og 60).

158 Det følger heraf, således som der er redegjort for i denne doms præmis 140, at de lovgivningsmæssige foranstaltninger, der vedrører behandlingen af disse data som sådan, herunder lagringen af og adgangen til disse data alene med henblik på at identificere den pågældende bruger, og uden at de nævnte data kan kædes sammen med oplysninger om den foretagne kommunikation, kan begrundes i det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed, hvortil artikel 15, stk. 1, første punktum, i direktiv 2002/58 henviser (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 62).

159 Henset til den nødvendige afvejning af de omhandlede rettigheder og interesser og af de grunde, der er anført i denne doms præmis 131 og 158, skal det under disse omstændigheder fastslås, at selv i de tilfælde, hvor der ikke foreligger nogen forbindelse mellem samtlige brugere af elektroniske kommunikationsmidler og de forfulgte mål, er artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke til hinder for en lovgivningsmæssig foranstaltning, der uden at fastsætte en særlig frist pålægger udbydere af elektroniske kommunikationstjenester at foretage lagring af data, der vedrører identiteten på alle de brugere, der anvender elektroniske kommunikationsmidler, med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger samt beskyttelse af den offentlige sikkerhed, uden at det er nødvendigt, at der foreligger alvorlige strafbare handlinger eller alvorlige trusler eller angreb mod den offentlige sikkerhed.

– De lovgivningsmæssige foranstaltninger, der foreskriver hurtig lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet

160 Hvad angår de trafikdata og lokaliseringsdata, som behandles og lagres af udbydere af elektroniske kommunikationstjenester på grundlag af artikel 5, 6 og 9 i direktiv 2002/58, eller på grundlag af de lovgivningsmæssige foranstaltninger, der er vedtaget i henhold til dette direktivs artikel 15, stk. 1, således som disse er beskrevet i denne doms præmis 134-159, skal det bemærkes, at disse data principielt skal slettes eller gøres anonyme efter udløbet af de lovbestemte frister, inden for hvilke disse data skal behandles og lagres i overensstemmelse med de nationale bestemmelser, der gennemfører dette direktiv.

161 Under denne behandling og lagring kan der imidlertid opstå situationer, hvori det er nødvendigt at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed, såvel i den situation, hvor disse strafbare handlinger eller disse angreb allerede har kunnet konstateres, som i den situation, hvor der efter en objektiv undersøgelse af samtlige relevante omstændigheder foreligger rimelig grund til at mistænke, at der er begået sådanne strafbare handlinger eller angreb.

162 I denne henseende bemærkes, at artikel 14 i Europarådets konvention af 23. november 2001 om [it]-kriminalitet (European Treaty Series – nr. 185), som blev undertegnet af 27 medlemsstater og ratificeret af 25 af disse medlemsstater, og hvis formål er at lette bekæmpelsen af strafbare handlinger, der begås ved hjælp af it-netværk, bestemmer, at de kontraherende parter med henblik på konkret efterforskning eller retsforfølgning af straffesager skal vedtage visse foranstaltninger med hensyn til allerede lagrede trafikdata, såsom hurtig lagring af disse data. Navnlig bestemmer denne konventions artikel 16, stk. 1, at de kontraherende parter skal vedtage de lovgivningsmæssige foranstaltninger, som måtte være nødvendige for, at deres kompetente myndigheder kan meddele pålæg om eller på anden lignende måde opnå hurtig sikring af data, herunder trafikdata, der er lagret ved hjælp af et it-system, navnlig hvis der er grund til at antage, at disse data er særligt udsat for at gå tabt eller blive ændret.

163 I en situation som den, der er omhandlet i denne doms præmis 161, står det, henset til den nødvendige afvejning af de omhandlede rettigheder og interesser, der er nævnt i denne doms præmis 130, medlemsstaterne frit for i en lovgivning, der vedtages i henhold til artikel 15, stk. 1, i direktiv 2002/58, at fastsætte muligheden for ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som de råder over.

164 For så vidt som formålet med en sådan hurtig lagring ikke længere svarer til de formål, hvortil oplysningerne oprindeligt blev indsamlet og lagret, og eftersom enhver behandling af data i henhold til chartrets artikel 8, stk. 2, skal opfylde udtrykkeligt angivne formål, skal medlemsstaterne i deres lovgivning præcisere det formål, med henblik på hvilket en hurtig lagring af data kan finde sted. Henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som en sådan lagring kan indebære, er det kun bekæmpelsen af grov kriminalitet og a fortiori beskyttelsen af den nationale sikkerhed, der kan begrunde dette indgreb. For at sikre, at det indgreb, som en foranstaltning af denne type indebærer, er begrænset til det strengt nødvendige, må lagringspligten desuden for det første kun vedrøre de trafikdata og lokaliseringsdata, der kan bidrage til at opklare alvorlige strafbare handlinger eller angreb mod den berørte nationale sikkerhed. For det andet skal datalagringens varighed begrænses til det strengt nødvendige, idet denne dog kan forlænges, når dette er begrundet i omstændighederne og det formål, der forfølges med den nævnte foranstaltning.

165 Det skal i denne forbindelse præciseres, at en sådan hurtig lagring ikke skal begrænses til data om de personer, der konkret er mistænkt for at have begået en strafbar handling eller et angreb mod den nationale sikkerhed. Under overholdelse af den ramme, der er fastsat i artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, og under hensyn til de

betragtninger, der fremgår af denne doms præmis 133, kan en sådan foranstaltning afhængigt af det valg, som lovgiver træffer, og såfremt den holder sig inden for det strengt nødvendige, udvides til at omfatte de trafikdata og lokaliseringsdata, der vedrører andre personer end dem, der mistænkes for at have planlagt eller begået en alvorlig strafbar handling eller et angreb mod den nationale sikkerhed, for så vidt som disse data på grundlag af objektive og ikke-diskriminerende forhold kan bidrage til at opklare en sådan strafbar handling eller et sådant angreb mod den nationale sikkerhed, såsom oplysninger om offeret for den strafbare handling eller angrebet, om den pågældendes sociale og arbejdsmæssige omgangskreds eller om bestemte geografiske områder, såsom de steder, hvor den omhandlede strafbare handling eller det omhandlede angreb mod den nationale sikkerhed blev begået eller planlagt. De kompetente myndigheders adgang til de således lagrede data skal desuden finde sted under iagttagelse af de betingelser, der følger af den retspraksis, hvori der er anlagt en fortolkning af direktiv 2002/58 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 118-121 og den deri nævnte retspraksis).

166 Det skal desuden tilføjes, således som det navnlig fremgår af denne doms præmis 115 og 133, at adgangen til de trafikdata og lokaliseringsdata, som udbyderne lagrer som følge af en foranstaltning, der er vedtaget i henhold til artikel 15, stk. 1, i direktiv 2002/58, i princippet kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring. Det følger navnlig heraf, at der under ingen omstændigheder kan gives adgang til sådanne data med henblik på at retsforfølge og straffe en almindelig strafbar handling, når lagringen heraf er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed. I overensstemmelse med proportionalitetsprincippet, således som dette er blevet præciseret i denne doms præmis 131, kan en adgang til data, der er lagret med henblik på bekæmpelse af grov kriminalitet, under forudsætning af, at de i den foregående præmis nævnte materielle og proceduremæssige betingelser, der gælder for at opnå en sådan adgang, overholdes, til gengæld begrundes i formålet om beskyttelse af den nationale sikkerhed.

167 I denne henseende står det medlemsstaterne frit for i deres lovgivning at fastsætte, at der under overholdelse af disse samme materielle og proceduremæssige betingelser kan gives adgang til trafikdata og lokaliseringsdata med henblik på bekæmpelsen af grov kriminalitet eller beskyttelsen af den nationale sikkerhed, når de nævnte data af en udbyder lagres på en måde, der er i overensstemmelse med artikel 5, 6 og 9 eller artikel 15, stk. 1, i direktiv 2002/58.

168 Henset til samtlige ovenfor anførte betragtninger skal de første spørgsmål i sagerne C-511/18 og C-512/18 og det første og det andet spørgsmål i sag C-520/18 besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for lovgivningsmæssige foranstaltninger, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata. Den nævnte artikel 15, stk. 1, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, er derimod ikke til hinder for lovgivningsmæssige foranstaltninger

– der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består

– der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges

– der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige

– der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og

– der med henblik på bekæmpelse af grov kriminalitet og a fortiori med henblik på beskyttelsen af den nationale sikkerhed, gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over

for så vidt som disse foranstaltninger ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.

Det andet og det tredje spørgsmål i sag C-511/18

169 Med det andet og det tredje spørgsmål i sag C-511/18 ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at anvende foranstaltninger i deres netværk, der gør det muligt dels at foretage automatiseret analyse og indsamling i realtid af trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, uden at der er fastsat bestemmelse om, at de berørte personer skal underrettes om disse behandlinger og disse indsamlinger.

170 Den forelæggende ret har præciseret, at de teknikker til indsamling af efterretninger, der er fastsat i CSI's artikel L. 851-2 til L. 851-4, ikke indebærer et specifikt krav om, at udbydere af elektroniske kommunikationstjenester skal foretage lagring af trafikdata og lokaliseringsdata. Hvad navnlig angår den automatiserede analyse, der er omhandlet i CSI's artikel L. 851-3, har denne ret anført, at denne behandling har til formål på grundlag af de kriterier, der er fastsat med henblik herpå, at opdage forbindelser, der kan afsløre en terrortrussel. Hvad angår den indsamling i realtid, der er nævnt i CSI's artikel L. 851-2, har denne ret konstateret, at denne indsamling kun vedrører en eller flere personer, der på forhånd er identificeret som personer, der kan have forbindelse til en terrortrussel. Denne samme ret har anført, at disse to teknikker kun kan anvendes med henblik på at forebygge terrorisme, og at de vedrører de data, der er omhandlet i CSI's artikel L. 851-1 og R. 851-5.

171 Det skal indledningsvis præciseres, at den omstændighed, at det af CSI's artikel L. 851-3 fremgår, at den deri fastsatte automatiserede analyse ikke som sådan gør det muligt at identificere de brugere, hvis data er genstand for denne analyse, ikke er til hinder for, at sådanne data kan kvalificeres som »personoplysninger«. Eftersom den procedure, der er fastsat i denne samme bestemmelses stk. IV, gør det muligt på et senere tidspunkt at identificere den eller de personer, der er omfattet af data, i hvilken forbindelse den automatiserede analyse har vist, at der kan foreligge en terrortrussel, er det nemlig

fortsat muligt ud fra disse data at identificere alle de personer, hvis oplysninger har været genstand for den automatiserede analyse. Det fremgår imidlertid af den definition af personoplysninger, der er indeholdt i artikel 4, nr. 1), i forordning 2016/679, at sådanne data udgør oplysninger, der bl.a. vedrører en identificerbar person.

Automatiseret analyse af trafikdata og lokaliseringsdata

172 Det fremgår af CSI's artikel L. 851-3, at den deri fastsatte automatiserede analyse i det væsentlige indebærer en filtrering af alle de trafikdata og lokaliseringsdata, der er lagret af udbyderne af elektroniske kommunikationstjenester, og som disse udbydere har foretaget på anmodning af de kompetente nationale myndigheder og under anvendelse af de parametre, som disse har fastsat. Det følger heraf, at alle de data, der vedrører brugerne af elektroniske kommunikationsmidler, kontrolleres, såfremt de opfylder disse parametre. En sådan automatiseret analyse skal derfor anses for at indebære, at de pågældende udbydere af elektroniske kommunikationstjenester på den kompetente myndigheds vegne foretager en generel og udifferentieret behandling i form af brug, der sker ved hjælp af en automatiseret behandling som omhandlet i artikel 4, nr. 2), i forordning 2016/679, og som omfatter samtlige trafikdata og lokaliseringsdata for alle brugere af elektroniske kommunikationsmidler. Denne behandling er uafhængig af den efterfølgende indsamling af de data, der vedrører de personer, som er blevet identificeret i forbindelse med den automatiserede analyse, idet en sådan indsamling er tilladt i henhold til CSI's artikel L. 851-3, stk. IV.

173 En national lovgivning, der gør det muligt at foretage en sådan automatiseret analyse af trafikdata og lokaliseringsdata, indebærer imidlertid en fravigelse fra den principielle forpligtelse, der er fastsat i artikel 5 i direktiv 2002/58, til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data. En sådan lovgivning udgør endvidere et indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, uanset hvilken brug der efterfølgende gøres af disse data. Endelig kan den nævnte lovgivning i overensstemmelse med den retspraksis, der er nævnt i denne doms præmis 118, have afskrækkende virkning på udøvelsen af ytringsfriheden, som er sikret ved chartrets artikel 11.

174 Desuden må et indgreb, der følger af en automatiseret analyse af trafikdata og lokaliseringsdata som den i hovedsagen omhandlede, anses for at være særlig alvorligt, når den generelt og udifferentieret omfatter data om de personer, der gør brug af elektroniske kommunikationsmidler. Denne konstatering gælder så meget desto mere når de data, der er genstand for den automatiserede analyse, således som det fremgår af den i hovedsagen omhandlede nationale lovgivning, kan afsløre arten af de oplysninger, der er blevet tilgået online. En sådan automatiseret analyse finder endvidere generelt anvendelse på alle de personer, der gør brug af elektroniske kommunikationsmidler, og dermed også på de personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til terrorvirksomhed.

175 Hvad angår begrundelsen for et sådant indgreb skal det præciseres, at det krav, der er fastsat i chartrets artikel 52, stk. 1, om, at enhver begrænsning af udøvelsen af de grundlæggende rettigheder skal være fastlagt i lovgivningen, indebærer, at det retsgrundlag, som tillader et indgreb i disse rettigheder, selv skal definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed (jf. i denne retning dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 175 og den deri nævnte retspraksis).

176 Desuden bemærkes, at for at opfylde kravet om proportionalitet, som er nævnt i denne doms præmis 130 og 131, ifølge hvilket undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige, skal en national lovgivning, der regulerer de kompetente myndigheders adgang til lagrede trafikdata og lokaliseringsdata, overholde de krav, som følger af den retspraksis, der er henvist til i denne doms præmis 132. En sådan lovgivning kan navnlig ikke begrænse sig til at opstille et krav om, at myndighedernes adgang til oplysninger skal

opfylde det med denne lovgivning forfulgte formål, men skal tillige fastsætte de materielle og processuelle betingelser for denne brug (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 192 og den deri nævnte retspraksis).

177 I denne henseende skal det bemærkes, at det særligt alvorlige indgreb, som en generel og udifferentieret lagring af trafikdata og lokaliseringsdata indebærer, og som er omhandlet i de betragtninger, der er anført i denne doms præmis 134-139, og det særligt alvorlige indgreb, som den automatiserede analyse indebærer, kun kan opfylde kravet om proportionalitet i de situationer, hvor en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, og på betingelse af, at varigheden af denne lagring er begrænset til det strengt nødvendige.

178 I situationer som dem, der er nævnt i den foregående præmis, skal anvendelsen af en automatiseret analyse af trafikdata og lokaliseringsdata, der vedrører alle brugere af elektroniske kommunikationsmidler, i en strengt begrænset periode, anses for at være begrundet i forhold til de krav, der følger af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.

179 Når dette er sagt, er det med henblik på at sikre, at anvendelsen af en sådan foranstaltning faktisk begrænser sig til, hvad der er strengt nødvendigt for at beskytte den nationale sikkerhed, og nærmere bestemt for at forebygge terrorisme, og i overensstemmelse med det i denne doms præmis 139 fastslåede, afgørende, at den afgørelse, der giver tilladelse til at foretage automatiseret analyse, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om der foreligger en situation, der kan begrunde den nævnte foranstaltning, og om de betingelser og garantier, der skal være fastsat, er overholdt.

180 I denne henseende skal det præciseres, at de forud fastsatte modeller og kriterier, som ligger til grund for denne form for databehandlinger, dels skal være specifikke og pålidelige, hvorved det bliver gjort muligt at nå frem til resultater, som identificerer de personer, om hvilke der kan foreligge en rimelig mistanke om, at de deltager i terrorhandlinger, dels ikke-diskriminerende (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 172).

181 Det skal desuden bemærkes, at enhver automatiseret analyse, der foretages på grundlag af modeller og kriterier, som er baseret på et postulat om, at racemæssig og etnisk baggrund, politisk, religiøs og filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, eller en persons helbredsforhold og seksualliv i sig selv og uafhængigt af denne persons adfærd kan være relevant med henblik på at forebygge terrorisme, vil være i strid med de rettigheder, der er sikret ved chartrets artikel 7 og 8, sammenholdt med chartrets artikel 21. De modeller og kriterier, der er fastsat på forhånd med henblik på at foretage en automatiseret analyse, der har til formål at forhindre terrorvirksomhed, som udgør en alvorlig trussel mod den nationale sikkerhed, kan således ikke alene baseres på disse følsomme oplysninger (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 165).

182 Eftersom automatiserede analyser af trafikdata og lokaliseringsdata nødvendigvis indebærer en vis fejlmargen, skal ethvert positivt resultat, der opnås som følge af en automatiseret behandling, i øvrigt undergives en individuel ikke-automatisk gennemgang inden vedtagelsen af en individuel foranstaltning, der er bebyrdende for de pågældende personer, såsom den efterfølgende indsamling af trafikdata og lokaliseringsdata i realtid, idet en sådan foranstaltning nemlig ikke kan være endeligt baseret alene på resultatet af en automatiseret behandling. For i praksis at sikre, at de forud fastsatte modeller og kriterier, brugen heraf og de anvendte databaser ikke er udtryk for forskelsbehandling og er begrænset til det strengt nødvendige i forhold til formålet om at forebygge terrorvirksomhed, der indebærer en alvorlig trussel mod den nationale sikkerhed, skal spørgsmålet om, hvorvidt disse forud

fastsatte modeller og kriterier samt de anvendte databaser er pålidelige og aktuelle, desuden gøres til genstand for en regelmæssig gennemgang (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 173 og 174).

Indsamling i realtid af trafikdata og lokaliseringsdata

183 Hvad angår den indsamling i realtid af trafikdata og lokaliseringsdata, der er omhandlet i CSI's artikel L. 851-2, skal det bemærkes, at denne indsamling kan godkendes individuelt for så vidt angår »en person, som på forhånd er identificeret som en person, der kan have forbindelse til en [terror]trussel«. Det følger ligeledes af denne bestemmelse, at »[h]vis der foreligger tungtvejende grunde til at antage, at en eller flere personer, der tilhører den personkreds, som den person, der er omfattet af tilladelsen, færdes i, er i stand til at tilvejebringe oplysninger, der vedrører det formål, som ligger til grund for tilladelsen, kan der desuden individuelt gives en sådan tilladelse med hensyn til hver enkelt af disse personer«.

184 De data, der er genstand for en foranstaltning af denne art, gør det muligt for de kompetente nationale myndigheder i løbet af tilladelsens varighed kontinuerligt og i realtid at overvåge de personer, som de berørte personer kommunikerer med, de midler, som de anvender, varigheden af deres kommunikation og disse personers opholdssted og færden. Disse data synes desuden at kunne afsløre arten af de oplysninger, der er blevet tilgået online. Disse oplysninger gør det, således som det fremgår af denne doms præmis 117, samlet set muligt at drage meget præcise konklusioner vedrørende de berørte personers privatliv og at udfærdige en profil af disse personer, idet en sådan oplysning i lyset af retten til respekt for privatlivet er lige så følsom som selve indholdet af kommunikationen.

185 Hvad angår den i CSI's artikel L. 851-4 omhandlede indsamling af data i realtid tillader denne bestemmelse indsamling af de tekniske data, der vedrører lokaliseringen af terminaludstyr, og overførsel i realtid til en tjeneste under premierministeren. Det fremgår, at sådanne data giver den kompetente tjeneste mulighed for til enhver tid i løbet af tilladelsens varighed kontinuerligt og i realtid at foretage lokalisering af det anvendte terminaludstyr, såsom mobiltelefoner.

186 En national lovgivning, der tillader sådanne indsamlinger i realtid, fraviger i lighed med den lovgivning, der tillader automatiseret dataanalyse, den principielle forpligtelse, der er fastsat i artikel 5 i direktiv 2002/58, til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data. Denne lovgivning udgør derfor ligeledes et indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, og som kan have afskrækkende virkning på udøvelsen af ytringsfriheden, der er sikret ved chartrets artikel 11.

187 Det skal bemærkes, at det indgreb, som indsamlingen af data i realtid, der gør det muligt at lokalisere et terminaludstyr, indebærer, forekommer særlig alvorligt, idet disse data giver de kompetente nationale myndigheder et middel til at foretage præcis og varig sporing af mobiltelefonbrugernes færden. Eftersom disse data således skal anses for at være særligt følsomme, skal der foretages en sondring mellem den adgang, som de kompetente myndigheder har til at tilgå sådanne data i realtid, og den adgang til disse data, der ikke sker i realtid, idet denne førstnævnte adgang er mere indgribende, for så vidt som den gør det muligt at foretage en næsten fuldstændig overvågning af disse brugere (jf. analogt for så vidt angår EMRK's artikel 8, Menneskerettighedsdomstolen, 8.2.2018, Ben Faiza mod Frankrig, CE:ECHR:2018:0208JUD003144612, § 74). Indgrebets intensitet forstærkes desuden, når indsamlingen i realtid også omfatter trafikdata vedrørende de berørte personer.

188 Selv om det formål om forebyggelse af terrorisme, der forfølges med den i hovedsagen omhandlede nationale lovgivning, henset til dets betydning, kan begrunde det indgreb, som indsamlingen i realtid af trafikdata og lokaliseringsdata indebærer, kan en sådan foranstaltning på grund af dens særligt indgribende karakter kun iværksættes over for de personer, i forhold til hvilke der foreligger en gyldig grund til at mistænke, at de på den ene eller den anden måde er involveret i terrorvirksomhed. Hvad

angår de personoplysninger, der ikke er omfattet af denne kategori, kan disse oplysninger kun gøres til genstand for en adgang, der ikke sker i realtid, idet en sådan adgang i overensstemmelse med Domstolens praksis kun kan finde sted i særlige situationer, såsom de situationer, hvori der er tale om terrorvirksomhed, og når der foreligger objektive forhold, som gør det muligt at antage, at disse data i en konkret sag kan bidrage effektivt til bekæmpelsen af en sådan virksomhed (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 119 og den deri nævnte retspraksis).

189 En afgørelse, der tillader indsamling i realtid af trafikdata og lokaliseringsdata, skal endvidere være baseret på objektive kriterier, der er fastsat i den nationale lovgivning. Denne lovgivning skal i overensstemmelse med den retspraksis, der er nævnt i denne doms præmis 176, navnlig fastlægge de omstændigheder og betingelser, hvorunder en sådan indsamling kan tillades, og fastsætte, at det, således som det er blevet præciseret i den foregående præmis, kun er de personer, der har en forbindelse til formålet om at forebygge terrorisme, som kan gøres til genstand for en sådan indsamling. En afgørelse, der tillader indsamling i realtid af trafikdata og lokaliseringsdata, skal desuden være baseret på objektive og ikke-diskriminerende kriterier, der er fastsat i den nationale lovgivning. Med henblik på i praksis at sikre iagttagelse af disse betingelser er det afgørende, at anvendelsen af den foranstaltning, der tillader indsamling i realtid, er undergivet en forudgående prøvelse, der foretages af enten en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, idet denne domstol eller enhed bl.a. skal sikre sig, at en sådan indsamling i realtid kun tillades inden for rammerne af, hvad der er strengt nødvendigt (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 120). I et behørigt begrundet hastende tilfælde skal denne prøvelse foretages hurtigst muligt.

Underretning af de personer, hvis oplysninger er blevet indsamlet eller analyseret

190 Det er væsentligt, at de kompetente nationale myndigheder, der foretager indsamling i realtid af trafikdata og lokaliseringsdata, underretter de berørte personer herom inden for rammerne af de gældende nationale procedurer, for så vidt som og fra det tidspunkt, hvor denne underretning ikke kan skade udførelsen af de opgaver, der påhviler disse myndigheder. En sådan underretning er nemlig de facto nødvendig for at gøre det muligt for disse personer at udøve deres ret i henhold til chartrets artikel 7 og 8 til at anmode om indsigt i de personoplysninger, der vedrører dem, og som er omfattet af disse foranstaltninger, og til i givet fald at anmode om berigtigelse eller sletning af disse oplysninger, samt til i overensstemmelse med chartrets artikel 47, stk. 1, at have adgang til effektive retsmidler for en domstol, idet en sådan ret i øvrigt udtrykkeligt er sikret ved artikel 15, stk. 2, i direktiv 2002/58, sammenholdt med artikel 79, stk. 1, i forordning 2016/679 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 121 og den deri nævnte retspraksis, og udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 219 og 220).

191 Hvad angår de oplysninger, der kræves i forbindelse med en automatiseret analyse af trafikdata og lokaliseringsdata, har den kompetente nationale myndighed pligt til at offentliggøre generelle oplysninger om denne analyse uden at skulle foretage en individuel underretning af de berørte personer. I det tilfælde, hvor dataene opfylder de parametre, der er præciseret i den foranstaltning, som gør det muligt at foretage en automatiseret analyse, og hvor denne myndighed identificerer den berørte person med henblik på at foretage en mere dybtgående analyse af de data, der vedrører den pågældende, er det til gengæld nødvendigt at give vedkommende en individuel underretning. En sådan underretning skal imidlertid kun ske for så vidt som og fra det tidspunkt, hvor den ikke kan skade udførelsen af de opgaver, der påhviler den nævnte myndighed (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 222-224).

192 Henset til samtlige ovenfor anførte betragtninger skal det andet og det tredje spørgsmål i sag C-511/18 besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse ikke er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester dels at gøre brug af automatiseret analyse og indsamling i realtid af navnlig trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, når

– brugen af automatiseret analyse er begrænset til de situationer, hvor en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, og brugen af denne analyse kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om der foreligger en situation, der kan begrunde den nævnte foranstaltning, og om de betingelser og garantier, der skal være fastsat, er overholdt, og når

– indsamlingen i realtid af trafikdata og lokaliseringsdata er begrænset til de personer, med hensyn til hvilke der foreligger rimelig grund til at mistænke, at de på den ene eller den anden måde er involveret i terrorvirksomhed, og er underlagt en forudgående prøvelse, der foretages af enten en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, for at sikre, at en sådan indsamling i realtid kun tillades inden for rammerne af, hvad der er strengt nødvendigt. I et behørigt begrundet hastende tilfælde skal denne prøvelse foretages hurtigst muligt.

Det andet spørgsmål i sag C-512/18

193 Med det andet spørgsmål i sag C-512/18 ønsker den forelæggende ret nærmere bestemt oplyst, om bestemmelserne i direktiv 2000/31, sammenholdt med chartrets artikel 6-8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at disse bestemmelser er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, som disse tjenester gør brug af.

194 Den forelæggende ret har anført, at sådanne tjenester er omfattet af anvendelsesområdet for direktiv 2000/31 og ikke anvendelsesområdet for direktiv 2002/58, og er af den opfattelse, at artikel 15, stk. 1 og 2, i direktiv 2000/31, sammenholdt med dette direktivs artikel 12 og 14, ikke i sig selv indfører et principielt forbud mod lagring af data, der vedrører skabelsen af indhold, som det kun undtagelsesvis er muligt at fravige. Denne ret er ikke desto mindre i tvivl om, hvorvidt denne vurdering skal følges, når der henses til den nødvendige hensyntagen til overholdelsen af de grundlæggende rettigheder, der er sikret ved chartrets artikel 6-8 og 11.

195 Den forelæggende ret har præciseret, at dens spørgsmål omhandler den lagringspligt, der er fastsat i LCEN's artikel 6, sammenholdt med dekret 2011-219. De data, som de pågældende tjenesteudbydere skal lagre i denne forbindelse, omfatter navnlig oplysninger om identiteten på de personer, der har gjort brug af disse tjenester, såsom deres for- og efternavn, deres tilknyttede postadresser, e-mailadresser eller tilhørende konti, deres adgangskoder og, når der i forbindelse med indgåelsen af en aftale eller oprettelsen af en konto opkræves betaling, oplysninger om den anvendte betalingsmetode, betalingsreferencen, beløbet og datoen og tidspunktet for transaktionen.

196 De data, der er genstand for lagringspligten, omfatter identifikatorerne for abonnenterne, forbindelserne og det anvendte terminaludstyr, de identifikatorer, der er tildelt for indholdet, datoerne og tidspunkterne for forbindelsernes og aktiviteternes opstart og afslutning samt de protokoltyper, der anvendes ved forbindelsen til tjenesten og til overførsel af indhold. Der kan under straffesager og civile sager anmodes om adgang til disse data, for hvilke lagringsperioden er på et år, med henblik på at sikre overholdelsen af reglerne om civil- eller strafferetligt ansvar og i forbindelse med de foranstaltninger til indsamling af efterretninger, hvorpå CSI's artikel L. 851-1 finder anvendelse.

197 Det skal i denne henseende bemærkes, at der i henhold til artikel 1, stk. 2, i direktiv 2000/31 ved dette direktiv foretages en tilnærmelse af visse nationale bestemmelser om informationssamfundstjenester som omhandlet i dette direktivs artikel 2, litra a).

198 Sådanne tjenester omfatter ganske vist de tjenester, der teleformidles ved hjælp af elektronisk databehandlingsudstyr og dataoplagringsudstyr på individuel anmodning af en tjenestemodtager, og normalt mod vederlag, såsom internetadgangstjenester eller tjenester i form af adgang til et kommunikationsnet, og hostingtjenester (jf. i denne retning dom af 24.11.2011, Scarlet Extended, C-70/10, EU:C:2011:771, præmis 40, af 16.2.2012, SABAM, C-360/10, EU:C:2012:85, præmis 34, af 15.9.2016, Mc Fadden, C-484/14, EU:C:2016:689, præmis 55, og af 7.8.2018, SNB-REACT, C-521/17, EU:C:2018:639, præmis 42 og den deri nævnte retspraksis).

199 Det fremgår imidlertid af artikel 1, stk. 5, i direktiv 2000/31, at dette direktiv ikke finder anvendelse på spørgsmål, der vedrører informationssamfundstjenester, som er omfattet af direktiv 95/46 og 97/66. Det fremgår i denne forbindelse af 14. og 15. betragtning til direktiv 2000/31, at beskyttelsen af kommunikationshemmeligheden og beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger med hensyn til informationssamfundstjenester udelukkende er reguleret ved direktiv 95/46 og 97/66, idet dette sidstnævnte direktiv i dets artikel 5 af hensyn til beskyttelsen af kommunikationshemmeligheden forbyder enhver form for opfangning eller overvågning af kommunikation.

200 De spørgsmål, der vedrører beskyttelsen af kommunikationshemmeligheden og af personoplysninger, skal således vurderes i lyset af direktiv 2002/58 og forordning 2016/679, som har erstattet henholdsvis direktiv 97/66 og direktiv 95/46, idet det præciseres, at den beskyttelse, som direktiv 2000/31 har til formål at sikre, under ingen omstændigheder kan berøre de krav, der følger af direktiv 2002/58 og forordning 2016/679 (jf. i denne retning dom af 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, præmis 57).

201 Den forpligtelse, der i henhold til den nationale lovgivning, der er nævnt i denne doms præmis 195, påhviler udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester, til at lagre de personoplysninger, der knytter sig til disse tjenester, skal, således som generaladvokaten i det væsentlige har anført i punkt 141 i forslag til afgørelse La Quadrature du Net m.fl. (C-511/18 og C-512/18, EU:C:2020:6), derfor vurderes i lyset af direktiv 2002/58 eller forordning 2016/679.

202 Afhængigt af, om leveringen af de tjenester, der er omfattet af denne nationale lovgivning, henhører eller ikke henhører under direktiv 2002/58, vil den således være reguleret enten ved dette sidstnævnte direktiv, navnlig ved dette direktivs artikel 15, stk. 1, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, eller ved forordning 2016/679, navnlig ved den nævnte forordnings artikel 23, stk. 1, sammenholdt med de samme bestemmelser i chartret.

203 I det foreliggende tilfælde kan det derfor ikke udelukkes, således som Europa-Kommissionen har anført i sit skriftlige indlæg, at visse af de tjenester, hvorpå den nationale lovgivning, der er omhandlet i denne doms præmis 195, finder anvendelse, udgør elektroniske kommunikationstjenester som omhandlet i direktiv 2002/58, hvilket det tilkommer den forelæggende ret at efterprøve.

204 Det skal i denne henseende bemærkes, at direktiv 2002/58 omfatter de elektroniske kommunikationstjenester, der opfylder de betingelser, der er nævnt i artikel 2, litra c), i direktiv 2002/21, hvortil der er henvist i artikel 2 i direktiv 2002/58, og hvori elektronisk kommunikationstjeneste er defineret som »en tjeneste, som normalt ydes mod betaling, og som udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet, herunder telekommunikationstjenester og transmissionstjenester på net, der anvendes til radio- og tv-spredning«. Hvad angår informationssamfundstjenester som dem, der er omhandlet i denne doms præmis 197 og 198, og som er omfattet af direktiv 2000/31, udgør disse tjenester elektroniske

kommunikationstjenester, idet de udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet (jf. i denne retning dom af 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, præmis 47 og 48).

205 Internetadgangstjenester, som synes at være omfattet af den nationale lovgivning, der er nævnt i denne doms præmis 195, udgør, som det bekræftes i tiende betragtning til direktiv 2002/21, således elektroniske kommunikationstjenester i dette direktivs forstand (jf. i denne retning dom af 5.6.2019, Skype Communications, C-142/18, EU:C:2019:460, præmis 37). Dette er ligeledes tilfældet for meddelelsestjenester på internettet, i hvilken forbindelse det ikke synes udelukket, at disse tjenester også er omfattet af denne nationale lovgivning, idet de rent teknisk udelukkende eller overvejende består i overføring af signaler via elektroniske kommunikationsnet (jf. i denne retning dom af 13.6.2019, Google, C-193/18, EU:C:2019:498, præmis 35 og 38).

206 Hvad angår de krav, der følger af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal der henvises til samtlige de konstateringer og vurderinger, der er foretaget i forbindelse med bevarelsen af de første spørgsmål i sagerne C-511/18 og C-512/18 og det første og det andet spørgsmål i sag C-520/18.

207 Hvad angår de krav, der følger af forordning 2016/679, skal det bemærkes, at denne forordning navnlig har til formål, således som det fremgår af tiende betragtning hertil, at sikre et højt niveau for beskyttelse af fysiske personer inden for Unionen, og med henblik herpå sikre, at reglerne for beskyttelse af disse personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen (jf. i denne retning dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 101).

208 I denne henseende skal enhver behandling af personoplysninger med forbehold af de undtagelser, der er tilladte i henhold til artikel 23 i forordning 2016/679, overholde de principper, der gælder for behandling af personoplysninger, og de rettigheder, der tilkommer den berørte person, og som er fastsat i henholdsvis denne forordnings kapitel II og III. Navnlig skal enhver behandling af personoplysninger være i overensstemmelse med de principper, der er fastsat i den nævnte forordnings artikel 5, og desuden opfylde de betingelser for lovlighed, der er anført i denne samme forordnings artikel 6 (jf. analogt for så vidt angår direktiv 95/46 dom af 30.5.2013, Worten, C-342/12, EU:C:2013:355, præmis 33 og den deri nævnte retspraksis).

209 Hvad nærmere bestemt angår artikel 23, stk. 1, i forordning 2016/679 skal det bemærkes, at denne bestemmelse i lighed med, hvad der er fastsat i artikel 15, stk. 1, i direktiv 2002/58, gør det muligt for medlemsstaterne med henblik på de deri fastsatte formål og ved hjælp af lovgivningsmæssige foranstaltninger at begrænse rækkevidden af de deri omhandlede forpligtelser og rettigheder, »når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til« det forfulgte formål. Enhver lovgivningsmæssig foranstaltning, der vedtages på dette grundlag, skal navnlig opfylde de specifikke krav, der er fastsat i denne forordnings artikel 23, stk. 2.

210 Artikel 23, stk. 1 og 2, i forordning 2016/679 skal derfor ikke fortolkes således, at den kan tildele medlemsstaterne beføjelse til i strid med chartrets artikel 7 at foretage indgreb i retten til respekt for privatlivet og i de andre garantier, der er fastsat heri (jf. analogt for så vidt angår direktiv 95/46, dom af 20.5.2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 og C-139/01, EU:C:2003:294, præmis 91). Nærmere bestemt kan den beføjelse, som medlemsstaterne er tildelt i medfør af artikel 23, stk. 1, i forordning 2016/679, i lighed med, hvad der gælder for artikel 15, stk. 1, i direktiv 2002/58, kun udøves under iagttagelse af kravet om proportionalitet, ifølge hvilket undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige (jf. analogt for så vidt angår direktiv 95/46 dom af 7.11.2013, IPI, C-473/12, EU:C:2013:715, præmis 39 og den deri nævnte retspraksis).

211 Det følger heraf, at de konstateringer og vurderinger, der er foretaget i forbindelse med besvarelsen af de første spørgsmål i sagerne C-511/18 og C-512/18 samt det første og det andet spørgsmål i sag C-520/18, finder tilsvarende anvendelse på artikel 23 i forordning 2016/679.

212 Henset til de ovenfor anførte betragtninger skal det andet spørgsmål i sag C-512/18 besvares med, at direktiv 2000/31 skal fortolkes således, at dette direktiv med hensyn til informationssamfundstjenester ikke finder anvendelse på området for beskyttelse af kommunikationshemmeligheden og af fysiske personer i forbindelse med behandlingen af personoplysninger, idet denne beskyttelse alt efter omstændighederne er reguleret ved direktiv 2002/58 eller forordning 2016/679. Artikel 23, stk. 1, i forordning 2016/679, sammenholdt med chartres artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, der er forbundet med brugen af disse tjenester.

Det tredje spørgsmål i sag C-520/18

213 Med det tredje spørgsmål i sag C-520/18 ønsker den forelæggende ret nærmere bestemt oplyst, om en national ret kan anvende en bestemmelse i den nationale lovgivning, som giver denne ret bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester med henblik på bl.a. at forfølge formålene om at beskytte den nationale sikkerhed og om at bekæmpe kriminalitet, at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som følge af, at denne lovgivning er uforenelig med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.

214 Ifølge princippet om EU-rettens forrang har EU-retten en fortrinsstilling i forhold til medlemsstaternes nationale ret. Dette princip medfører derfor en forpligtelse for alle instanser i medlemsstaterne til at sikre, at de forskellige EU-retlige regler gennemføres fuldt ud, idet medlemsstaternes nationale ret ikke kan ændre den virkning, som disse forskellige regler tillægges på disse staters område (dom af 15.7.1964, Costa, 6/64, EU:C:1964:66, s. 1159 og 1160, og af 19.11.2019, A.K. m.fl. (Den øverste domstols disciplinærafdelings uafhængighed), C-585/18, C-624/18 og C-625/18, EU:C:2019:982, præmis 157 og 158 og den deri nævnte retspraksis).

215 Den nationale ret, der inden for sit kompetenceområde skal anvende EU-retlige bestemmelser, har i henhold til princippet om forrang pligt til – såfremt det ikke er muligt at anlægge en fortolkning af national lovgivning, der er i overensstemmelse med de EU-retlige krav – at sikre disse bestemmelsers fulde virkning, idet den om fornødent af egen drift skal undlade at anvende enhver modstående bestemmelse i national lovgivning, endog en senere national bestemmelse, uden at den behøver at anmode om eller afvente en forudgående ophævelse af denne bestemmelse ad lovgivningsvejen eller ved noget andet forfatningsmæssigt middel (dom af 22.6.2010, Melki og Abdeli, C-188/10 og C-189/10, EU:C:2010:363, præmis 43 og den deri nævnte retspraksis, af 24.6.2019, Popławski, C-573/17, EU:C:2019:530, præmis 58, og af 19.11.2019, A.K. m.fl. (Den øverste domstols disciplinærafdelings uafhængighed), C-585/18, C-624/18 og C-625/18, EU:C:2019:982, præmis 160).

216 Det er alene Domstolen, der undtagelsesvis og af tvingende retssikkerhedsmæssige hensyn kan træffe bestemmelse om en midlertidig udsættelse af den fortrængende virkning, som en EU-bestemmelse har i forhold til national ret, der er i strid hermed. Der kan alene træffes bestemmelse om en sådan tidsmæssig begrænsning af virkningerne af Domstolens fortolkning af EU-retten i selve den dom, der afgør fortolkningsspørgsmålet (jf. i denne retning dom af 23.10.2012, Nelson m.fl., C-581/10 og C-629/10, EU:C:2012:657, præmis 89 og 91, af 23.4.2020, Herst, C-401/18, EU:C:2020:295, præmis 56 og 57, og af 25.6.2020, A m.fl. (Vindmøller i Aalter og Nevele), C-24/19, EU:C:2020:503, præmis 84 og den deri nævnte retspraksis).

217 Hvis de nationale retsinstanser havde beføjelse til at give nationale bestemmelser forrang for EU-retten, som disse bestemmelser strider mod, også selv om det blot er midlertidigt, ville dette være til skade for EU-rettens forrang og ensartede anvendelse (jf. i denne retning dom af 29.7.2019, Inter-Environnement Wallonie og Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, præmis 177 og den deri nævnte retspraksis).

218 Domstolen fastslog imidlertid i en sag, der omhandlede spørgsmålet om, hvorvidt foranstaltninger, der var vedtaget i strid med den forpligtelse, som er fastsat i EU-retten, til at foretage en forudgående vurdering af et projekts indvirkning på miljøet og på en beskyttet lokalitet, at en national domstol, hvis dens nationale ret tillader det, undtagelsesvis kan opretholde virkningerne af sådanne foranstaltninger, hvis denne opretholdelse er begrundet ved tvingende hensyn knyttet til nødvendigheden af at fjerne en reel og alvorlig trussel om afbrydelse af forsyningen med elektricitet i den pågældende medlemsstat, som ikke kan imødegås med andre midler og alternativer, herunder navnlig inden for rammerne af det indre marked, idet den nævnte opretholdelse kun kan omfatte den tidsperiode, som er strengt nødvendig for at afhjælpe denne ulovlighed (jf. i denne retning dom af 29.7.2019, Inter-Environnement Wallonie og Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, præmis 175, 176, 179 og 181).

219 En tilsidesættelse af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, kan i modsætning til tilsidesættelsen af en proceduremæssig forpligtelse, såsom den forudgående vurdering af virkningerne af et projekt inden for det særlige område for miljøbeskyttelse, imidlertid ikke afhjælpes ved en procedure, der kan sammenlignes med den procedure, som er nævnt i den foregående præmis. Opretholdelsen af virkningerne af en national lovgivning som den i hovedsagen omhandlede ville nemlig indebære, at denne lovgivning fortsat ville pålægge udbydere af elektroniske kommunikationstjenester forpligtelser, der er i strid med EU-retten, og som ville medføre alvorlige indgreb i de grundlæggende rettigheder, der tilkommer de personer, hvis oplysninger er blevet lagret.

220 Den forelæggende ret kan derfor ikke anvende en bestemmelse i den nationale lovgivning, der giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til den i hovedsagen omhandlede nationale lovgivning.

221 Når dette er sagt, skal det bemærkes, at VZ, WY og XX i deres indlæg for Domstolen har gjort gældende, at det tredje spørgsmål indirekte, men nødvendigvis, rejser spørgsmålet om, hvorvidt EU-retten er til hinder for, at der i forbindelse med en straffesag anvendes oplysninger og beviser, der er opnået ved en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten.

222 I denne henseende og med henblik på at give den forelæggende ret et hensigtsmæssigt svar skal det bemærkes, at det på EU-rettens nuværende udviklingstrin principielt er overladt alene til den nationale lovgivning at fastsætte de regler, der inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået grov kriminalitet, gælder for antagelse og bedømmelse af oplysninger og beviser, som er opnået ved en sådan lagring af data i strid med EU-retten.

223 Det fremgår således af Domstolens faste praksis, at det i mangel af EU-retlige bestemmelser på området i medfør af princippet om procesautonomi tilkommer hver enkelt medlemsstat i sin interne retsorden at fastsætte de processuelle regler for sagsanlæg til sikring af beskyttelsen af de rettigheder, som borgerne har i medfør af EU-retten, dog på den betingelse, at disse ikke må være mindre gunstige end dem, som regulerer tilsvarende situationer, der er underlagt national ret (ækvivalensprincippet), og at de i praksis ikke umuliggør eller uforholdsmæssigt vanskeliggør udøvelsen af rettigheder, der er tillagt ved EU-retten (effektivitetsprincippet) (jf. i denne retning dom af

6.10.2015, Târşia, C-69/14, EU:C:2015:662, præmis 26 og 27, af 24.10.2018, XC m.fl., C-234/17, EU:C:2018:853, præmis 21 og 22 og den deri nævnte retspraksis, og af 19.12.2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, præmis 33).

224 Hvad angår ækvivalensprincippet tilkommer det den nationale ret, ved hvilken en straffesag er indledt på grundlag af oplysninger eller beviser, der er opnået i strid med de krav, som følger af direktiv 2002/58, at efterprøve, om den nationale lovgivning, der gælder for en sådan sag, fastsætter regler, der er mindre gunstige med hensyn til antagelsen og bedømmelsen af sådanne oplysninger og sådanne beviser end dem, der gælder for de oplysninger og beviser, der er opnået i strid med den nationale lovgivning.

225 Hvad angår effektivitetsprincippet skal det bemærkes, at de nationale regler om antagelse og anvendelse af oplysninger og beviser har til formål i overensstemmelse med de valg, der er truffet i national ret, at undgå, at oplysninger og beviser, der er opnået ulovligt, uberettiget skader en person, der er mistænkt for at have begået strafbare handlinger. Dette formål kan i henhold til national ret imidlertid nås ikke blot ved et forbud mod at anvende sådanne oplysninger og sådanne beviser, men også ved de nationale regler og den nationale praksis, der gælder for bedømmelsen og vægtningen af oplysninger og beviser, eller ved i forbindelse med fastsættelsen af straffen at tage hensyn til disse oplysninger og bevisers ulovlige karakter.

226 Når dette er sagt, fremgår det af Domstolens praksis, at nødvendigheden af at udelukke oplysninger og beviser, der er indhentet i strid med kravene i EU-retten, navnlig skal vurderes i lyset af, hvilken risiko antagelsen af sådanne oplysninger og beviser vil medføre for iagttagelsen af kontradiktionsprincippet og dermed for retten til en retfærdig rettergang (jf. i denne retning dom af 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, præmis 76 og 77). En ret, som er af den opfattelse, at en part ikke er i stand til effektivt at udtale sig om et bevismiddel, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på dens vurdering af de faktiske omstændigheder, skal fastslå, at der er sket en tilsidesættelse af retten til en retfærdig rettergang, og udelukke dette bevismiddel for at undgå en sådan tilsidesættelse (jf. i denne retning dom af 10.4.2003, Steffensen, C-276/01, EU:C:2003:228, præmis 78 og 79).

227 Effektivitetsprincippet pålægger derfor den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder.

228 Henset til de ovenfor anførte betragtninger skal det tredje spørgsmål i sag C-520/18 besvares med, at en national ret ikke kan anvende en bestemmelse i den nationale lovgivning, som giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester navnlig med henblik på beskyttelse af den nationale sikkerhed og bekæmpelse af kriminalitet, at foretage en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1. Denne artikel 15, stk. 1, som fortolket i lyset af effektivitetsprincippet, pålægger den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder.

Sagsomkostninger

229 Da sagernes behandling i forhold til hovedsagernes parter udgør et led i de sager, der verserer for de forelæggende retter, tilkommer det disse at træffe afgørelse om sagsomkostningerne. Bortset fra de nævnte parters udgifter kan de udgifter, som er afholdt i forbindelse med afgivelse af indlæg for Domstolen, ikke erstattes.

På grundlag af disse præmisser kender Domstolen (Store Afdeling) for ret:

1) **Artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, skal fortolkes således, at denne bestemmelse er til hinder for lovgivningsmæssige foranstaltninger, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata. Artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, er derimod ikke til hinder for lovgivningsmæssige foranstaltninger**

   – **der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består**

   – **der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges**

   – **der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige**

   – **der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og**

   – **der med henblik på bekæmpelse af grov kriminalitet og a fortiori med henblik på beskyttelsen af den nationale sikkerhed, gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge**

udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over

for så vidt som disse foranstaltninger ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.

2) **Artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i chartret om grundlæggende rettigheder, skal fortolkes således, at denne bestemmelse ikke er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester dels at gøre brug af automatiseret analyse og indsamling i realtid af navnlig trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, når**

   – **brugen af automatiseret analyse er begrænset til de situationer, hvor en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, og brugen af denne analyse kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om der foreligger en situation, der kan begrunde den nævnte foranstaltning, og om de betingelser og garantier, der skal være fastsat, er overholdt, og når**

   – **indsamlingen i realtid af trafikdata og lokaliseringsdata er begrænset til de personer, med hensyn til hvilke der foreligger rimelig grund til at mistænke, at de på den ene eller den anden måde er involveret i terrorvirksomhed, og er underlagt en forudgående prøvelse, der foretages af enten en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, for at sikre, at en sådan indsamling i realtid kun tillades inden for rammerne af, hvad der er strengt nødvendigt. I et behørigt begrundet hastende tilfælde skal denne prøvelse foretages hurtigst muligt.**

3) **Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«) skal fortolkes således, at dette direktiv med hensyn til informationssamfundstjenester ikke finder anvendelse på området for beskyttelse af kommunikationshemmeligheden og af fysiske personer i forbindelse med behandlingen af personoplysninger, idet denne beskyttelse alt efter omstændighederne er reguleret ved direktiv 2002/58, som ændret ved direktiv 2009/136 eller Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46. Artikel 23, stk. 1, i forordning 2016/679, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i chartret om grundlæggende rettigheder, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, der er forbundet med brugen af disse tjenester.**

4) **En national ret kan ikke anvende en bestemmelse i den nationale lovgivning, som giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester navnlig med henblik på beskyttelse af den nationale sikkerhed og bekæmpelse af kriminalitet at foretage**

en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i chartret om grundlæggende rettigheder. Denne artikel 15, stk. 1, som fortolket i lyset af effektivitetsprincippet, pålægger den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder.

Underskrifter