Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 6 oktober 2020*

[Text rättad genom beslut av den 16 november 2020]

Innehållsförteckning

* Rättegångsspråk: franska.

”Begäran om förhandsavgörande – Behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation – Leverantörer av elektroniska kommunikationstjänster – Leverantörer av värdtjänster och internetleverantörer – Generell och odifferentierad lagring av trafikuppgifter och lokaliseringsuppgifter – Automatiserad analys av uppgifter – Åtkomst till uppgifterna i realtid – Skydd av nationell säkerhet och bekämpning av terrorism – Brottsbekämpning – Direktiv 2002/58/EG – Tillämpningsområde – Artikel 1.3 och artikel 3 – Konfidentialitet vid elektronisk kommunikation – Skydd – Artikel 5 och artikel 15.1 – Direktiv 2000/31/EG – Tillämpningsområde – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 4, 6–8 och 11 samt artikel 52.1 – Artikel 4.2 FEU”

I de förenade målen C-511/18, C-512/18 och C-520/18,

angående beslut att begära förhandsavgörande enligt artikel 267 FEUF, från Conseil d'État (Högsta förvaltningsdomstolen, Frankrike), av den 26 juli 2018, som inkom till domstolen den 3 augusti 2018 (C-511/18 och C-512/18), och från Cour constitutionnelle (Författningsdomstolen, Belgien), av den 19 juli 2018, som inkom till domstolen den 2 augusti 2018 (C-520/18), i målen

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

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

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

Igwan.net (C-511/18),

mot

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

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

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), ytterligare deltagare i rättegången:

Privacy International (C-512/18),

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

och

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des droits de Homme ASBL,

VZ,

WY,

XX

mot

Conseil des ministres,

ytterligare deltagare i rättegången:

Child Focus (C-520/18),

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden K. Lenaerts, vice ordföranden R. Silva de Lapuerta, avdelningsordförandena J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb och L.S. Rossi samt domarna J. Malenovský, L. Bay Larsen, T. von Danwitz (referent), C. Toader, K. Jürimäe, C. Lycourgos och N. Piçarra,

generaladvokat: M. Campos Sánchez-Bordona,

justitiesekreterare: handläggaren C. Strömholm,

efter det skriftliga förfarandet och förhandlingen den 9 och den 10 september 2019,

med beaktande av de yttranden som avgetts av:

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

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

– Privacy International, genom H. Roy, avocat,

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

– Académie Fiscale ASBL och UA, genom J.-P. Riquet,

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

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

– VZ, WY och XX, genom D. Pattyn, avocat,

– Child Focus, genom N. Buisseret, K. De Meester och J. Van Cauter, avocats,

– Frankrikes regering, inledningsvis genom D. Dubois, F. Alabrune, D. Colas, E. de Moustier och A.-L. Desjonquères, därefter genom D. Dubois, F. Alabrune, E. de Moustier och A.-L. Desjonquères, samtliga i egenskap av ombud,

– Belgiens regering, genom J.-C. Halleux, P. Cottin och C. Pochet, samtliga i egenskap av ombud, biträdda av J. Vanpraet, Y Peeters, S. Depré och E. de Lophem, avocats,

– Tjeckiens regering, genom M. Smolek, J. Vláčil och O. Serdula, samtliga i egenskap av ombud,

– Danmarks regering, inledningsvis genom J. Nymann-Lindegren, M. Wolff och P. Ngo, därefter av J. Nymann-Lindegren och M. Wolff, samtliga i egenskap av ombud,

– Tysklands regering, inledningsvis genom J. Möller, M. Hellmann, E. Lankenau, R. Kanitz och T. Henze, därefter genom J. Möller, M. Hellmann, E. Lankenau och R. Kanitz, samtliga i egenskap av ombud,

– Estlands regering, genom N. Grünberg och A. Kalbus, båda i egenskap av ombud,

– Irlands regering, genom A. Joyce, M. Browne och G. Hodge, samtliga i egenskap av ombud, biträdda av D. Fennelly, BL,

– Spaniens regering, inledningsvis genom L. Aguilera Ruiz och A. Rubio González, därefter av L. Aguilera Ruiz, samtliga i egenskap av ombud,

– Cyperns regering, genom E. Neofytou, i egenskap av ombud,

– Lettlands regering, genom V. Soņeca, i egenskap av ombud,

– Ungerns regering, inledningsvis genom M.Z. Fehér och Z. Wagner, därefter genom M.Z. Fehér, samtliga i egenskap av ombud,

– Nederländernas regering, genom M.K. Bulterman och M.A.M. de Ree, båda i egenskap av ombud,

– Polens regering, genom B. Majczyna, J. Sawicka och M. Pawlicka, samtliga i egenskap av ombud,

– Sveriges regering, inledningsvis genom H. Shev, H. Eklinder, C. Meyer-Seitz, och A. Falk, därefter genom H. Shev, H. Eklinder, C. Meyer-Seitz och J. Lundberg, samtliga i egenskap av ombud,

– Förenade kungarikets regering, genom S. Brandon, i egenskap av ombud, biträdd av G. Facenna, QC, och C. Knight, barrister,

– [Strecksats struken enligt beslut av den 16 november 2020]

– Europeiska kommissionen, inledningsvis genom H. Kranenborg, M. Wasmeier och P. Costa de Oliveira, därefter av H. Kranenborg och M. Wasmeier, samtliga i egenskap av ombud,

– Europeiska datatillsynsmannen, genom T. Zerdick och A. Buchta, båda i egenskap av ombud,

och efter att den 15 januari 2020 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Respektive begäran om förhandsavgörande avser tolkningen av dels artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11) (nedan kallat direktiv 2002/58), dels artiklarna 12–15 i Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (Direktiv om elektronisk handel) (EGT L 178, 2000, s. 1), jämförda med artiklarna 4, 6–8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) och artikel 4.2 FEU.

2 Begäran i mål C-511/18 har framställts i mål mellan, å ena sidan, Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs och Igwan.net och, å andra sidan, Premier ministre (Premiärministern, Frankrike), Garde des Sceaux, ministre de la Justice (Justitieministern, Frankrike) samt Ministre des Armées (Försvarsministern, Frankrike). Målet rör lagenligheten av décret nº 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (dekret nr 2015-1185 av den 28 september 2015 om inrättande av

speciella underrättelsetjänster) (JORF av den 29 september 2015, text 1 av 97) (nedan kallat dekret nr 2015-1185), décret nº 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekret nr 2015-1211 av den 1 oktober 2015 om tvister avseende användning av tillståndspliktig underrättelseteknik och registeruppgifter som rör statens säkerhet) (JORF av den 2 oktober 2015, text 7 av 108) (nedan kallat dekret nr 2015-1211), 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 nr 2015-1639 av den 11 december 2015 om inrättande av andra tjänster än de speciella underrättelsetjänsterna, med behörighet att använda den teknik som anges i avdelning V, kapitel VIII i lagen om inre säkerhet, antaget med stöd artikel L. 811-4 lagen om inre säkerhet) (JORF av den 12 december 2015, text 28 av 127) (nedan kallat dekret nr 2015-1639), och décret nº 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (dekret nr 2016-67 av den 29 januari 2016 om teknik för insamling av underrättelseuppgifter) (JORF av den 31 januari 2016, text 2 av 113) (nedan kallat dekret nr 2016-67).

3 Begäran i mål C-512/18 har framställts i mål mellan, å ena sidan, French Data Network, Quadrature du Net och Fédération des fournisseurs d'accès à Internet associatifs, å ena sidan, och Premier ministre (Premiärministern, Frankrike) och Garde des Sceaux, ministre de la justice (Justitieministern, Frankrike). Målet rör lagenligheten av artikel R. 10-13 i code des postes et des communications électroniques (lagen om postväsendet och elektronisk kommunikation) (nedan kallad CPCE) och 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 nr 2011-219 av den 25 februari 2011 om lagring av uppgifter som gör det möjligt att identifiera varje person som har bidragit till skapandet av innehåll som har lagts ut på internet) (JORF av den 1 mars 2011, text 32 av 170) (nedan kallat dekret nr 2011-219).

4 Begäran i mål C-520/18 har framställts i mål mellan, å ena sidan, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des droits de l'Homme ASBL, VZ, WY och XX, och, å andra sidan, Conseil des ministres (Ministerrådet, Belgien). Målet rör lagenligheten av loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (lagen av den 29 maj 2016 om insamling och lagring av uppgifter inom sektorn för elektronisk kommunikation) (*Moniteur belge* av den 18 juli 2016, s. 44717) (nedan kallad lagen av den 29 maj 2016).

Tillämpliga bestämmelser

Unionsrätt

Direktiv 95/46

5 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s. 31) upphävdes med verkan från och med den 25 maj 2018 genom Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46 (EUT L 119, 2016, s. 1). Artikel 3.2 i direktiv 95/46 hade följande lydelse:

”Detta direktiv gäller inte för sådan behandling av personuppgifter

– som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,

– av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll.”

6 Artikel 22 i direktiv 95/46, som återfinns i kapitel III i direktivet, med rubriken ”Rättslig prövning, ansvar och sanktioner”, hade följande lydelse:

”Medlemsstaterna skall – utan att det påverkar möjligheten att utnyttja något administrativt förfarande, till exempel vid den tillsynsmyndighet som avses i artikel 28, som kan användas innan ett ärende anhängiggörs hos en rättslig instans – föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling.”

Direktiv 97/66

7 Artikel 5 i Europaparlamentets och rådets direktiv 97/66/EG av den 15 december 1997 om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet (EGT L 24, 1997, s. 1) med rubriken ”Telehemlighet vi[d] kommunikation” har följande lydelse:

”1. Medlemsstaterna skall genom nationella regler säkra telehemligheten vid kommunikation via allmänt tillgängliga telenät och allmänt tillgängliga teletjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra sätt på vilka kommunikationen kan fångas upp eller övervakas av andra än användarna utan de berörda användarnas samtycke, utom när sådana åtgärder är lagligen tillåtna, i enlighet med artikel 14.1.

2. Punkt 1 påverkar inte inspelning som är tillåten enligt lag av kommunikation i samband med bedrivande av laglig affärsverksamhet för att tillhandahålla bevis om en affärstransaktion eller annan affärskommunikation.”

Direktiv 2000/31

8 Skälen 14 och 15 i direktiv 2000/31 har följande lydelse:

”(14) Skyddet för enskilda personer med avseende på behandling av personuppgifter regleras endast av direktiv [95/46] och direktiv [97/66], som i sin helhet är tillämpliga på informationssamhällets tjänster. I dessa direktiv upprättas redan en gemenskapsrättslig ram för personuppgifter, och denna fråga behöver därför inte behandlas i detta direktiv för att säkerställa att den inre marknaden fungerar väl, i synnerhet den fria rörligheten för personuppgifter mellan medlemsstaterna. Genomförandet och tillämpningen av detta direktiv bör stå i full överensstämmelse med principerna om skydd för personuppgifter, särskilt avseende icke begärda kommersiella meddelanden och mellanhänders ansvar. Detta direktiv kan inte förhindra anonym användning av öppna nätverk som Internet.

(15) Konfidentialiteten vid kommunikation garanteras genom artikel 5 i direktiv [97/66]. Enligt det direktivet måste medlemsstaterna förbjuda alla andra än avsändarna och mottagarna att på något sätt fånga upp eller övervaka kommunikationen, utom när sådana åtgärder är lagligen tillåtna.”

9 Artikel 1 i direktiv 2000/31 har följande lydelse:

”1. Syftet med detta direktiv är att bidra till att den inre marknaden fungerar väl genom att säkerställa den fria rörligheten för informationssamhällets tjänster mellan medlemsstaterna.

2. Genom detta direktiv tillnärmas, i den mån det krävs för att nå det mål som avses i punkt 1, vissa nationella bestämmelse om informationssamhällets tjänster som rör den inre marknaden, tjänsteleverantörers etablering, kommersiella meddelanden, avtal slutna på elektronisk väg, mellanhänders ansvar, uppförandekoder, utomrättslig lösning av tvister, möjlighet att föra talan inför domstol samt samarbete mellan medlemsstaterna.

3. Detta direktiv kompletterar den gemenskapsrätt som är tillämplig på informationssamhällets tjänster, utan att det påverkar nivån på skyddet av i synnerhet folkhälsan och konsumentintressena såsom de fastställs i gemenskapsrättsakter och nationell lagstiftning för genomförande av dessa, i den mån detta inte begränsar friheten att tillhandahålla informationssamhällets tjänster.

…

5. Detta direktiv skall inte tillämpas på

…

b) frågor beträffande informationssamhällets tjänster som omfattas av direktiv [95/46] och direktiv [97/66],

…”

10 Artikel 2 i direktiv 2000/31 har följande lydelse:

”I detta direktiv avses med

a) informationssamhällets tjänster: tjänster i den mening som avses i artikel 1.2 i [Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter (EGT L 204, 1998, s. 37)], i dess lydelse enligt [Europaparlamentets och rådets direktiv 98/48/EG av den 20 juli 1998 (EUT L 217, 1998, s. 18)],

…”

11 I artikel 15 i direktiv 2000/31 föreskrivs följande:

”1. Medlemsstaterna får inte ålägga tjänsteleverantörerna en allmän skyldighet att, i samband med tillhandahållande av sådana tjänster som avses i artiklarna 12, 13 och 14, övervaka den information de överför eller lagrar, och inte heller någon allmän skyldighet att aktivt efterforska fakta eller omständigheter som kan tyda på olaglig verksamhet.

2. Medlemsstaterna kan fastställa skyldigheter för leverantörer av informationssamhällets tjänster att omedelbart informera de behöriga myndigheterna om påstådda olagliga verksamheter som utförts eller olaglig information som tillhandahållits av mottagarna av deras tjänster eller att till behöriga myndigheter på deras begäran lämna information som gör det möjligt att identifiera de mottagare av deras tjänster med vilka de ingått lagringsavtal.”

Direktiv 2002/21

12 Skäl 10 i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) (EGT L 108, 2002, s. 33), har följande lydelse:

”Definitionen av ’informationssamhällets tjänster’ i artikel 1 i [direktiv 98/34], i dess lydelse enligt [direktiv 98/48] omfattar en lång rad av ekonomiska verksamheter som bedrivs on-line. Flertalet av dessa verksamheter omfattas inte av det här direktivets räckvidd, eftersom de inte helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. Taltelefoni och överföring av elektronisk post omfattas av det här direktivet. Samma företag, exempelvis en tillhandahållare av Internettjänster, kan erbjuda både elektroniska kommunikationstjänster, till exempel tillgång till Internet, och tjänster som inte omfattas av det här direktivet, till exempel tillhandahållande av innehåll på nätet.”

13 I artikel 2 i direktiv 2002/21 föreskrivs följande:

”I detta direktiv används följande beteckningar med de betydelser som här anges:

…

c) *elektronisk kommunikationstjänst*: en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät, däribland teletjänster och överföringstjänster i nät som används för rundradio, men inte tjänster i form av tillhandahållande av innehåll som överförts med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller utövande av redaktionellt ansvar över detta innehåll. Den omfattar inte de av informationssamhällets tjänster enligt definitionen i artikel 1 i direktiv 98/34/EG som inte helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.

…”

Direktiv 2002/58

14 I skälen 2, 6, 7, 11, 22, 26 och 30 i direktiv 2002/58 anges följande:

”(2) I detta direktiv eftersträvas respekt för de grundläggande rättigheterna och iakttagande av de principer som erkänns i synnerhet i [stadgan]. I synnerhet eftersträvas i detta direktiv att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i den stadgan.

…

(6) Internet bryter upp traditionella marknadsstrukturer genom att tillhandahålla en gemensam, global infrastruktur för leverans av en mängd olika elektroniska kommunikationstjänster. Allmänt tillgängliga kommunikationstjänster via Internet öppnar nya möjligheter för användarna, men för även med sig nya risker för deras personuppgifter och integritet.

(7) När det gäller allmänna kommunikationsnät bör särskilda rättsliga och tekniska bestämmelser antas för att skydda fysiska personers grundläggande fri- och rättigheter samt juridiska personers berättigade intressen, särskilt med hänsyn till den ökade kapaciteten för automatiserad lagring och behandling av uppgifter om abonnenter och användare.

…

(11) I likhet med direktiv [95/46] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av [unions]lagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna [undertecknad i Rom den 4 november 1950] i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna [nedan kallad Europadomstolen]. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

…

(22) Förbudet mot lagring av kommunikationer och tillhörande trafikuppgifter av andra än användarna eller utan deras samtycke är inte avsett att förbjuda någon automatisk, mellanliggande och tillfällig lagring av denna information, i den mån lagringen enbart görs för att utföra överföringen i det elektroniska kommunikationsnätet och under förutsättning att informationen inte lagras längre än vad som är nödvändigt för överföringen och trafikstyrningen och att konfidentialiteten förblir garanterad under lagringsperioden. …

…

(26) De uppgifter om abonnenter som behandlas inom elektroniska kommunikationsnät i samband med uppkoppling och överföring av information innehåller upplysningar om fysiska personers privatliv och gäller rätten till skydd för deras korrespondens eller omsorgen om juridiska personers berättigade intressen. Sådana uppgifter får endast lagras i den utsträckning det är nödvändigt för att tillhandahålla tjänsten när det gäller fakturering och betalning av samtrafikavgifter, och endast under en begränsad tid. [Ytterligare behandling av sådana uppgifter får] endast ske om abonnenten givit sitt samtycke till detta efter att ha erhållit korrekt och uttömmande information av den berörda leverantören om vilka typer av ytterligare behandling som denne avser att företa och om abonnentens rätt att inte ge sitt samtycke eller att återkalla sitt samtycke till en sådan behandling. Trafikuppgifter som används vid saluföring av kommunikationstjänster bör också utplånas eller avidentifieras …

…

(30) Systemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum. …”

15 I artikel 1 i direktiv 2002/58, med rubriken ”Tillämpningsområde och syfte”, föreskrivs följande:

”1. Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom [Europeiska unionen].

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv [95/46] för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för [FEUF], t.ex. de som omfattas av avdelningarna V och VI i Fördraget om Europeiska unionen, och inte i något fall på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

16 I artikel 2 i direktiv 2002/58, som har rubriken ”Definitioner”, anges följande:

”Om inte annat anges ska definitionerna i direktiv [95/46] och direktiv [2002/21] gälla i detta direktiv.

Dessutom skall följande definitioner gälla:

a) användare: en fysisk person som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk utan att nödvändigtvis ha abonnerat på denna tjänst.

b) trafikuppgifter: alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den.

c) lokaliseringsuppgifter: alla uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst.

d) Meddelande: kommunikation: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Detta inbegriper inte information som överförs som del av en sändningstjänst för rundradio eller TV till allmänheten via ett elektroniskt kommunikationsnät utom i den mån informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen.

…”

17 I artikel 3 i direktiv 2002/58, med rubriken ”Berörda tjänster”, föreskrivs följande:

”Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.”

18 Artikel 5, som har rubriken ”Konfidentialitet vid kommunikation”, i direktiv 2002/58 har följande lydelse:

”1. Medlemsstaterna skall genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1. Denna punkt får inte förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet.

…

3. Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv [95/46], bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt."

19 I artikel 6 i direktiv 2002/58, med rubriken "Trafikuppgifter", föreskrivs följande:

"1. Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.

2. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter får behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning.

3. I syfte att saluföra elektroniska kommunikationstjänster eller i syfte att tillhandahålla mervärdestjänster får en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i punkt 1 i den utsträckning och under den tidsperiod som är nödvändig för sådana tjänster eller sådan marknadsföring, om den abonnent eller användare som uppgifterna gäller i förväg har samtyckt till detta. Användare eller abonnenter ska ha möjlighet att när som helst dra tillbaka sitt samtycke till behandling av trafikuppgifter.

…

5. Behandlingen av trafikuppgifter skall, i enlighet med punkterna 1, 2, 3 och 4, begränsas till sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta fakturering, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst, och behandlingen skall begränsas till sådant som är nödvändigt för dessa verksamheter."

20 I artikel 9 i direktivet, med rubriken "Andra lokaliseringsuppgifter än trafikuppgifter", föreskrivs följande i punkt 1:

"Om andra lokaliseringsuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst. Innan användaren eller abonnenten ger sitt samtycke skall tjänsteleverantören informera denne om vilken typ av andra lokaliseringsuppgifter än trafikuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. …"

21 Artikel 15 i direktivet, med rubriken "Tillämpningen av vissa bestämmelser i direktiv [95/46]", har följande lydelse:

"1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och

proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv [95/46]. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i [unions]lagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.

…

2. Bestämmelserna om rättslig prövning, ansvar och sanktioner i kapitel III i direktiv [95/46] skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet.

…”

Förordning 2016/679

22 Skäl 10 i förordning 2016/679 har följande lydelse:

”För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. …”

23 I artikel 2 i förordningen föreskrivs följande:

”1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

…

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

…

4. Denna förordning påverkar inte tillämpningen av direktiv [2000/31], särskilt bestämmelserna om tjänstelevererande mellanhänders ansvar i artiklarna 12–15 i det direktivet.”

24 I artikel 4 i nämnda förordning föreskrivs följande:

”I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer, eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

…”

25 I artikel 5 i förordning 2016/679 föreskrivs följande:

”1. Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade *(laglighet, korrekthet och öppenhet*).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*riktighet*).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

…”

26 I artikel 6 i denna förordning anges följande:

”1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

…

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

…

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

a) unionsrätten, eller

b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden … Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

…”

27 I artikel 23 i nämnda förordning föreskrivs följande:

”1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

f) skydd av rättsväsendets oberoende och rättsliga åtgärder,

g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,

i) skydd av den registrerade eller andras rättigheter och friheter,

j) verkställighet av civilrättsliga krav.

2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,

g) riskerna för de registrerades rättigheter och friheter, och

h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.”

28 Enligt artikel 79.1 i förordningen gäller följande:

”Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.”

29 Artikel 94 i förordning nr 2016/679 har följande lydelse:

”1. Direktiv [95/46] ska upphöra att gälla med verkan från och med den 25 maj 2018.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv [95/46], ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.”

30 I artikel 95 i förordningen föreskrivs följande:

”Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv [2002/58].”

Fransk rätt

Code de la sécurité intérieure (lagen om inre säkerhet)

31 I del VIII i code de la sécurité intérieure (lagen om inre säkerhet) (nedan kallad CSI) föreskrivs, i artiklarna L. 801-1 till L. 898-1, bestämmelser om underrättelseverksamhet.

32 L. 811-3 CSI har följande lydelse:

”De specialiserade underrättelseenheterna får endast för att utföra sina respektive uppgifter använda sig av de metoder som anges i avdelning V i denna del för att samla in information om tillvaratagande och främjande av följande grundläggande nationella intressen:

1. Nationellt oberoende, territoriets integritet och det nationella försvaret,

2. De viktigaste intressena för utrikespolitiken, fullgörandet av Frankrikes europeiska och internationella åtaganden och förhindrande av varje form av utländskt ingrepp,

3. Viktiga ekonomiska, industriella och vetenskapliga intressen för Frankrike,

4. Förebyggande av terrorism

5. Förhindrande av:
   a) undergrävande av det republikanska statsskicket,
   b) åtgärder för att bibehålla eller återskapa grupper som upplösts enligt artikel L. 212-1,
   c) kollektiva våldshandlingar som allvarligt kan skada den allmänna ordningen,

6. Förebyggande av brott och organiserad brottslighet,

7. Förhindrande av spridning av massförstörelsevapen.”

33 I artikel L. 811-4 CSI föreskrivs följande:

”I dekret av Conseil d’État (Högsta förvaltningsdomstolen, Frankrike), som antagits efter yttrande från nationella kommissionen för kontroll av underrättelseteknik, anges andra myndigheter än de specialiserade underrättelsemyndigheterna, som lyder under försvars-, inrikes- och justitieministrarna samt ministrarna med ansvar för ekonomi, budget eller tull, som kan tillåtas att använda de tekniker som anges i avdelning V i denna del på de villkor som anges i samma del. I artikeln anges för varje myndighet de ändamål som anges i artikel L. 811-3 och vilka tekniker för vilka tillstånd kan ges.”

34 I artikel L. 821-1 första stycket CSI föreskrivs följande:

”För att de tekniker för insamling av underrättelseuppgifter som anges i kapitlen I–IV i avdelning V i denna del ska kunna användas i landet krävs förhandstillstånd från premiärministern, efter yttrande från nationella kommissionen för kontroll av underrättelseteknik.”

35 I artikel L. 821-2 CSI föreskrivs följande:

”Det tillstånd som avses i artikel L. 821-1 ska utfärdas efter skriftlig och motiverad ansökan av försvarsministern, inrikesministern, justitieministern eller ministern med ansvar för ekonomi, budget eller tull. Ministern får endast delegera tilldelningen av sådant tillstånd till direkta medarbetare som är behöriga att ta del av försvarshemligheter.

I ansökan ska anges

1) Den eller de tekniker som ska användas,

2) Den tjänsteavdelning som avses,

3) Det eller de mål som eftersträvas,

4) Det eller de skäl som ligger till grund för åtgärderna,

5) Tillståndets giltighetstid.

6) Den eller de berörda personerna, platserna eller fordonen.

Vid tillämpning av punkt 6 får personer vars identitet inte är känd anges med sina kännetecken eller egenskaper och platser eller fordon får anges med hänvisning till de personer som avses i ansökan.

…”

36 Artikel L. 821-3 första stycket CSI har följande lydelse:

”Begäran ska tillställas ordföranden eller, om detta inte är möjligt, en av ledamöterna i den nationella kommissionen för kontroll av underrättelseteknik, bland dem som nämns i punkterna 2 och 3 i artikel L. 831-1, som ska avge ett yttrande till premiärministern inom 24 timmar. Om ansökan prövas av den särskilda sammansättningen eller av kommissionen i plenum ska premiärministern omedelbart underrättas och yttrandet ska lämnas inom 72 timmar.”

37 Artikel L. 821-4 CSI har följande lydelse:

”Tillstånd att använda de tekniker som anges i kapitlen I-IV i avdelning V i denna del utfärdas av premiärministern för högst fyra månader. … Tillståndet ska innehålla de skäl och uppgifter som anges i punkterna 1–6 i artikel L. 821-2. Varje tillstånd ska kunna förnyas på samma villkor som anges i detta kapitel.

Om tillståndet beviljas efter ett negativt yttrande från nationella kommissionen för kontroll av underrättelseteknik ska den ange skälen till varför detta yttrande inte har följts.

…”

38 I artikel L. 833-4 CSI, som återfinns i kapitel III i denna avdelning, föreskrivs följande:

”Kommissionen ska på eget initiativ, eller när klagomål har ingetts av en person som vill kontrollera att ingen underrättelseteknik har använts på ett felaktigt sätt avseende vederbörande, undersöka den eller de tekniker som åberopas för att kontrollera att dessa har använts eller används i enlighet med denna del. Kommissionen ska underrätta klaganden om att nödvändiga kontroller har utförts, utan att vare sig bekräfta eller förneka att dessa kontroller ägt rum.”

39 Artikel L. 841-1 första och andra styckena CSI har följande lydelse:

”Om inte annat följer av de särskilda bestämmelserna i artikel L. 854-9 i denna lag är Conseil d’État (Högsta förvaltningsdomstolen) behörig att, på de villkor som anges i kapitel III a i avdelning VII i del VII i code de justice administrative (förvaltningsprocesslagen), pröva ansökningar om användning av de informationstekniker som anges i avdelning V i denna del.

Följande personer kan vända sig till denna domstol:

1. var och en som vill kontrollera att ingen underrättelseteknik har använts på ett felaktigt sätt i förhållande till honom och som motiverar att det förfarande som föreskrivs i artikel L. 833-4 först genomförs,

2. Nationella kommissionen för kontroll av underrättelseteknik, i enlighet med de villkor som föreskrivs i artikel L. 833-8.”

40 Avdelning V i del VIII CSI, som rör ”tekniker för insamling av underrättelseuppgifter som kräver tillstånd”, innehåller bland annat ett kapitel I, med rubriken ”Administrativ tillgång till uppkopplingsuppgifter”, som innehåller artiklarna L. 851-1 till L. 851-7 CSI.

41 Artikel L. 851-1 CSI har följande lydelse:

”Under de förutsättningar som föreskrivs i kapitel 1 i avdelning II i denna del får tillstånd beviljas för insamling, hos operatörer som tillhandahåller elektronisk kommunikation och personer som anges i artikel L. 34-1 [CPCE] samt hos de personer som anges i artikel 6.1 och 6.2 i loi nr 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique [(lag nr 2004-575 av den 21 juni 2004 om förtroende för den digitala ekonomin) (JORF av den 22 juni 2004, s. 11168)], av uppgifter eller handlingar som behandlas eller lagras genom deras nät eller tjänster för elektronisk kommunikation, däribland tekniska uppgifter om identifiering av abonnent- eller uppringningsnummer för elektroniska kommunikationstjänster, sammanställning av alla abonnent- eller uppringningsnummer för en angiven person, lokalisering av använd terminalutrustning samt om en abonnents kommunikationer med avseende på in- och utgående nummer, varaktighet och datum.

Med avvikelse från artikel L. 821-2 ska skriftliga och motiverade ansökningar om tekniska uppgifter om identifikation av abonnemangsnummer, anslutning till elektroniska kommunikationstjänster eller om sammanställningen av en angiven persons samtliga abonnemangs- eller uppringningsnummer överlämnas direkt till den nationella kommissionen för kontroll av underrättelseteknik av enskilda utsedda tjänstemän och som är befullmäktigade av de underrättelsemyndigheter som avses i artiklarna L. 811-2 och L. 811-4. Kommissionen ska yttra sig i enlighet med artikel L. 821-3

En avdelning hos premiärministern har till uppgift att samla in information eller dokumentation från de aktörer och personer som nämns i första stycket i denna artikel. Nationella kommissionen för kontroll av underrättelseteknik ska ha permanent, fullständig, direkt och omedelbar tillgång till den information eller de handlingar som samlats in.

Tillämpningsföreskrifterna för denna artikel ska fastställas genom dekret av Conseil d’État (Högsta förvaltningsdomstolen), som ska antas efter yttrande från Nationella kommissionen för informationsteknik och friheter och av Nationella kommissionen för kontroll av underrättelseteknik.”

42 I artikel L. 851-2 CSI föreskrivs följande:

”I. I enlighet med de villkor som anges i kapitel I i avdelning II i denna del, och uteslutande för att förebygga terrorism, kan insamling i realtid av uppgifter eller handlingar som anges i artikel L. 851-1 avseende en tidigare identifierad person som kan ha samband med ett hot, tillåtas på de nät som drivas av sådana operatörer och personer som anges i artikel L. 851-1. Om det finns vägande skäl att anta att en eller flera personer kring den person som berörs av tillståndet kan lämna uppgifter med hänsyn till det ändamål som ligger till grund för tillståndet, får tillstånd även beviljas individuellt för var och en av dessa personer.

I bis. Det högsta antalet tillstånd som utfärdas med tillämpning av denna artikel och som samtidigt är i kraft ska fastställas av premiärministern efter yttrande från Nationella kommissionen för kontroll av underrättelseteknik. Kommissionen ska underrättas om beslutet om fastställande av denna kvot och dess fördelning mellan de ministrar som anges i artikel L. 821-2 första stycket och antalet tillstånd till ingripande.

…”

43 I artikel L. 851-3 CSI föreskrivs följande:

”I. I enlighet med de villkor som anges i kapitel I i avdelning II i denna del, och enbart för att förebygga terrorism, kan operatörer och personer som avses i artikel L. 851-1 åläggas att i sina system för automatiserad behandling utföra automatiserad behandling i syfte att, i enlighet med de parametrar som anges i tillståndet, uppdaga anslutningar som kan visa att det föreligger ett terroristhot.

Denna automatiserade behandling ska endast använda de uppgifter eller handlingar som anges i artikel L. 851-1, utan att några andra uppgifter än de som motsvarar deras parametrar inhämtas och utan att det är möjligt att identifiera de personer till vilka uppgifterna eller handlingarna hänför sig.

Med beaktande av proportionalitetsprincipen preciserar premiärministerns tillstånd det tekniska området för genomförandet av dessa behandlingar.

II. Nationella kommissionen för kontroll av underrättelseteknik ska yttra sig över ansökan om tillstånd avseende den automatiserade behandlingen och de valda uppdagandeparametrarna. Den ska ha permanent, fullständig och direkt tillgång till denna behandling samt till den information och de uppgifter som samlats in. Kommissionen ska underrättas om ändringar i behandlingen och parametrarna och kan utfärda rekommendationer.

Det första tillståndet för automatiserad behandling enligt I i denna artikel utfärdas för en period på två månader. Tillståndet kan förnyas på de villkor som anges i kapitel I i avdelning II i denna del. Ansökan om förnyelse ska innehålla en sammanställning av antalet identifierande personer som anges i den automatiserade behandlingen och en analys av relevansen av dessa angivanden.

III. Villkoren i artikel L. 871-6 är tillämpliga på transaktioner som utförs för detta ändamål av de aktörer och personer som anges i artikel L. 851-1.

IV. Om det i de behandlingar som anges i punkt I i denna artikel framkommer uppgifter som kan visa att det föreligger ett terrorhot, får premiärministern eller någon av de personer som denne delegerat denna befogenhet till, efter att ha inhämtat yttrande från Nationella kommissionen för kontroll av underrättelseteknik i enlighet med villkoren i kapitel I i avdelning II i denna del, tillåta identifiering av den eller de berörda personerna och insamlingen av därtill hörande uppgifter. Uppgifterna ska användas inom 60 dagar från att de samlats in och förstöras efter fristens utgång, såvida det inte finns allvarliga uppgifter som bekräftar att en eller flera av de berörda personerna utgör ett terroristhot.

…”

44 Artikel 851–4 CSI har följande lydelse:

”I enlighet med de villkor som anges i kapitel I i avdelning II i denna del får de tekniska uppgifter om var terminalutrustning som anges i artikel L. 851-1 på begäran hämtas från nätet och av operatörerna i realtid överföras till en avdelning hos premiärministern.”

45 I artikel R. 851-5 CSI, som ingår i lagstiftningsdelen av denna lag, föreskrivs följande:

”I. De uppgifter eller de handlingar som anges i artikel L. 851-1 ska, med undantag av innehållet i skriftväxlingen eller den information som har konsulterats, vara

1. de som räknas upp i artiklarna R. 10-13 och R. 10-14 i [CPCE] och i artikel 1 i dekret [nr 2011-219],

2. andra tekniska uppgifter än de som nämns i punkt 1:

a) som gör det möjligt att lokalisera terminalutrustning,

b) som avser tillträde till terminalutrustning till nät eller tjänster för överföring till allmänheten online,

c) som avser överföring av elektronisk kommunikation via nätet,

d) som avser identifiering och autentisering av en användare, en anslutning, ett nät eller en tjänst för överföring till allmänheten på internet,

e) som avser terminalutrustningens egenskaper och konfigureringsdata för utrustningens programvara.

II. Endast de uppgifter och handlingar som anges i I punkt 1 kan samlas in med stöd av artikel L. 851-1. Denna insamling ska inte ske i realtid.

De uppgifter som anges i I punkt 2 får endast inhämtas med tillämpning av artiklarna L. 851-2 och L. 851-3, på de villkor och med de begränsningar som föreskrivs i dessa artiklar och med förbehåll för tillämpningen av artikel R. 851-9.”

CPCE

46 Artikel L. 34-1 CPCE har följande lydelse:

”I. Denna artikel ska tillämpas på behandling av personuppgifter i samband med tillhandahållande av elektroniska kommunikationstjänster till allmänheten. Artikeln ska i synnerhet tillämpas på nät som stöder insamling av uppgifter och identifiering.

II. Operatörer som tillhandahåller elektronisk kommunikation, i synnerhet sådana vars verksamhet består i att erbjuda allmänheten tillgång till kommunikationstjänster online, ska utplåna eller avidentifiera alla trafikuppgifter, med förbehåll för vad som anges i punkterna III, IV, V och VI.

Personer som tillhandahåller elektroniska kommunikationstjänster till allmänheten ska, med iakttagande av bestämmelserna i föregående stycke, upprätta interna förfaranden som gör det möjligt att besvara en begäran från behöriga myndigheter.

Personer som i en yrkesmässig huvud- eller sidoverksamhet erbjuder allmänheten en uppkoppling som möjliggör kommunikation online med hjälp av en nätanslutning ska, även om detta görs kostnadsfritt, iaktta de bestämmelser som gäller för operatörer som tillhandahåller elektronisk kommunikation enligt denna artikel.

III. När det behövs för att utreda, avslöja och lagföra brott eller åsidosättanden av skyldigheten enligt artikel L. 336-3 i code de la propriété intellectuelle (immaterialrättslagen) eller för att förhindra sådant intrång i automatiserade databehandlingssystem som är straffbelagt enligt artiklarna 323-1 till 323-3-1 i code pénal (strafflagen), och i det enda syftet att vid behov låta den rättsliga myndighet eller den höga myndighet som avses i artikel L. 331-12 i immaterialrättslagen eller den nationella säkerhetsmyndighet

för informationssystem som avses i artikel L. 2321-1 i code de la défense (försvarslagen) ta del av uppgifterna, får uppskov i högst ett år medges för åtgärder avsedda att utplåna eller avidentifiera vissa kategorier av tekniska uppgifter. Conseil d'État ska efter att ha hört Nationella kommissionen för informationsteknik och friheter genom dekret fastställa dessa kategorier av uppgifter och lagringstider, inom ramen för de gränser som anges i punkt VI, utifrån operatörernas verksamhet och kommunikationstyp samt förutsättningarna för eventuell ersättning för identifierbara och specifika merkostnader för de tjänster som operatörerna således tillhandahåller på statens begäran.

…

VI. Uppgifter som lagras eller behandlas enligt de villkor som anges i punkterna III, IV och V får enbart handla om identifiering av användarna av de tjänster som operatörerna tillhandahåller, de tekniska egenskaperna hos de kommunikationer som operatörerna säkerställer samt terminalutrustningens lokalisering.

De får under inga omständigheter handla om innehållet i den korrespondens som utbytts eller den information som sökts, i någon form, inom ramen för dessa kommunikationer.

Lagringen och behandlingen av uppgifterna ska ske med iakttagande av bestämmelserna i loi nº 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (lag nr 78–17 av den 6 januari 1978 om datasystem, register och friheter).

Operatörerna ska vidta alla åtgärder som krävs för att förhindra att dessa uppgifter används för andra ändamål än de som föreskrivs i denna artikel."

47 Artikel R. 10-13 CPCE har följande lydelse:

"I. Enligt artikel L. 34-1 III ska operatörer av elektronisk kommunikation behålla följande för utredning, fastställande och åtal av brott:

a) Information som gör det möjligt att identifiera användaren.

b) Uppgifter om den terminalutrustning för kommunikation som använts.

c) Tekniska egenskaper, samt datum, klockslag och varaktighet för varje kommunikation.

d) Uppgifter om kompletterande tjänster som har efterfrågats eller använts och leverantörerna av dessa tjänster.

e) Uppgifter som gör det möjligt att identifiera den eller de som kommunikationen riktade sig till.

II. När det gäller operatörens telefoniverksamhet ska de uppgifter som anges i II bevaras, och dessutom de uppgifter som gör det möjligt att identifiera kommunikationens ursprung och lokalisering.

III. Lagringstiden för de uppgifter som anges i denna artikel är ett år från och med registreringstidpunkten.

IV. Identifierbara och specifika merkostnader för de berörda operatörerna för tillhandahållande av uppgifter i de kategorier som anges i denna artikel som krävs av de rättsliga myndigheterna ska kompenseras i enlighet med artikel R. 213-1 i straffprocesslagen."

48 I artikel L. 10-14 CPCE föreskrivs följande:

”I. Enligt IV i artikel L. 34-1 har operatörer av elektronisk kommunikation rätt att för fakturerings- och betalningstransaktioner lagra tekniska data som gör det möjligt att identifiera användaren samt de uppgifter som anges i artikel R. 10-13 b, c och d i avsnitt I i artikel R. 10-13.

II. Vad gäller telefoniverksamhet får operatörerna, utöver de uppgifter som anges i punkt I, lagra tekniska uppgifter om var kommunikationen sker, om identifiering av adressaterna och uppgifter som behövs för fakturering.

III. De uppgifter som anges i I och II i denna artikel får lagras endast om de är nödvändiga för fakturering och betalning av de tillhandahållna tjänsterna. Deras bevarande ska begränsas till den tid som är absolut nödvändig för detta ändamål och får inte överstiga ett år.

IV. För nät- och anläggningssäkerhet får operatörerna under högst tre månader behålla

a) Uppgifter som gör det möjligt att identifiera kommunikationens ursprung.

b) Tekniska egenskaper, samt datum, klockslag och varaktighet för varje kommunikation.

c) Uppgifter som gör det möjligt att identifiera mottagaren eller mottagarna av kommunikationen.

d) Uppgifter om kompletterande tjänster som har efterfrågats eller använts och leverantörerna av dessa tjänster.”

Lag nr 2004–575 av den 21 juni 2004 om förtroende för den digitala ekonomin

49 I artikel 6 i la loi n° 2004–575, du 21 juin 2004, pour la confiance dans l’économie numérique (lag nr 2004–575 av den 21 juni 2004 om förtroende för den digitala ekonomin) (nedan kallad LCEN) (JORF av den 22 juni 2004, s. 11168) föreskrivs följande:

”I. 1. Personer vars verksamhet består i att erbjuda allmänheten tillgång till elektroniska kommunikationstjänster på internet ska informera sina abonnenter om att det finns tekniska medel som gör det möjligt att begränsa tillgången till vissa tjänster eller att välja ut dem och erbjuda dem åtminstone en av dessa resurser.

…

2. Fysiska eller juridiska personer som, även kostnadsfritt, på internet tillhandahåller allmänheten elektroniska kommunikationstjänster för lagring av signaler, skrivna meddelanden, bilder, ljud eller meddelanden av alla slag som tillhandahålls av tjänstemottagarna, kan inte ådra sig skadeståndsansvar för verksamhet eller information som lagrats på begäran av en tjänstemottagare, om de inte har haft faktisk kännedom om tjänsternas olagliga karaktär eller om fakta och omständigheter som tyder på att uppgifterna är olagliga eller om de, så snart de har fått kännedom om den eller om de har fått kännedom om den, inte har agerat för att ta bort dessa uppgifter eller omöjliggöra tillgång till dem,

…

II. De personer som nämns i punkterna 1 och 2 i I ska inneha och lagra uppgifter som gör det möjligt att identifiera den som har bidragit till skapandet av innehållet eller ett innehåll i de tjänster som de tillhandahåller.

De ska tillhandahålla personer som driver en elektronisk kommunikationstjänst på internet sådana tekniska hjälpmedel som gör det möjligt för dem att uppfylla de identifieringsvillkor som föreskrivs i III.

Den rättsliga myndigheten kan begära att få tillgång till de uppgifter som nämns i första stycket från de tjänsteleverantörer som nämns i I punkterna 1 och 2.

Bestämmelserna i artiklarna 226-17, 226-21 och 226-22 i strafflagen är tillämpliga på behandling av sådana uppgifter.

I ett dekret från Conseil d'État (Högsta förvaltningsdomstolen), som antagits efter yttrande från Nationella kommissionen för informationsteknik och friheter, fastställs de uppgifter som nämns i första stycket och hur länge lagringen ska pågå och hur de ska lagras.

…"

Dekret nr 2011-219

50 Kapitel I i dekret nr 2011-219, som har antagits med stöd av artikel 6 II sista stycket LCEN, innehåller artiklarna 1–4 i detta dekret.

51 I artikel 1 i dekret 2011-219 föreskrivs följande:

"De uppgifter som nämns i artikel 6 II i [LCEN], vilka personerna är skyldiga att lagra enligt denna bestämmelse, är följande:

1. För de personer som nämns i I punkt 1 och för varje anslutning för deras abonnenter

a) Identifieringsuppgift för anslutningen,

b) Den identifikationskod som dessa personer tilldelar abonnenten,

c) Identifiering av den terminal som används för anslutningen när denna är åtkomlig,

d) Datum och tidpunkt för anslutningens början och slut,

e) Kännetecknen för abonnentens linje.

2. För de personer som nämns i punkt I i punkt 2 i samma artikel och för varje initiering av verksamhet

a) Identifieringsuppgift av den anslutning som ligger till grund för kommunikationen,

b) Den identifikationskod som tilldelas genom informationssystemet för det innehåll som är föremål för transaktionen,

c) Typ av protokoll som används för anslutning till tjänsten och för överföring av innehåll,

d) Kommunikationens beskaffenhet,

e) Datum och tid för kommunikationen,

f) Den identifikationskod som används av den som utfört kommunikation när denne har tillhandahållit en sådan kod.

3. När det gäller de personer som nämns i I punkt 1 och 2 i samma artikel, ska följande uppgifter lämnas när en användare ingår ett avtal eller vid skapandet av ett konto:

a) Vid den tidpunkt då kontot upprättas, uppgift om anslutningen,

b) Efternamn och förnamn, eller firma,

c) Därtill hörande postadresser,

d) Använda pseudonymer,

e) E-postadresser eller anknutna konton,

f) Telefonnummer,

g) Lösenordet och de uppgifter som gör det möjligt att kontrollera eller ändra det, i den senaste uppdaterade versionen.

4. För de personer som nämns i I punkterna 1 och 2 i samma artikel, följande information om betalningen, för varje betalningstransaktion:

a) Den typ av betalning som används,

b) Uppgift om betalningen,

c) Belopp,

d) Datum och klockslag för transaktionen.

De uppgifter som nämns i punkterna 3 och 4 får endast lagras i den mån personerna vanligtvis samlar in dem.”

52 I artikel 2 i detta dekret anges följande:

”Skapande av innehåll ska omfatta följande moment:

a) Initialt skapande av innehåll,

b) Ändringar av innehåll och data som rör innehållet,

c) Radering av innehåll.”

53 I artikel 3 i samma dekret anges följande:

”De uppgifter som anges i artikel 1 ska lagras i ett år

a) när det gäller de uppgifter som nämns i punkterna 1 och 2, från och med den dag då innehållet skapades, för varje moment som bidrar till skapandet av ett innehåll enligt definitionen i artikel 2,

b) när det gäller de uppgifter som anges i punkt 3, från och med dagen för uppsägningen av avtalet eller stängningen av kontot,

c) när det gäller de uppgifter som anges i punkt 4, från och med den dag då fakturan utfärdades eller betalningstransaktionen genomfördes, för varje faktura eller betalningstransaktion.”

Belgisk rätt

54 Lagen av den 29 maj 2016 ändrar, bland annat, loi du 13 juin 2005 relative aux communications électroniques (lagen av den 13 juni 2005 om elektronisk kommunikation) (nedan kallad lagen av den 13 juni 2005) (Moniteur belge av den 20 juni 2005, s. 28070), code d’instruction criminelle (förundersökningslagen) och loi organique des services de renseignements et de sécurité (lagen av den 30 november 1998 om underrättelse- och säkerhetstjänsterna) (nedan kallad lagen av den 30 november 1998) (Moniteur belge av den 18 december 1998, s. 40312).

55 I artikel 126 i lagen av den 13 juni 2005, i dess lydelse enligt lagen av den 29 maj 2016, föreskrivs följande:

”§ 1. Utan att det påverkar tillämpningen av lagen av den 8 december 1992 om skydd för privatlivet i samband med behandling av personuppgifter, ska leverantörer av allmänt tillgängliga telefonitjänster, inbegripet via internet, internetanslutningar och e-post, operatörer som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät och operatörer som tillhandahåller en av dessa tjänster lagra de uppgifter som avses i punkt 3 som de genererat eller behandlat i samband med tillhandahållande av de aktuella kommunikationstjänsterna.

Denna artikel berör inte innehållet i kommunikationen.

Skyldigheten att lagra de uppgifter som avses i punkt 3 gäller också obesvarade samtal, under förutsättning att uppgifterna ingår i tillhandahållandet av de berörda kommunikationstjänsterna

1. uppgifter om telefoni som genererats eller behandlats av operatörer av allmänt tillgängliga elektroniska kommunikationstjänster eller av ett allmänt elektroniskt kommunikationsnät, eller

2. när det gäller Internetuppgifter som är sparade av dessa leverantörer.

§ 2. Endast följande myndigheter kan, på begäran från de leverantörer och operatörer som avses i punkt 1 första stycket, erhålla uppgifter som lagrats enligt denna artikel, för de syften och på de villkor som räknas upp nedan:

1. Rättsliga myndigheter, för utredning och lagföring av brott, för genomförandet av de åtgärder som avses i artiklarna 46bis och 88bis i straffprocesslagen och i enlighet med de villkor som fastställs i dessa artiklar.

2. Underrättelse- och säkerhetstjänsterna, för att genomföra underrättelseuppdrag och använda sig av de metoder för uppgiftsinsamling som avses i artiklarna 16/2, 18/7 och 18/8 i lagen av den 30 november 1998 om underrättelse- och säkerhetstjänsterna och på de villkor som föreskrivs i denna lag.

3. Varje polistjänsteman vid [Institut belge des services postaux et des télécommunications (belgiska institutet för post- och teletjänster)], för utredning och beivrande av brott enligt artiklarna 114, 124 och mot denna artikel.

4. Räddningstjänst som tillhandahåller hjälp på plats, när den efter ett nödsamtal inte kan få uppgifter om den uppringandes identitet med hjälp av den uppgiftsdatabas som avses i artikel 107 § 2 tredje stycket, eller endast får ofullständiga eller felaktiga uppgifter. Endast uppgifter om den uppringandes identitet får begäras, och det måste ske inom 24 timmar efter samtalet.

5. Polistjänsteman vid den federala polisens enhet med ansvar för eftersökning av försvunna personer, inom ramen för sin uppgift att bistå personer i fara och eftersöka personer vilkas försvinnande är oroande och när det kan antas eller föreligger tydliga indikationer på att den försvunna personen befinner sig i omedelbar fysisk fara. Endast sådana uppgifter som avses i punkt 3 första och andra styckena, som rör den försvunna personen och som lagrats under 48 timmar före begäran om att få ut uppgifterna kan begäras från den berörda operatören eller leverantören genom den polismyndighet som utses av Konungen.

6. Service de médiation pour les télécommunications (teleombudsmannen), i syfte att identifiera den person som har gjort en otillbörlig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst i enlighet med villkoren i artikel 43a § 3 punkt 7 i loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (lag av den 21 mars 1991 om reform av vissa offentliga affärsdrivande företag). Endast identitetsuppgifter får begäras ut.

De leverantörer och aktörer som avses i punkt 1 första stycket ska se till att sådana uppgifter som avses i punkt 3 är obegränsat åtkomliga från Belgien och att de uppgifterna och all annan nödvändig information rörande dessa uppgifter kan överföras utan dröjsmål och endast till de myndigheter som avses i denna punkt.

Utan att det påverkar andra bestämmelser, får de leverantörer och operatörer som avses i punkt 1 första stycket inte använda de uppgifter som lagrats med stöd av punkt 3 för andra ändamål.

§ 3. Uppgifter för att identifiera användaren eller abonnenten samt kommunikationsmedlen, med undantag för de uppgifter som särskilt föreskrivs i andra och tredje styckena, ska bevaras i tolv månader från och med den dag då kommunikation är möjlig för sista gången med hjälp av den tjänst som används.

Uppgifter om tillgång och anslutning av terminalutrustning till nätverket och om placeringen av denna utrustning, inklusive nätanslutningspunkten, ska bevaras i tolv månader från och med dagen för kommunikationen.

Uppgifter om kommunikationer, dock med undantag för deras innehåll, däribland om deras ursprung och slutmål, lagras under tolv månader från dagen för kommunikationen.

Konungen fastställer, genom kungörelse som antas av regeringen på förslag av justitieministern och ministern och efter att ha hört Kommissionen för integritetsskydd och Institutet, vilka slags uppgifter, enligt kategorierna i första till tredje styckena, som ska lagras och de krav som dessa uppgifter ska uppfylla.

…”

Målen vid de nationella domstolarna och tolkningsfrågorna

Mål C-511/18

56 Quadrature du Net, French Data Network och Fédération des fournisseurs d’accès à Internet associatifs samt Igwan.net väckte den 30 november 2015 respektive den 16 mars 2016 talan vid Conseil d’État (Högsta förvaltningsdomstolen, Frankrike) och yrkade att dekreten nr 2015-1185, 2015-1211, 2015-1639 och 2016-67 skulle ogiltigförklaras, bland annat på grund av att de stred mot Frankrikes

konstitution, Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad Europakonventionen) samt direktiven 2000/31 och 2002/58, jämförda med artiklarna 7, 8 och 47 i stadgan.

57 Vad särskilt gäller grunderna om åsidosättande av direktiv 2000/31 har den hänskjutande domstolen påpekat att bestämmelserna i artikel L. 851-3 CSI ålägger operatörer för elektronisk kommunikation och tekniska leverantörer att ”utföra automatiserade behandlingar i sina nät för att, i enlighet med de parametrar som anges i tillståndet, uppdaga anslutningar som kan visa att det föreligger ett terroristhot”. Tekniken är enbart avsedd att användas för att under en begränsad period, bland alla anslutningsuppgifter som behandlas av sådana personer, samla in uppgifter som skulle kunna ha anknytning till ett sådant grovt brott. Under dessa omständigheter anser den hänskjutande domstolen att nämnda bestämmelser inte strider mot artikel 15 i direktiv 2000/31, eftersom de inte föreskriver någon generell aktiv övervakningsskyldighet.

58 Vad gäller grunden avseende åsidosättande av direktiv 2002/58 anser den hänskjutande domstolen att det följer av bland annat bestämmelserna i detta direktiv och av domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970) (nedan kallad Tele2-domen) att de nationella bestämmelser som ålägger dessa leverantörer av elektroniska kommunikationstjänster skyldigheter, såsom en generell och odifferentierad lagring av trafikuppgifter och lokaliseringsuppgifter för användare och abonnenter, för de ändamål som avses i artikel 15.1 i direktivet, bland annat skydd av nationell säkerhet, försvar och allmän säkerhet, faller därmed inom tillämpningsområdet för det direktivet, i den mån de reglerar deras verksamhet. Detsamma gäller bestämmelser som reglerar nationella myndigheters åtkomst till och användning av uppgifterna.

59 Den hänskjutande domstolen har härav dragit slutsatsen att tillämpningsområdet för direktiv 2002/58 omfattar såväl den lagringsskyldighet som följer av artikel L. 851-1 CSI som myndigheternas åtkomst till dessa uppgifter, inklusive uppgifter i realtid, som föreskrivs i artiklarna L. 851-1, L. 851-2 och L. 851-4 i nämnda lag. Samma sak gäller enligt den hänskjutande domstolen bestämmelserna i artikel L. 851-3I CSI. De ålägger visserligen inte på förhand de berörda operatörerna och personerna en lagringsskyldighet, men förpliktar dem ändå att i sina nät tillämpa en automatiserad behandling i syfte att uppdaga anslutningar som kan avslöja ett terroristhot.

60 Den hänskjutande domstolen anser däremot att de bestämmelser i CSI som avses i yrkandena om ogiltigförklaring, vilka avser tekniker för insamling av underrättelseuppgifter som direkt genomförts av staten utan att reglera den verksamhet som bedrivs av leverantörer av elektroniska kommunikationstjänster genom att ålägga dem särskilda skyldigheter, inte omfattas av tillämpningsområdet för direktiv 2002/58. Dessa bestämmelser kan således inte anses utgöra en tillämpning av unionsrätten, vilket innebär att sökandena inte med framgång kan åberopa grunder som avser att nämnda bestämmelser åsidosätter direktiv 2002/58.

61 För att avgöra huruvida dekreten nr 2015-1185, nr 2015-1211, 2015-1639 och 2016-67 är lagenliga med avseende på direktiv 2002/58, i den mån dekreten antagits för att genomföra artiklarna L. 851-1 till L. 851-4 CSI, uppkommer enligt den hänskjutande domstolen tre frågor om tolkningen av unionsrätten.

62 När det gäller tolkningen av artikel 15.1 i direktiv 2002/58 söker den hänskjutande domstolen för det första klarhet i huruvida en generell och odifferentierad lagringsskyldighet som åläggs leverantörer av elektroniska kommunikationstjänster med stöd av artiklarna L. 851-1 och R. 851-5 CSI, i synnerhet mot bakgrund av de garantier och kontroller som är förenade med myndigheternas åtkomst till anslutningsuppgifterna och användningen av dessa uppgifter, inte ska anses utgöra ett ingrepp som är motiverat av den rätt till säkerhet som garanteras i artikel 6 i stadgan och kraven avseende nationell säkerhet, ett område för vilket ansvaret enligt artikel 4 FEU, helt tillkommer medlemsstaterna.

63 Vad för det andra gäller de övriga skyldigheter som kan åläggas leverantörer av elektroniska kommunikationstjänster, har den hänskjutande domstolen påpekat att bestämmelserna i artikel L. 851-2 CSI tillåter insamling av uppgifter och handlingar som avses i artikel L. 851-1 CSI hos samma personer, för terrorförebyggande ändamål. Denna insamling, som endast avser en eller flera enskilda personer som på förhand identifierats som personer som kan ha anknytning till ett terroristhot, utförs i realtid. Samma sak gäller bestämmelserna i artikel L. 851-4 i samma lag, enligt vilka operatörerna i realtid får överföra endast tekniska uppgifter om lokaliseringen av terminalutrustningar. Dessa tekniker styr, för olika syften och på olika sätt, myndigheternas åtkomst i realtid till uppgifter som lagrats enligt CPCE och LCEN, utan att de berörda leverantörerna för den skull åläggs ett ytterligare krav på lagring i förhållande till vad som är nödvändigt för fakturering och tillhandahållande av deras tjänster. Inte heller bestämmelserna i artikel L. 851-3 CSI, i vilka det föreskrivs en skyldighet för tjänsteleverantörerna att genomföra en automatiserad analys av anslutningar på sina nät, innebär en generell och odifferentierad lagring av uppgifter.

64 Den hänskjutande domstolen anser att såväl generell och odifferentierad lagring som åtkomst till anslutningsuppgifter i realtid, i en kontext som präglas av allvarliga och bestående hot mot den nationella säkerheten, särskilt vad gäller terrorrisken, har en operativ nytta utan motsvarighet. En generell och odifferentierad lagring gör det nämligen möjligt för underrättelsetjänsterna att få åtkomst till trafikuppgifter innan skälen för att anse att den berörda personen utgör ett hot mot allmän säkerhet, försvar eller statens säkerhet identifieras. Åtkomst i realtid till uppkopplingsuppgifter gör det möjligt att med hög reaktivitet följa beteendet hos enskilda personer som kan utgöra ett omedelbart hot mot allmän ordning.

65 Vidare innebär den teknik som föreskrivs i artikel L. 851-3 CSI att det på grundval av kriterier som fastställts just i detta syfte blir möjligt att uppdaga personer vars beteende, med hänsyn till deras kommunikationssätt, kan utgöra ett terrorhot.

66 Vad för det tredje gäller de behöriga myndigheternas tillgång till lagrade uppgifter, vill den hänskjutande domstolen få klarhet i huruvida direktiv 2002/58, mot bakgrund av stadgan, ska tolkas så, att de registrerade måste underrättas för att förfarandena för insamling av anslutningsuppgifter ska vara lagenliga, när en sådan information inte längre kan äventyra de behöriga myndigheternas utredningar, eller om sådana förfaranden kan anses vara lagenliga med beaktande av samtliga andra processrättsliga skyddsregler som föreskrivs i nationell rätt, när nämnda skyddsregler säkerställer rätten till ett effektivt rättsmedel.

67 När det gäller dessa övriga processrättsliga skyddsregler har den hänskjutande domstolen bland annat preciserat att var och en som önskar kontrollera att någon underrättelseteknik inte har använts på ett felaktigt sätt kan vända sig till en specialiserad avdelning vid Conseil d'État (Högsta förvaltningsdomstolen), på vilken det ankommer att kontrollera, mot bakgrund av de uppgifter som lämnats till den utan kontradiktoriskt förfarande huruvida någon teknik för insamling av underrättelseuppgifter har använts mot sökanden och om denna har använts i enlighet med del VIII i CSI. De befogenheter som denna avdelning har att handlägga ansökningar säkerställer att den domstolsprövning som den utövar är effektiv. Den är således behörig att handlägga ansökningar, ex officio pröva samtliga rättsstridigheter som den konstaterar och förelägga myndigheterna att vidta alla nödvändiga åtgärder för att avhjälpa de konstaterade rättsstridigheterna. Dessutom ankommer det på Nationella kommissionen för kontroll av underrättelseteknik att kontrollera att teknikerna för insamling av underrättelseuppgifter har genomförts inom landet i enlighet med de krav som följer av CSI. Den omständigheten att det i de lagbestämmelser som är aktuella i det nationella målet inte föreskrivs att berörda personer ska underrättas om de övervakningsåtgärder som dessa personer har varit föremål för utgör således inte i sig en orimlig kränkning av rätten till respekt för privatlivet.

68 Mot denna bakgrund beslutade Conseil d'État (Högsta förvaltningsdomstolen) att vilandeförklara målet och ställa följande tolkningsfrågor till EU-domstolen:

”1. Ska den generella och odifferentierade lagringsskyldighet som åläggs leverantörerna med stöd av bestämmelserna i artikel 15.1 i direktiv [2002/58], i ett sammanhang som präglas av ihållande, allvarliga hot mot den nationella säkerheten, i synnerhet risken för terrorism, ses som ett ingrepp som motiveras av rätten till personlig säkerhet enligt artikel 6 i [stadgan] och kraven på nationell säkerhet, vilket uteslutande är medlemsstaternas ansvar enligt artikel 4 [FEU]?

2. Ska direktiv [2002/58], jämförd med stadgan, tolkas så att det medger sådana lagstiftningsåtgärder som åtgärder för insamling i realtid av trafik- och lokaliserings-uppgifter avseende vissa bestämda personer som visserligen påverkar rättigheterna och skyldigheterna för leverantörer av elektroniska kommunikationstjänster men för den skull inte ålägger dem någon specifik skyldighet att lagra uppgifterna?

3. Ska direktiv [2002/58], jämfört med [stadgan], tolkas så, att det under alla omständigheter kräver att förfarandena för insamling av uppkopplingsuppgifter för att vara lagenliga måste inbegripa information till de berörda personerna när en sådan information inte längre kan skada de behöriga myndigheternas undersökningar, eller kan sådana förfaranden anses vara lagenliga med hänsyn till alla andra befintliga processuella garantier, i och med att dessa garantier omfattar ett effektivt rättsmedel?”

Mål C-512/18

69 Genom ansökan som ingavs den 1 september 2015 väckte French Data Network, Quadrature du Net och Fédération des fournisseurs d'accès à Internet associatifs talan vid Conseil d'État (Högsta förvaltningsdomstolen) om ogiltigförklaring av det tysta avslagsbeslut som följde av premiärministerns underlåtenhet att besvara deras begäran om upphävande av artikel R. 10-13 i CPCE och av dekret nr 2011-219, bland annat med motiveringen att dessa dekret stred mot artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 11 i stadgan. Privacy International och Center for Democracy and Technology tilläts intervenera i det nationella målet.

70 När det gäller artikel R. 10-13 CPCE och den däri föreskrivna skyldigheten att generellt och odifferentierat lagra trafikuppgifter, har den hänskjutande domstolen, som ger uttryck för överväganden som liknar dem som gjorts i mål C-511/18, påpekat att en sådan lagring gör det möjligt för den rättsliga myndigheten att få tillgång till uppgifter om kommunikationer som en person har genomfört innan vederbörande är misstänkt för brott, så att denna lagring är ojämförligt mest användbar för utredning, fastställande och lagföring.

71 Vad gäller dekret nr 2011-219 anser den hänskjutande domstolen att artikel 6 II LCEN, som endast föreskriver en skyldighet att inneha och lagra uppgifter hänförliga till skapande av innehåll, inte heller omfattas av tillämpningsområdet för direktiv 2002/58, eftersom det direktivet enligt artikel 3.1 är begränsat till tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät inom unionen, utan av tillämpningsområdet för direktiv 2000/31.

72 Den hänskjutande domstolen anser emellertid att det framgår av punkterna 1 och 2 i artikel 15 i direktiv 2000/31 att direktivet inte innebär ett principiellt förbud mot lagring av uppgifter hänförliga till skapande av innehåll, från vilket det endast undantagsvis kan göras avvikelser. Således uppkommer frågan huruvida artiklarna 12, 14 och 15 i nämnda direktiv, jämförda med artiklarna 6–8 och 11 samt artikel 52.1 i stadgan, ska tolkas så, att de gör det möjligt för en medlemsstat att införa en nationell lagstiftning, såsom artikel 6 II LCEN, som ålägger de berörda personerna att lagra uppgifter som kan göra det möjligt att identifiera den person som har bidragit till upprättandet av innehållet i eller något

av innehållet i de tjänster som de tillhandahåller, för att den rättsliga myndigheten i förekommande fall ska kunna begära att få ut kommunikationen för att se till att bestämmelser om skadeståndsansvar och straffrättsligt ansvar iakttas.

73 Mot denna bakgrund beslutade Conseil d'État (Högsta förvaltningsdomstolen) att vilandeförklara målet och ställa följande tolkningsfrågor till EU-domstolen:

”1. Ska en generell och odifferentierad lagringsskyldighet för tjänsteleverantörer i enlighet med bestämmelserna i artikel 15.1 i direktiv [2002/58], inte minst med hänsyn till de garantier och kontroller som sedan gäller för insamling och användning av dessa uppkopplingsuppgifter, betraktas som ett ingrepp som kan motiveras av rätten till personlig säkerhet enligt artikel 6 i [stadgan] och kraven på nationell säkerhet, vilket uteslutande är medlemsstaternas ansvar enligt artikel 4 [FEU]?

2. Ska bestämmelserna i direktiv [2000/31], jämförda med artiklarna 6, 7, 8 och 11 samt artikel 52.1 i [stadgan], tolkas så, att de tillåter en medlemsstat att införa en nationell lagstiftning som innebär att de personer vars verksamhet består i att tillhandahålla tillgång till kommunikationstjänster online till allmänheten och fysiska eller juridiska personer som, även kostnadsfritt, för tillhandahållandet av kommunikationstjänster online till allmänheten svarar för lagring av alla former av signaler, skrift, bilder, ljud eller meddelanden som tillhandahållits av mottagarna av dessa tjänster, är skyldiga att lagra uppgifter som gör det möjligt att identifiera en person som har bidragit till skapandet av innehåll eller något av innehållet i de tjänster som de tillhandahåller, så att en rättslig myndighet vid behov kan begära att få ta del av uppgifterna för att se till att bestämmelser om civilrättsligt eller straffrättsligt ansvar iakttas?”

Mål C-520/18

74 Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL och UA, Liga voor Mensenrechten ASBL och Ligue des droits de l'Homme ASBL och Ligue des droits de l'Homme ASBL samt VZ, WY och XX väckte talan vid Cour constitutionnelle (Författningsdomstolen, Belgien) genom ansökningar som ingavs den 10 januari, den 16 januari, den 17 januari och den 18 januari 2017 om ogiltigförklaring av lagen av den 29 maj 2016. Det gjordes gällande att nämnda lag åsidosätter artiklarna 10 och 11 i Belgiens konstitution, jämförda med artiklarna 5, 6–11, 14, 15, 17 och 18 i Europakonventionen, artiklarna 7, 8, 11 och 47 samt artikel 52.1 i stadgan, artikel 17 i den internationella konventionen om medborgerliga och politiska rättigheter, som ingicks i New York den 16 december 1966 och som trädde i kraft den 23 mars 1976, de allmänna principerna om rättssäkerhet, proportionalitet och självbestämmande i fråga om information samt artikel 5.4 FEU.

75 Sökandena i det nationella målet har till stöd för sin talan i huvudsak gjort gällande att lagen av den 29 maj 2016 är rättsstridig bland annat på grund av att lagen går utöver vad som är strängt nödvändigt och inte föreskriver tillräckliga skyddsgarantier. I synnerhet uppfyller varken bestämmelserna om lagring av uppgifter eller om myndigheternas åtkomst till lagrade uppgifter de krav som följer av domen av den 8 april 2014, Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238) (nedan kallad Digital Rights-domen), och domen av den 21 december 2016, Tele2 (C-203/15 och C-698/15, EU:C:2016:970). Dessa bestämmelser innebär nämligen en risk för att kartläggning av personer, vilket innebär en risk för missbruk från behöriga myndigheters sida, och de föreskriver inte heller en lämplig nivå för säkring och skydd av lagrade uppgifter. Lagen omfattar slutligen personer som har tystnadsplikt och personer som är skyldiga att iaktta sekretess, och lagen rör känsliga personuppgifter som inte innehåller några särskilda garantier för att skydda sistnämnda uppgifter.

76 Den hänskjutande domstolen har påpekat att de uppgifter som leverantörer av telefonitjänster, inbegripet internet, tillgång till Internet och e-post samt operatörer som tillhandahåller allmänna elektroniska kommunikationsnät ska lagra enligt lagen av den 29 maj 2016, är identiska med de uppgifter som räknas upp i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, 2006, s. 54), utan att det görs någon skillnad vad gäller berörda personer eller det eftersträvade syftet. Den hänskjutande domstolen har preciserat att lagstiftarens syfte med denna lag inte bara är att bekämpa terrorism och barnpornografi, utan även att kunna använda lagrade uppgifter i många olika situationer inom ramen för brottsutredningar. Den hänskjutande domstolen har dessutom konstaterat att det framgår av förarbetena till nämnda lag att den nationella lagstiftaren ansåg att det mot bakgrund av det eftersträvade målet var omöjligt att införa en riktad och differentierad lagringsskyldighet och att den valde att förena skyldigheten att bevara generell och odifferentierad lagring med strikta garantier, såväl i fråga om de lagrade uppgifterna som i fråga om tillgång till dessa, för att begränsa ingreppet i rätten till respekt för privatlivet till ett minimum.

77 Den hänskjutande domstolen har tillagt att det i artikel 126.2 punkterna 1 och 2 i lagen av den 13 juni 2005, i dess lydelse enligt lagen av den 29 maj 2016, föreskrivs på vilka villkor de rättsliga myndigheterna respektive underrättelse- och säkerhetstjänsten kan få tillgång till lagrade uppgifter, vilket innebär att prövningen av denna lags lagenlighet mot bakgrund av unionsrättens krav ska vilandeförklaras till dess att EU-domstolen meddelar sina avgöranden i två mål om begäran om förhandsavgörande som är anhängiga vid dem.

78 Den hänskjutande domstolen har slutligen påpekat att lagen av den 29 maj 2016 syftar till att möjliggöra en effektiv förundersökning och effektiva straffrättsliga påföljder vid sexuellt utnyttjande av underåriga och att göra det möjligt att identifiera gärningsmannen, även när elektroniska kommunikationsmedel används. Under förfarandet vid domstolen uppmärksammades i detta avseende de positiva skyldigheter som följer av artiklarna 3 och 8 i Europakonventionen. Dessa skyldigheter kan även följa av bestämmelserna i stadgan, vilket skulle kunna påverka tolkningen av artikel 15.1 i direktiv 2002/58.

79 Mot denna bakgrund beslutade Cour constitutionnelle (Författningsdomstolen) att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”1. Ska artikel 15.1 i direktiv [2002/58], jämförd med rätten till säkerhet, som garanteras av artikel 6 i [stadgan], och rätten till skydd för personuppgifter, som garanteras av artiklarna 7, 8, och 52.1 i stadgan, tolkas på så sätt att den utgör hinder för en nationell lagstiftning som den som är aktuell i det nationella målet, i vilken det föreskrivs en generell skyldighet för operatörer och leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, i den mening som avses i direktiv [2002/58], som genereras eller behandlas av dem i samband med att de tillhandahåller dessa tjänster och vars syfte inte endast omfattar undersökning, avslöjande av och åtal för grov brottslighet, utan även skydd för nationell säkerhet, försvaret och allmän säkerhet samt undersökning, avslöjande av och åtal för annan brottslighet än grov brottslighet eller förebyggande av otillåten användning av elektroniska kommunikationssystem eller uppnåendet av något annat mål enligt artikel 23.1 i förordning (EU) 2016/679, och i vilken nämnda skyldighet dessutom åtföljs av i lagstiftningen närmare angivna skyddsmekanismer med avseende på lagringen av och tillgången till uppgifterna?

2. Ska artikel 15.1 i direktiv [2002/58], jämförd med artiklarna 4, 7, 8, 11 och 52.1 i [stadgan], tolkas på så sätt att den utgör hinder för en nationell lagstiftning som den som är aktuell i det nationella målet, där det föreskrivs en generell skyldighet för operatörer och leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, i den mening som avses i direktiv [2002/58], som genereras eller behandlas av dem i samband med att de tillhandahåller

dessa tjänster, om nämnda lagstiftning bland annat har till syfte att uppfylla de positiva skyldigheter som åligger myndigheten enligt artiklarna 4 och [7] i stadgan, vilka består i att inrätta en rättslig ram som möjliggör effektiv brottsutredning och verkningsfulla straff för sexuella övergrepp mot underåriga och som gör det möjligt att på ett effektivt sätt identifiera gärningsmannen, även när elektroniska kommunikationstjänster används?

3. Om Cour constitutionnelle [(Författningsdomstolen)], på grundval av svaren på den första eller den andra frågan, skulle komma fram till att den angripna lagen strider mot en eller flera skyldigheter enligt de bestämmelser som nämns i dessa frågor, skulle den då kunna besluta att verkningarna av [den omtvistade lagen] tills vidare ska bestå för att undvika rättsosäkerhet och möjliggöra att tidigare insamlade och lagrade uppgifter fortfarande kan användas för de mål som uppställs i den lagen?”

Förfarandet vid domstolen

80 Domstolens ordförande har genom beslut av den 25 september 2018 förenat målen C-511/18 och C-512/18 vad gäller det skriftliga och det muntliga förfarandet samt domen. Domstolens ordförande beslutade den 9 juli 2020 att förena mål C-520/18 med dessa mål vad gäller domen.

Prövning av tolkningsfrågorna

Fråga 1 i mål C-511/18 respektive mål C-512/18 samt frågorna 1 och 2 i mål C-520/18

81 De hänskjutande domstolarna har ställt fråga 1 i mål C-511/18 respektive mål C-512/18 samt frågorna 1 och 2 i mål C-520/18, vilka ska prövas tillsammans, för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58 ska tolkas så, att den utgör hinder för nationell lagstiftning i vilken leverantörer av elektroniska kommunikationstjänster åläggs att, för de ändamål som föreskrivs i nämnda artikel 15.1, på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter.

Inledande synpunkter

82 Det framgår av de handlingar i målen som domstolen förfogar över att de lagstiftningar som är i fråga i de nationella målen omfattar samtliga elektroniska kommunikationsmedel och samtliga användare av dessa kommunikationsmedel, utan att det görs någon åtskillnad eller något undantag i detta avseende. Dessutom utgörs de uppgifter som leverantörer av elektroniska kommunikationstjänster åläggs att lagra enligt dessa lagstiftningar bland annat av de uppgifter som krävs för att spåra källan och slutmålet för kommunikationen, fastställa datum, tidpunkt, varaktighet och typ av kommunikation, identifiera den kommunikationsutrustning som används samt för att lokalisera terminalutrustning och kommunikationer. Bland dessa uppgifter återfinns bland annat användarens namn och adress, uppringarens respektive den uppringdas telefonnummer samt IP-adressen för internettjänster. Innehållet i de berörda kommunikationerna innefattas emellertid inte av dessa uppgifter.

83 De uppgifter som, enligt de nationella lagstiftningar som är i fråga i de nationella målen, ska lagras i ett år gör det således bland annat möjligt att få kännedom om med vilken person en användare av ett elektroniskt kommunikationsmedel har kommunicerat och vilket kommunikationsmedel som har använts, att fastställa datum, tidpunkt och varaktighet för kommunikationen och internetuppkopplingarna samt från vilken plats dessa har ägt rum, och att få kännedom om terminalutrustningens lokalisering, utan att någon kommunikation nödvändigtvis har överförts. Nämnda uppgifter gör det dessutom möjligt att fastställa hur ofta användaren har kommunicerat med vissa personer under en viss period. Vad slutligen gäller den nationella lagstiftning som är i fråga i

målen C-511/18 och C-512/18, förefaller det som om den, i den mån den även omfattar uppgifter om överföring av elektronisk kommunikation via nät, även gör det möjligt att fastställa vilken slags information som användaren har sökt efter på internet.

84 Vad gäller de syften som eftersträvas ska det påpekas att bland dessa syften ingår bland annat, i fallet med de lagstiftningar som är i fråga i målen C-511/18 och C-512/18, undersökning, fastställande och lagföring av brott i allmänhet, nationellt oberoende, territoriell integritet och nationellt försvar, betydande utrikespolitiska intressen, fullgörandet av Frankrikes europeiska och internationella åtaganden, Frankrikes betydande ekonomiska, industriella och vetenskapliga intressen samt förebyggande av terrorism, angrepp på det republikanska statsskicket och upplopp vilket allvarligt hotar den allmänna ordningen. Vad gäller den lagstiftning som är i fråga i mål C-520/18 utgörs de eftersträvade syftena bland annat av undersökning, avslöjande och lagföring av brott samt av skydd för nationell säkerhet, försvaret och allmän säkerhet.

85 De hänskjutande domstolarna vill särskilt få klarhet i vilken inverkan den i artikel 6 i stadgan stadfästa rätten till säkerhet eventuellt har på tolkningen av artikel 15.1 i direktiv 2002/58. De vill även få klarhet i huruvida det ingrepp i de grundläggande rättigheterna i artiklarna 7 och 8 i stadgan som den lagring av uppgifter som föreskrivs i de lagstiftningar som är i fråga i de nationella målen innebär, kan anses vara motiverat, med hänsyn till att det finns bestämmelser som begränsar de nationella myndigheternas åtkomst till lagrade uppgifter. Eftersom frågan har ställts i en kontext som präglas av allvarliga och bestående hot mot nationell säkerhet, ska den enligt Conseil d'État (Högsta förvaltningsdomstolen) även bedömas mot bakgrund av artikel 4.2 FEU. Cour constitutionnelle (Författningsdomstolen) har å sin sida understrukit att den nationella lagstiftning som är i fråga i mål C-520/18 även genomför positiva skyldigheter som följer av artiklarna 4 och 7 i stadgan, vilka består i att anta lagbestämmelser som gör det möjligt att effektivt bekämpa sexuella övergrepp av underåriga.

86 Såväl Conseil d'État (Högsta förvaltningsdomstolen) som Cour constitutionnelle (Författningsdomstolen) utgår från att de nationella lagstiftningar som är i fråga i de nationella målen, vilka reglerar lagring av trafik- och lokaliseringsuppgifter samt de nationella myndigheternas åtkomst till dessa uppgifter för de ändamål som anges i artikel 15.1 i direktiv 2002/58, såsom skyddet av nationell säkerhet, omfattas av detta direktivs tillämpningsområde. Vissa av parterna i de nationella målen och vissa av de medlemsstater som har inkommit med skriftliga yttranden till domstolen har emellertid gett uttryck för en avvikande åsikt i detta avseende, i synnerhet vad avser tolkningen av artikel 1.3 i detta direktiv. Det ska således först prövas huruvida nämnda lagstiftningar omfattas av tillämpningsområdet för detta direktiv.

Tillämpningsområdet för direktiv 2002/58

87 La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International och Center for Democracy and Technology har, med hänvisning till domstolens rättspraxis avseende tillämpningsområdet för direktiv 2002/58, i huvudsak anfört att såväl lagring av uppgifter som åtkomst till lagrade uppgifter omfattas av direktivets tillämpningsområde, oberoende av om åtkomsten sker i realtid eller ej. Eftersom syftet att skydda nationell säkerhet uttryckligen nämns i artikel 15.1 i direktivet medför eftersträvandet för att uppnå detta mål inte att direktivet inte är tillämpligt. Artikel 4.2 FEU, som de hänskjutande domstolarna har hänvisat till, påverkar inte denna bedömning.

88 Vad gäller de underrättelseåtgärder som de behöriga franska myndigheterna vidtar direkt utan att reglera verksamheten för leverantörer av elektroniska kommunikationstjänster genom att ålägga dem specifika skyldigheter, har Center for Democracy and Technology påpekat att dessa åtgärder med

nödvändighet omfattas av tillämpningsområdet för direktiv 2002/58 och stadgan, eftersom de utgör undantag från den konfidentialitetsprincip som garanteras i artikel 5 i direktivet. Nämnda åtgärder måste således uppfylla de krav som följer av artikel 15.1 i direktivet.

89 Den franska, den tjeckiska och den estniska regeringen, Irland, den cypriotiska, den ungerska, den polska och den svenska regeringen samt Förenade kungarikets regering har däremot i huvudsak gjort gällande att direktiv 2002/58 inte är tillämpligt på sådana nationella lagstiftningar som dem som är i fråga i de nationella målen, eftersom dessa syftar till att skydda nationell säkerhet. Underrättelsetjänsternas verksamhet, i den mån den avser upprätthållande av allmän ordning och skydd för inre säkerhet och territoriell integritet, omfattas av medlemsstaternas väsentliga statliga funktioner och, följaktligen, av deras exklusiva befogenhet, vilket bland annat framgår av artikel 4.2 tredje meningen FEU.

90 Dessa regeringar och Irland har dessutom hänvisat till artikel 1.3 i direktiv 2002/58, enligt vilken verksamhet som avser allmän säkerhet, försvar och statens säkerhet inte omfattas av direktivets tillämpningsområde, i likhet med vad som redan föreskrevs i artikel 3.2 första strecksatsen i direktiv 95/46. De stödjer sig i detta avseende på tolkningen av sistnämnda bestämmelse i domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346).

91 Det ska noteras att enligt lydelsen i artikel 1.1 i direktiv 2002/58 möjliggörs genom direktivet en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation.

92 I artikel 1.3 i nämnda direktiv utesluts ”statens verksamheter” på vissa angivna områden från direktivets tillämpningsområde, bland annat statens verksamheter på straffrättens område liksom verksamheter som avser allmän säkerhet, försvar, statens säkerhet, inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet. De verksamheter som nämns som exempel är i samtliga fall verksamheter som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 32 och där angiven rättspraxis).

93 I artikel 3 i direktiv 2002/58 anges dessutom att direktivet ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning (nedan kallade elektroniska kommunikationstjänster). Direktivet ska därför anses reglera verksamheten för leverantörer av sådana tjänster (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 33 och där angiven rättspraxis).

94 I detta sammanhang låter artikel 15.1 i direktiv 2002/58 medlemsstaterna, på de villkor som föreskrivs i den artikeln, ”genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv” (dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 71).

95 Artikel 15.1 i direktiv 2002/58 förutsätter emellertid med nödvändighet att den nationella lagstiftning som avses i den bestämmelsen omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast om de däri angivna villkoren är uppfyllda. Sådan lagstiftning reglerar dessutom, för de ändamål som anges i bestämmelsen, verksamheten för leverantörer av elektroniska kommunikationstjänster (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 34 och där angiven rättspraxis).

96 Det är bland annat mot bakgrund av dessa överväganden som domstolen har slagit fast att artikel 15.1 i direktiv 2002/58, jämförd med artikel 3 i samma direktiv, ska tolkas så, att tillämpningsområdet för direktivet inte bara omfattar lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, utan även lagstiftning som ålägger dessa leverantörer att ge de behöriga nationella myndigheterna åtkomst till dessa uppgifter. Sådan lagstiftning medför nämligen med nödvändighet behandling av nämnda uppgifter från leverantörernas sida och kan, i den mån de reglerar dessa leverantörers verksamhet, inte likställas med sådana staten förbehållna verksamheter som avses i artikel 1.3 i nämnda direktiv (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkterna 35 och 37 och där angiven rättspraxis).

97 Mot bakgrund av övervägandena i punkt 95 ovan och systematiken i direktiv 2002/58 skulle en tolkning av detta direktiv, enligt vilken sådan lagstiftning som avses i artikel 15.1 i direktivet skulle vara undantagen från direktivets tillämpningsområde på grund av att de syften som denna lagstiftning måste eftersträva i materiellt hänseende väsentligen överlappar med syftena med de verksamheter som avses i artikel 1.3 i direktivet, innebära att nämnda artikel 15.1 helt fråntogs sin ändamålsenliga verkan (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 72 och 73).

98 Begreppet ”verksamheter” i artikel 1.3 i direktiv 2002/58 kan således inte, såsom generaladvokaten i huvudsak fann i punkt 75 i sitt förslag till avgörande i de förenade målen La Quadrature du Net m.fl. (C-511/18 och C-512/18, EU:C:2020:6), tolkas så, att det omfattar sådan lagstiftning som den som avses i artikel 15.1 i detta direktiv.

99 Denna slutsats påverkas inte av artikel 4.2 FEU som de regeringar som nämns i punkt 89 ovan har hänvisat till. Enligt domstolens fasta praxis kan den omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet nämligen inte, trots att det ankommer på medlemsstaterna att definiera sina väsentliga säkerhetsintressen och att vidta de åtgärder som är nödvändiga för att säkerställa inre och yttre säkerhet, leda till att unionsrätten inte är tillämplig och befria medlemsstaterna från skyldigheten att iaktta unionsrätten (se, för ett liknande resonemang, dom av den 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punkt 38, dom av den 20 mars 2018, kommissionen/Österrike (Statstryckeri), C-187/16, EU:C:2018:194, punkterna 75 och 76, och dom av den 2 april 2020, kommissionen/Polen, Ungern och Republiken Tjeckien (Tillfällig mekanism för omplacering av personer som ansöker om internationellt skydd), C-715/17, C-718/17 och C-719/17, EU:C:2020:257, punkterna 143 och 170).

100 Det är riktigt att domstolen i domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346, punkterna 56–59), slog fast att lufttrafikföretags överföring av personuppgifter till myndigheter i tredjeland i syfte att förebygga och bekämpa terrorism och andra grova brott i kraft av artikel 3.2 första strecksatsen i direktiv 95/46 inte omfattades av tillämpningsområdet för detta direktiv, eftersom denna överföring sker inom en ram som inrättats av statsmakterna och som avser allmän säkerhet.

101 Med beaktande av övervägandena i punkterna 93, 95 och 96 ovan kan denna rättspraxis emellertid inte överföras på tolkningen av artikel 1.3 i direktiv 2002/58. Såsom generaladvokaten i huvudsak anförde i punkterna 70–72 i sitt förslag till avgörande i de förenade målen La Quadrature du Net m.fl. (C-511/18 och C-512/18, EU:C:2020:6), utesluter artikel 3.2 första strecksatsen i direktiv 95/46, vilken är den bestämmelse som avses i nämnda rättspraxis, nämligen från sitt tillämpningsområde generellt ”behandlingar som rör allmän säkerhet, försvar, statens säkerhet” utan att någon åtskillnad görs med avseende på vem som behandlar uppgifterna i fråga. En sådan åtskillnad måste däremot göras vid tolkningen av artikel 1.3 i direktiv 2002/58. Såsom framgår av punkterna 94–97 ovan omfattas nämligen all behandling av personuppgifter som utförs av leverantörer av elektroniska kommunikationstjänster av detta direktivs tillämpningsområde, inbegripet den behandling som följer av skyldigheter som ålagts dem av statsmakten. Den sistnämnda behandlingen kunde emellertid, i förekommande fall, omfattas av undantaget i artikel 3.2 första strecksatsen i direktiv 95/46, med

hänsyn till den mer vidsträckta utformningen av den bestämmelsen, vilken avsåg all behandling, oavsett vem som är uppgiftsbehandlare och oavsett om den avser allmän säkerhet, försvar eller statens säkerhet.

102 Det ska dessutom påpekas att direktiv 95/46 som var i fråga i det mål som avgjordes genom domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346), enligt artikel 94.1 i förordning 2016/679 upphävdes och ersattes av denna förordning, med verkan från och med den 25 maj 2018. Även om det i artikel 2.2 d i nämnda förordning anges att den inte ska tillämpas på behandling som utförs av ”behöriga myndigheter” i syfte att bland annat förebygga och avslöja brott, i vilket även ingår att förhindra hot mot allmän säkerhet och förebygga sådana hot, framgår det av artikel 23.1 d och h i samma förordning att förordningen är tillämplig på behandling av personuppgifter som utförs av enskilda för samma ändamål. Härav följer att ovannämnda tolkning av artikel 1.3, artikel 3 och artikel 15.1 i direktiv 2002/58 är förenlig med den avgränsning av tillämpningsområdet för förordning 2016/679 som direktivet kompletterar och preciserar.

103 När medlemsstaterna däremot direkt genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, utan att ålägga tjänsteleverantörer av sådan kommunikation någon skyldighet att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktiv 2002/58, utan enbart av nationell rätt, med förbehåll för tillämpningen av Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89), vilket innebär att åtgärderna i fråga bland annat måste vara förenliga med nationell rätt på grundlagsnivå och kraven i Europakonventionen.

104 Av övervägandena ovan följer att nationell lagstiftning vilken ålägger leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet och bekämpa brottslighet, såsom de lagstiftningar som är i fråga i de nationella målen, omfattas av tillämpningsområdet för direktiv 2002/58.

Tolkningen av artikel 15.1 i direktiv 2002/58

105 Domstolen erinrar inledningsvis om att det framgår av fast rättspraxis att vid tolkningen av en unionsbestämmelse ska inte bara lydelsen beaktas, utan också sammanhanget och de mål som eftersträvas med de föreskrifter som bestämmelsen ingår i. Därutöver ska bland annat förarbetena till bestämmelserna beaktas (se, för ett liknande resonemang, dom av den 17 april 2018, Egenberger, C-414/16, EU:C:2018:257, punkt 44)

106 Syftet med direktiv 2002/58 är, såsom framgår av bland annat skälen 6 och 7 i direktivet, att skydda användarna av elektroniska kommunikationstjänster mot de faror för deras personuppgifter och deras privatliv som följer av ny teknik och särskilt den ökade kapaciteten för automatiserad lagring och behandling av uppgifter. Direktivet syftar särskilt, såsom anges i dess skäl 2, till att säkerställa full respekt för de rättigheter som anges i artiklarna 7 och 8 i stadgan. Det framgår av motiveringen till förslaget till Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (COM(2000) 385 final), som ligger till grund för direktiv 2002/58, att unionslagstiftaren avsåg att ”garantera en fortsatt hög skyddsnivå för personuppgifter och privatliv för alla elektroniska kommunikationstjänster, oavsett vilken teknik som används”.

107 I detta syfte fastställs i artikel 5.1 i direktiv 2002/58 principen om konfidentialitet för såväl elektronisk kommunikation som därmed förbundna trafikuppgifter. Detta innebär bland annat ett principiellt förbud för andra personer än användarna att, utan användarnas samtycke, lagra sådan kommunikation och sådana uppgifter.

108 Vad särskilt gäller den behandling och lagring av trafikuppgifter som genomförs av leverantörer av elektroniska kommunikationstjänster, framgår det av artikel 6 samt av skälen 22 och 26 i direktiv 2002/58 att en sådan behandling endast är tillåten i den utsträckning och under den tid som krävs för att kunna saluföra tjänster, fakturera för dem och tillhandahålla mervärdestjänster. När den perioden har löpt ut, ska de behandlade och lagrade uppgifterna utplånas eller avidentifieras. Vad gäller andra lokaliseringsuppgifter än trafikuppgifter, föreskriver artikel 9.1 i direktivet att de endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke (dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 86 och där angiven rättspraxis).

109 Genom att anta detta direktiv har unionslagstiftaren således konkretiserat de rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan, vilket innebär att användarna av elektroniska kommunikationsmedel i princip har rätt att förvänta sig att deras kommunikationer och därmed förbundna uppgifter förblir anonyma och inte kan registreras, såvida de inte har samtyckt till detta.

110 Enligt artikel 15.1 i direktiv 2002/58 får medlemsstaterna emellertid införa undantag från den principiella skyldigheten enligt artikel 5.1 i direktivet att garantera konfidentialiteten för personuppgifter och från motsvarande skyldigheter, vilka nämns bland annat i artiklarna 6 och 9 i direktivet, när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period när det är motiverat av ett av dessa skäl.

111 Möjligheten att göra undantag från de rättigheter och skyldigheter som föreskrivs i artiklarna 5, 6 och 9 i direktiv 2002/58 kan emellertid inte motivera att ett undantag från den principiella skyldigheten att säkerställa konfidentialiteten för elektronisk kommunikation och därmed tillhörande uppgifter, och i synnerhet från det förbud mot lagring av sådana uppgifter som uttryckligen föreskrivs i artikel 5 i direktivet, blir huvudregeln (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 89 och 104).

112 Vad gäller de mål som kan motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58, har domstolen redan slagit fast att uppräkningen av mål i artikel 15.1 första meningen i detta direktiv är uttömmande. En lagstiftningsåtgärd som har vidtagits med stöd av denna bestämmelse måste därför faktiskt och strikt avse ett av dessa mål (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 52 och där angiven rättspraxis).

113 Det framgår dessutom av artikel 15.1 tredje meningen i direktiv 2002/58 att medlemsstaterna endast får vidta lagstiftningsåtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som avses i artiklarna 5, 6 och 9 i direktivet i enlighet med de allmänna principerna i unionsrätten, däribland proportionalitetsprincipen, och de grundläggande rättigheter som garanteras i stadgan. Domstolen har redan slagit fast att när en medlemsstat i nationell lagstiftning ålägger leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra trafikuppgifter i syfte att, i förekommande fall, göra dem tillgängliga för behöriga nationella myndigheter väcker detta frågor om en sådan lagstiftnings förenlighet inte bara med artiklarna 7 och 8 i stadgan, vilka rör skyddet för privatlivet respektive skyddet av personuppgifter, utan även med artikel 11 i stadgan, som rör yttrandefriheten

(se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkterna 25 och 70, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 91 och 92 och där angiven rättspraxis).

114 Vid tolkningen av artikel 15.1 i direktiv 2002/58 ska således betydelsen av såväl rätten till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan, som rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, såsom denna betydelse framgår av domstolens praxis, samt betydelsen av rätten till yttrandefrihet beaktas. Denna grundläggande rättighet, som garanteras i artikel 11 i stadgan, utgör nämligen en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som unionen enligt artikel 2 FEU bygger på (se, för ett liknande resonemang, dom av den 6 mars 2001, Connolly/kommissionen, C-274/99 P, EU:C:2001:127, punkt 39, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 93 och där angiven rättspraxis).

115 Det ska i detta avseende preciseras att lagring av trafik- och lokaliseringsuppgifter i sig utgör dels ett undantag från förbudet i artikel 5.1 i direktiv 2002/58 för andra personer än användarna att lagra dessa uppgifter, dels ett ingrepp i de grundläggande rättigheter till respekt för privatlivet och skydd av personuppgifter, vilka är stadfästa i artikel 7 respektive artikel 8 i stadgan, oberoende av om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkterna 124 och 126 och där angiven rättspraxis; se, analogt, vad avser artikel 8 i Europakonventionen, Europadomstolen, 30 januari 2020, Breyer mot Tyskland, CE:ECHR:2020:0130JUD005000112, 81 §).

116 Det är inte heller relevant huruvida de lagrade uppgifterna därefter används eller inte (se, analogt, vad gäller artikel 8 i Europakonventionen, Europadomstolen, 16 februari 2000, Amann mot Schweiz, CE:ECHR:2000:0216JUD002779895, 69 §, samt Europadomstolen, 13 februari 2020, Trjakovski och Chipovski mot Nordmakedonien, CE:ECHR:2020:0213JUD005320513, 51 §), eftersom åtkomsten till sådana uppgifter, oberoende av hur de senare används, utgör ett separat ingrepp i de grundläggande rättigheter som avses i föregående punkt (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkterna 124 och 126).

117 Denna slutsats framstår som än mer motiverad med hänsyn till att trafik- och lokaliseringsuppgifter kan avslöja information om ett stort antal aspekter av de berörda personernas privatliv, inbegripet känslig information, såsom sexuell läggning, politisk åskådning, religiös, filosofisk eller annan övertygelse, samhällsåskådning samt hälsotillstånd, med hänsyn till att sådana uppgifter dessutom omfattas av ett särskilt skydd enligt unionsrätten. Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. I synnerhet gör dessa uppgifter det möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt med avseende på rätten till respekt för privatlivet som själva innehållet i kommunikationerna (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkt 27, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 99).

118 Lagring av trafik- och lokaliseringsuppgifter för polisiära ändamål kan således i sig utgöra ett åsidosättande av rätten till respekt för kommunikationer, vilken är stadfäst i artikel 7 i stadgan, och ha en avhållande inverkan på användarna av elektroniska kommunikationsmedels utövande av sin yttrandefrihet, vilken garanteras i artikel 11 i stadgan (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkt 28, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 101). En sådan avhållande inverkan kan särskilt påverka personer vars kommunikationer enligt nationella regler omfattas av tystnadsplikt och visselblåsare, vilkas verksamhet skyddas av Europaparlamentets och rådets

direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som avslöjar överträdelser av unionsrätten (EUT L 305, 2019, s. 17). Den omständigheten att antalet lagrade uppgifter är stort och att det rör sig om många olika slags uppgifter förstärker dessutom allvaret av dessa effekter.

119 Med hänsyn till den stora mängd trafik- och lokaliseringsuppgifter som kan bli föremål för fortlöpande lagring genom en generell och odifferentierad lagringsåtgärd och till att den information som dessa uppgifter kan innehålla är känslig, medför den omständigheten att leverantörer av elektroniska kommunikationstjänster lagrar dessa uppgifter dessutom i sig en risk för missbruk och olovlig åtkomst.

120 Möjligheten för medlemsstaterna att enligt artikel 15.1 i direktiv 2002/58 införa de undantag som avses i punkt 110 ovan avspeglar emellertid den omständigheten att de rättigheter som är stadfästa i artiklarna 7, 8 och 11 i stadgan inte är några absoluta rättigheter, utan måste bedömas utifrån deras funktion i samhället (se, för ett liknande resonemang, dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559, punkt 172 och där angiven rättspraxis).

121 Såsom framgår av artikel 52.1 i stadgan är det enligt stadgan tillåtet att begränsa utövandet av dessa rättigheter, under förutsättning att begränsningarna föreskrivs i lag, att de är förenliga med det väsentliga innehållet i dessa rättigheter och att de, med beaktande av proportionalitetsprincipen, är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter.

122 En tolkning av artikel 15.1 i direktiv 2002/58 mot bakgrund av stadgan kräver således även att det tas hänsyn till betydelsen av de rättigheter som är stadfästa i artiklarna 3, 4, 6 och 7 i stadgan och till den betydelse som målen att skydda nationell säkerhet och bekämpa grov brottslighet har för att bidra till skyddet för andra människors rättigheter och friheter.

123 I artikel 6 i stadgan, till vilken Conseil d'État (Högsta förvaltningsdomstolen) och Cour constitutionnelle (Författningsdomstolen) har hänvisat, anges att var och en har rätt till frihet, men också till personlig säkerhet. Nämnda artikel garanterar rättigheter som motsvarar dem som garanteras i artikel 5 i Europakonventionen (se, för ett liknande resonemang, dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 47, dom av den 28 juli 2016, JZ, C-294/16 PPU, EU:C:2016:610, punkt 48, och dom av den 19 september 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, punkt 42 och där angiven rättspraxis).

124 Det ska dessutom erinras om att artikel 52.3 i stadgan syftar till att trygga den nödvändiga koherensen mellan rättigheterna i stadgan och motsvarande rättigheter i Europakonventionen, utan att undergräva unionsrättens och Europeiska unionens domstols autonomi. Vid tolkningen av stadgan ska således hänsyn tas till motsvarande rättigheter i Europakonventionen såsom lägsta tillåtna skyddsnivå (se, för ett liknande resonemang, dom av den 12 februari 2019, TC, C-492/18 PPU, EU:C:2019:108, punkt 57, och dom av den 21 maj 2019, kommissionen/Ungern (Nyttjanderätter till jordbruksmark), C-235/17, EU:C:2019:432, punkt 72 och där angiven rättspraxis).

125 Vad avser artikel 5 i Europakonventionen, vilken fastslår ”rätten till frihet” och ”rätten till säkerhet”, syftar denna, enligt Europadomstolens rättspraxis, till att skydda individen mot godtyckliga eller oberättigade frihetsberövanden (se, för ett liknande resonemang, Europadomstolen, 18 mars 2008, Ladent mot Polen, CE:ECHR:2008:0318JUD001103603, 45 § och 46 §, Europadomstolen, 29 mars 2010, Medvedyev m.fl. mot Frankrike, CE:ECHR:2010:0329JUD000339403, 76 § och 77 §, och Europadomstolen, 13 december 2012, El-Masri mot ”The former Yugoslav Republic of Macedonia”, CE:ECHR:2012:1213JUD003963009, 239 §). Eftersom denna bestämmelse avser frihetsberövanden som företas av myndigheter, kan artikel 6 i stadgan emellertid inte tolkas så, att den ålägger statsmakten en skyldighet att vidta specifika åtgärder för att beivra vissa brott.

126 Vad däremot särskilt gäller den effektiva bekämpningen av brott som bland annat underåriga och andra utsatta personer utsätts för, vilken Cour constitutionnelle (Författningsdomstolen) har hänvisat till, ska det understrykas att det av artikel 7 i stadgan kan följa positiva skyldigheter för statsmakten att vidta rättsliga åtgärder som syftar till att skydda privatlivet och familjelivet (se, för ett liknande resonemang, dom av den 18 juni 2020, kommissionen/Ungern (Insyn i föreningar), C-78/18, EU:C:2020:476, punkt 123 och där angiven rättspraxis från Europadomstolen). Sådana skyldigheter kan även följa av nämnda artikel 7 vad gäller skyddet av bostaden och kommunikationer, och av artiklarna 3 och 4 vad gäller skyddet av personers fysiska och mentala integritet och förbudet mot tortyr och omänsklig och förnedrande behandling.

127 Mot bakgrund av dessa olika positiva skyldigheter är det nödvändigt att göra en avvägning mellan de olika intressen och rättigheter som är i fråga.

128 Europadomstolen har nämligen slagit fast att de positiva skyldigheter som följer av artiklarna 3 och 8 i Europakonventionen, för vilka motsvarande garantier återfinns i artiklarna 4 och 7 i stadgan, bland annat innebär att det ska antas materiella och processuella bestämmelser samt vidtas praktiska åtgärder som möjliggör en effektiv brottsbekämpning genom effektiv utredning och lagföring av personer. Denna skyldighet är särskilt viktig när ett barns fysiska och psykiska välbefinnande är hotat. De åtgärder som behöriga myndigheter vidtar måste emellertid till fullo respektera rättssäkerheten, övriga garantier som begränsar omfattningen av de befogenheter som myndigheterna har vid brottsutredningar samt andra fri- och rättigheter. Enligt Europadomstolen bör en rättslig ram inrättas som möjliggör en avvägning mellan de olika intressen och rättigheter som ska skyddas (Europadomstolen, 28 oktober 1998, Osman mot Förenade kungariket, CE:ECHR:1998:1028JUD002345294, 115 § och 116 §, Europadomstolen, 4 mars 2004, M.C. mot Bulgarien, CE:ECHR:2003:1204JUD003927298, 151 §, Europadomstolen, 24 juni 2004, Von Hannover mot Tyskland, CE:ECHR:2004:0624JUD005932000, 57 § och 58 §, och Europadomstolen, 2 december 2008, K.U. mot Finland, CE:ECHR:2008:1202JUD 000287202, 46 §, 48 § och 49 §).

129 Vad gäller iakttagandet av proportionalitetsprincipen föreskrivs i artikel 15.1 första meningen i direktiv 2002/58 att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed tillhörande trafikuppgifter, när en sådan åtgärd är ”nödvändig, lämplig och proportionerlig” ”i ett demokratiskt samhälle”, med hänsyn till de mål som anges i denna bestämmelse. I skäl 11 i direktivet anges att en åtgärd av detta slag ska vara i ”strikt” proportion till det avsedda ändamålet.

130 Det ska i detta avseende erinras om att skyddet för den grundläggande rätten till respekt för privatlivet enligt domstolens fasta praxis kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt. Uppnåendet ett mål av allmänt samhällsintresse kan dessutom inte ske utan att det beaktas att detta mål måste vara förenligt med de grundläggande rättigheter som berörs av åtgärden, varvid en balanserad avvägning ska göras mellan, å ena sidan, målet av allmänt samhällsintresse, och, å andra sidan, rättigheterna i fråga (se, för ett liknande resonemang, dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 56, dom av den 9 november 2010, Volker und Markus Schecke och Eifert, C-92/09 och C-93/09, EU:C:2010:662, punkterna 76, 77 och 86, och dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkt 52; yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 140).

131 Det framgår av domstolens praxis att medlemsstaternas möjlighet att motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58 ska bedömas med hänsyn till hur allvarligt det ingrepp är som en sådan begränsning medför. Det ska också kontrolleras att betydelsen av det mål av allmänt samhällsintresse som eftersträvas med denna begränsning står i proportion till hur allvarligt ingreppet är (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 55 och där angiven rättspraxis).

132 För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkterna 54 och 55, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 117; yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 141).

133 Lagstiftning som föreskriver lagring av personuppgifter måste således alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade målet (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 191 och där angiven rättspraxis, och dom av den 3 oktober 2019, A m.fl., C-70/18, EU:C:2019:823, punkt 63).

– Lagstiftningsåtgärder som föreskriver lagring i förebyggande syfte av trafik- och lokaliseringsuppgifter för att skydda nationell säkerhet

134 Det ska påpekas att målet att skydda nationell säkerhet, vilket har åberopats av de hänskjutande domstolarna och de regeringar som har inkommit med yttranden, ännu inte specifikt har prövats av EU-domstolen i dess domar om tolkning av direktiv 2002/58.

135 Det ska inledningsvis påpekas att det i artikel 4.2 FEU anges att nationell säkerhet också i fortsättningen ska vara varje medlemsstats eget ansvar. Detta ansvar motsvarar det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet.

136 Betydelsen av målet att skydda nationell säkerhet, tolkad mot bakgrund av artikel 4.2 FEU, är dock mer omfattande än betydelsen av de övriga mål som anges i artikel 15.1 i direktiv 2002/58, bland annat målen att bekämpa brottslighet i allmänhet, även grov brottslighet, och att skydda allmän säkerhet. Sådana hot som avses i föregående punkt skiljer sig nämligen, till sin art och på grund av sitt särskilda allvar, från risken i allmänhet för oroligheter eller störningar, även allvarliga sådana, av den allmänna säkerheten. Under förutsättning att övriga krav i artikel 52.1 i stadgan iakttas, kan målet att skydda nationell säkerhet således motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera.

137 I sådana situationer som de som beskrivs i punkterna 135 och 136 ovan utgör artikel 15.1 i direktiv 2002/58, tolkad mot bakgrund av artiklarna 7, 8, 11 och 52.1 i stadgan, således i princip inte hinder för en lagstiftning som ger behöriga myndigheter rätt att ålägga leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter för samtliga användare av elektroniska kommunikationer under en begränsad tid, såvida det föreligger tillräckligt konkreta omständigheter för att anse att den berörda medlemsstaten står inför ett sådant allvarligt hot mot nationell säkerhet som avses i punkterna 135 och 136 ovan, beträffande vilket det är visat att det är verkligt och aktuellt eller förutsebart. Även om en sådan lagstiftning utan åtskillnad avser samtliga användare av elektroniska kommunikationsmedel, utan att det vid ett första påseende förefaller

föreligga något samband, i den mening som avses i den rättspraxis som tas upp i punkt 133 ovan, mellan dessa användare och ett hot mot den nationella säkerheten i denna medlemsstat, finner domstolen att förekomsten av ett sådant hot är ägnat att styrka att ett sådant samband föreligger.

138 Åläggandet att i förebyggande syfte lagra uppgifter som avser samtliga användare av elektroniska kommunikationsmedel måste emellertid vara tidsmässigt begränsat till vad som är strängt nödvändigt. Även om det inte kan uteslutas att åläggandet för leverantörer av elektroniska kommunikationstjänster att lagra uppgifter kan komma att förlängas på grund av att hotet kvarstår, får varje åläggande inte överskrida en förutsebar tidsrymd. En sådan lagring av uppgifter måste dessutom vara föremål för begränsningar och åtföljas av strikta garantier för att på ett effektivt sätt skydda de berördas personuppgifter från riskerna för missbruk. Lagringen får således inte vara systematisk.

139 Med hänsyn till det allvarliga ingrepp i de grundläggande rättigheter i artiklarna 7 och 8 i stadgan som följer av en sådan generell och odifferentierad åtgärd för lagring av uppgifter, är det viktigt att säkerställa att användningen av en sådan åtgärd de facto är begränsad till situationer där det föreligger ett allvarligt hot mot nationell säkerhet, såsom de situationer som avses i punkterna 135 och 136 ovan. För detta ändamål är det av väsentlig betydelse att ett beslut genom vilket leverantörer av elektroniska kommunikationstjänster åläggs att genomföra en sådan lagring av uppgifter kan bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda.

– Lagstiftning som föreskriver lagring i förebyggande syfte av trafik- och lokaliseringsuppgifter för att bekämpa brottslighet och skydda allmän säkerhet

140 Vad gäller målet att förebygga, undersöka, avslöja och lagföra brott är det, i enlighet med proportionalitetsprincipen, endast bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som kan motivera allvarliga ingrepp i de grundläggande rättigheter som anges i artiklarna 7 och 8 i stadgan, såsom de ingrepp som följer av lagring av trafik- och lokaliseringsuppgifter. Därmed kan endast ingrepp i nämnda grundläggande rättigheter vilka inte är av allvarligt slag motiveras av målet att förebygga, undersöka, avslöja och lagföra brott i allmänhet (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 102, och dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkterna 56 och 57; yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 149).

141 Nationell lagstiftning om generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet går utöver vad som är strängt nödvändigt och kan inte anses vara motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 107)

142 Med hänsyn till att den information som kan framkomma genom trafik- och lokaliseringsuppgifter kan vara av känslig art, är det nämligen av grundläggande betydelse för rätten till respekt för privatlivet att dessa uppgifter är konfidentiella. Med beaktande av dels att en lagring av dessa uppgifter kan ha en avhållande inverkan på utövandet av de grundläggande rättigheter som anges i artiklarna 7 och 11 i stadgan, vilken avses i punkt 118 ovan, dels allvaret i det ingrepp som en sådan lagring innebär, måste, i ett demokratiskt samhälle, ett sådant intrång utgöra ett undantag och inte huvudregeln, i enlighet med vad som föreskrivs i det system som inrättats genom direktiv 2002/58, och uppgifterna får inte lagras systematiskt och fortlöpande. Denna slutsats gäller även med avseende på målen att bekämpa grov brottslighet och att förebygga allvarliga hot mot allmän säkerhet samt den betydelse som ska tillmätas dem.

143 Domstolen har dessutom understrukit att lagstiftning som föreskriver generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter omfattar praktiskt taget hela befolkningens elektroniska kommunikationer, utan att det görs några åtskillnader, inskränkningar eller undantag utifrån det eftersträvade målet. I strid med det krav som domstolen erinrat om i punkt 133 ovan, berör en sådan lagstiftning på ett heltäckande sätt samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan leda till lagföring. Den är således även tillämplig på personer beträffande vilka det inte finns något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med målet att bekämpa grov brottslighet och, i synnerhet, utan att det krävs något samband mellan de uppgifter som ska lagras och ett hot mot allmän säkerhet (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkterna 57 och 58, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 105).

144 Såsom domstolen redan har fastställt är sådan lagstiftning inte begränsad till lagring av uppgifter avseende en viss tidsperiod och/eller ett visst geografiskt område och/eller en viss krets av personer som på något sätt kan vara inblandade i ett grovt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av grova brott (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights, C-293/12 och C-594/12, EU:C:2014:238, punkt 59, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 106).

145 Inte ens de positiva skyldigheter för medlemsstaterna som, beroende på omständigheterna i det enskilda fallet, kan följa av artiklarna 3, 4 och 7 i stadgan och som, såsom påpekats i punkterna 126 och 128 ovan, avser införande av bestämmelser som möjliggör en effektiv bekämpning av brott, kan medföra att så allvarliga ingrepp i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan som en lagstiftning om lagring av praktiskt taget hela befolkningens trafik- och lokaliseringsuppgifter innebär är motiverade, utan att det finns ett, åtminstone indirekt, samband mellan de berörda personerna och det eftersträvade målet.

146 Däremot kan, i enlighet med vad som anges i punkterna 142–144 ovan och med beaktande av den avvägning som ska göras mellan de olika intressen och rättigheter som är i fråga, målen att bekämpa grov brottslighet, att förebygga handlingar som utgör allvarligt men mot allmän säkerhet och, i ännu högre grad, att skydda nationell säkerhet motivera – med hänsyn till deras betydelse mot bakgrund av de positiva skyldigheter som det erinras om i föregående punkt och som bland annat Cour constitutionnelle (Författningsdomstolen) har hänvisat till – det synnerligen allvarliga ingrepp som en riktad lagring av trafik- och lokaliseringsuppgifter innebär.

147 Såsom domstolen redan har slagit fast utgör artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, inte hinder för att en medlemsstat antar lagstiftning som tillåter riktad lagring av trafik- och lokaliseringsuppgifter i förebyggande syfte, när detta sker för att bekämpa grov brottslighet och förebygga allvarliga hot mot allmän säkerhet, liksom för att skydda nationell säkerhet, förutsatt att lagringen av uppgifterna, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 108).

148 Vad gäller den avgränsning som måste göras med avseende på en sådan åtgärd för lagring av uppgifter, kan den bland annat grunda sig på den kategori av personer som berörs, eftersom artikel 15.1 i direktiv 2002/58 inte utgör hinder för lagstiftning som grundar sig på objektiva faktorer som gör det möjligt att ta sikte på personer vilkas uppgifter kan uppdaga en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för allmän säkerhet eller en risk för nationell säkerhet (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 111).

149 Det ska i detta avseende preciseras att de personer som är föremål för lagring av uppgifter bland annat kan vara personer som, inom ramen för tillämpliga nationella förfaranden och på grundval av objektiva kriterier, tidigare har befunnits utgöra ett hot mot allmän säkerhet eller nationell säkerhet i den berörda medlemsstaten.

150 Avgränsningen av en åtgärd som föreskriver lagring av trafik- och lokaliseringsuppgifter kan även grunda sig på ett geografiskt kriterium när behöriga nationella myndigheter på grundval av objektiva och icke-diskriminerande faktorer bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av grov brottslighet (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 111). Dessa områden kan bland annat utgöras av platser som utmärks av att det där begås ett stort antal grova brott, platser vilka är särskilt utsatta med avseende på grov brottslighet, såsom platser och infrastruktur som regelbundet besöks eller nyttjas av ett stort antal personer, eller strategiskt viktiga platser, såsom flygplatser, järnvägsstationer eller motorvägsbetalstationer.

151 För att säkerställa att det ingrepp som de riktade åtgärderna för lagring som beskrivs ovan i punkterna 147–150 innebär är förenligt med proportionalitetsprincipen, får åtgärderna inte pågå längre än vad som är strängt nödvändigt med hänsyn till det eftersträvade målet och de omständigheter som motiverar dem, utan att detta påverkar möjligheten att förnya åtgärderna om nämnda lagring fortsätter att vara nödvändig.

– Lagstiftning som föreskriver lagring i förebyggande syfte av IP-adresser och uppgifter om fysisk identitet för att bekämpa brottslighet och skydda allmän säkerhet

152 Det ska noteras att IP-adresser, trots att de ingår bland trafikuppgifterna, genereras utan anknytning till en viss kommunikation och huvudsakligen har till syfte att, via leverantörer av elektroniska kommunikationstjänster, identifiera den fysiska person som äger den terminalutrustning från vilken en kommunikation sker via internet. När det gäller e-post och bredbandstelefoni avslöjar dessa adresser, i den mån som endast IP-adresserna till kommunikationskällan lagras och inte mottagarens IP-adresser, inte i sig någon information om de tredje män som har haft kontakt med den person från vilken kommunikationen utgick. Denna kategori av uppgifter har således en lägre grad av känslighet än andra trafikuppgifter.

153 Eftersom IP-adresser kan användas för att bland annat på ett uttömmande sätt kartlägga en internetanvändares hela klickström, och därmed dennes online-aktivitet, är det emellertid möjligt att med användning av dessa adresser utförligt kartlägga internetanvändaren. Den lagring och analys av dessa IP-adresser som krävs för en sådan kartläggning utgör således allvarliga ingrepp i internetanvändarens grundläggande rättigheter enligt artiklarna 7 och 8 i stadgan, vilka kan ha sådana avhållande effekter som dem som avses i punkt 118 ovan.

154 Vid den avvägning som ska göras mellan de intressen och rättigheter som är i fråga, vilken krävs enligt den rättspraxis som anges i punkt 130 ovan, ska det beaktas att IP-adressen, när det är fråga om brott som begåtts på internet, kan utgöra den enda utredningsmetod som gör det möjligt att identifiera den person, till vilken denna adress var tilldelad vid den tidpunkt då brottet begicks. Därtill kommer att lagring av IP-adresser av leverantörer av elektroniska kommunikationstjänster vilken fortgår efter det att tilldelningen av dessa uppgifter har upphört i princip inte kan anses vara nödvändig för att fakturera för tjänsterna i fråga, vilket innebär att det, av denna anledning, såsom flera regeringar har anfört i sina yttranden till domstolen, kan bli omöjligt att upptäcka brott som har begåtts på internet utan att använda sig av lagstiftning enligt artikel 15.1 i direktiv 2002/58. Såsom nämnda regeringar har gjort gällande kan detta bland annat vara fallet med synnerligen grova brott avseende barnpornografi, såsom förvärv, spridning, överföring eller uppladdning på internet av barnpornografi, i den mening som avses i artikel 2 c i Europaparlamentets och rådets direktiv 2011/93/EU av den

13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 2011, s. 1 och rättelse i EUT L 335, 2011, s. 1).

155 Det är visserligen riktigt att en lagstiftning som föreskriver att IP-adresser ska lagras för samtliga fysiska personer som äger en terminalutrustning från vilken det går att få åtkomst till internet skulle omfatta personer som vid första anblicken inte har något samband, i den mening som avses i den rättspraxis som anges i punkt 133 ovan, med de eftersträvade målen och att internetanvändare, i enlighet med vad som konstateras i punkt 109 ovan, har rätt att förvänta sig, på grundval av artiklarna 7 och 8 i stadgan, att deras identitet i princip inte kommer att avslöjas, men under dessa omständigheter strider en lagstiftning som föreskriver generell och odifferentierad lagring av enbart de IP-adresser som har tilldelats källan till en internetanslutning i princip inte mot artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, under förutsättning att denna möjlighet används med beaktande av de stränga materiella och formella villkor som måste styra användningen av dessa uppgifter.

156 Med hänsyn till det allvarliga ingrepp i de grundläggande rättigheter i artiklarna 7 och 8 i stadgan som denna lagring innebär, är det endast bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som, i likhet med skyddet av nationell säkerhet, kan motivera detta ingrepp. Lagringstiden får inte heller överstiga den tid som är strängt nödvändig med hänsyn till det eftersträvade målet. Slutligen måste en åtgärd av detta slag föreskriva stränga villkor och garantier vad gäller utnyttjandet av dessa uppgifter, bland annat genom kartläggning av de berörda personernas kommunikation och aktivitet på internet.

157 Vad slutligen gäller uppgifter om användarna av elektroniska kommunikationsmedels fysiska identitet, är det inte möjligt att enbart på grundval av dessa uppgifter få kännedom om datum, tidpunkt och varaktighet för samt mottagarna av de kommunikationer som har ägt rum. Det är inte heller möjligt att få kännedom om platserna där kommunikationen har ägt rum eller hur ofta den har ägt rum med vissa personer under en viss tidsperiod, vilket innebär att dessa uppgifter, med undantag för personernas kontaktuppgifter, såsom deras adresser, inte ger någon information om de specifika kommunikationerna, och därmed om deltagarnas privatliv. Det ingrepp som en lagring av dessa uppgifter innebär kan därför i princip inte anses vara allvarligt (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkterna 59 och 60).

158 Av detta följer, i enlighet med vad som anges i punkt 140 ovan, att lagstiftning som avser behandling av dessa uppgifter som sådana, bland annat lagring av och åtkomst till uppgifterna enbart i syfte att identifiera den berörda användaren, och utan att uppgifterna kan kopplas till information om de kommunikationer som har ägt rum, kan motiveras av målet att förebygga, undersöka, avslöja och åtala för brott i allmänhet, vilket det hänvisas till i artikel 15.1 första meningen i direktiv 2002/58 (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 62).

159 Under dessa omständigheter och med hänsyn till den avvägning som ska göras mellan de intressen och rättigheter som är i fråga och av de skäl som anges i punkterna 131 och 158 ovan, utgör artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, trots att det inte finns något samband mellan samtliga användare av elektroniska kommunikationsmedel och de mål som eftersträvas, inte hinder för lagstiftning som innebär att leverantörer av elektroniska kommunikationstjänster, utan någon specifik tidsbegränsning, åläggs att lagra uppgifter om den fysiska identiteten för samtliga användare av elektroniska kommunikationsmedel, i syfte att förebygga, undersöka, avslöja och åtala för brott i allmänhet samt att skydda allmän säkerhet, utan att det är nödvändigt att brotten eller hoten mot eller handlingarna till men för allmän säkerhet är allvarliga.

– Lagstiftning som föreskriver ett skyndsamt säkrande av trafik- och lokaliseringsuppgifter för att bekämpa grov brottslighet

160 Vad gäller trafik- och lokaliseringsuppgifter som behandlas och lagras av leverantörer av elektroniska kommunikationstjänster med stöd av artiklarna 5, 6 och 9 i direktiv 2002/58, eller med stöd av lagstiftning enligt artikel 15.1 i direktivet, såsom den lagstiftning beskrivs i punkterna 134–159 ovan, ska dessa uppgifter i princip antingen utplånas eller avidentifieras vid utgången av de lagstadgade tidsperioder inom vilka, i enlighet med de nationella bestämmelser som införlivar direktivet, behandling och lagring får ske.

161 Under behandlingen och lagringen av uppgifterna kan det emellertid uppkomma situationer där det krävs att uppgifterna fortsätter att lagras efter utgången av dessa tidsperioder för att klarlägga grova brott eller hot mot nationell säkerhet. Så kan vara fallet både i situationer där ovannämnda brott eller handlingar redan har kunnat konstateras och i situationer där förekomsten av dem, efter en objektiv bedömning av samtliga relevanta omständigheter, rimligen kan misstänkas.

162 Det ska i detta avseende noteras att artikel 14 i Europarådets konvention om it-relaterad brottslighet av den 23 november 2001 (European Treaty Series nr 185), som undertecknats av de 27 medlemsstaterna samt ratificerats av 25 av dem och vars syfte är att underlätta kampen mot brott som begåtts med hjälp av datorsystem, föreskrivs att varje part, för utrednings- och lagföringsändamål, ska vidta vissa åtgärder beträffande redan sparade trafikuppgifter, såsom skyndsamt säkrande av dessa uppgifter. I artikel 16.1 i denna konvention föreskrivs särskilt att varje part ska vidta nödvändiga lagstiftningsåtgärder för att dess behöriga myndigheter genom förelägganden eller på liknande sätt ska kunna åstadkomma skyndsamt säkrande av trafikuppgifter, som har lagrats med hjälp av ett datorsystem, särskilt i de fall där det finns anledning att förmoda att dessa uppgifter löper särskild risk att gå förlorade eller förändras.

163 I sådana situationer som dem som avses i punkt 161 ovan står det medlemsstaterna fritt att, mot bakgrund av den avvägning som ska göras mellan de rättigheter och intressen som är i fråga och som avses i punkt 130 ovan, i lagstiftning som antagits med stöd av artikel 15.1 i direktiv 2002/58 föreskriva en möjlighet, genom ett beslut av den behöriga myndigheten vilket kan vara föremål för en effektiv domstolsprövning, att ålägga leverantörer av elektroniska kommunikationstjänster att under en bestämd tidsperiod skyndsamt säkra de trafik- och lokaliseringsuppgifter som de har tillgång till.

164 Eftersom ändamålet med ett sådant skyndsamt säkrande inte längre motsvarar de ändamål för vilka uppgifterna inledningsvis samlades in och lagrades, och varje behandling av uppgifter enligt artikel 8.2 i stadgan ska ske för bestämda ändamål, måste medlemsstaterna i sin lagstiftning precisera det ändamål för vilket det får företas ett skyndsamt säkrande av uppgifter. Med hänsyn till det allvarliga ingrepp i de grundläggande rättigheterna i artiklarna 7 och 8 i stadgan som ett sådant säkrande kan medföra, är det endast bekämpning av grov brottslighet och, i ännu högre grad, skyddet av nationell säkerhet som kan motivera detta ingrepp. För att säkerställa att det ingrepp som en sådan åtgärd innebär begränsas till vad som är strängt nödvändigt, ska skyldigheten att säkra uppgifter endast avse trafik- och lokaliseringsuppgifter som kan bidra till att klarlägga det aktuella grova brottet eller den aktuella handlingen till men för nationell säkerhet. Vidare ska lagringstiden för uppgifterna begränsas till vad som är strängt nödvändigt. Lagringstiden får emellertid förlängas när omständigheterna och det mål som eftersträvas med åtgärden motiverar det.

165 Det ska härvidlag preciseras att ett sådant skyndsamt säkrande inte behöver vara begränsat till uppgifter avseende de personer som konkret misstänks ha begått ett brott eller ha vidtagit handlingar till men för nationell säkerhet. I enlighet med lagstiftarens val och förutsatt att gränserna för vad som är strängt nödvändigt inte överskrids, får en sådan åtgärd – med iakttagande av den ram som fastställs i artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan samt med beaktande av övervägandena i punkt 133 ovan – utsträckas till att omfatta trafik- och lokaliseringsuppgifter för andra personer än dem som misstänks ha planerat eller begått ett grovt brott alternativt misstänks ha

planerat att vidta eller ha vidtagit handlingar till men för nationell säkerhet, under förutsättning att dessa uppgifter, på grundval av objektiva och icke-diskriminerande faktorer, kan bidra till att klarlägga ett sådant brott eller en sådan handling. Det kan härvidlag röra sig om uppgifter om offret, offrets sociala bekantskapskrets eller yrkeskontakter, eller om vissa geografiska områden, såsom de platser på vilka brottet eller handlingen till men för nationell säkerhet har ägt rum eller förberetts. Behöriga myndigheters tillgång till de sålunda säkrade uppgifterna ska dessutom ske med beaktande av de villkor som följer av den rättspraxis som avser tolkningen av direktiv 2002/58 (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 118–121 och där angiven rättspraxis).

166 Det ska vidare tilläggas att åtkomst till trafik- och lokaliseringsuppgifter som lagrats av leverantörer med stöd av en åtgärd som vidtagits i enlighet med artikel 15.1 i direktiv 2002/58, såsom framgår särskilt av punkterna 115 och 133 ovan, i princip endast kan motiveras av det mål av allmänt samhällsintresse som ligger till grund för leverantörernas skyldighet att lagra uppgifterna. Av detta följer i synnerhet att åtkomst till sådana uppgifter i syfte att lagföra och beivra ordinära brott inte i något fall kan medges när lagringen av dem har motiverats med målet att bekämpa grov brottslighet eller, i ännu högre grad, målet att skydda nationell säkerhet. I enlighet med proportionalitetsprincipen, såsom angetts i punkt 131 ovan, kan däremot åtkomst till uppgifter som lagrats i syfte att bekämpa grov brottslighet vara motiverad av målet att skydda nationell säkerhet, under förutsättning att de materiella och formella villkor för sådan åtkomst som avses i föregående punkt iakttas.

167 Det står i detta avseende medlemsstaterna fritt att i sin lagstiftning föreskriva att åtkomst till trafik-och lokaliseringsuppgifter får, med beaktande av dessa materiella och formella villkor, ske i syfte att bekämpa grov brottslighet eller skydda nationell säkerhet när uppgifterna lagras av en leverantör på ett sätt som är förenligt med artiklarna 5, 6 och 9 eller artikel 15.1 i direktiv 2002/58.

168 Mot bakgrund av det ovan anförda ska fråga 1 i mål C-511/18 respektive mål C-512/18 samt frågorna 1 och 2 i mål C-520/18 besvaras enligt följande. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att den utgör hinder för lagstiftning vilken, för de ändamål som anges i nämnda artikel 15.1, föreskriver generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter i förebyggande syfte. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 11 och artikel 52.1 i stadgan, utgör däremot inte hinder för lagstiftning

– som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart, varvid beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda, och varvid åläggandet endast får meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår,

– som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en riktad lagring av trafik- och lokaliseringsuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,

– som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en generell och odifferentierad lagring av IP-adresser som har tilldelats källan för en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,

– som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om den fysiska identiteten för användare av elektroniska kommunikationsmedel, och

– som, för att bekämpa grov brottslighet eller, i ännu högre grad, skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket är föremål för effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra de trafik- och lokaliseringsuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk.

Frågorna 2 och 3 i mål C-511/18

169 Den hänskjutande domstolen har ställt frågorna 2 och 3 i mål C-511/18 för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan ska tolkas så, att den utgör hinder för en nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster är skyldiga att på sina nät vidta åtgärder som möjliggör dels automatiserad analys och insamling i realtid av trafik- och lokaliseringsuppgifter, dels insamling i realtid av tekniska uppgifter om lokaliseringen av de terminalutrustningar som används, utan att det föreskrivs att de personer som berörs av denna behandling respektive insamling ska underrättas om detta.

170 Den hänskjutande domstolen har preciserat att de tekniker för insamling av underrättelseuppgifter som föreskrivs i artiklarna L. 851-2 till L. 851-4 CSI inte ålägger leverantörer av elektroniska kommunikationstjänster något specifikt krav att lagra trafik- och lokaliseringsuppgifter. Vad särskilt gäller den automatiserade analys som avses i artikel L. 851-3 CSI, har den hänskjutande domstolen påpekat att denna behandling syftar till att, enligt kriterier som är fastställda för detta ändamål, uppdaga uppkopplingar som kan avslöja terrorhot. När det gäller den insamling i realtid som avses i artikel L. 851-2 CSI har den hänskjutande domstolen konstaterat att den endast avser en eller flera personer som på förhand har identifierats som personer som kan ha koppling till ett terrorhot. Enligt samma domstol kan dessa båda tekniker endast användas i syfte att förebygga terrorism och de avser de uppgifter som anges i artiklarna L. 851-1 och R. 851-5 CSI.

171 Det ska inledningsvis preciseras att den omständigheten att den automatiserade analys som föreskrivs i artikel L. 851-3 CSI inte i sig gör det möjligt att identifiera de användare vilkas uppgifter analyseras inte utgör hinder för att sådana uppgifter kvalificeras som ”personuppgifter”. Eftersom det förfarande som föreskrivs i punkt IV i samma bestämmelse i ett senare skede gör det möjligt att identifiera den eller de personer som berörs av de uppgifter, som genom en automatiserad analys har visat att det föreligger ett terrorhot, kan samtliga personer vars uppgifter är föremål för automatiserad analys fortfarande identifieras utifrån dessa uppgifter. Enligt definitionen av personuppgifter i artikel 4.1 i förordning 2016/679 utgör upplysningar som bland annat avser en identifierbar person personuppgifter.

Den automatiserade analysen av trafik- och lokaliseringsuppgifter

172 Det framgår av artikel L. 851-3 CSI att den automatiserade analys som föreskrivs i den bestämmelsen i princip innebär en filtrering av samtliga trafik- och lokaliseringsuppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster, vilken utförs av nämnda leverantörer på begäran av behöriga nationella myndigheter och med tillämpning av de parametrar som dessa myndigheter har fastställt. Härav följer att samtliga uppgifter om användare av elektroniska kommunikationsmedel kontrolleras om de motsvarar dessa parametrar. En sådan automatiserad analys ska således anses innebära att de

berörda leverantörerna av elektroniska kommunikationstjänster, för den behöriga myndighetens räkning, gör en generell och odifferentierad behandling i form av en automatiserad åtgärd i den mening som avses i artikel 4.2 i förordning 2016/679, som omfattar samtliga trafik- och lokaliseringsuppgifter för samtliga användare av elektroniska kommunikationsmedel. Denna behandling är fristående från den efterföljande, med stöd av artikel L. 851-3 IV CSI tillåtna, insamlingen av uppgifter om personer som identifierats efter den automatiserade analysen.

173 En nationell lagstiftning som tillåter en sådan automatiserad analys av trafik- och lokaliseringsuppgifter utgör emellertid ett undantag från den principiella skyldigheten enligt artikel 5 i direktiv 2002/58 att säkerställa konfidentialitet vid elektronisk kommunikation och för därmed förbundna uppgifter. En sådan lagstiftning utgör även ett ingrepp i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan, oavsett hur dessa uppgifter senare används. Slutligen kan nämnda lagstiftning, i enlighet med den rättspraxis som det hänvisas till i punkt 118 ovan, ha en avhållande inverkan på utövandet av den yttrandefrihet som är stadfäst i artikel 11 i stadgan.

174 Dessutom är det ingrepp som följer av en automatiserad analys av trafik- och lokaliseringsuppgifter, såsom det som är aktuellt i det nationella målet, synnerligen allvarligt eftersom det på ett generellt och odifferentierat sätt omfattar uppgifter om personer som använder elektroniska kommunikationsmedel. Detta gäller i än högre grad när, såsom framgår av den nationella lagstiftning som är aktuell i det nationella målet, de uppgifter som är föremål för automatiserad analys kan uppdaga vilken typ av information som sökts på internet. En sådan automatiserad analys tillämpas på ett heltäckande sätt på samtliga personer som använder elektroniska kommunikationsmedel och följaktligen även på personer beträffande vilka det inte finns något indicium som ger anledning att tro att deras beteende skulle kunna ha ett samband, inte ens indirekt eller avlägset, med terrorverksamhet.

175 När det gäller motiveringen av ett sådant ingrepp innebär det krav, som uppställs i artikel 52.1 i stadgan, på att samtliga begränsningar i utövandet av grundläggande rättigheter ska vara föreskrivna i lag, att räckvidden av begränsningen i utövandet av den aktuella rättigheten ska vara definierad i själva den rättsliga grund som tillåter ingreppet (se, för ett liknande resonemang, dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559, punkt 175 och där angiven rättspraxis).

176 För att uppfylla det krav på proportionalitet som det erinrats om i punkterna 130 och 131 ovan, enligt vilket undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt, måste en nationell lagstiftning som reglerar behöriga myndigheters åtkomst till lagrade trafik- och lokaliseringsuppgifter uppfylla de krav som följer av den rättspraxis som anges i punkt 132 ovan. En sådan lagstiftning kan i synnerhet inte vara begränsad till att kräva att myndigheternas åtkomst till uppgifterna svarar mot det ändamål som eftersträvas med lagstiftningen, utan den måste även fastställa de materiella och formella villkor som gäller för sådan användning (se, analogt, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 192 och där angiven rättspraxis).

177 Domstolen erinrar i detta avseende om att det synnerligen allvarliga ingrepp som en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter innebär, vilket avses i övervägandena i punkterna 134–139 ovan, samt det synnerligen allvarliga ingrepp som en automatiserad analys av dessa uppgifter innebär, endast kan uppfylla kravet på proportionalitet i situationer där en medlemsstat står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart och under förutsättning att den tid under vilken uppgifterna lagras är begränsad till vad som är strängt nödvändigt.

178 I sådana situationer som de som avses i föregående punkt kan genomförandet av automatiserad analys av trafik- och lokaliseringsuppgifter för samtliga användare av elektroniska kommunikationsmedel, under en strikt begränsad tidsperiod, anses vara motiverat med hänsyn till de krav som följer av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan.

179 För att säkerställa att användningen av en sådan åtgärd verkligen begränsas till vad som är strängt nödvändigt för att skydda nationell säkerhet, och i synnerhet för att förebygga terrorism, är det, i enlighet med vad som konstaterats i punkt 139 ovan, av väsentlig betydelse att det beslut genom vilket tillstånd lämnas för den automatiserade analysen kan bli föremål för en effektiv kontroll – antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda.

180 Det ska i detta hänseende preciseras att de förhandsbestämda modeller och kriterier som ligger till grund för denna typ av behandling av uppgifter ska vara dels specifika och tillförlitliga, för att göra det möjligt att erhålla resultat som identifierar individer mot vilka det kan finnas en skälig misstanke om delaktighet i terroristbrott, dels icke-diskriminerande (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 172).

181 Det ska dessutom erinras om att en automatiserad analys som görs utifrån modeller och kriterier som grundar sig på premissen att ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, fackföreningstillhörighet eller en persons hälsotillstånd eller sexualliv, i sig själv och oberoende av personens individuella uppträdande, skulle vara relevant för att förebygga terrorism, kränker de rättigheter som garanteras i artiklarna 7 och 8 i stadgan, jämförda med artikel 21 i stadgan. Förhandsbestämda modeller och kriterier som används vid automatiserad analys i syfte att förhindra terrorverksamhet som utgör ett allvarligt hot mot nationell säkerhet kan därför inte enbart vara baserade på sådana känsliga uppgifter (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 165).

182 Det finns en viss felmarginal vid automatiserade analyser av trafik- och lokaliseringsuppgifter och varje positivt resultat som erhållits efter en automatiserad behandling måste därför vara föremål för en icke-automatiserad, individuell omprövning innan det vidtas någon individuell åtgärd som har negativa verkningar för de berörda personerna, såsom en efterföljande insamling av trafik- och lokaliseringsuppgifter i realtid. En sådan åtgärd får nämligen inte på ett avgörande sätt grunda sig enbart på resultatet av en automatiserad behandling. På motsvarande sätt ska det för att säkerställa att de förhandsbestämda modellerna och kriterierna, den användning som görs av dem och de databaser som används i praktiken inte är diskriminerande och att de – med hänsyn till målet att förhindra terrorverksamhet som utgör ett allvarligt hot mot nationell säkerhet – är begränsade till vad som är strängt nödvändigt, göras regelbundna omprövningar av de förhandsbestämda modellernas och kriteriernas tillförlitlighet och aktualitet samt de databaser som används (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkterna 173 och 174).

Insamling i realtid av trafik- och lokaliseringsuppgifter

183 När det gäller den insamling i realtid av trafik- och lokaliseringsuppgifter som anges i artikel L. 851-2 CSI får den tillåtas i individuella fall avseende ”en på förhand identifierad person som kan ha en anknytning till ett [terror]hot”. På samma sätt föreskrivs i denna bestämmelse att ”om det finns vägande skäl att anta att en eller flera personer kring den person som berörs av tillståndet kan lämna uppgifter med hänsyn till det ändamål som ligger till grund för tillståndet, får tillstånd även beviljas individuellt för var och en av dessa personer”.

184 De uppgifter som omfattas av en sådan åtgärd gör det möjligt för behöriga nationell myndigheter att under den period som tillståndet avser fortlöpande och i realtid övervaka de samtalspartner med vilka de berörda personerna kommunicerar, vilka kommunikationsmedel de använder, hur länge deras kommunikation pågår samt var de vistas och hur de förflyttar sig. På samma sätt förefaller dessa uppgifter kunna avslöja vilken typ av information som sökts på internet. Sammantagna gör dessa

uppgifter det möjligt, såsom framgår av punkt 117 ovan, att dra mycket precisa slutsatser om de berörda personernas privatliv och ger underlag för att kartlägga dem. Sådan information är, med avseende på rätten till respekt för privatlivet, lika känslig som själva innehållet i kommunikationerna.

185 När det gäller den insamling i realtid av uppgifter som avses i artikel L. 851-4 CSI, är det enligt denna bestämmelse tillåtet att samla in tekniska uppgifter om lokaliseringen av terminalutrustning och att i realtid överföra dessa till behörig myndighet under premiärministern. Det framgår att sådana uppgifter gör det möjligt för den behöriga myndigheten att när som helst under den period som tillståndet avser fortlöpande och i realtid lokalisera den terminalutrustning som används, såsom mobiltelefoner.

186 En nationell lagstiftning som tillåter sådan insamling av uppgifter i realtid utgör således, i likhet med nationell lagstiftning som tillåter automatiserad analys av uppgifter, ett undantag från den principiella skyldigheten enligt artikel 5 i direktiv 2002/58 att säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna uppgifter. Den utgör således även ett ingrepp i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan och kan ha en avhållande inverkan på utövandet av den yttrandefrihet som garanteras i artikel 11 i stadgan.

187 Det ska understrykas att det ingrepp som en insamling i realtid av uppgifter som gör det möjligt att lokalisera en terminalutrustning innebär är synnerligen allvarligt, eftersom dessa uppgifter gör det möjligt för behöriga nationella myndigheter att exakt och varaktigt bevaka mobiltelefonanvändarnas förflyttningar. Eftersom dessa uppgifter således ska anses vara särskilt känsliga, måste behöriga myndigheters åtkomst i realtid till sådana uppgifter särskiljas från åtkomst som inte sker i realtid. Den första typen av åtkomst är mer ingripande då den möjliggör en nästintill fullständig övervakning av mobiltelefonanvändarna (se, analogt, angående artikel 8 i Europakonventionen, Europadomstolen, 8 februari 2018, Ben Faiza mot Frankrike, CE:ECHR:2018:0208JUD003144612, § 74). Ingreppet blir dessutom än mer långtgående när insamlingen i realtid även omfattar berörda personers trafikuppgifter.

188 Även om det mål att förebygga terrorism som eftersträvas med den aktuella nationella lagstiftningen, med hänsyn till dess betydelse, kan motivera det ingrepp som en insamling i realtid av trafik- och lokaliseringsuppgifter innebär, får en sådan åtgärd, med hänsyn till dess synnerligen ingripande karaktär, endast vidtas gentemot personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i terrorverksamhet. När det gäller uppgifter avseende personer som inte ingår i denna kategori, får dessa uppgifter endast vara föremål för en åtkomst som inte sker i realtid, vilken i enlighet med domstolens praxis endast får ske i särskilda fall, såsom då det är fråga om terrorverksamhet, och när det föreligger objektiva omständigheter som gör det möjligt att anse att dessa uppgifter i ett konkret fall faktiskt skulle kunna bidra till bekämpningen av terrorism (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 119 och där angiven rättspraxis).

189 Ett beslut att tillåta insamling i realtid av trafik- och lokaliseringsuppgifter måste dessutom vara grundat på objektiva kriterier som föreskrivs i den nationella lagstiftningen. I denna lagstiftning ska det särskilt, i enlighet med den rättspraxis som det hänvisas till i punkt 176 ovan, anges under vilka omständigheter och på vilka villkor en sådan insamling får tillåtas samt, såsom angetts i föregående punkt, föreskrivas att endast personer som har ett samband med målet att förebygga terrorism får vara föremål för sådan insamling. Ett beslut att tillåta insamling i realtid av trafik- och lokaliseringsuppgifter måste dessutom vara grundat på objektiva och icke-diskriminerande kriterier som föreskrivs i den nationella lagstiftningen. För att säkerställa att dessa villkor uppfylls i praktiken är det väsentligt att genomförandet av den åtgärd varigenom insamlingen i realtid tillåts är underkastad en förhandskontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan. Domstolen eller myndigheten ska bland annat försäkra sig om att en sådan insamling i realtid endast är tillåten inom ramen för vad som är strängt nödvändigt (se, för ett

liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 120). I vederbörligen motiverade fall som ställer krav på skyndsamhet ska kontrollen ske utan dröjsmål.

Underrättelse av de personer vilkas uppgifter har samlats in eller analyserats

190 De behöriga nationella myndigheter som samlar in trafik- och lokaliseringsuppgifter i realtid ska, inom ramen för tillämpliga nationella förfaranden, underrätta de berörda personerna om detta, i den omfattning som, och så snart som, en sådan underrättelse inte längre riskerar att äventyra de uppdrag som tilldelats dessa myndigheter. Denna underrättelse är nämligen nödvändig för att dessa personer ska kunna utöva sina rättigheter enligt artiklarna 7 och 8 i stadgan att begära tillgång till de av deras personuppgifter som är föremål för dessa åtgärder och, i förekommande fall, få dem rättade eller raderade, samt att i enlighet med artikel 47 första stycket i stadgan utöva sin rätt till ett effektivt rättsmedel inför en domstol. En sådan rättighet garanteras för övrigt uttryckligen i artikel 15.2 i direktiv 2002/58, jämförd med artikel 79.1 i förordning 2016/679 (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 121 och där angiven rättspraxis, och yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkterna 219 och 220).

191 Vad gäller den underrättelse som krävs vid automatiserad analys av trafik- och lokaliseringsuppgifter är den behöriga nationella myndigheten skyldig att offentliggöra generella upplysningar om analysen, men behöver inte underrätta de berörda personerna individuellt. Om uppgifterna däremot motsvarar de parametrar som angetts i den åtgärd varigenom den automatiserade analysen tillåts och myndigheten identifierar den berörda personen i syfte att mer ingående analysera de uppgifter som rör vederbörande, måste personen i fråga underrättas individuellt. Denna underrättelse ska emellertid endast lämnas i den omfattning som och från och med den tidpunkt då den inte längre riskerar att äventyra de uppdrag som tilldelats myndigheten (se, analogt, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkterna 222–224).

192 Mot denna bakgrund ska frågorna 2 och 3 i mål C-511/18 besvaras enligt följande. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att den inte utgör hinder för en nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs dels att använda automatiserad analys av bland annat trafik- och lokaliseringsuppgifter och samla in sådana uppgifter i realtid, dels att i realtid samla in tekniska uppgifter om lokaliseringen av de terminalutrustningar som används, när

– användningen av automatiserad analys är begränsad till situationer där en medlemsstat står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart och användningen av sådan analys kan bli föremål för en effektiv kontroll – antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan – i syfte att kontrollera att det föreligger en situation som motiverar åtgärden och att de villkor och garantier som måste ställas upp är uppfyllda, och när

– användningen av insamling i realtid av trafik- och lokaliseringsuppgifter är begränsad till personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i terrorverksamhet och är underkastad en förhandskontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att säkerställa att en sådan insamling i realtid endast är tillåten inom ramen för vad som är strängt nödvändigt. I vederbörligen motiverade fall som ställer krav på skyndsamhet ska kontrollen ske utan dröjsmål.

Fråga 2 i mål C-512/18

193 Den hänskjutande domstolen har ställt fråga 2 i mål C-512/18 för att få klarhet i huruvida bestämmelserna i direktiv 2000/31, jämförda med artiklarna 6–8, 11 och artikel 52.1 i stadgan, ska tolkas så, att de utgör hinder för en nationell lagstiftning enligt vilken leverantörer som tillhandahåller allmänheten tillgång till internetkommunikationstjänster och värdtjänstleverantörer är skyldiga att generellt och odifferentierat bland annat lagra personuppgifter förbundna med dessa tjänster.

194 Även om den hänskjutande domstolen anser att sådana tjänster omfattas av tillämpningsområdet för direktiv 2000/31, och inte av tillämpningsområdet för direktiv 2002/58, anser den att artikel 15.1 och 15.2 i direktiv 2000/31, jämförd med artiklarna 12 och 14 i samma direktiv, inte i sig inför ett principiellt förbud mot lagring av uppgifter om skapande av innehåll från vilket det endast i undantagsfall får göras avsteg. Den hänskjutande domstolen undrar emellertid om denna bedömning ska vidhållas, med beaktande av att de grundläggande rättigheterna som stadfästs i artiklarna 6–8 och 11 i stadgan måste iakttas.

195 Den hänskjutande domstolen har dessutom preciserat att dess fråga avser den lagringsskyldighet som föreskrivs i artikel 6 LCEN, jämförd med dekret nr 2011-219. De uppgifter som de berörda tjänsteleverantörerna ska lagra med stöd av denna bestämmelse innefattar bland annat uppgifter om den fysiska identiteten för de personer som har använt tjänsterna, såsom deras för- och efternamn, deras postadress, deras e-postadress eller därmed förbundna konton, deras lösenord och, när abonnemanget för avtalet eller kontot är avgiftsbelagt, den typ av betalning som använts, betalningsreferens, belopp samt datum och klockslag för transaktionen.

196 Lagringsskyldigheten innefattar även identifikatorerna avseende abonnenterna, anslutningarna och den terminalutrustning som används, de identifikatorer som tilldelats innehållet samt datum och klockslag för inledande och avslutande av anslutningar och aktiviteter samt de typer av protokoll som använts för anslutning till tjänsten och för överföring av innehåll. Åtkomst till dessa uppgifter, vars lagringstid uppgår till ett år, får begäras inom ramen för brottmåls- och tvistemålsförfaranden, i syfte att säkerställa efterlevnaden av bestämmelserna om skadeståndsansvar eller straffrättsligt ansvar, samt i samband med de åtgärder för insamling av underrättelseuppgifter som artikel L. 851-1 CSI är tillämplig på.

197 Enligt artikel 1.2 i direktiv 2000/31 tillnärmas genom detta direktiv vissa nationella bestämmelser som är tillämpliga på informationssamhällets tjänster, vilka anges i artikel 2 a i direktivet.

198 Bland sådana tjänster ingår visserligen tjänster som tillhandahålls på distans med hjälp av utrustning för elektronisk behandling och lagring av uppgifter, på individuell begäran från en tjänstemottagare och som typiskt sett tillhandahålls mot betalning, såsom anslutningstjänster till internet eller till ett kommunikationsnät samt värdtjänster (se, för ett liknande resonemang, dom av den 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punkt 40, dom av den 16 februari 2012, SABAM, C-360/10, EU:C:2012:85, punkt 34, dom av den 15 september 2016, Mc Fadden, C-484/14, EU:C:2016:689, punkt 55, och dom av den 7 augusti 2018, SNB-REACT, C-521/17, EU:C:2018:639, punkt 42 och där angiven rättspraxis.

199 I artikel 1.5 i direktiv 2000/31 föreskrivs emellertid att direktivet inte ska tillämpas på frågor beträffande informationssamhällets tjänster som omfattas av direktiv 95/46 och direktiv 97/66. Det framgår i detta hänseende av skälen 14 och 15 i direktiv 2000/31 att skyddet för konfidentialitet vid kommunikation och för enskilda personer med avseende på behandling av personuppgifter i samband med informationssamhällets tjänster endast regleras i direktiven 95/46 och 97/66. För att skydda konfidentialiteten vid kommunikation förbjuds alla former av uppfångande eller övervakning av kommunikation i artikel 5 i det sistnämnda direktivet.

200 Frågor med anknytning till skyddet för konfidentialitet vid kommunikation och skyddet för personuppgifter ska således bedömas mot bakgrund av direktiv 2002/58 och förordning 2016/679, vilka har ersatt direktiv 97/66 respektive direktiv 95/46. Det ska härvidlag preciseras att det skydd som direktiv 2000/31 är avsett att säkerställa under inga omständigheter får undergräva de krav som följer av direktiv 2002/58 och förordning 2016/679 (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 57).

201 Skyldigheten i den nationella lagstiftning som avses i punkt 195 ovan, vilken åläggs leverantörer som tillhandahåller allmänheten tillgång till internetkommunikationstjänster och värdtjänstleverantörer, att lagra personuppgifter förbundna med dessa tjänster ska således, såsom generaladvokaten har påpekat i punkt 141 i sitt förslag till avgörande i de förenade målen La Quadrature du Net m.fl. (C-511/18 och C-512/18, EU:C:2020:6), bedömas mot bakgrund av direktiv 2002/58 eller förordning 2016/679.

202 Beroende på om tillhandahållandet av de tjänster som omfattas av den aktuella nationella lagstiftningen faller inom tillämpningsområdet för direktiv 2002/58 eller ej, regleras detta tillhandahållande antingen av det sistnämnda direktivet, i synnerhet av artikel 15.1 i det direktivet, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, eller av förordning 2016/679, i synnerhet artikel 23.1 i nämnda förordning, jämförd med samma bestämmelser i stadgan.

203 I förevarande fall kan det inte uteslutas, såsom Europeiska kommissionen har påpekat i sitt skriftliga yttrande, att vissa av de tjänster som den nationella lagstiftning som avses i punkt 195 ovan är tillämplig på, utgör elektroniska kommunikationstjänster i den mening som avses i direktiv 2002/58, vilket det ankommer på den hänskjutande domstolen att kontrollera.

204 Direktiv 2002/58 omfattar elektroniska kommunikationstjänster som uppfyller rekvisiten i artikel 2 c i direktiv 2002/21, till vilken det hänvisas i artikel 2 i direktiv 2002/58. I förstnämnda bestämmelse definierar en elektronisk kommunikationstjänst som ”en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät, däribland teletjänster och överföringstjänster i nät som används för rundradio”. Vad gäller informationssamhällets tjänster, vilka anges i punkterna 197 och 198 ovan och som omfattas av direktiv 2000/31 utgör dessa elektroniska kommunikationstjänster om de helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (se, för ett liknande resonemang, dom av den 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punkterna 47 och 48).

205 Internetanslutningstjänster, vilka förefaller omfattas av den nationella lagstiftning som avses i punkt 195 ovan, utgör således, såsom bekräftas i skäl 10 i direktiv 2002/21, elektroniska kommunikationstjänster i den mening som avses i detta direktiv (se, för ett liknande resonemang, dom av den 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punkt 37). Detta är även fallet vad gäller internetbaserade e-posttjänster, beträffande vilka det inte kan uteslutas att de även omfattas av den nationella lagstiftningen, eftersom de tekniskt sett helt eller huvudsakligen innebär överföring av signaler i elektroniska kommunikationsnät (se, för ett liknande resonemang, dom av den 13 juni 2019, Google, C-193/18, EU:C:2019:498, punkterna 35 och 38).

206 Vad gäller de krav som följer av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, hänvisar domstolen till de konstateranden och bedömningar som gjorts i samband med svaret på fråga 1 i mål C-511/18 respektive mål C-512/18 samt på frågorna 1 och 2 i mål C-520/18.

207 När det gäller de krav som följer av förordning 2016/679 ska det erinras om att denna förordning, såsom framgår av dess skäl 10, bland annat syftar till att säkerställa en hög skyddsnivå för fysiska personer inom unionen och för att uppnå detta ändamål säkerställa en konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter i hela unionen (se, för ett liknande resonemang, dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559, punkt 101).

208 All behandling av personuppgifter ska i detta syfte, med förbehåll för de undantag som medges i artikel 23 i förordning nr 2016/679, vara förenlig med de principer som reglerar behandlingen av personuppgifter och de rättigheter som registrerade personer har enligt kapitel II respektive III i förordningen. All behandling av personuppgifter ska i synnerhet dels stå i överensstämmelse med de principer som anges i artikel 5 i förordningen, dels uppfylla de laglighetsvillkor som anges i artikel 6 i samma förordning (se, analogt, beträffande direktiv 95/46, dom av den 30 maj 2013, Worten, C-342/12, EU:C:2013:355, punkt 33 och där angiven rättspraxis).

209 Vad närmare bestämt gäller artikel 23.1 i förordning 2016/679 ska det påpekas att den artikeln, i likhet med vad som föreskrivs i artikel 15.1 i direktiv 2002/58, tillåter medlemsstaterna att, med hänsyn till de mål som föreskrivs däri och genom lagstiftningsåtgärder, begränsa tillämpningsområdet för de skyldigheter och rättigheter som avses i artikeln ”om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa” det eftersträvade målet. Varje lagstiftningsåtgärd som vidtas på denna grund ska i synnerhet uppfylla de specifika krav som uppställs i artikel 23.2 i förordningen.

210 Artikel 23.1 och 23.2 i förordning nr 2016/679 kan således inte tolkas så, att den kan ge medlemsstaterna befogenhet att kränka respekten för privatlivet, i strid med artikel 7 i stadgan, eller andra garantier som föreskrivs i stadgan (se, analogt, beträffande direktiv 95/46, dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 91). I likhet med vad som gäller för artikel 15.1 i direktiv 2002/58, kan den befogenhet som medlemsstaterna har enligt artikel 23.1 i förordning 2016/679 endast utövas med iakttagande av kravet på proportionalitet, enligt vilket undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (se, analogt, beträffande direktiv 95/46, dom av den 7 november 2013, IPI, C-473/12, EU:C:2013:715, punkt 39 och där angiven rättspraxis).

211 Härav följer att de konstateranden och bedömningar som gjorts i samband med svaret på fråga 1 i mål C-511/18 respektive mål C-512/18 samt på frågorna 1 och 2 i mål C-520/18, i tillämpliga delar gäller för artikel 23 i förordning 2016/679.

212 Mot bakgrund av det anförda ska fråga 2 i mål C-512/18 besvaras enligt följande. Direktiv 2000/31 ska tolkas så, att det inte är tillämpligt på skyddet för konfidentialitet vid kommunikationer och på skyddet för fysiska personer med avseende på behandlingen av personuppgifter i samband med informationssamhällets tjänster, då detta skydd, beroende på omständigheterna, regleras av direktiv 2002/58 eller av förordning 2016/679. Artikel 23.1 i förordning 2016/679, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att den utgör hinder för en nationell lagstiftning enligt vilken leverantörer som tillhandahåller allmänheten tillgång till internetkommunikationstjänster och värdtjänstleverantörer är skyldiga att generellt och odifferentierat lagra bland annat personuppgifter förbundna med dessa tjänster.

Fråga 3 i mål C-520/18

213 Den hänskjutande domstolen har ställt fråga 3 i mål C-520/18 för att få klarhet i huruvida en nationell domstol får tillämpa en bestämmelse i nationell rätt som ger den behörighet att tidsmässigt begränsa verkningarna av en förklaring om rättsstridighet som den domstolen är skyldig att meddela enligt nationell rätt med avseende på nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs att – i syfte att bland annat skydda nationell säkerhet och bekämpa brottslighet – generellt och odifferentierat lagra trafik- och lokaliseringsuppgifter, till följd av att den lagstiftningen är oförenlig med artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan.

214 Enligt principen om unionsrättens företräde har unionsrätten företräde framför respektive medlemsstats nationella rätt. Denna princip medför således en skyldighet för samtliga myndigheter i medlemsstaterna att säkerställa unionsbestämmelsernas fulla verkan, och medlemsstaternas nationella rätt kan inte påverka dessa bestämmelsers verkan i medlemsstaterna (dom av den 15 juli 1964, Costa, 6/64, EU:C:1964:66, s. 1159 och 1160, och dom av den 19 november 2019, A.K. m.fl. (Oavhängigheten hos avdelningen för disciplinära mål vid Högsta domstolen), C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkterna 157 och 158 och där angiven rättspraxis.

215 Av principen om unionsrättens företräde följer att om det inte är möjligt att tolka nationell rätt i enlighet med kraven i unionsrätten, är den nationella domstol som inom ramen för sin behörighet ska tillämpa unionsbestämmelser skyldig att säkerställa att dessa bestämmelser ges full verkan genom att, med stöd av sin egen behörighet, vid behov, underlåta att tillämpa nationell lagstiftning som strider mot unionsbestämmelserna, även senare sådan, utan att vare sig begära eller avvakta ett föregående upphävande av denna genom ett lagstiftnings- eller annat konstitutionellt förfarande (dom av den 22 juni 2010, Melki och Abdeli, C-188/10 och C-189/10, EU:C:2010:363, punkt 43 och där angiven rättspraxis, dom av den 24 juni 2019, Popławski, C-573/17, EU:C:2019:530, punkt 58, och dom av den 19 november 2019, A.K. m.fl. (Oavhängigheten hos avdelningen för disciplinära mål vid Högsta domstolen), C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkt 160).

216 Det är endast EU-domstolen som, undantagsvis och av tvingande rättssäkerhetshänsyn, får förordna om ett tillfälligt uppskjutande av en unionsbestämmelses undanträngningsverkan i förhållande till nationell rätt som strider mot den förstnämnda bestämmelsen. Det får endast förordnas om en sådan begränsning i tiden av verkningarna av domstolens tolkning av unionsrätten i den dom varigenom den begärda tolkningen meddelas (se, för ett liknande resonemang, dom av den 23 oktober 2012, Nelson m.fl., C-581/10 och C-629/10, EU:C:2012:657, punkterna 89 och 91, dom av den 23 april 2020, Herst, C-401/18, EU:C:2020:295, punkterna 56 och 57, och dom av den 25 juni 2020, A m.fl. (Vindkraftverk i Aalter och Nevele), C-24/19, EU:C:2020:503, punkt 84 och där angiven rättspraxis).

217 Om de nationella domstolarna hade kunnat ge nationella bestämmelser som strider mot unionsrätten, ens tillfälligt, företräde, skulle det äventyra unionsrättens företräde och den enhetliga tillämpningen av unionsrätten (se, dom av den 29 juli 2019, Inter-Environnement Wallonie och Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punkt 177 och där angiven rättspraxis).

218 Domstolen har emellertid, i ett mål där det var fråga om lagenligheten av åtgärder som vidtagits i strid med den skyldighet som föreskrivs i unionsrätten att göra en förhandsbedömning av ett projekts konsekvenser för miljön och för ett skyddat område, slagit fast att en nationell domstol, om detta är tillåtet enligt nationell rätt, undantagsvis får låta verkningarna av sådana åtgärder bestå när detta är motiverat av tvingande skäl hänförliga till nödvändigheten av att undanröja ett verkligt och allvarligt hot om avbrott i den berörda medlemsstatens elförsörjning, vilket inte skulle kunna avvärjas med andra medel och alternativ, särskilt inom ramen för den inre marknaden. Ett bibehållande av nämnda åtgärders rättsverkningar får endast omfatta den tidsrymd som är strängt nödvändig för att avhjälpa rättsstridigheten (se, för ett liknande resonemang, dom av den 29 juli 2019, Inter-Environnement Wallonie och Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punkterna 175, 176, 179 och 181).

219 Till skillnad från en underlåtenhet att uppfylla en formell skyldighet såsom att på miljöskyddsområdet göra en förhandsbedömning av ett projekts konsekvenser, kan ett åsidosättande av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, emellertid inte legaliseras genom ett förfarande som är jämförbart med det som nämns i föregående punkt. Att låta verkningarna av en sådan nationell lagstiftning som den som är aktuell i det nationella målet bestå skulle innebära att denna lagstiftning skulle fortsätta att ålägga leverantörer av elektroniska kommunikationstjänster skyldigheter som strider mot unionsrätten och som innebär allvarliga ingrepp i de grundläggande rättigheterna för de personer vars uppgifter har lagrats.

220 Den hänskjutande domstolen kan följaktligen inte tillämpa en bestämmelse i nationell rätt som ger den behörighet att tidsmässigt begränsa verkningarna av en förklaring om rättsstridighet som den domstolen är skyldig att meddela enligt nationell rätt med avseende på den aktuella nationella lagstiftningen.

221 VZ, WY och XX har emellertid i sina yttranden till domstolen gjort gällande att fråga 3 underförstått men nödvändigtvis aktualiserar frågan huruvida unionsrätten utgör hinder för att, inom ramen för ett brottmålsförfarande, använda information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten.

222 I detta hänseende och för att ge den hänskjutande domstolen ett användbart svar ska det erinras om att på unionsrättens nuvarande stadium bestäms reglerna om tillåtlighet och värdering – i ett brottmålsförfarande mot personer som är misstänkta för grova brott – av information och bevisning som erhållits genom en lagring av trafik- och lokaliseringsuppgifter i strid med unionsrätten, i princip uteslutande i nationell rätt.

223 Det följer nämligen av fast rättspraxis att det, i avsaknad av unionsbestämmelser på området, ankommer på varje medlemsstat att i sin rättsordning, enligt principen om processuell autonomi, fastställa de processuella regler som gäller för talan som syftar till att säkerställa skyddet av de rättigheter som enskilda har till följd av unionsrätten. Dessa regler får emellertid varken vara mindre förmånliga än dem som gäller för liknande situationer som regleras av nationell rätt (likvärdighetsprincipen) eller medföra att det i praktiken blir omöjligt eller orimligt svårt att utöva de rättigheter som följer av unionsrätten (effektivitetsprincipen) (se, för ett liknande resonemang, dom av den 6 oktober 2015, Târşia, C-69/14, EU:C:2015:662, punkterna 26 och 27, dom av den 24 oktober 2018, XC m.fl., C-234/17, EU:C:2018:853, punkterna 21 och 22 och där angiven rättspraxis, och dom av den 19 december 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, punkt 33).

224 När det gäller likvärdighetsprincipen ankommer det på den nationella domstol som har att pröva ett brottmålsförfarande som grundar sig på information eller bevisning som erhållits i strid med de krav som följer av direktiv 2002/58, att pröva huruvida den nationella lagstiftning som reglerar brottmålsförfaranden föreskriver mindre förmånliga regler i fråga om tillåtlighet och användning av sådan information och sådan bevisning än dem som gäller för information och bevisning som har erhållits i strid med nationell rätt.

225 Vad gäller effektivitetsprincipen ska det påpekas att nationella bestämmelser om tillåtlighet och användning av information och bevisning har till syfte, i enlighet med de val som gjorts i nationell rätt, att förhindra att olagligt erhållen information och bevisning otillbörligen är till förfång för en person som är misstänkt för brott. Detta syfte kan emellertid i nationell rätt uppnås inte bara genom ett förbud mot att använda sådan information och sådan bevisning, utan även genom nationella bestämmelser och nationell praxis som reglerar bedömningen och värdet av informationen och bevisningen, eller till och med genom att informationens och bevisningens rättstridighet tas i beaktande vid påföljdsbestämningen.

226 Det framgår emellertid av domstolens praxis att frågan huruvida det är nödvändigt att bortse från information och bevisning som erhållits i strid med kraven i unionsrätten bland annat måste bedömas mot bakgrund av den risk som tillåtligheten av sådan information och bevisning medför för iakttagandet av den kontradiktoriska principen och därmed rätten till en rättvis rättegång (se, för ett liknande resonemang, dom av den 10 april 2003, Steffensen, C-276/01, EU:C:2003:228, punkterna 76 och 77). En domstol som anser att en part inte beretts tillfälle att på effektivt sätt yttra sig över ett bevismedel som hänför sig till ett område som domarna saknar sakkunskap om och som kan påverka bedömningen av omständigheterna på ett avgörande sätt, måste därför fastställa att rätten till en

rättvis rättegång har åsidosatts och bortse från denna bevisning för att förhindra ett sådant åsidosättande (se, för ett liknande resonemang, dom av den 10 april 2003, Steffensen, C-276/01, EU:C:2003:228, punkterna 78 och 79).

227 Effektivitetsprincipen kräver således att en nationell brottmålsdomstol – inom ramen för ett brottmålsförfarande mot personer som är misstänkta för brott – bortser från information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten, om dessa personer inte bereds tillfälle att på ett effektivt sätt yttra sig över informationen och bevisningen, vilka hänför sig till ett område som domarna saknar sakkunskap om och som kan påverka bedömningen av omständigheterna på ett avgörande sätt.

228 Mot bakgrund av det anförda ska fråga 3 i mål C-520/18 besvaras enligt följande. En nationell domstol får inte tillämpa en bestämmelse i nationell rätt som ger den behörighet att tidsmässigt begränsa verkningarna av en förklaring om rättsstridighet som den domstolen är skyldig att meddela enligt nationell rätt med avseende på nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs en skyldighet att – i syfte att bland annat skydda nationell säkerhet och bekämpa brottslighet – generellt och odifferentierat lagra trafik- och lokaliseringsuppgifter som är oförenlig med artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan. Nämnda artikel 15.1, tolkad mot bakgrund av effektivitetsprincipen, innebär en skyldighet för en nationell brottmålsdomstol att – inom ramen för ett brottmålsförfarande mot personer som är misstänkta för brott – bortse från information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten, om dessa personer inte bereds tillfälle att på ett effektivt sätt yttra sig över informationen och bevisningen, vilka hänför sig till ett område som domarna saknar sakkunskap om och som kan påverka bedömningen av omständigheterna på ett avgörande sätt.

Rättegångskostnader

229 Eftersom förfarandet i förhållande till parterna i de nationella målen utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

1) **Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 och jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas så, att den utgör hinder för lagstiftning vilken, för de ändamål som anges i nämnda artikel 15.1, föreskriver generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter i förebyggande syfte. Artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136 och jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna, utgör däremot inte hinder för lagstiftning**

   – **som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart, varvid beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en**

oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda, och varvid åläggandet endast får meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår,

– **som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en riktad lagring av trafik- och lokaliseringsuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,**

– **som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en generell och odifferentierad lagring av IP-adresser som har tilldelats källan till en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,**

– **som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om den fysiska identiteten för användare av elektroniska kommunikationsmedel, och**

– **som, för att bekämpa grov brottslighet eller, i ännu högre grad, skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket är föremål för effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra de trafik- och lokaliseringsuppgifter som dessa tjänsteleverantörer har tillgång till,**

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk.

2) **Artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136 och jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna, ska tolkas så, att den inte utgör hinder för en nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs dels att använda automatiserad analys av bland annat trafik- och lokaliseringsuppgifter och samla in sådana uppgifter i realtid, dels att i realtid samla in tekniska uppgifter om lokaliseringen av de terminalutrustningar som används, när**

– **användningen av automatiserad analys är begränsad till situationer där en medlemsstat står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart och användningen av sådan analys kan bli föremål för en effektiv kontroll – antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan – i syfte att kontrollera att det föreligger en situation som motiverar åtgärden och att de villkor och garantier som måste ställas upp är uppfyllda, och när**

– **användningen av insamling i realtid av trafik- och lokaliseringsuppgifter är begränsad till personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i terrorverksamhet och är underkastad en förhandskontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att säkerställa att en sådan insamling i realtid endast är tillåten inom ramen för vad som är strängt nödvändigt. I vederbörligen motiverade fall som ställer krav på skyndsamhet ska kontrollen ske utan dröjsmål.**

3) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) ska tolkas så, att det inte är tillämpligt på skyddet för konfidentialitet vid kommunikationer och skyddet för fysiska personer med avseende på behandlingen av personuppgifter i samband med informationssamhällets tjänster, då detta skydd, beroende på omständigheterna, regleras av direktiv 2002/58, i dess lydelse enligt direktiv 2009/136, eller av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46. Artikel 23.1 i förordning 2016/679, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna, ska tolkas så, att den utgör hinder för en nationell lagstiftning enligt vilken leverantörer som tillhandahåller allmänheten tillgång till internetkommunikationstjänster och värdtjänstleverantörer är skyldiga att generellt och odifferentierat lagra bland annat personuppgifter förbundna med dessa tjänster.

4) En nationell domstol får inte tillämpa en bestämmelse i nationell rätt som ger den behörighet att tidsmässigt begränsa verkningarna av en förklaring om rättsstridighet som den domstolen är skyldig att meddela enligt nationell rätt med avseende på nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs en skyldighet att – i syfte att bland annat skydda nationell säkerhet och bekämpa brottslighet – generellt och odifferentierat lagra trafik- och lokaliseringsuppgifter som är oförenlig med artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136 och jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna. Nämnda artikel 15.1, tolkad mot bakgrund av effektivitetsprincipen, innebär en skyldighet för en nationell brottmålsdomstol att – inom ramen för ett brottmålsförfarande mot personer som är misstänkta för brott – bortse från information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten, om dessa personer inte bereds tillfälle att på ett effektivt sätt yttra sig över informationen och bevisningen, vilka hänför sig till ett område som domarna saknar sakkunskap om och som kan påverka bedömningen av omständigheterna på ett avgörande sätt.

Underskrifter