Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
CAMPOS SÁNCHEZ-BORDONA
föredraget den 15 januari 2020[1]

Förenade målen C-511/18 och C-512/18

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

(begäran om förhandsavgörande från Conseil d'État (Högsta förvaltningsdomstolen, Frankrike))

"Begäran om förhandsavgörande – Behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation – Skydd av nationell säkerhet och bekämpning av terrorism – Direktiv 2002/58/EG – Tillämpningsområde – Artikel 1.3 – Artikel 15.3 – Artikel 4.2 FEU – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 6, 7, 8, 11, 47 och 52.1 – Generell och odifferentierad lagring av uppkopplingsuppgifter och av uppgifter som gör det möjligt att identifiera de personer som skapar innehåll – Insamling av trafik- och lokaliseringsuppgifter – Tillgång till uppgifter"

1. Domstolen har under de senaste åren hållit en fast linje i sin rättspraxis vad gäller lagring av och tillgång till personuppgifter, där de viktigaste domarna är följande:

– Dom av den 8 april 2014, Digital Rights Ireland m.fl.,[2] i vilken domstolen slog fast att direktiv 2006/24/EG[3] var ogiltigt, på grund av att det medgav en oproportionerlig begränsning av de rättigheter som erkänns i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

– Dom av den 21 december 2016, Tele2 Sverige och Watson m.fl.,[4] i vilken domstolen tolkade artikel 15.1 i direktiv 2002/58/EG.[5]

1 Originalspråk: spanska.

2 Målen C-293/12 och C-594/12, nedan kallad domen Digital Rights, EU:C:2014:238.

3 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).

4 Målen C-203/15 och C-698/15, nedan kallad domen Tele2 Sverige och Watson, EU:C:2016:970.

5 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).

– Dom av den 2 oktober 2018, Ministerio Fiscal,[6] i vilken domstolen bekräftade tolkningen av samma bestämmelse i direktiv 2002/58.

2. Myndigheterna i vissa medlemsstater anser att dessa domar (i synnerhet den andra) är oroväckande, eftersom de uppfattar dem så att konsekvensen blir att de berövas ett instrument som de anser är nödvändigt för att kunna upprätthålla den nationella säkerheten samt bekämpa brottslighet och terrorism. Några av dessa medlemsstater anser därför att denna rättspraxis bör ändras eller nyanseras.

3. Vissa domstolar i medlemsstaterna har gett uttryck för denna oro genom att begära förhandsavgöranden i fyra olika mål[7] och jag kommer att föredra mina förslag till avgörande i samtliga dessa mål samtidigt.

4. De fyra målen aktualiserar framför allt frågan om tillämpningen av direktiv 2002/58 på verksamhet som rör nationell säkerhet och bekämpning av terrorism. Om det direktivet är tillämpligt i ett sådant sammanhang måste det avgöras i vilken mån medlemsstaterna får inskränka den rätt till integritet som direktivet skyddar. Det ska avslutningsvis prövas i vilken mån de olika nationella lagstiftningarna (den brittiska,[8] den belgiska[9] och den franska[10]) rörande detta område är förenliga med unionsrätten, så som domstolen har tolkat den.

I. Tillämpliga bestämmelser

A. Unionsrätt

1. Direktiv 2002/58

5. I artikel 1 (”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 gemenskapen.

…

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för Fördraget om upprättandet av Europeiska gemenskapen, 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.”

6 Mål C-207/16, nedan kallad domen Ministerio Fiscal, EU:C:2018:788.

7 Förutom dessa två (mål C-511/18 och C-512/18) rör det sig om mål C-623/17, Privacy International, och mål C-520/18, Ordre des barreaux francophones et germanophone m.fl.

8 Målet Privacy International, C-623/17.

9 Målet Ordre des barreaux francophones et germanophone m.fl., C-520/18.

10 Förenade målen La Quadrature du Net m.fl., C-511/18 och C-512/18

6. Artikel 3 (”Berörda tjänster”) har följande lydelse:

”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.”

7. I punkt 1 i artikel 5 (”Konfidentialitet vid kommunikation”) föreskrivs följande:

”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.”

8. Artikel 6 (”Trafikuppgifter”) har följande lydelse:

”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.”

9. I artikel 15 (”Tillämpningen av vissa bestämmelser i direktiv 95/46/EG[11]”) föreskrivs följande i punkt 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/EG. 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 gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.”

11 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).

2. Direktiv 2000/31/EG[12]

10. I artikel 14 föreskrivs följande:

”1. Medlemsstaterna skall se till att en tjänsteleverantör som levererar någon av informationssamhällets tjänster bestående av lagring av information som tillhandahållits av tjänstemottagaren inte skall vara ansvarig för information som lagrats på begäran av en tjänstemottagare av tjänsten, under förutsättning att

…

3. Denna artikel skall inte påverka möjligheten för en domstol eller administrativ myndighet att i enlighet med medlemsstaternas rättssystem kräva att tjänsteleverantören upphör med eller förhindrar en överträdelse, inte heller skall den påverka medlemsstaternas möjlighet att inrätta förfaranden för att avlägsna information eller göra den oåtkomlig.”

11. I artikel 15 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.”

3. Förordning (EU) 2016/679[13]

12. I artikel 2 (”Materiellt tillämpningsområde”) 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,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

12 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).

13 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/EG (allmän dataskyddsförordning) (EUT L 119, 2016, s. 1).

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.

…”

13. Punkt 1 i artikel 23 (”Begränsningar”) har följande lydelse:

”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) statens säkerhet,

b) försvaret,

c) allmän säkerhet,

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.”

14. Artikel 95 (”Förhållande till direktiv 2002/58/EG”) har följande lydelse:

”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/EG.”

B. Nationell rätt

1. Code de la sécurité intérieure (lagen om inre säkerhet)

15. Artikel L. 851–1 har följande lydelse:

”Under de förutsättningar som föreskrivs i kapitel 1 i avdelning II i denna bok får tillstånd beviljas för insamling, hos operatörer som tillhandahåller elektronisk kommunikation och personer som anges i artikel L. 34–1 i code des postes et des communications électroniques (lagen om elektronisk post och kommunikation) samt hos de personer som anges i artikel 6.1 och 6.2 i loi nr 2004–575 pour la confiance dans l’économie numérique (lag nr 2004–575 om förtroende för den digitala ekonomin), av uppgifter eller handlingar som behandlas eller lagras genom deras nät eller tjänster för elektronisk kommunikation, däribland tekniska uppgifter om identifiering av abonnent- eller anslutningsnummer för elektroniska kommunikationstjänster, fastställande av alla abonnent- eller anslutningsnummer för en angiven person, lokalisering av använd terminalutrustning samt om en abonnents kommunikationer med avseende på in- och utgående nummer, varaktighet och datum …”

16. I artiklarna L. 851–2 och L. 851–4 i lagen om inre säkerhet anges hur den administrativa åtkomsten i realtid till således lagrade uppkopplingsuppgifter ska organiseras för olika ändamål och med olika metoder.

17. Enligt artikel L. 851–2 i lagen om inre säkerhet får de uppgifter eller handlingar som avses i artikel L. 851–1 samlas in från samma personer i det enda syftet att förebygga terrorism. Denna insamling, som endast ska avse en eller flera enskilda personer som på förhand identifierats som personer som kan ha anknytning till ett terroristhot, ska utföras 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. [14]

18. Enligt artikel L. 851–3 i lagen om inre säkerhet får operatörer som tillhandahåller elektroniska kommunikationsnät och elektroniska kommunikationstjänster ”på sina nät tillämpa automatisk behandling i syfte att, enligt de parametrar som anges i tillståndet, spåra uppkopplingar som kan avslöja terroristhot”. [15]

19. I artikel L. 851–5 föreskrivs det att det under vissa förutsättningar ”får godkännas att en teknisk anordning används som gör det möjligt att lokalisera en person, ett fordon eller ett föremål i realtid”.

20. Enligt punkt I i artikel L. 851–6, är det under vissa förutsättningar möjligt att ”direkt, med hjälp av en sådan apparat eller teknisk anordning som avses i artikel 226–3.1 i code pénal (strafflagen), samla in … sådana tekniska uppkopplingsuppgifter som gör det möjligt att identifiera en terminalutrustning eller användarens abonnentnummer, samt uppgifter om lokalisering av använd terminalutrustning”.

14 Enligt den hänskjutande domstolen medför denna teknik inte något krav på leverantörerna på mer lagring än vad som är nödvändigt för att fakturera, marknadsföra och tillhandahålla tjänster med ett mervärde.

15 Enligt den hänskjutande domstolen innebär inte denna teknik någon generell och odifferentierad lagring. Syftet med den är bara att under en begränsad tid samla in sådana uppgifter som har samband med ett allvarligt brott av det slaget bland alla de uppkopplingsuppgifter som dessa personer behandlar.

2. Code des postes et des communications électroniques (lagen om elektronisk post och kommunikation)

21. I artikel L. 34–1, i den lydelse som är tillämplig på de faktiska omständigheterna i målet, föreskrivs följande:

”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 personer 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 förebygga, undersöka, 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 323–1–323–3-1 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 Commission Nationale de l’Informatique et des Libertés (nationell myndighet för it- och frihetsrelaterade frågor) 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 tillhandahåller 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 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.”

22. Enligt artikel R. 10–13.I, ska operatörerna lagra följande uppgifter i syfte att utreda, fastställa och bekämpa 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.”

23. Enligt punkt II i samma artikel ska operatören när det rör sig om telefoni dessutom lagra uppgifter som gör det möjligt att identifiera kommunikationens ursprung och lokalisering.

24. Enligt punkt III i samma artikel ska dessa uppgifter lagras i ett år, från och med den dag då de registrerades.

3. Loi n.º 2004–575 du 21 juin 2004 pour la confiance dans l'économie numérique (lag nr 2004–575 av den 21 juni 2004 om förtroendet för den digitala ekonomin)

25. I det första stycket i artikel 6.II i lag nr 2004–575 föreskrivs att personer vars verksamhet består i att erbjuda allmänheten tillgång till kommunikationstjänster online 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 till dessa tjänster ”ska inneha och lagra uppgifter som gör det möjligt att identifiera varje person som har bidragit till skapandet av innehåll eller något av innehållet i de tjänster som de tillhandahåller”.

26. I det tredje stycket i punkt II föreskrivs att en rättslig myndighet kan begära att de uppgifter som anges i första stycket avseende dessa personer ska lämnas ut.

27. I det sista stycket i punkt II anges att Conseil d'État genom dekret ”ska definiera de uppgifter som avses i första stycket och fastställa hur länge och på vilket sätt de ska lagras”. [16]

16 Denna definition gjordes genom décret n.º 2011–219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (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 erbjudits online). I detta dekret kan följande framhållas: a) Artikel 1.1, i vilken det föreskrivs att den som erbjuder tillgång till kommunikationstjänster online ska lagra följande uppgifter: uppkopplings-ID, tilldelat abonnent-ID, ID för den terminal som använts för uppkopplingen, datum och klockslag för uppkopplingens början och slut, egenskaperna hos abonnentens linje. b) Enligt artikel 1.2 ska den 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 till dessa tjänster, ska lagra uppgifter för varje operation: uppkopplings-ID vid kommunikationens uppkomst, ID som tilldelats det innehåll som operationen avser, de typer av protokoll som använts för uppkopplingen till tjänsten och för överföringen av innehåll, operationens karaktär, datum och klockslag för operationen, ID som använts av operationens upphovsman. c) Avslutningsvis föreskrivs det i artikel 1.3 att de personer som avses i de två föregående punkterna ska lagra följande information som tillhandahålls av en användare när ett avtal ingås eller ett konto skapas: uppkopplings-ID när kontot skapades; förnamn, efternamn eller firma; anknytande postadresser, pseudonymer som använts, anknytande e-postadresser eller kontoadresser, telefonnummer, aktuellt lösenord och andra uppgifter som gör det möjligt att verifiera eller ändra den.

II. Bakgrund och tolkningsfrågor

A. Mål C-511/18

28. Quadrature du Net, French Data Network, Igwan.net och Fédération des fournisseurs d'accès à internet associatifs (nedan kallade sökandena) väckte talan vid Conseil d'État om ogiltigförklaring av flera dekret med tillämpningsföreskrifter för vissa bestämmelser i lagen om inre säkerhet.[17]

29. Sökandena gjorde i korthet gällande att såväl dekreten i fråga som de ifrågavarande bestämmelserna i lagen om inre säkerhet strider mot rätten till ett privatliv, rätten till skydd av personuppgifter och rätten till ett effektivt rättsmedel, enligt artiklarna 7, 8 respektive 47 i stadgan.

30. I detta sammanhang har Conseil d'État hänskjutit följande frågor till domstolen för förhandsavgörande:

"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 Europeiska unionens stadga om de grundläggande rättigheterna och kraven på nationell säkerhet, vilket uteslutande är medlemsstaternas ansvar enligt artikel 4 i fördraget om Europeiska unionen?

2) Ska direktiv 2002/58, jämfört med Europeiska unionens stadga om de grundläggande rättigheterna, tolkas så, att det medger sådana lagstiftningsåtgärder som åtgärder för insamling i realtid av trafik- och lokaliseringsuppgifter 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 Europeiska unionens stadga om de grundläggande rättigheterna, 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?"

B. Mål C-512/18

31. Sökandena i den tvist som har gett upphov till mål C-511/18, med undantag av Igwan.net, har även yrkat att Conseil d'État ska ogiltigförklara det tysta avslagsbeslut som följer av det uteblivna svaret på deras begäran om upphävande av artikel R. 10–13 i code des postes et des communications électroniques (lag om post och elektronisk kommunikation) och dekret nr 2011–219 av den 25 februari 2011.

17 Talan avsåg följande dekret: a) décret n.° 2015–1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (dekret nr 2015–1185 av den 28 september 2015 om inrättande av särskilda underrättelsetjänster); b) décret n.° 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); c) décret n.° 2015–1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (dekret nr 2015–1639 av den 11 december 2015 om inrättande av andra tjänster än de särskilda underrättelsetjänsterna, med behörighet att använda den teknik som anges i avdelning V, kapitel VIII i lagen om inre säkerhet); och d) décret n.° 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).

32. Enligt sökandena ålägger de bestämmelser som de begärt ska upphävas en skyldighet att lagra trafik-, lokaliserings- och uppkopplingsuppgifter, som på grund av sin generella karaktär utgör ett oproportionellt ingrepp i rätten till respekt för privatlivet och familjelivet, rätten till skydd av personuppgifter och yttrandefriheten, enligt artiklarna 7, 8 och 11 i stadgan om de grundläggande rättigheterna, samt ett åsidosättande av artikel 15.1 i rådets direktiv 2002/58.

33. I detta mål har Conseil d'État hänskjutit följande tolkningsfrågor:

”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 Europeiska unionens stadga om de grundläggande rättigheterna och kraven på nationell säkerhet, vilket uteslutande är medlemsstaternas ansvar enligt artikel 4 i fördraget om Europeiska unionen?

2) Ska bestämmelserna i direktiv 2000/31, jämförda med artiklarna 6, 7, 8 och 11 samt artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, 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?”

III. Förfarandet vid domstolen och parternas ståndpunkter

34. Begäran om förhandsavgörande i de två målen inkom till domstolens kansli den 3 augusti 2018.

35. Skriftliga yttranden har getts in av La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, den tyska, den belgiska, den brittiska, den tjeckiska, den cypriotiska, den danska, den spanska, den estniska, den franska, den ungerska, den irländska, den polska och den svenska regeringen, samt av kommissionen.

36. Den 9 september 2019 hölls en förhandling, då målet behandlades gemensamt med målen C-623/17, Privacy International, och C-520/18, Ordre des barreaux francophones et germanophone m.fl., vid vilken parterna i de fyra målen om förhandsavgörande, de ovannämnda regeringarna, Nederländernas regering och Norges regering, samt kommissionen och Europeiska datatillsynsmannen| var närvarande.

IV. Bedömning

37. Conseil d'États frågor kan sammanställas till tre frågeställningar:

– För det första, huruvida en nationell lagstiftning som föreskriver en generell och odifferentierad skyldighet för leverantörer av elektroniska kommunikationstjänster att lagra uppkopplingsuppgifter (den första frågan i mål C-511/18 och i mål C-512/18) och, i synnerhet, uppgifter som gör det möjligt att identifiera de personer som skapar det innehåll som leverantörerna tillhandahåller (den andra frågan i mål C-512/18), är förenlig med unionsrätten.

– För det andra, huruvida förfarandena för insamling av uppkopplingsuppgifter för att vara lagenliga under alla förhållanden måste inbegripa information till de berörda personerna när en sådan information inte längre kan skada undersökningarna (den tredje frågan i mål C-511/18).

– För det tredje, huruvida insamling i realtid av trafik- och lokaliseringsuppgifter, utan skyldighet att lagra uppgifterna, är förenlig med direktiv 2002/58 och i så fall enligt vilka villkor (den andra frågan i mål C-511/18).

38. Det handlar med andra ord om att få klarlagt huruvida en nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster två typer av skyldigheter, nämligen a) dels *insamling* av vissa uppgifter, men inte lagring av dem; b) dels *lagring* av uppkopplingsuppgifter och uppgifter som gör det möjligt att identifiera de personer som skapar innehållet i de tjänster som leverantörerna tillhandahåller, är förenlig med unionsrätten.

39. Till att börja med ska det dock klarläggas huruvida direktiv 2002/58 är tillämpligt, just med tanke på det sammanhang [18] i vilket den nationella lagstiftningen har antagits (det vill säga under omständigheter där den nationella säkerheten kan vara i fara).

A. Huruvida direktiv 2002/58 är tillämpligt

40. Den hänskjutande domstolen utgår från att den omtvistade lagstiftningen omfattas av tillämpningsområdet för direktiv 2002/58. Detta följer enligt den hänskjutande domstolen av EU-domstolens praxis i domen Tele2 Sverige och Watson, vilken bekräftades i domen Ministerio Fiscal.

41. Några av de regeringar som har medverkat i målet har däremot gjort gällande att den omtvistade lagstiftningen inte omfattas av direktivet. För att motivera sin ståndpunkt har de bland annat hänvisat till domstolens dom av den 30 maj 2006, parlamentet/rådet och kommissionen. [19]

42. Jag anser liksom Conseil d'État att domstolen genom domen Tele2 Sverige och Watson har bilagt den här delen av tvisten, genom att den där bekräftade att direktiv 2002/58 i princip är tillämpligt när leverantörer av elektroniska kommunikationstjänster enligt lag är skyldiga att lagra uppgifter om sina abonnenter och ge myndigheter tillgång till dem. Denna ståndpunkt påverkas inte av att leverantörerna åläggs denna skyldighet av skäl som rör nationell säkerhet.

43. Jag vill redan här påpeka att om det skulle finnas någon bristande överensstämmelse mellan domen Tele2 Sverige och Watson och tidigare domar, så borde den förstnämnda domen ges företräde eftersom den är av senare datum och har bekräftats genom domen Ministerio Fiscal. Jag anser emellertid inte att det föreligger någon sådan bristande överensstämmelse, vilket jag ska försöka förklara.

18 ”Ett sammanhang som präglas av ihållande, allvarliga hot mot den nationella säkerheten, i synnerhet risken för terrorism”, enligt vad som anges i den första tolkningsfrågan i mål C-511/18.

19 Målen C-317/04 och C-318/04, nedan kallad domen parlamentet/rådet och kommissionen, EU:C:2006:346.

1. Domen parlamentet/rådet och kommissionen

44. De mål som avgjordes genom domen parlamentet/rådet och kommissionen rörde följande:

– Avtalet mellan Europeiska gemenskapen och Amerikas förenta stater om lufttrafikföretags behandling och överföring av PNR-uppgifter [Passenger Name Records (passageraruppgifter)] till Förenta staternas myndigheter. [20]

– Adekvat skydd av de personuppgifter som finns i sådana register över flygpassagerare (Passenger Name Records) som överförs till dessa myndigheter. [21]

45. Domstolen fann att överföringen av dessa uppgifter var en behandling som rörde allmän säkerhet och statens verksamhet på straffrättens område. Enligt artikel 3.2 första strecksatsen i direktiv 95/46 omfattades de två besluten i fråga inte av tillämpningsområdet för direktiv 95/46.

46. Uppgifterna samlades till att börja med in av lufttrafikföretagen inom ramen för en verksamhet – biljettförsäljning – som omfattades av unionsrätten. Som framgick av beslutet i fråga var behandlingen av uppgifterna inte en behandling som är ”nödvändig för tillhandahållandet av en tjänst, utan en behandling som anses vara nödvändig för att säkerställa allmän säkerhet och för att tillgodose repressiva syften”. [22]

47. Domstolen gjorde således en teleologisk tolkning och såg till uppgiftsbehandlingens ändamål. Eftersom den avsåg allmän säkerhet, skulle den anses falla utanför tillämpningsområdet för direktiv 95/46. Detta ändamål var emellertid inte det enda avgörande kriteriet [23] och därför betonade domstolen i domen att överföringen ”sker … inom en ram som inrättats av statsmakterna och som avser allmän säkerhet”. [24]

48. Domen parlamentet/rådet och kommissionen visar således skillnaden mellan undantagsklausulen och begränsningsklausulen i direktiv 95/46 (vilka motsvarar klausulerna i direktiv 2002/58). Båda gäller emellertid i själva verket liknande mål av allmänt intresse, vilket ger upphov till viss förvirring när det gäller räckvidden för var och en av dem, såsom generaladvokat Bot påpekade. [25]

20 Rådets beslut 2004/496/EG av den 17 maj 2004 om ingående av ett avtal mellan Europeiska gemenskapen och Amerikas förenta stater om lufttrafikföretags behandling och överföring av passageraruppgifter till Bureau of Customs and Border Protection inom Förenta staternas Department of Homeland Security (EUT L 183, 2004, s. 83, och rättelse i EUT L 255, 2005, s. 168) (mål C-317/04).

21 Kommissionens beslut 2004/535/EG av den 14 maj 2004 om adekvat skydd av personuppgifter som finns i Passenger Name Record för flygpassagerare som överförs till Förenta staternas tull- och gränsskyddsmyndighet (EUT L 235, 2004, s. 11) (mål C-318/04).

22 Domen parlamentet/rådet och kommissionen, punkt 57. I punkt 58 underströk domstolen att den omständigheten att ”… uppgifterna har samlats in av privata operatörer för kommersiella syften och att det är dessa operatörer som sköter överföringen av uppgifterna till en tredje stat”, inte innebär att denna överföring inte utgör ett av de fall där direktiv 95/46 inte ska tillämpas som anges i artikel 3.2 första strecksatsen i det direktivet, eftersom ”[d]enna överföring sker … inom en ram som inrättats av statsmakterna och som avser allmän säkerhet”.

23 Detta framhölls senare av den framlidne generaladvokaten Bot i hans förslag till avgörande i målet Irland/parlamentet och rådet (C-301/06, EU:C:2008:558). Han menade att domen parlamentet/rådet och kommissionen ”inte [innebär] att det endast är relevant att undersöka syftena med behandling av personuppgifter för att fastställa huruvida behandlingen ska falla inom ramen för tillämpningsområdet för det skyddssystem för uppgifter som har inrättats genom direktiv 95/46. Det måste också undersökas inom vilket slags verksamhet behandlingen av uppgifterna sker. Det är enbart då nämnda behandling förekommer i sådan verksamhet som är statens eller statliga myndigheters specifika verksamhet och den inte omfattas av enskildas verksamhetsområden som den inte omfattas av gemenskapens skyddssystem för personuppgifter, som har inrättats genom direktiv 95/46. Stöd för detta finns i artikel 3.2 första strecksatsen i nämnda direktiv” (punkt 122).

24 Domen parlamentet/rådet och kommissionen, punkt 58. Huvudsyftet med avtalet var att kräva att de lufttrafikföretag som transporterade passagerare mellan unionen och Förenta staterna skulle ge myndigheterna där elektronisk tillgång till uppgifterna i det Passenger Name Record som fanns i deras automatiska boknings- och avgångskontrollsystem. Genom avtalet infördes således en form av internationellt samarbete mellan unionen och Förenta staterna för att bekämpa terrorism och annan grov brottslighet, samtidigt som man försökte förena detta syfte med syftet att skydda passagerarnas personuppgifter. I det sammanhanget skiljde sig den skyldighet som ålades bolagen inte så mycket från ett direkt utbyte av uppgifter mellan myndigheter.

25 Förslag till avgörande av generaladvokaten Bot i målet Irland/parlamentet och rådet (C-301/06, EU:C:2008:558, punkt 127).

49. Sannolikt är det denna förvirring som ligger till grund för den ståndpunkt som de medlemsstater intagit som anser att direktiv 2002/58 inte är tillämpligt i detta sammanhang. Enligt dessa medlemsstater skyddas bara det nationella säkerhetsintresset genom det undantag som föreskrivs i artikel 1.3 i direktiv 2002/58. De begränsningar som är tillåtna enligt artikel 15.1 i det ifrågavarande direktivet, däribland den som rör den nationella säkerheten, skyddar emellertid också samma intresse. Den sistnämnda bestämmelsen skulle ha varit överflödig om direktiv 2002/58 inte hade varit tillämpligt vid hänvisningar till den nationella säkerheten.

2. Domen Tele2 Sverige och Watson

50. I domen Tele2 Sverige och Watson prövade domstolen huruvida vissa nationella system som ålade leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster en allmän skyldighet att lagra uppgifter om denna kommunikation, var förenliga med unionsrätten. De fallen var således i allt väsentligt identiska med dem som är föremål för prövning i förevarande mål.

51. När domstolen på nytt skulle pröva om unionsrätten var tillämplig – här i enlighet med direktiv 2002/58 – började den med att påpeka att ”tillämpningsområdet för direktiv 2002/58 ska bedömas med hänsyn bland annat till direktivets allmänna systematik”. [26]

52. Mot bakgrund av detta slog domstolen fast att ”[d]e lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 … förvisso [avser] sådan verksamhet som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda personer … De syften som dessa åtgärder ska ha enligt nämnda bestämmelse, det vill säga att skydda nationell säkerhet …, sammanfattar också väsentligen syftena med de verksamheter som avses i artikel 1.3 i direktivet.” [27]

53. Syftet med de åtgärder som medlemsstaterna enligt artikel 15.1 i direktiv 2002/58 får vidta för att begränsa integriteten sammanfaller (på den här punkten) med det syfte som motiverar att vissa statliga verksamheter undantas från direktivets tillämpningsområde, enligt artikel 1.3.

54. Domstolen slog emellertid fast att ”[s]ett till den allmänna systematiken i direktiv 2002/58” betydde det dock inte ”att de lagstiftningsåtgärder som avses i artikel 15.1 i direktivet ska anses uteslutna från direktivets tillämpningsområde. Det skulle helt frånta den bestämmelsen dess ändamålsenliga verkan. Nämnda bestämmelse förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna … omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda.” [28]

55. De begränsningar som är tillåtna enligt artikel 15.1 i direktiv 2002/58 ”reglerar dessutom – för de syften som anges i bestämmelsen – verksamheten för leverantörer av elektroniska kommunikationstjänster”. Den bestämmelsen, jämförd med artikel 3 i samma direktiv, ska därför ”tolkas på så sätt att sådana lagstiftningsåtgärder omfattas av direktivets tillämpningsområde”. [29]

26 Domen Tele2 Sverige och Watson, punkt 67.

27 *Ibidem*, punkt 72.

28 *Ibidem*, punkt 73.

29 *Ibidem*, punkt 74.

56. Följaktligen slog domstolen fast att tillämpningsområdet för direktiv 2002/58 omfattar en rättslig åtgärd som ålägger leverantörerna ”en skyldighet att lagra trafikuppgifter och lokaliseringsuppgifter. Deras verksamhet innebär nämligen med nödvändighet att de behandlar personuppgifter”.[30] Det omfattar även en åtgärd som den som innebär att nationella myndigheter får tillgång till uppgifter som lagrats av leverantörerna.[31]

57. Den tolkning av direktiv 2002/58 som domstolen gjorde i domen Tele2 Sverige och Watson gjorde den även i domen Ministerio Fiscal.

58. Kan domen Tele2 Sverige och Watson anses ha inneburit en, mer eller mindre underförstådd, avvikelse från den praxis som följer av domen parlamentet/rådet och kommissionen? Det anser till exempel den irländska regeringen, som menar att det bara är den sistnämnda domen som är förenlig med den rättsliga grunden för direktiv 2002/58 och som iakttar artikel 4.2 FEU.[32]

59. Den franska regeringen anser å sin sida att man skulle kunna undvika motsägelsen om man ser till att den praxis som följer av domen Tele2 Sverige och Watson rör verksamhet i medlemsstaterna på straffrättens område, medan den praxis som följer av domen parlamentet/rådet och kommissionen rör statens säkerhet och försvaret. Det skulle innebära att den praxis som följer av domen Tele2 Sverige och Watson inte är tillämplig i förevarande mål, i vilket man i stället får se till den lösning som domstolen kom fram till i domen parlamentet/rådet och kommissionen.[33]

60. Som jag redan har nämnt anser jag att det kan finnas ett annat sätt att integrera de båda domarna än det som den franska regeringen har förespråkat. Jag instämmer inte med det sistnämnda, eftersom jag anser att övervägandena i domen Tele2 Sverige och Watson som uttryckligen rör bekämpning av terrorism,[34] även kan tillämpas på alla andra hot mot den nationella säkerheten (där terrorism bara är ett av flera).

3. Möjligheten att göra en samstämmig tolkning av domen parlamentet/rådet och kommissionen och domen Tele2 Sverige och Watson

61. Jag anser att domstolen i domarna Tele2 Sverige och Watson och Ministerio Fiscal beaktade skälen för undantags- och begränsningsklausulerna, liksom det systematiska förhållandet mellan de två typerna av klausuler.

62. Om domstolen i domen parlamentet/rådet och kommissionen fann att behandlingen av uppgifterna inte omfattades av tillämpningsområdet för direktiv 95/46, så berodde det, såsom jag erinrat om, på att inom ramen för samarbetet mellan Europeiska unionen och Förenta staterna, i ett typiskt internationellt sammanhang, borde den statliga dimensionen av verksamheten ges företräde framför den omständigheten att behandlingen även hade en kommersiell eller privat dimension. En av de frågor som var omtvistade i det målet var just vilken den lämpliga rättsliga grunden för det omtvistade beslutet var.

63. När det däremot gällde de nationella åtgärder som prövades i domen Tele2 Sverige och Watson och domen Ministerio Fiscal, beaktade domstolen i första hand det nationella tillämpningsområdet för behandlingen av uppgifter: den rättsliga ram inom vilken den genomfördes var uteslutande nationell och den saknade därför den yttre dimension som karaktäriserade föremålet för domen parlamentet/rådet och kommissionen.

30 *Ibidem*, punkt 75.

31 *Ibidem*, punkt 76.

32 Punkterna 15 och 16 i den irländska regeringens skriftliga yttrande.

33 Punkterna 34–50 i den franska regeringens skriftliga yttrande.

34 Domen Tele2 Sverige och Watson, punkterna 103 och 119.

64. Skillnaden i betydelse mellan den internationella och den nationella (kommersiella och privata) dimensionen av uppgiftsbehandlingen, fick till följd att det i det förstnämnda fallet slogs fast att en klausul om undantag från unionsrätten var den mest lämpade för att skydda det allmänna intresse som utgjordes av den nationella säkerheten. I det sistnämnda fallet kunde emellertid detta intresse tillgodoses på ett effektivt sätt med hjälp av den begränsningsklausul som föreskrivs i artikel 15.1 i direktiv 2002/58.

65. Det kan också anses föreligga en annan skillnad som hänger samman med de olika normativa sammanhangen: De båda domarna handlade om tolkningen av två bestämmelser som inte är likadana, även om det kan förefalla så.

66. Domen parlamentet/rådet och kommissionen handlade om tolkningen av artikel 3.2 i direktiv 95/46, medan domen Tele2 Sverige och Watson rörde artikel 1.3 i direktiv 2002/58. En noggrann granskning av dessa artiklar visar att det finns en skillnad som är tillräckligt stor för att motivera innebörden av domstolens domar i respektive mål.

67. I artikel 3.2 i direktiv 95/46 föreskrivs det att ”[d]etta direktiv *gäller inte för sådan behandling av personuppgifter* … som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten … 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”.[35]

68. I artikel 1.3 i direktiv 2002/58 föreskrivs däremot att direktivet ”*inte tillämpas på verksamheter* som faller utanför tillämpningsområdet för Fördraget om upprättandet av Europeiska gemenskapen … 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”.[36]

69. Medan artikel 3.2 i direktiv 95/46 utesluter sådan *behandling av uppgifter* som – såvitt här är av intresse – handlar om statens säkerhet, utesluter artikel 1.3 i direktiv 2002/58 sådan *verksamhet* som syftar till att skydda – såvitt här är av intresse – statens säkerhet.

70. Denna skillnad är inte betydelselös. Direktiv 95/46 uteslöt från sitt tillämpningsområde en verksamhet (”behandling av personuppgifter”) som vem som helst kan utföra. Från denna verksamhet undantogs uttryckligen sådan behandling som bland annat rörde statens säkerhet. Det saknade däremot betydelse vilken typ av *subjekt* som utförde behandlingen av uppgifterna. Den metod som användes för att identifiera de undantagna handlingarna var således teleologisk eller ändamålsinriktad och det spelade ingen roll vilka aktörer som utförde dem.

71. Detta visar att domstolen i målet parlamentet/rådet och kommissionen främst såg till syftet med behandlingen av uppgifterna. Det saknade betydelse att ”uppgifterna har samlats in av privata operatörer för kommersiella syften och att det är dessa operatörer som sköter överföringen av uppgifterna till en tredje stat”, eftersom det viktiga var att ”[d]enna överföring sker … inom en ram som inrättats av statsmakterna och som avser allmän säkerhet”.[37]

72. ”Verksamheter som rör statens säkerhet”, vilka faller utanför tillämpningsområdet för direktiv 2002/58 som prövades i målet Tele2 Sverige och Watson, gäller däremot inte vilken person som helst utan bara staten själv. I dessa verksamheter ingår dessutom inte statens lagstiftande funktion, utan enbart myndigheternas materiella agerande.

35 Min kursivering.

36 Min kursivering.

37 Domen parlamentet/rådet och kommissionen, punkt 58.

73. De *verksamheter* som nämns i artikel 1.3 i direktiv 2002/58 ”[avser] i samtliga fall … statens eller statliga myndigheters specifika verksamhet och … omfattas [inte] av enskildas verksamhetsområden”.[38] Dessa ”verksamheter” kan inte vara av lagstiftande karaktär. Om så hade varit fallet skulle alla bestämmelser som medlemsstaterna antar rörande behandling av personuppgifter falla utanför tillämpningsområdet för direktiv 2002/58, om de inte anses vara nödvändiga för att garantera statens säkerhet.

74. Dels skulle det påtagligt minska den ändamålsenliga verkan av direktivet, eftersom det skulle räcka att bara hänvisa till ett så vagt rättsligt begrepp som den nationella säkerheten för att de garantier som unionslagstiftaren har utformat för att skydda medborgarnas personuppgifter inte ska kunna tillämpas mot medlemsstaterna. Detta skydd är omöjligt utan medlemsstaternas medverkan och garantin för det säkerställs, för medborgarna, även gentemot de nationella myndigheterna.

75. Dels skulle en tolkning av begreppet ”statliga verksamheter” som innefattar sådana verksamheter som tar sig uttryck i lagstiftning medföra att artikel 15 i direktiv 2002/58 blev meningslös, en artikel som just ger medlemsstaterna rätt att – för att skydda bland annat den nationella säkerheten – genom ”lagstiftning” vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i direktivet.[39]

76. Såsom domstolen betonade i målet Tele2 Sverige och Watson ”[ska] tillämpningsområdet för direktiv 2002/58 … bedömas med hänsyn bland annat till direktivets allmänna systematik”.[40] En tolkning av artikel 1.3 och artikel 15.1 i direktiv 2002/58 som gör dem meningsfulla utan att de förlorar sin ändamålsenliga verkan, är således en tolkning som vad beträffar den förstnämnda artikeln identifierar ett materiellt undantag som rör medlemsstaternas *verksamheter* inom det nationella säkerhetsområdet (och motsvarande områden), och vad beträffar den sistnämnda bestämmelsen en befogenhet att anta *lagstiftning* (det vill säga allmänt tillämpliga bestämmelser) som för att skydda den nationella säkerheten påverkar verksamheter som bedrivs av individer som är underkastade medlemsstaternas makt och inskränker de rättigheter som garanteras i direktiv 2002/58.

4. Undantag för den nationella säkerheten i direktiv 2002/58

77. Den nationella säkerheten (eller det synonyma begreppet ”statens säkerhet”, enligt artikel 15.1) behandlas i två olika avseenden i direktiv 2002/58. För det första utgör den ett skäl för *undantag* (från direktivets tillämpning) för alla sådana verksamheter i medlemsstaterna som uttryckligen ”avser” statens säkerhet. För det andra utgör den ett skäl för *begränsning*, som ska vara föreskriven i lag, av de rättigheter och skyldigheter som fastställs i direktiv 2002/58, det vill säga i fråga om privata eller kommersiella verksamheter som faller utanför området för verksamheter som är förbehållna staten.[41]

38 Domen Ministerio Fiscal, punkt 32. Se, för ett liknande resonemang, domen Tele2 Sverige och Watson, punkt 72.

39 Det kan således knappast hävdas att artikel 15.1 i direktiv 2002/58 medger en inskränkning av rättigheter och skyldigheter som föreskrivs inom ett område som, liksom den nationella säkerheten, i princip faller utanför direktivets tillämpningsområde, enligt artikel 1.3 i själva direktivet. Såsom domstolen slog fast i punkt 73 i domen Tele2 Sverige och Watson, förutsätter artikel 15.1 i direktiv 2002/58 ”med nödvändighet att de där avsedda nationella åtgärderna … omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda”.

40 Domen Tele2 Sverige och Watson, punkt 67.

41 Såsom generaladvokat Saugmandsgaard Øe påpekade i punkt 47 i sitt förslag till avgörande i målet Ministerio Fiscal (C-207/16, EU:C:2018:300), ”är [det] viktigt att inte blanda samman å ena sidan personuppgifter som *direkt* behandlas inom ramen för statens verksamhet – av ’regal’ karaktär – på ett straffrättsligt område och å andra sidan personuppgifter som behandlas inom ramen för verksamhet – av kommersiell karaktär – som bedrivs av en leverantör av elektroniska kommunikationstjänster och som *därefter* används av behöriga statliga myndigheter”.

78. Vad är det då för verksamheter som avses i artikel 1.3 i direktiv 2002/58? Jag anser att Conseil d'État (Högsta förvaltningsdomstolen) själv ger ett bra exempel på det när den nämner artiklarna L. 851–5 och L. 851–6 i lagen om inre säkerhet och hänvisar till ”metoder för insamling av underrättelseuppgifter som tillämpas direkt av staten, men inte reglerar verksamheter som bedrivs av leverantörer av elektroniska kommunikationstjänster genom att ålägga dem specifika skyldigheter”. [42]

79. Jag anser att detta är av central betydelse för att klargöra omfattningen av undantaget i artikel 1.3 i direktiv 2002/58. Det omfattar inte *verksamheter* som myndigheterna bedriver för att skydda nationell säkerhet, utan att ålägga enskilda att samarbeta och således utan att ålägga dem skyldigheter i deras företagsledning.

80. Uppräkningen av de myndighetsverksamheter som är undantagna från det allmänna regelverket för behandling av personuppgifter ska emellertid tolkas restriktivt. Närmare bestämt får begreppet *nationell säkerhet*, som uteslutande faller under varje medlemsstats eget ansvar enligt artikel 4.2 FEU, inte utsträckas till att omfatta andra mer eller mindre närliggande områden inom den offentliga förvaltningen.

81. Eftersom dessa tolkningsfrågor innefattar enskilda (det vill säga aktörer som tillhandahåller elektroniska kommunikationstjänster för användarna) och inte bara verksamheter vid statliga myndigheter, är det inte nödvändigt att gå närmare in på avgränsningen av begreppet nationell säkerhet i egentlig mening.

82. Jag anser emellertid att vägledning kan hämtas från det kriterium som tillämpas i rambeslut 2006/960/RIF, [43] i vilket det i artikel 2 a görs åtskillnad mellan å ena sidan brottsbekämpande myndigheter i vid mening – vilka innefattar ”en nationell polismyndighet, tullmyndighet eller annan myndighet som enligt nationell lagstiftning har behörighet att upptäcka, förebygga och utreda brott eller brottslig verksamhet och utöva myndighetsutövning samt i samband härmed vidta tvångsåtgärder” – och å andra sidan ”organ eller enheter som arbetar särskilt med nationella säkerhetsfrågor”. [44]

83. I skäl 11 i direktiv 2002/58 anges att direktivet ”[i] likhet med direktiv 95/46/EG [inte] omfattar … sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av [unionslagstiftningen]”. Direktiv 2002/58 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 … statens säkerhet …”.

84. Det finns således en kontinuitet mellan direktiv 95/46 och direktiv 2002/58 när det gäller medlemsstaternas befogenheter beträffande nationell säkerhet. Inget av de två direktiven har till syfte att skydda grundläggande rättigheter inom just det området, där medlemsstaternas verksamheter inte ”regleras av [unionslagstiftningen]”.

85. Den ”jämvikt” som avses i det skälet följer av behovet av att medlemsstaternas befogenheter inom området nationell säkerhet ska iakttas, när de utövar dessa befogenheter *direkt och med egna resurser*. När det däremot, även av nyss nämnda skäl avseende nationell säkerhet, krävs att enskilda medverkar och de åläggs vissa skyldigheter, innebär denna omständighet att det blir fråga om ett område (det vill säga det skydd för privatlivet som krävs av dessa privata aktörer) som regleras av unionsrätten.

42 Punkterna 18 och 21 i beslutet att begära förhandsavgörande i mål C-511/18.

43 Rådets rambeslut av den 18 december 2016 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (EUT L 386, 2006, s. 89).

44 På samma sätt föreskrevs det i artikel 1.4 i rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 2008, s. 60) att rambeslutet ”inte [påverkar] viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet”.

86. Både direktiv 95/46 och direktiv 2002/58 syftar till att uppnå en sådan jämvikt genom att de tillåter att enskildas rättigheter får begränsas genom lagstiftningsåtgärder som medlemsstaterna vidtar med stöd av artikel 13.1 respektive artikel 15.1 i nämnda direktiv. Det finns i detta avseende ingen skillnad mellan de båda direktiven.

87. Vad beträffar förordning nr 2016/679, som innehåller en (ny) allmän ram för skydd av personuppgifter, föreskrivs det i artikel 2.2 att förordningen inte ska tillämpas på ”behandling av personuppgifter” när medlemsstaterna ”bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget”.

88. Medan behandlingen av personuppgifter bara kvalificerades på grundval av sitt syfte i direktiv 95/46, oberoende av vem som behandlade uppgifterna, identifieras den undantagna behandlingen i förordning nr 2016/679 både genom sitt syfte och i förhållande till vilka som behandlar uppgifterna. Undantag görs för behandling som utförs av medlemsstaterna i samband med att de bedriver en *verksamhet* som inte omfattas av unionsrätten (artikel 2.2 a och b), och sådan behandling som utförs av myndigheterna *för att bekämpa brott och för att skydda* mot hot mot den allmänna säkerheten. [45]

89. Dessa myndighetsverksamheter måste nödvändigtvis definieras snävt, för att unionslagstiftningen rörande skydd för privatlivet inte ska berövas sin ändamålsenliga verkan. I artikel 23 i förordning nr 2016/679 föreskrivs – vilket ligger i linje med artikel 15.1 i direktiv 2002/58 – att de rättigheter och skyldigheter som föreskrivs i direktivet får begränsas genom en *lagstiftningsåtgärd*, om det är nödvändigt för att skydda bland annat den nationella säkerheten, försvaret eller den allmänna säkerheten. Såsom redan nämnts skulle det, om skyddet av dessa syften utgjorde ett tillräckligt skäl för att en viss verksamhet ska undantas från tillämpningsområdet för förordning nr 2016/679, inte finnas något behov av att hänvisa till den nationella säkerheten för att motivera begränsningen, genom lagstiftningsåtgärder, av de rättigheter som garanteras i nämnda förordning.

90. Liksom är fallet med direktiv 2002/58, skulle det vara ologiskt att de lagstiftningsåtgärder som avses i artikel 23 i förordning nr 2016/679 (vilken som sagt medger att staten begränsar medborgarnas rätt till integritet av skäl som rör den nationella säkerheten) skulle omfattas av dess tillämpningsområde och att skyddet för den nationella säkerheten samtidigt utan vidare skulle medföra att förordningen inte är tillämplig, vilket skulle innebära att inga subjektiva rättigheter kan erkännas.

B. Bekräftelse av och möjligheter att utveckla den rättspraxis som följer av domen Tele2 Sverige och Watson

91. I mitt förslag till avgörande i mål C-520/18 gör jag en ingående bedömning [46] av domstolens praxis inom detta område, vilken mynnar ut i förslaget att denna praxis ska bekräftas samtidigt som jag föreslår ett sätt att tolka den för att precisera dess innehåll.

92. Jag hänvisar till den bedömningen och jag anser att den av ekonomiska skäl inte behöver återges här. Nedanstående reflektioner rörande Conseil d’Etats tolkningsfrågor ska således ses mot bakgrund av de relevanta punkterna i förslaget till avgörande i målet C-520/18.

45 Förordning nr 2016/679 utesluter således behandling av uppgifter som utförs av medlemsstaterna inom ramen för en *verksamhet* som inte omfattas av unionsrätten, och sådan behandling som utförs av myndigheterna *för att skydda* den allmänna säkerheten.

46 Punkterna 27–68.

C. Besvarande av tolkningsfrågorna

1. Skyldigheten att lagra uppgifterna (den första tolkningsfrågan i målen C-511/18 och C-512/18 och den andra tolkningsfrågan i mål C-512/18)

93. Vad beträffar den skyldighet att lagra uppgifter som åläggs leverantörer av elektroniska kommunikationstjänster, vill den hänskjutande domstolen närmare bestämt veta följande:

– Huruvida denna skyldighet, som föreskrivs med stöd av artikel 15.1 i direktiv 2002/58, utgör ett ingrepp som kan motiveras av rätten till personlig säkerhet enligt artikel 6 i stadgan och kraven på nationell säkerhet (den första frågan i målen C-511/18 och C-512/18, och den tredje frågan i mål C-511/18).

– Huruvida direktiv 2000/31 medger lagring av uppgifter som gör det möjligt att identifiera en person som har bidragit till skapandet av innehåll som är tillgängligt för allmänheten online (den andra frågan i mål C-512/18).

a) Inledande anmärkning

94. Conseil d'État hänvisar till de grundläggande rättigheter som säkerställs i artiklarna 7 (respekt för privatlivet och familjelivet), 8 (skydd av personuppgifter) och 11 (yttrandefrihet och informationsfrihet) i stadgan. Det är sådana rättigheter som enligt domstolen kan påverkas av den skyldighet att lagra trafikuppgifter som de nationella myndigheterna ålägger leverantörer av elektroniska kommunikationstjänster. [47]

95. Den hänskjutande domstolen hänvisar även till den rätt till personlig säkerhet som skyddas av artikel 6 i stadgan. Den hänvisar till den som en faktor som skulle kunna motivera åläggandet av denna skyldighet, snarare än en rättighet som eventuellt skulle kunna beröras.

96. Jag anser liksom kommissionen att en sådan hänvisning till artikel 6 kan vara vilseledande. I likhet med kommissionen anser jag att den bestämmelsen inte ska tolkas så att den är ägnad att ”ålägga unionen en positiv skyldighet att vidta åtgärder som syftar till att skydda personer mot brottsliga handlingar”. [48]

97. Den säkerhet som garanteras genom den artikeln i stadgan är inte liktydig med den allmänna säkerheten. Den kan sägas ha lika mycket att göra med den allmänna säkerheten som alla andra grundläggande rättigheter, eftersom den allmänna säkerheten är ett nödvändigt villkor för att de grundläggande rättigheterna och friheterna ska kunna garanteras.

98. Såsom kommissionen har erinrat om motsvarar artikel 6 i stadgan artikel 5 i Europakonventionen om de mänskliga rättigheterna (nedan kallad Europakonventionen), vilket framgår av förklaringarna till den. Av lydelsen av artikel 5 i Europakonventionen framgår att den ”säkerhet” som skyddas där är den rent personliga säkerheten, i betydelsen garanti av rätten till fysisk frihet mot godtyckliga frihetsberövanden eller godtyckligt förvar. Denna säkerhet innebär således att ingen ska kunna frihetsberövas, utom i de fall, på de villkor och enligt de förfaranden som lagen föreskriver.

47 Se domen Tele2 Sverige och Watson, punkt 92, med hänvisning, analogt, till domen Digital Rights, punkterna 25 och 70.

48 Punkt 37 i kommissionens skriftliga yttrande.

99. Det rör sig således om den *personliga säkerhet* som avser de villkor på vilka en persons fysiska frihet får begränsas [49] och inte om den *allmänna säkerhet* som är en grundförutsättning för att det ska finnas en stat och som är en nödvändig förutsättning i ett utvecklat samhälle för att myndighetsutövning och åtnjutande av individuella rättigheter ska kunna förenas.

100. Vissa regeringar vill emellertid att rätten till säkerhet snarare ska anses ha den sistnämnda innebörden. I själva verket har domstolen inte bortsett från den, utan tvärtom nämnt den uttryckligen i sina domar [50] och yttranden. [51] Domstolen har aldrig förnekat betydelsen av de mål av allmänt samhällsintresse som skyddet för den nationella säkerheten och den allmänna ordningen, [52] bekämpning av internationell terrorism i syfte att upprätthålla internationell fred och säkerhet och bekämpning av grov brottslighet i syfte att garantera allmän säkerhet utgör, [53] vilka den med rätta har funnit är ”av största betydelse”. [54] Domstolen har tidigare konstaterat att ”skyddet för den allmänna säkerheten [bidrar] till skyddet för andra människors fri- och rättigheter”. [55]

101. Domstolen skulle kunna utnyttja den möjlighet som förevarande mål innebär för att tydligare lyfta fram strävan efter en jämvikt mellan å ena sidan rätten till personlig säkerhet och å andra sidan rätten till privatliv och rätten till skydd av personuppgifter. På så sätt skulle domstolen kunna undvika att kritiseras för att de sistnämnda rättigheterna gynnas framför den förstnämnda.

102. Jag anser att denna jämvikt tas upp i skäl 11 och artikel 15.1 i direktiv 2002/58, där det anges att åtgärderna måste vara nödvändiga och proportionerliga *i ett demokratiskt samhälle*. Rätten till personlig säkerhet utgör som nämnts en oskiljaktig del av en demokratis själva existens och överlevnad, vilket motiverar att denna proportionalitet beaktas fullt ut i samband med bedömningen. Om upprätthållandet av principen om uppgiftssekretess är av största betydelse i ett demokratiskt samhälle, bör med andra ord inte heller betydelsen av dess säkerhet underskattas.

103. Det bör således beaktas om det föreligger allvarliga och ihållande hot mot den nationella säkerheten och i synnerhet risk för terrorism, i överensstämmelse med vad som anges i den sista meningen i punkt 119 i domen Tele2 Sverige och Watson. Ett nationellt system kan reagera i proportion till karaktären och styrkan hos de hot som det ställs inför, utan att denna reaktion nödvändigtvis behöver vara identisk med andra medlemsstaters.

104. Jag vill avslutningsvis tillägga att ovanstående reflektioner inte hindrar att det i verkligt *exceptionella* situationer där det föreligger ett överhängande hot eller en extraordinär risk som motiverar ett officiellt utlysande av nödläge i en medlemsstat, under en begränsad tid föreskrivs en möjlighet i den nationella lagstiftningen att införa en så omfattande och allmän skyldighet att lagra uppgifter som anses nödvändig. [56]

105. Följaktligen bör den första tolkningsfrågan i de båda målen om förhandsavgörande omformuleras och i stället inriktas på möjligheten att motivera ingreppet med nationella säkerhetsskäl. Frågan skulle då handla om huruvida den skyldighet som åläggs operatörer som tillhandahåller elektroniska kommunikationstjänster är förenlig med artikel 15.1 i direktiv 2002/58.

49 Detta är Europadomstolens tolkning. Se bland annat § 84 i dom av den 5 juli 2016, Buzadji mot Republiken Moldavien, ECHR:2016:0705JUD002375507, i vilken Europadomstolen slog fast att det grundläggande syftet med den rätt som erkänns i artikel 5 i Europakonventionen, är att förhindra godtyckliga eller omotiverade frihetsberövanden.

50 Domen Digital Rights, punkt 42.

51 Yttrande 1/15 (PNR-avtalet EU-Kanada) av den 26 juli 2017 (nedan kallat yttrande 1/15, EU:C:2017:592, punkt 149 och där angiven rättspraxis).

52 Dom av den 15 februari 2016, N (C-601/15 PPU, EU:C:2016:84, punkt 53).

53 Domen Digital Rights, punkt 42 och där angiven rättspraxis.

54 *Ibidem*, punkt 51.

55 Yttrande 1/15, punkt 149.

56 Se punkterna 105–107 i mitt förslag till avgörande i mål C-520/18.

b) Bedömning

1) Karaktärisering av de nationella bestämmelserna, så som de beskrivs i de två målen, mot bakgrund av domstolens praxis

106. Enligt besluten att begära förhandsavgörande, ålägger den omtvistade lagstiftningen i de nationella målen följande aktörer att lagra uppgifter:

– Operatörer som tillhandahåller elektronisk kommunikation, i synnerhet sådana vars verksamhet består i att erbjuda allmänheten tillgång till kommunikationstjänster online.

– 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. [57]

107. Operatörerna ska i ett år från och med den dag då den registrerades lagra information som gör det möjligt att identifiera användaren, uppgifter om den terminalutrustning för kommunikation som använts, tekniska egenskaper, datum, klockslag och varaktighet för varje samtal, uppgifter om kompletterande tjänster som har efterfrågats eller använts och leverantörerna av dessa tjänster, samt uppgifter som gör det möjligt att identifiera kommunikationens mottagare och, när det rör sig om telefoni, kommunikationens ursprung och lokalisering. [58]

108. När det särskilt rör sig om internetanslutningstjänster och lagringstjänster, tycks den nationella lagstiftningen kräva lagring av IP-adresser, [59] lösenord och, om det finns ett avtal eller ett betalkonto, vilken typ av betalning som gjorts, samt referens, belopp och datum och klockslag för transaktionen. [60]

109. Denna skyldighet att spara uppgifter föreligger för att brott ska kunna utredas, fastställas och bekämpas. [61] Det innebär att till skillnad från vad som är fallet med skyldigheten att *samla in* trafikuppgifter och lokaliseringsuppgifter – vilket jag ska återkomma till – syftar skyldigheten att *lagra dem* inte bara till att förebygga terrorism. [62]

110. Vad beträffar villkoren för *tillgång* till de lagrade uppgifterna, framgår det av den information som föreligger i målet att det antingen är de som föreskrivs för det allmänna systemet (medverkan av den rättsliga myndigheten) eller så är denna tillgång förbehållen individuellt utsedda aktörer med befogenheter, efter godkännande av premiärministern utfärdat på grundval av ett icke bindande yttrande från en oberoende förvaltningsmyndighet. [63]

57 Detta följer av artikel L. 851–1 i lagen om inre säkerhet, i vilken det hänvisas till artikel L. 34–1 i lagen om post och elektronisk kommunikation och till artikel 6 i lag nr 2004–575 om förtroendet för den digitala ekonomin.

58 Detta föreskrivs i artikel R. 10–13 i lagen om post och elektronisk kommunikation.

59 Det ankommer på den hänskjutande domstolen att undersöka denna fråga, kring vilken det rådde oenighet vid förhandlingen.

60 Artikel 1 i dekret nr 2011–219.

61 Artikel R. 10–13 i lagen om post och elektronisk kommunikation.

62 Såväl La Quadrature du Net som Fédération des fournisseurs d'accès á Internet associatifs betonar den mängd olika syften som finns med lagringen, myndigheternas utrymme för skönsmässig bedömning, avsaknaden av objektiva kriterier när den definieras och den betydelse som tillmäts vissa former av brottslighet som inte kan betecknas som grov.

63 Commission nationale de contrôle des techniques de renseignement (nationell tillsynsmyndighet för underrättelseteknik). Se, beträffande detta, punkterna 145–148 i den franska regeringens skriftliga yttrande.

111. Såsom kommissionen har påpekat [64] kan det lätt konstateras att de uppgifter som ska lagras enligt de nationella bestämmelserna, i allt väsentligt överensstämmer med de uppgifter som domstolen prövade i domarna Digital Rights och Tele2 Sverige och Watson. [65] Nu liksom då omfattas dessa uppgifter av en ”generell och odifferentierad lagringsskyldighet”, vilket Conseil d’État helt uppriktigt betonar i början av sina tolkningsfrågor.

112. Om så är fallet, vilket det ankommer på den hänskjutande domstolen att pröva, kan ingen annan slutsats dras än att lagstiftningen i fråga medför ett ”ingrepp i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan [som] är långtgående och måste betraktas som synnerligen allvarligt”. [66]

113. Ingen av parterna i målet har ifrågasatt att bestämmelser av det här slaget utgör ett ingrepp i dessa rättigheter. Det är inte nödvändigt att gå närmare in på detta här, inte ens för att erinra om att en inskränkning av dessa rättigheter oundvikligen skadar själva grunderna för ett samhälle som har för avsikt att bland annat värna om den personliga integritet som stadfästs i stadgan.

114. Tillämpas den rättspraxis som följer av domen Tele2 Sverige och Watson och som senare bekräftades i domen Ministerio Fiscal, kan det utan vidare hävdas att en nationell lagstiftning som den som är aktuell här ”överskrider … gränserna för vad som är strängt nödvändigt och [inte] kan … anses 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”. [67]

115. Liksom den lagstiftning som var föremål för prövning i domen Tele2 Sverige och Watson, omfattar den här aktuella lagstiftningen ”på ett generellt sätt … samtliga abonnenter och registrerade användare och avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter … [och] det … görs [inte] några åtskillnader, begränsningar eller undantag utifrån det eftersträvade syftet”. [68] Följaktligen är den ”även tillämplig på personer beträffande vilka det inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med grov brottslighet”. Den föreskriver heller inte några undantag ”vilket innebär att den även är tillämplig på personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt”. [69]

116. Den omtvistade lagstiftningen ”kräver inte något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten. Den är 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 allvarligt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av brott.” [70]

117. Härav följer att denna lagstiftning ”överskrider … gränserna för vad som är strängt nödvändigt och … inte [kan] anses 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”. [71]

64 Punkt 60 i kommissionens skriftliga yttrande.

65 I själva verket är de lite mer omfattande, eftersom det även tycks föreskrivas att IP-adresser eller lösenord ska lagras när det gäller internetanslutningstjänster.

66 Domen Tele2 Sverige och Watson, punkt 100.

67 *Ibidem*, punkt 107.

68 *Ibidem*, punkt 105.

69 Se föregående fotnot.

70 Domen Tele2 Sverige och Watson, punkt 106.

71 *Ibidem*, punkt 107.

118. Detta var tillräckligt för att domstolen skulle dra slutsatsen att de därmed förknippade nationella bestämmelserna inte var förenliga med artikel 15.1 i direktiv 2002/58, eftersom de ”i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel”. [72]

119. Den fråga som nu uppkommer är om domstolens praxis rörande lagring av personuppgifter kan, om inte omprövas så åtminstone nyanseras, när syftet med denna ”generella och odifferentierade” lagring är att bekämpa terrorism. Den första frågan i mål C-511/18 ställs just ”i ett sammanhang som präglas av ihållande, allvarliga hot mot den nationella säkerheten, i synnerhet risken för terrorism”.

120. Även om detta är det *faktiska sammanhang* i vilket skyldigheten att lagra uppgifterna åläggs, så handlar den i sitt *normativa sammanhang* inte bara om terrorism. I det system för lagring av och tillgång till uppgifter som är omtvistat i målet vid Conseil d’État, föreligger denna skyldighet om syftet är att utreda, fastställa och bekämpa brott i allmänhet.

121. Jag vill under alla förhållanden erinra om att domstolen i sitt resonemang i domen Tele2 Sverige och Watson inte bortsåg från bekämpning av terrorism, men att domstolen då inte fann att denna brottsform krävde att den gjorde avsteg från sin praxis. [73]

122. I princip anser jag därför att den hänskjutande domstolens fråga, som särskilt handlar om terrorhot, bör besvaras på samma sätt som domstolen gjorde i domen Tele2 Sverige och Watson.

123. Såsom jag angav i mitt förslag till avgörande i målet Stichting Brein kräver ”[e]n säker rättstillämpning … visserligen inte att domstolarna utan undantag ska tillämpa principen om att appellationsdomstolar är bundna av sina egna avgöranden i principfrågor och att den högsta instansens avgöranden är bindande för underinstanserna (stare decisis), men däremot att de ska vinnlägga sig om att hålla sig till vad de själva, efter moget övervägande, har beslutat rörande ett visst rättsligt problem”. [74]

2) En begränsad lagring av uppgifter vid hot mot statens säkerhet, däribland terrorhot

124. Skulle det då vara möjligt att nyansera eller komplettera denna praxis, mot bakgrund av de konsekvenser den får för bekämpning av terrorism eller för statens skydd mot andra liknande hot mot den nationella säkerheten?

72 *Ibidem*, punkt 112.

73 *Ibidem*, punkt 103.

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

125. Jag har redan betonat att lagring av uppgifter i sig innebär ett ingrepp i de rättigheter som stadfästs i artiklarna 7, 8 och 11 i stadgan.[75] Oavsett om syftet med den när allt kommer omkring är att möjliggöra *tillgång*, i efterhand eller samtidigt, till uppgifterna vid en viss tidpunkt,[76] innebär en lagring av uppgifter som går utöver vad som är strikt nödvändigt för att överföra en kommunikation eller för att fakturera de tjänster som leverantören tillhandahåller, ett överskridande av de gränser som föreskrivs i artiklarna 5 och 6 i direktiv 2002/58.

126. De som använder sig av dessa tjänster (i själva verket nästan alla medborgare i de mest utvecklade samhällena) har, eller borde ha, rätt att förvänta sig att inga andra uppgifter om dem lagras än de som lagras i enlighet med de bestämmelserna om de inte har lämnat sitt samtycke till det. Undantagen i artikel 15.1 i direktiv 2002/58 ska ses mot bakgrund av denna premiss.

127. Såsom jag tidigare har förklarat slog domstolen i domen Tele2 Sverige och Watson fast att en generell och odifferentierad lagring av personuppgifter inte är tillåten, inte heller i samband med bekämpning av terrorism.[77]

128. När det gäller den kritik som framförts, anser jag inte att den praxis som följer av den domen underskattar terrorhot, vilket är en särskilt allvarlig form av brottslighet som har till uttryckligt syfte att undergräva statens auktoritet och destabilisera eller förstöra dess institutioner. Att bekämpa terrorism är bokstavligen av vital betydelse för staten och att lyckas med det är ett oundvikligt mål av allmänt samhällsintresse för en rättsstat.

129. Praktiskt taget alla regeringar som medverkat i målet, liksom kommissionen, är eniga om att en partiell och differentierad lagring, förutom de tekniska svårigheterna med detta skulle beröva de nationella underrättelsetjänsterna möjligheten att få tillgång till information som är nödvändig för att identifiera hot mot den allmänna säkerheten och mot statens försvar, och för att lagföra dem som gör sig skyldiga till terroristdåd.[78]

130. Det bör i detta sammanhang påpekas att man vid bekämpning av terrorism inte bara kan se till hur effektiv den är. Det är där svårigheten med denna bekämpning ligger, men också dess storhet när medlen och metoderna för det är förenliga med rättsstatens krav, vilka framför allt innebär att maktutövningen och tvånget är underkastade de rättsliga begränsningarna och framför allt en rättsordning vars existensberättigande bygger på försvaret av de grundläggande rättigheterna.

131. Medan det enda kriterium som rättfärdigar terrorismens medel är att den ska vara (maximalt) effektiv i sina angrepp på den rådande ordningen, måste när det gäller effektiviteten hos försvaret av rättsstaten hänsyn tas till de förfaranden och garantier som gör den till en legitim ordning. Om rättsstaten bara skulle se till effektiviteten skulle den förlora den egenskap som utmärker den och den

75 Domstolen har i punkt 124 i yttrande 1/15 erinrat om att ”utlämnande av personuppgifter till tredje man, såsom en myndighet, utgör ett ingrepp i den grundläggande rättighet som är stadfäst i artikel 7 i stadgan, oavsett vilken användning som de utlämnade uppgifterna senare blir föremål för. Det förhåller sig på samma sätt med lagringen av personuppgifter och åtkomsten till sådana uppgifter i syfte att myndigheter ska använda sig av dem. Det har i detta hänseende föga betydelse huruvida de uppgifter som avser privatlivet är av känslig art eller huruvida de berörda har fått utstå eventuella olägenheter på grund av ingreppet eller inte”.

76 Såsom generaladvokat Cruz Villalón påpekade i punkt 72 i sitt förslag till avgörande i målet Digital Rights, C-293/12 och C-594/12 (EU:C:2013:845) ”[utgör] insamlingen och framför allt lagringen i enorma databaser av en stor mängd olika uppgifter som genererats eller behandlats och som avser huvuddelen av unionsmedborgarnas dagliga elektroniska kommunikationer … ett väsentligt intrång i deras privatliv, också om det endast skapar möjlighet till kontroll i efterhand av deras privata och yrkesmässiga förehavanden.. Insamlingen av dessa uppgifter skapar förutsättningar för en övervakning som, även om den endast utövas retroaktivt i samband med att uppgifterna används, ändå på ett permanent sätt under hela den tid uppgifterna finns lagrade hotar unionsmedborgarnas rätt till skydd för privatlivets helgd. Den vaga känsla av att vara övervakad som detta skapar gör frågan om lagringstiden för uppgifterna särskilt angelägen”.

77 Domen Tele2 Sverige och Watson, punkt 103: ”kan … inte … motivera att en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter ska anses vara nödvändig för detta ändamål”.

78 Detta är till exempel den franska regeringens uppfattning och den pekar på konkreta exempel med nyttan av en generell lagring av uppgifter, som gjort det möjligt för staten att reagera på de allvarliga terrordåd som landet utsatts för på senare år (punkterna 107 och 122–126 i den franska regeringens skriftliga yttrande).

skulle i ytterlighetsfall själv kunna bli till ett hot mot medborgarna. Om myndigheterna skulle utrustas med orimliga instrument för att bekämpa brott, med vilka de skulle kunna bortse från eller undergräva de grundläggande rättigheterna, finns det inget som garanterar att deras okontrollerade och helt fria agerande i slutändan inte leder till att allas frihet inskränks.

132. Medborgarnas grundläggande rättigheter utgör en gräns för myndigheternas effektivitet som inte får överskridas och begränsningar av dessa rättigheter ska enligt artikel 52.1 i stadgan vara föreskrivna i lag och förenliga med deras väsentliga innehåll och de får endast göras ”om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter”. [79]

133. Vad beträffar villkoren för att en *riktad* lagring av uppgifter ska vara tillåten, enligt domen Tele2 Sverige och Watson, hänvisar jag till mitt förslag till avgörande i målet C-520/18. [80]

134. Omständigheter där den information som de brottsbekämpande myndigheterna förfogar över kan bekräfta välgrundade misstankar om förberedelse till terrordåd kan innebära att det är legitimt att ålägga en skyldighet att lagra vissa uppgifter. Det gäller i än högre grad när ett terrordåd i själva verket har begåtts. Medan förövandet av brottet i det sistnämnda fallet i sig kan vara en omständighet som motiverar att en sådan åtgärd vidtas, måste vid misstanke om ett eventuellt dåd de omständigheter som ligger till grund för misstanken uppvisa en viss grad av sannolikhet så att en objektiv bedömning kan göras av de indicier som kan motivera åtgärden.

135. Även om det är svårt, så är det inte omöjligt att med precision och på grundval av objektiva kriterier avgöra vilka kategorier av uppgifter vars lagring bedöms som oumbärlig och vilken personkrets som berörs. Det mest *praktiska och effektiva* vore visserligen att generellt och utan åtskillnad lagra alla uppgifter som leverantörer av elektroniska kommunikationstjänster kan komma att samla in, men som jag tidigare har påpekat kan frågan inte avgöras i termer av praktisk effektivitet, utan av rättslig effektivitet inom ramen för en rättsstat.

136. Det är typiskt sett en uppgift för lagstiftaren att avgöra frågor av nyss nämnt slag, inom ramen för de gränser som domstolen har uppställt i sin praxis. Jag hänvisar även på denna punkt till min bedömning i mitt förslag till avgörande i målet C-520/18. [81]

79 Dom av den 15 februari 2016, N (C-601/15 PPU, EU:C:2016:84, punkt 50). Det handlar således om den svåra balansen mellan den allmänna ordningen och friheten som jag tidigare har beskrivit och som i princip all unionslagstiftning eftersträvar att uppnå. Ett exempel på det är Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 2017, s. 6). Samtidigt som det i artikel 20.1 föreskrivs att medlemsstaterna ska säkerställa att ”effektiva utredningsverktyg … är tillgängliga för” de som har ansvaret för att utreda eller lagföra terroristbrott, anges det i skäl 21 att användningen av dessa effektiva verktyg ”bör vara riktad och ske med beaktande av proportionalitetsprincipen och arten och allvaret hos de brott som utreds och med iakttagande av rätten till skydd av personuppgifter”.

80 Punkterna 87–95.

81 Punkterna 100–107.

3) Tillgång till lagrade uppgifter

137. Om det förutsätts att operatörerna har samlat in uppgifterna i enlighet med bestämmelserna i direktiv 2002/58 och att de har lagrats i enlighet med artikel 15.1 i direktivet,[82] ska de behöriga myndigheterna ges tillgång till uppgifterna på de villkor som domstolen har slagit fast och som jag har undersökt i mitt förslag till avgörande i målet C-520/18, till vilket jag hänvisar.[83]

138. Även i det fallet måste det i den nationella lagstiftningen anges vilka materiella och formella villkor som gäller för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna.[84] I förevarande mål medges enligt dessa villkor tillgång till uppgifter om personer som misstänks planera, ha för avsikt att begå, ha begått eller kunna vara inblandade i en terroristhandling.[85]

139. Förutom i vederbörligen underbyggda brådskande fall gäller likväl att tillgång till de aktuella uppgifterna ska vara underkastad förhandskontroll av en domstol eller oberoende förvaltningsmyndighet vars beslut utgör svar på en motiverad begäran från de behöriga myndigheterna.[86] Detta innebär att i de fall där det inte är möjligt att göra en abstrakt bedömning enligt lagen, säkerställs en konkret bedömning av den oberoende förvaltningsmyndigheten, som ålägger sig både att skydda den nationella säkerheten och att försvara medborgarnas grundläggande rättigheter.

4) Skyldighet att lagra uppgifter som gör det möjligt att identifiera de personer som skapar innehåll, mot bakgrund av direktiv 2000/31 (den andra tolkningsfrågan i mål C-512/18)

140. Den hänskjutande domstolen hänvisar till direktiv 2000/31 som referenspunkt för att få klarlagt huruvida det är möjligt att ålägga vissa personer[87] och operatörer som tillhandahåller kommunikationstjänster till allmänheten 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”.

141. Jag anser liksom kommissionen att det saknas skäl att pröva om denna skyldighet är förenlig med direktiv 2000/31,[88] eftersom det i skäl 1.5 b i det direktivet anges att det inte ska tillämpas på ”frågor beträffande informationssamhällets tjänster som omfattas av direktiv 95/46/EG och direktiv 97/66/EG”, vilka nu motsvaras av förordning nr 2006/679 och direktiv 2002/58,[89] i vilka artiklarna 23.1 respektive 15.1 enligt min uppfattning ska tolkas på det sätt som jag redovisat ovan.

82 Under förutsättning att de villkor som nämns i punkt 122 i domen Tele2 Sverige och Watson är uppfyllda: Domstolen har erinrat om att artikel 15.1 i direktiv 2002/58 inte medger att medlemsstaterna avviker från artikel 4.1 och 4.1a i direktivet, enligt vilken leverantörerna ska vidta åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna. Domstolen slog fast att ”[m]ed hänsyn till att det är fråga om en stor mängd uppgifter och att dessa är av känslig natur samt att det finns en risk för otillåten tillgång till uppgifterna, måste leverantörerna av elektroniska kommunikationstjänster, för att säkerställa fullständig integritet och konfidentialitet för uppgifterna, garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder. Den nationella lagstiftningen måste i synnerhet föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut.”

83 Punkterna 52–60.

84 Domen Tele2 Sverige och Watson, punkt 118.

85 *Ibidem*, punkt 119.

86 *Ibidem*, punkt 120.

87 Sådana som ”lagrar … för tillhandahållandet av kommunikationstjänster online till allmänheten … alla former av signaler, skrift, bilder, ljud eller meddelanden som tillhandahållits av mottagarna till dessa tjänster”.

88 Detta direktiv nämner den hänskjutande domstolen i den andra frågan i mål C-512/18, i generella ordalag och utan att precisera någon bestämmelse i det.

89 Punkterna 112 och 113 i kommissionens skriftliga yttrande.

2. Skyldigheten att samla in trafik- och lokaliseringsuppgifter i realtid (den andra frågan i mål C-511/18)

142. Enligt den hänskjutande domstolen medger artikel L 851–2 i lagen om inre säkerhet, i det enda syftet att förebygga terrorism, insamling av information i realtid om personer som dessförinnan har identifierats som misstänkta för att ha anknytning till ett terrorhot. På samma sätt medger artikel L. 851–4 i samma lag att operatörerna i realtid överför tekniska uppgifter om lokaliseringen av terminalutrustningar.

143. Enligt den hänskjutande domstolen ålägger dessa metoder inte leverantörerna någon ytterligare lagringsskyldighet än den som krävs för fakturering och marknadsföring av deras tjänster.

144. Enligt artikel L. 851–3 i lagen om inre säkerhet får dessutom operatörer som tillhandahåller elektroniska kommunikationsnät och elektroniska kommunikationstjänster åläggas att ”på sina nät tillämpa automatisk behandling i syfte att, enligt de parametrar som anges i tillståndet, spåra uppkopplingar som kan avslöja terroristhot”. Denna metod medför inte någon generell och odifferentierad lagring av uppgifter, utan syftet med den är att under en begränsad tid samla in uppkopplingsuppgifter som kan ha samband med ett brott av terroristkaraktär.

145. Jag anser att de villkor som ska vara uppfyllda för att få tillgång till lagrade personuppgifter även ska tillämpas på tillgång i realtid till uppgifter som genereras i samband med elektronisk kommunikation. Jag hänvisar därför till det jag tidigare redovisat rörande dessa villkor. Huruvida det rör sig om lagrade uppgifter eller om uppgifter som inhämtats omgående är irrelevant, eftersom man i båda fallen får kännedom om personuppgifter och det saknar betydelse om de är historiska eller aktuella.

146. Om tillgången i realtid skulle vara en följd av uppkopplingar som upptäckts med hjälp av en automatisk behandling, som den som nämns i artikel L. 851–3 i lagen om inre säkerhet, måste de förhandsbestämda modellerna och kriterierna för den behandlingen vara specifika, tillförlitliga och icke-diskriminerande, för att göra det möjligt att peka ut enskilda mot vilka det kan föreligga en skälig misstanke om delaktighet i terroristbrott. [90]

3. Skyldigheten att informera de berörda personerna (den tredje frågan i mål C-511/18)

147. Domstolen har slagit fast att myndigheter som beviljats tillgång till lagrade uppgifter ska informera de berörda personerna om detta, under förutsättning att det inte riskerar att skada myndigheternas utredningar. Skälet till denna skyldighet är att den informationen är nödvändig för att dessa personer ska kunna utöva sin rätt till rättslig prövning, vilken uttryckligen nämns i artikel 15.2 i direktiv 2002/58, vid kränkning av deras rättigheter. [91]

148. Conseil d’État vill med sin tredje fråga i mål C-511/18 få klarlagt om detta krav på information alltid gäller eller om undantag från kravet kan medges när andra garantier har föreskrivits, som de som den beskriver i beslutet att begära förhandsavgörande.

149. Enligt den hänskjutande domstolens redogörelse [92] utgörs dessa garantier av en möjlighet för den som vill kontrollera om en informationsmetod har använts på ett olagligt sätt att vända sig till Conseil d’État. Conseil d’État kan eventuellt upphäva godkännandet av åtgärden och besluta att de insamlande uppgifterna ska förstöras, inom ramen för ett förfarande i vilket den vanliga kontradiktoriska principen för domstolsförfaranden inte tillämpas.

90 Domen Digital Rights, punkt 59.

91 Domen Tele2 Sverige och Watson, punkt 121.

92 Punkterna 8–11 i beslutet att begära förhandsavgörande.

150. Den hänskjutande domstolen anser att den lagstiftningen inte åsidosätter rätten till rättslig prövning. Jag anser att det rent teoretiskt skulle kunna förhålla sig så för den som vill kontrollera om han eller hon är föremål för en underrättelseoperation. Den rätten iakttas däremot inte om den som är eller har varit föremål för en sådan operation inte upplyses om detta och därmed inte ens kan få prövat om hans eller hennes rättigheter har åsidosatts eller inte.

151. Det processrättsliga skydd som den hänskjutande domstolen hänvisar till, tycks förutsätta att den som misstänker att han eller hon är föremål för insamling av information om honom eller henne själv tar initiativ till skyddet. Tillgången till en effektiv domstolsprövning för att tillvarata sina rättigheter bör emellertid gälla för alla, vilket innebär att den som varit utsatt för en behandling av personuppgifter ska ha möjlighet att i domstol få prövat om denna behandling har varit laglig och därmed bör han eller hon få kännedom om dess existens.

152. Det framgår emellertid av den information som har tillhandahållits att domstolsprövningen kan ske ex officio eller genom en anmälan från myndigheterna, men den berörda personen bör under alla förhållanden ges möjlighet att själv ta initiativ till den och det är därför nödvändigt att han eller hon känner till att personuppgifterna har varit föremål för en viss behandling. Försvaret av hans eller hennes rättigheter kan inte göras avhängigt av att han eller hon får kännedom om behandlingen genom tredje man eller på eget initiativ.

153. I den mån det inte skadar den utredning för vilken tillgången till de lagrade uppgifterna har beviljats, bör den berörda personen således informeras om denna tillgång.

154. En annan fråga är huruvida det domstolsförfarande som genomförs efter det att den berörda personen har initierat en domstolsprövning när han eller hon har fått kännedom om tillgången till uppgifterna, uppfyller kraven på konfidentialitet och sekretess som föreligger vid prövning av myndigheternas agerande inom känsliga områden som statens säkerhet och försvar. Denna fråga faller emellertid utanför ramen för detta mål och jag anser därför att domstolen inte ska uttala sig om den.

V. Förslag till avgörande

155. Mot bakgrund av det ovan anförda föreslår jag att domstolen ger följande svar till Conseil d'État:

”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), jämförd med artiklarna 7, 8 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas enligt följande.

1) Denna artikel utgör hinder för nationell lagstiftning varigenom operatörerna och de som tillhandahåller elektroniska kommunikationer, i ett sammanhang som präglas av ihållande, allvarliga hot mot den nationella säkerheten, i synnerhet risken för terrorism, åläggs en generell och odifferentierad skyldighet att lagra trafik- och lokaliseringsuppgifter avseende alla abonnenter, samt uppgifter som gör det möjligt att identifiera de personer som skapar det innehåll som leverantörerna tillhandahåller.

2) Denna artikel utgör hinder för nationell lagstiftning där det inte föreskrivs en skyldighet att informera de berörda personerna om de behöriga myndigheternas behandling av deras personuppgifter, såvida inte denna information skadar myndigheternas verksamhet.

3) Denna artikel utgör inte hinder för nationell lagstiftning enligt vilken det är tillåtet att i realtid samla in trafik- och lokaliseringsuppgifter avseende enskilda personer, i den mån sådana åtgärder vidtas i enlighet med de förfaranden som föreskrivs för tillgång till personuppgifter som lagligen har lagrats samt med samma garantier.”