Rättsfallssamlingen

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

Mål C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
mot
Conseil des ministres,
ytterligare deltagare i rättegången:
Child Focus

(begäran om förhandsavgörande från Cour constitutionnelle (Författningsdomstolen, Belgien))

”Begäran om förhandsavgörande – Behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation – Direktiv 2002/58/EG – Tillämpningsområde – Artikel 1.3 – Artikel 15.1 – Artikel 4.2 FEU – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 4, 6–8, 11 och 52.1 – Generell skyldighet att lagra trafik- och lokaliseringsuppgifter – Brottsutredningars effektivitet och andra mål av allmänt intresse”

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 ett oproportionerligt ingrepp i de rättigheter som säkerställs i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna.

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).

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

– 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 och 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 förhandsavgörande. Detta gäller fyra olika mål,[7] och jag föredrar 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 bekämpande 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 i slutändan 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.

5. När Cour constitutionnelle (Författningsdomstolen, Belgien) fick kännedom om domen Digital Rights ogiltigförklarade den de nationella bestämmelser som delvis hade införlivat direktiv 2006/24 med den nationella rätten, eftersom direktivet ogiltigförklarades i den domen. Den belgiska lagstiftaren antog då nya bestämmelser, vilkas förenlighet med unionsrätten också har ifrågasatts till följd av domen Tele2 Sverige och Watson.

6. Ett särdrag hos denna begäran om förhandsavgörande är att den aktualiserar möjligheten att tillfälligt förlänga rättsverkningarna av en nationell bestämmelse som de nationella domstolarna ska ogiltigförklara på grund av att den är oförenlig med unionsrätten.

I. Tillämpliga bestämmelser

A. Unionsrätt

7. Jag hänvisar till den motsvarande punkten i mitt förslag till avgörande i målen C-511/18 och C-512/18.

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).

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

7 Förutom förevarande mål (mål C-520/18, Ordre des barreaux francophones et germanophone m.fl.) handlar det om de förenade målen C-511/18 och C-512/18, La Quadrature du Net m.fl., och mål C-623/17, Privacy International.

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.

B. Nationell rätt. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. I artikel 4 föreskrivs att artikel 126 i loi du 13 juin 2005 relative aux communications électroniques [12] ska ha följande lydelse:

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

Denna artikel berör inte innehållet i kommunikationen.

…

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

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

2.º Underrättelse- och säkerhetstjänster, för att genomföra underrättelseuppdrag och använda sig av de metoder för uppgiftsinsamling som avses i artiklarna 16/2, 18/7 och 18/8 i loi du 30 1998 organique des services de renseignement et de Sécurité [13] och på de villkor som föreskrivs i denna lag.

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

4.º Räddningstjänst som tillhandahåller hjälp på plats, när den efter ett nödsamtal inte kan få uppgifter, eller endast får ofullständiga eller felaktiga uppgifter, om den uppringandes identitet från den berörda leverantören eller operatören …. Endast uppgifter om den uppringandes identitet får begäras, och det måste ske inom 24 timmar efter samtalet.

5.º Polistjänsteman vid den federala polisens enhet med ansvar för sökande efter försvunna personer, inom ramen för sin uppgift att bistå personer i fara och eftersöka personer vilkas försvinnande är oroande och när det kan antas eller föreligger tydliga indikationer på att den försvunna personen befinner sig i omedelbar fysisk fara. Endast sådana uppgifter som avses i

11 Lagen av den 29 maj 2016 om insamling och lagring av uppgifter inom sektorn för elektronisk kommunikation, nedan kallad lagen av den 29 maj 2016 (Moniteur belge av den 18 juli 2016, s. 44717).

12 Lagen av den 13 juni 2005 om elektronisk kommunikation, nedan kallad 2005 års lag (*Moniteur belge* av den 20 juni 2005, s. 28070).

13 Lagen av den 30 november 1998 om underrättelse- och säkerhetstjänster, nedan kallad 1998 års lag (*Moniteur belge* av den 18 december 1998, s. 40312).

punkt 3 första och andra styckena, som rör den försvunna personen och som lagrats under 48 timmar före begäran om att få ut uppgifterna kan begäras från den berörda operatören eller leverantören genom den polismyndighet som utses av Konungen.

6.º Medlingstjänsten för telekommunikationer, för att identifiera en person som gjort en felaktig användning av ett nät eller av elektroniska kommunikationstjänster. … Endast identitetsuppgifter kan begäras ut.

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

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

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

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

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

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

4. För lagring av de uppgifter som avses i punkt 3, ska de leverantörer och operatörer som avses i punkt 1 första stycket

1.º säkerställa att de lagrade uppgifterna är av samma kvalitet och omfattas av samma säkerhets- och skyddskrav som uppgifterna i nätverket,

2.º se till att de lagrade uppgifterna omfattas av lämpliga tekniska och organisatoriska åtgärder för att skyddas mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust eller ändring eller otillåten eller olaglig lagring, behandling, tillgång eller avslöjande,

3.º garantera att det endast är en eller flera av medlemmarna i den samordningsgrupp som avses i artikel 126/1.1 som har tillgång till de uppgifter som lagrats för att kunna besvara en begäran från de myndigheter som avses i punkt 2,

4.º lagra uppgifterna inom Europeiska unionens territorium,

5.º vidta tekniska skyddsåtgärder som direkt vid lagringen gör uppgifterna oläsliga och oanvändbara för alla personer som inte är behöriga att få tillgång till dem,

6.º förstöra uppgifter lagrade på alla slags medier när tidsperioden för lagring av den typen av uppgifter, som stadgas i punkt 3, löper ut, dock utan att det påverkar tillämpningen av artiklarna 122 och 123, och

7.º säkerställa att användningen av lagrade uppgifter är spårbar för varje begäran om att få tillgång till dessa uppgifter från en sådan myndighet som avses i punkt 2.

Spårbarheten enligt första stycket 7° utförs med en loggbok. Institutet och Kommissionen för integritetsskydd kan konsultera loggboken eller begära att få en kopia av hela eller delar av loggboken. Institutet och Kommissionen för integritetsskydd ska ingå ett samarbetsavtal angående inhämtandet av upplysningar om och kontrollen över loggbokens innehåll.

5. Ministern och justitieministern ska varje år till representanthuset skicka statistik över lagring av uppgifter som genererats eller behandlats inom ramen för tillhandahållande av tjänster eller kommunikationsnät som är tillgängliga för allmänheten.

Denna statistik ska bland annat omfatta följande:

1º De fall där information skickats till behöriga myndigheter i enlighet med nationell lagstiftning.

2º Den tid som förflutit mellan den tidpunkt då uppgifterna har lagrats och den tidpunkt då de behöriga myndigheterna har skickat en förfrågan om att få tillgång till uppgifterna.

3º De fall där förfrågan om uppgifter inte har kunnat tillgodoses.

Denna statistik får inte innefatta personuppgifter.

…”

9. I artikel 5 föreskrivs att en artikel 126/1 med följande lydelse ska föras in i 2005 års lag:

”1. Hos varje operatör, och hos varje sådan leverantör som avses i artikel 126 punkt 1 första stycket, ska inrättas en samordningsgrupp med ansvar för att tillhandahålla behöriga belgiska myndigheter, på deras begäran, uppgifter som lagrats med stöd av artiklarna 122, 123 och 126, nummervisning enligt artikel 107 punkt 2 första stycket eller uppgifter som kan begäras ut enligt artiklarna 46 bis, 88 bis och 90 ter i straffprocesslagen och artiklarna 18/7, 18/8, 18/16 och 18/17 i [1998 års lag].

…

2. Varje leverantör och varje operatör som avses i artikel 126 punkt 1 första stycket ska införa ett internt förfarande för att svara på förfrågningar från myndigheterna om tillgång till användarnas personuppgifter. De ska på begäran förse Institutet med information om dessa förfaranden, antalet förfrågningar som mottagits, vilken rättslig grund som åberopats och vilket svar de lämnat.

…

3. Varje leverantör och varje operatör som avses i artikel 126 punkt 1 första stycket ska utse en eller flera ansvariga för skydd av personuppgifter, som ska uppfylla samtliga villkor som anges i punkt 1 tredje stycket.

…

Den ansvarige för skydd av personuppgifter ska utöva sina uppgifter helt självständigt, och ska ha tillgång till alla personuppgifter som överförs till myndigheterna och till alla leverantörens eller operatörens relevanta lokaler.

…

4. Konungen fastställer, genom kungörelse som antas av regeringen efter att ha hört Kommissionen för integritetsskydd och Institutet,

…

2.º vilka villkor som samordningsgruppen måste uppfylla, med beaktande av situationen för operatörer och leverantörer som tar emot få förfrågningar från de rättsliga myndigheter, som saknar driftställe i Belgien eller som huvudsakligen bedriver sin verksamhet i utlandet,

3.º vilka uppgifter som ska lämnas till Institutet och till Kommissionen för integritetsskydd i enlighet med punkterna 1 och 3 liksom vilka myndigheter som ska ha tillgång till dessa uppgifter,

4.º övriga bestämmelser för samarbetet mellan de operatörer och leverantörer som avses i artikel 126 punkt 1 första stycket och de belgiska myndigheterna eller vissa av dem, för att tillhandahålla de uppgifter som avses i punkt 1, inbegripet, om nödvändigt och av den berörda myndigheten, formen på och innehållet i begäran.

…”

10. I artikel 8 föreskrivs att artikel 46 bis punkt 1 i straffprocesslagen ska ha följande lydelse:

”1. När allmänna åklagaren utreder brott får denne genom ett skriftligt, motiverat beslut, genom att begära nödvändigt bistånd av en operatör som driver ett elektroniskt kommunikationsnät eller en leverantör av en elektronisk kommunikationstjänst eller en polismyndighet som utsetts av Konungen, på grundval av alla uppgifter som denne innehar eller genom tillgång till information om kunderna hos operatören eller leverantören, genomföra eller låta genomföra

1º identifiering av abonnenten eller av den brukliga användaren av en elektronisk kommunikationstjänst eller av det elektroniska kommunikationsmedel som använts,

2º identifiering av elektroniska kommunikationstjänster som en viss person abonnerar på som regelmässigt används av en viss person.

Skälen ska återspegla att åtgärden ska vara proportionerlig i förhållande till respekten för privatlivet och endast får tillgripas i den mån andra utredningsmöjligheter saknas.

I ytterst brådskande fall kan varje polistjänsteman inom kriminalpolisen inhämta sådana uppgifter, med muntligt förhandsgodkännande från åklagaren och genom ett motiverat, skriftligt beslut. Polistjänstemannen ska överlämna detta motiverade, skriftliga beslut liksom de uppgifter som inhämtats till åklagaren inom 24 timmar.

För brott av sådan art att det är ägnat att medföra ett års fängelse eller mer, får åklagaren eller, i ytterst brådskande fall, en polistjänsteman inom kriminalpolisen, endast begära sådana uppgifter som avses i första stycket inom en period på sex månader före beslutet.

2. Varje operatör som driver ett elektroniskt kommunikationsnät och varje leverantör av elektroniska kommunikationstjänster som är skyldig att överlämna sådana uppgifter som avses i punkt 1 ska överlämna de begärda uppgifterna till åklagaren eller polisen inom en tidsfrist som fastställs av Konungen ….

…

Var och en som genom sina arbetsuppgifter får kännedom om åtgärden eller bistår i denna har tystnadsplikt. Varje brott mot sekretessen ska bestraffas enligt artikel 458 i strafflagen.

En vägran att överlämna uppgifter medför böter med 26 till 10 000 euro.

11. Enligt artikel 9 ska artikel 88 bis i straffprocesslagen ha följande lydelse:

”1. Om det föreligger allvarliga indikationer på att ett brott är av sådan art att det är ägnat att medföra ett års fängelse eller mer och om undersökningsdomaren finner att det finns omständigheter som gör spårning av elektronisk kommunikation eller lokalisering av ursprunget eller slutmålet för elektronisk kommunikation nödvändig för att utreda sakomständigheterna, får denne genom att, direkt eller genom en polismyndighet som utses av Konungen, begära nödvändigt tekniskt bistånd från operatören av det elektroniska kommunikationsnätet eller leverantören av den elektroniska tjänsten låta

1.º spåra trafikuppgifter från elektroniska kommunikationsmedel som sänt eller mottagit elektronisk kommunikation,

2.º lokalisera ursprunget eller slutmålet för elektronisk kommunikation.

I de fall som avses i första stycket ska, för varje elektroniskt kommunikationsmedel för vilka samtalsuppgifter har samlats in eller för vilka telekommunikationens ursprung eller slutmål lokaliserats, dag, klockslag, varaktighet och om nödvändigt platsen för den elektroniska kommunikationen anges och tas upp i ett protokoll.

Undersökningsdomaren ska i ett motiverat beslut ange de faktiska omständigheter som motiverar åtgärden och varför den är proportionerlig med hänsyn till skyddet för privatlivet och endast tillgrips då andra utredningsmöjligheter saknas.

Undersökningsdomaren ska också ange under vilken tid åtgärden kan tillämpas i framtiden. Den tiden får inte överstiga två månader från dagen för beslutet, utan att detta påverkar möjligheten till förlängning eller, i förekommande fall, den period bakåt i tiden som beslutet enligt punkt 2 ska avse.

…

2. Vad gäller tillämpningen av den åtgärd som avses i punkt 1 första stycket om trafik- eller lokaliseringsuppgifter som lagrats med stöd av artikel 126 i [2005 års lag] ska följande bestämmelser gälla:

– För ett brott enligt bok II avdelning I ter i Code pénal (strafflagen) kan undersökningsdomaren begära ut uppgifter avseende en period på tolv månader före beslutet.

– För ett annat brott som avses i artikel 90 ter punkterna 2–4 som inte avses i första stycket eller för ett brott som begåtts inom ramen för en sådan kriminell organisation som avses i artikel 324 bis i strafflagen, eller för ett brott av sådan art att det är ägnat att medföra fem års fängelse eller mer, kan undersökningsdomaren i sitt beslut begära ut uppgifter avseende en period på nio månader före beslutet.

– För andra brott kan undersökningsdomaren endast begära ut uppgifter avseende en period på sex månader före beslutet.

3. Åtgärden får inte omfatta en advokats eller en läkares elektroniska kommunikationsmedel, utom om denne misstänks för att ha begått eller medverkat till ett sådant brott som avses i punkt 1 eller om det på grundval av tydliga uppgifter kan antas att en tredje man som misstänks ha begått ett brott som avses i punkt 1 använder sig av dessa elektroniska kommunikationsmedel.

Åtgärden får inte utföras utan att ordföranden i det lokala advokatsamfundet respektive företrädaren för läkarsällskapet i provinsen har underrättats. Dessa personer ska informeras av undersökningsdomaren om omständigheter som denne bedömer omfattas av sekretess. Dessa omständigheter får inte protokollföras.

4. …

Var och en som genom sina arbetsuppgifter får kännedom om åtgärden eller bistår i denna har tystnadsplikt. Varje brott mot sekretessen ska bestraffas enligt artikel 458 i strafflagen.

…”

12. Enligt artikel 12 ska artikel 13 i 1998 års lag ha följande lydelse:

”Underrättelse- och säkerhetstjänster kan söka, samla in, ta emot och behandla information och personuppgifter som kan vara användbara för utövandet av deras uppgifter och upprätthålla en uppdaterad dokumentation om bland annat händelser, grupper och enskilda personer av intresse för utförandet av deras uppdrag.

Upplysningarna i dokumentationen ska ha samband med ändamålet med akten och vara begränsad till vad som fordras sett till detta ändamål.

Underrättelse- och säkerhetstjänster ska garantera säkerheten för uppgifterna om deras källor och för upplysningar och personuppgifter som inhämtas från dessa källor.

Underrättelse- och säkerhetstjänsternas personal ska ha tillgång till information, uppgifter och personuppgifter som samlas in och bearbetas av dessa verksamheter, under förutsättning att dessa är användbara vid fullgörandet av deras uppgifter eller uppdrag.”

13. I artikel 14 föreskrivs en ny lydelse för artikel 18/3, som nu föreskriver följande:

”1. De särskilda metoder för uppgiftsinsamling som avses i artikel 18/2 punkt 1 får genomföras med hänsyn till de potentiella hot som avses i artikel 18/1, förutsatt att de reguljära metoderna för uppgiftsinsamling bedöms otillräckliga för att inhämta den information som behövs för ett underrättelseuppdrag. Den särskilda metoden ska väljas utifrån hur allvarligt det potentiella hotet är mot vilket den genomförs.

Den särskilda metoden får endast genomföras efter skriftligt och motiverat beslut av myndighetschefen och efter att detta beslut anmälts till kommissionen.

2. Myndighetschefens beslut ska innehålla

1.° den särskilda metodens art,

2.° de fysiska eller juridiska personer, sammanslutningar eller grupper, föremål, platser, händelser eller uppgifter som omfattas av den särskilda metoden,

3.° det potentiella hot som motiverar den särskilda metoden,

4.° de faktiska omständigheter som motiverar den särskilda metoden, en motivering av varför andra åtgärder inte är tillräckliga och varför åtgärden är proportionerlig, inbegripet sambandet mellan 2° och 3°,

5.° den period under vilken den särskilda metoden kan tillämpas, räknat från dagen för anmälan av beslutet till kommissionen,

…

9.° i förekommande fall de tydliga indikationerna på att en advokat, läkare eller journalist personligen aktivt deltar eller har deltagit i uppkomsten eller utvecklingen av det potentiella hotet,

10.° vid tillämpning av artikel 18/8, en motivering av den period som uppgiftsinsamlingen avser,

…

8. Myndighetschefen ska avsluta den särskilda metoden när det potentiella hot som motiverar metoden har upphört, när den inte längre är användbar för sitt avsedda ändamål eller om en rättsstridighet konstateras. Han eller hon ska utan dröjsmål meddela kommissionen sitt beslut.”

14. Artikel 18/8 i 1988 års lag ska ha följande lydelse:

”1. Underrättelse- och säkerhetstjänsterna får, för att utföra sina uppgifter, vid behov genom att begära tekniskt stöd i detta syfte från operatören för ett elektroniskt kommunikationsnät eller leverantören av en elektronisk kommunikationstjänst,

1.º spåra eller låta spåra trafikuppgifter från elektroniska kommunikationsmedel som sänt eller mottagit elektronisk kommunikation,

2.º lokalisera eller låta lokalisera ursprunget eller slutmålet för elektronisk kommunikation.

…

2. Vad gäller tillämpningen av den åtgärd som avses i punkt 1 första stycket om trafik- eller lokaliseringsuppgifter som lagrats med stöd av artikel 126 i [2005 års lag] ska följande bestämmelser gälla:

1.º För ett potentiellt hot som hänför sig till en verksamhet som kan vara kopplad till kriminella organisationer eller till samhällsfarliga sektliknande organisationer, får myndighetschefen i sitt beslut begära ut uppgifter från upp till sex månader före beslutet.

2.º För ett annat potentiellt hot än de som avses i 1° och 3° får chefen kan tjänsten i sitt beslut begära ut uppgifter från upp till nio månader före beslutet.

3.º För ett potentiellt hot som hänför sig till en verksamhet som kan vara kopplad till kriminella organisationer eller till samhällsfarliga sektliknande organisationer, får myndighetschefen i sitt beslut begära ut uppgifter från upp till tolv månader före beslutet. …”

II. Bakgrund och tolkningsfrågor

15. Genom dom av den 11 juni 2015[14] ogiltigförklarade Cour constitutionnelle (Författningsdomstolen) den nya lydelsen av artikel 126 i 2005 års lag, av samma skäl som föranledde EU-domstolen att ogiltigförklara direktiv 2006/24 i domen Digital Rights.

16. Mot bakgrund av denna ogiltigförklaring antog den nationella lagstiftaren (innan domen Tele2 Sverige och Watson meddelades) lagen av den 29 maj 2016.

17. VZ m.fl., Ordre des barreaux francophones et germanophone, Liga voor Mensenrechten ASBL, Ligue des Droits de l’Homme ASBL och Académie Fiscale ASBL har väckt talan vid den hänskjutande domstolen om ogiltigförklaring av nämnda lag. De har i korthet gjort gällande att den gick utöver vad som var absolut nödvändigt och inte föreskrev tillräckliga garantier för skydd.

18. Cour constitutionnelle (Författningsdomstolen) beslutade mot denna bakgrund att ställa följande frågor till EU-domstolen:

”1) Ska artikel 15.1 i direktiv 2002/58/EG, jämförd med rätten till säkerhet, som garanteras av artikel 6 i Europeiska unionens stadga om de grundläggande rättigheterna, och rätten till skydd för personuppgifter, som garanteras av artiklarna 7, 8, och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna [(nedan kallad stadgan)], tolkas på så sätt att den utgör hinder för en nationell lagstiftning som den som är aktuell i det nationella målet, i vilken det föreskrivs en generell skyldighet för operatörer och leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, i den mening som avses i direktiv 2002/58/EG, som genereras eller behandlas av dem i samband med att de tillhandahåller dessa tjänster och vars syfte inte endast omfattar undersökning, avslöjande av

[14] Dom nr 84/2015, *Moniteur belge* av den 11 augusti 2015.

och åtal för grov brottslighet, utan även skydd för nationell säkerhet, försvaret och allmän säkerhet samt undersökning, avslöjande av och åtal för annan brottslighet än grov brottslighet eller förebyggande av otillåten användning av elektroniska kommunikationssystem eller uppnåendet av något annat mål enligt artikel 23.1 i [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), och i vilken nämnda skyldighet dessutom åtföljs av i lagstiftningen närmare angivna skyddsmekanismer med avseende på lagringen av och tillgången till uppgifterna?

2) Ska artikel 15.1 i direktiv 2002/58/EG, jämförd med artiklarna 4, 7, 8, 11 och 52.1 i [stadgan], tolkas på så sätt att den utgör hinder för en nationell lagstiftning som den som är aktuell i det nationella målet, där det föreskrivs en generell skyldighet för operatörer och leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, i den mening som avses i direktiv 2002/58/EG, som genereras eller behandlas av dem i samband med att de tillhandahåller dessa tjänster, om nämnda lagstiftning bland annat har till syfte att uppfylla de positiva skyldigheter som åligger myndigheten enligt artiklarna 4 och 8 i stadgan, vilka består i att inrätta en rättslig ram som möjliggör effektiv brottsutredning och verkningsfulla straff för sexuella övergrepp mot minderåriga och som gör det möjligt att på ett effektivt sätt identifiera gärningsmannen, även när elektroniska kommunikationstjänster används?

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

III. Förfarandet vid domstolen

19. Begäran om förhandsavgörande inkom till domstolen den 2 augusti 2018.

20. Skriftliga yttranden har getts in av VZ m.fl., Académie Fiscale ASBL, LMR, LDH, Ordre des barreaux francophones et germanophone, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), den tyska, den belgiska, den brittiska, den tjeckiska, den cypriotiska, den danska, den spanska, den estniska, den franska, den ungerska, den irländska, den nederländska, den polska och den svenska regeringen samt kommissionen.

21. Den 9 september 2019 hölls en förhandling, då målet behandlades gemensamt med målen C-511/18, C-512/18 och C-623/17, vid vilken parterna i de fyra målen om förhandsavgörande, de ovannämnda regeringarna, Norges regering samt kommissionen och Europeiska datatillsynsmannen var närvarande.

IV. Bedömning

22. Den första frågan i detta mål om förhandsavgörande sammanfaller i allt väsentligt med frågorna i målen C-511/18 och C-512/28. Den skiljer sig emellertid från de sistnämnda vad beträffar målen för den nationella lagstiftningen: dessa är inte bara att bekämpa terrorism och grov brottslighet eller att skydda nationell säkerhet, utan även ”försvaret och allmän säkerhet samt undersökning, avslöjande av och åtal för annan brottslighet än grov brottslighet” och, generellt, något av de andra mål som uppställs i artikel 23.1 i förordning nr 2016/679.

23. Den andra frågan har samband med den första, men den kompletterar den genom att den hänskjutande domstolen där vill få klarlagt huruvida de positiva skyldigheter som åligger myndigheten beträffande utredning och straff för sexuella övergrepp mot minderåriga motiverar de omtvistade åtgärderna.

24. Den tredje frågan ställs för det fallet att den nationella bestämmelsen är oförenlig med unionsrätten. Den hänskjutande domstolen vill i så fall veta om verkningarna av lagen av den 29 maj 2016 tills vidare kan bestå.

25. Jag ska ta mig an dessa frågor genom att för det första pröva huruvida direktiv 2002/58 är tillämpligt, och jag hänvisar då till mina förslag till avgörande i andra av dessa mål om förhandsavgörande. För det andra ska jag redovisa huvudlinjerna i domstolens praxis inom detta område och undersöka om det finns någon möjlighet att utveckla den. Avslutningsvis ska jag ta upp svaren på var och en av tolkningsfrågorna.

A. Huruvida direktiv 2002/58 är tillämpligt

26. Liksom i de tre andra målen om förhandsavgörande har det även i detta mål ifrågasatts om direktiv 2002/58 är tillämpligt. Med hänsyn till att medlemsstaternas ståndpunkter rörande detta är likartade här, hänvisar jag på den här punkten till mitt förslag till avgörande i målen C-511/18 och C-512/18. [15]

B. Domstolens praxis rörande lagring och myndigheternas tillgång till personuppgifter inom ramen för direktiv 2002/58

1. Principen om konfidentialitet vid kommunikation och därmed förbundna uppgifter

27. Bestämmelserna i direktiv 2002/58 ”skall precisera och komplettera” direktiv 95/46/EG, [16] för att garantera en hög skyddsnivå för personuppgifter i samband med tillhandahållande av tjänster avseende elektronisk kommunikation. [17]

15 Punkt 40 och följande punkter.

16 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). Se artikel 1.2 i direktiv 2002/58. Direktiv 95/46 har, med verkan från den 25 maj 2018, upphävts genom förordning nr 2016/679. I den mån direktiv 2002/58 hänvisar till direktiv 95/46 eller inte föreskriver egna regler, måste således bestämmelserna i den förordningen beaktas (se artikel 94.1 och 94.2 i förordning nr 2016/679).

17 Domen Tele2 Sverige och Watson, punkterna 82 och 83.

28. I artikel 5.1 i direktivet anges att medlemsstaterna genom nationell lagstiftning ska säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

29. Konfidentialitet vid kommunikation innebär bland annat (artikel 5.1 andra meningen i direktiv 2002/58) förbud för andra personer än användarna att utan användarnas samtycke lagra trafikuppgifter avseende elektronisk kommunikation. Undantag gäller endast för ”personer som har laglig rätt att göra detta … samt för teknisk lagring som är nödvändig för överföring av kommunikationen”. [18]

30. Artiklarna 5, 6 och 9.1 i direktiv 2002/58 syftar till att säkerställa konfidentialitet vid kommunikation och därmed förbundna uppgifter och minimera riskerna för missbruk. Räckvidden av dessa bestämmelser ska bedömas mot bakgrund av skäl 30 i direktivet, där det anges att ”systemen bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut *minimum*”. [19]

31. Vad beträffar dessa uppgifter kan följande åtskillnad göras:

– *Trafikuppgifter*, som bara får behandlas och lagras i den utsträckning och under den tid som krävs för att kunna fakturera för tjänster, marknadsföra tjänster eller tillhandahålla kringtjänster (artikel 6 i direktiv 2002/58). När den tiden har löpt ut, ska de behandlade och lagrade uppgifterna utplånas eller avidentifieras. [20]

– Andra *lokaliseringsuppgifter* än trafikuppgifter, vilka endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke (artikel 9.1 i direktiv 2002/58). [21]

2. Begränsningsklausulen i artikel 15.1 i direktiv 2002/58

32. I artikel 15.1 i direktiv 2002/58 föreskrivs att medlemsstaterna ”genom lagstiftning [får] begränsa omfattningen av de rättigheter och skyldigheter som anges i artiklarna 5 och 6 samt artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9” i det direktivet.

33. En sådan begränsning måste ”vara nödvändig, lämplig och proportionell i ett demokratiskt samhälle för att skydda nationell säkerhet (det vill säga 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]”.

34. Denna uppräkning av målen är uttömmande: [22] Till exempel (”bland annat”) får medlemsstaterna ”vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt”.

18 *Ibidem*, punkt 85 och där angiven rättspraxis.

19 *Ibidem*, punkt 87. Min kursivering.

20 *Ibidem*, punkt 86 och där angiven rättspraxis.

21 *Ibidem*, artikel 86, *in fine*.

22 *Ibidem*, punkt 90.

35. Under alla förhållanden ska ”[a]lla åtgärder som avses i denna punkt … vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen”. Artikel 15.1 ska alltså tolkas mot bakgrund av de grundläggande rättigheter som garanteras i stadgan. [23]

36. Bland dessa rättigheter som säkerställs i stadgan har domstolen, i detta sammanhang, nämnt rätten till respekt för privatlivet (artikel 7), rätten till skydd för personuppgifter (artikel 8) och yttrandefriheten (artikel 11). [24]

37. Domstolen har vidare, som vägledning för tolkningen av artikel 15.1 i direktiv 2002/58, betonat att medlemsstaternas möjlighet att begränsa omfattningen av skyldigheten att säkerställa konfidentialiteten vid kommunikation och därmed förbundna trafikuppgifter ska tolkas strikt.

38. Den har närmare bestämt slagit fast att ”[e]n sådan bestämmelse … inte [kan] motivera att undantaget från denna principiella skyldighet, i synnerhet förbudet i artikel 5 i direktivet mot att lagra dessa uppgifter, görs till huvudregel. Det skulle i stor utsträckning förta verkan av sistnämnda bestämmelse.” [25]

39. Jag anser att detta dubbla påpekande är av avgörande betydelse för att förstå varför domstolen har slagit fast att en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter rörande elektronisk kommunikation är oförenlig med direktiv 2002/58.

40. När domstolen slog fast detta gjorde den bara en ”strikt” [26] tillämpning av det proportionalitetskriterium som den hade använt sig av tidigare: [27] ”skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt”. [28]

3. Proportionaliteten vid lagring av personuppgifter

a) Huruvida en generell och odifferentierad lagring är proportionerlig

41. Domstolen medgav att bekämpningen av grov brottslighet, och särskilt av organiserad brottslighet och terrorism, är av största betydelse för att garantera allmän säkerhet och att dess effektivitet i stor utsträckning kan bero på användningen av moderna utredningstekniker. Den tillade att ”[e]tt sådant mål av allmänt samhällsintresse … emellertid inte, trots dess grundläggande betydelse, i sig ensamt [kan] motivera att en sådan lagringsåtgärd som den genom direktiv 2006/24 införda ska anses vara nödvändig för nämnda bekämpande”. [29]

23 *Ibidem*, punkt 91 och där angiven rättspraxis.

24 *Ibidem*, punkt 93 och där angiven rättspraxis.

25 *Ibidem*, punkt 89.

26 Användningen av detta adverb i punkt 95 i domen Tele2 Sverige och Watson bygger på skäl 11 i direktiv 2002/58.

27 Domen Digital Rights, punkt 48. ”I föreliggande fall är unionslagstiftarens utrymme för skönsmässig bedömning begränsat med hänsyn till den stora betydelse som skyddet för personuppgifter har för den grundläggande rätten till respekt för privatlivet och med hänsyn till det långtgående och allvarliga ingrepp i denna rätt som direktiv 2006/24 innebär. Det ska därför göras en strikt kontroll.”

28 Domen Tele2 Sverige och Watson, punkt 96 och där angiven rättspraxis.

29 Domen Digital Rights, punkt 51. Se även domen Tele2 Sverige och Watson, punkt 103.

42. För att avgöra om en åtgärd av det slaget var strängt nödvändig, underströk domstolen framför allt att det ingrepp som den utgör i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan är synnerligen allvarligt.[30] Det beror just på att den nationella lagstiftningen föreskrev ”en generell och odifferentierad lagring av *samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel* och ålade leverantörer av elektroniska kommunikationstjänster att *systematiskt och kontinuerligt* lagra dessa uppgifter, *utan undantag*”.[31]

43. Det ingrepp som denna lagstiftning medförde i medborgarnas liv återspeglas i dessa bedömningar från domstolen rörande verkningarna av uppgifternas lagring.

Dessa uppgifter[32]

– ”gör det möjligt att spåra och identifiera en kommunikationskälla, identifiera slutmålet för en kommunikation, identifiera en kommunikations datum, tidpunkt, varaktighet och typ, identifiera användarnas kommunikationsutrustning och identifiera lokaliseringen av mobil kommunikationsutrustning”,[33]

– ”gör det möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett. Uppgifterna gör det dessutom möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod.”[34]

– ”Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i.”[35]

– ”Dessa uppgifter gör det möjligt att … kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna.”[36]

44. Ingreppet kan även ”ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning”, eftersom det ”sker utan att abonnenten eller den registrerade användaren är underrättad om detta”.[37]

30 Domen Digital Rights, punkt 65, och domen Tele2 Sverige och Watson, punkt 100.

31 Domen Tele2 Sverige och Watson, punkt 97. Min kursivering.

32 Bland dessa uppgifter ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda numret och IP-adressen för internettjänster.

33 Domen Tele2 Sverige och Watson, punkt 98.

34 *Ibidem*, punkt 98.

35 *Ibidem*, punkt 99.

36 *Ibidem*, artikel 99, *in fine*.

37 *Ibidem*, punkt 100.

45. Med hänsyn till ingreppets omfattning, kan endast bekämpning av grov brottslighet motivera en lagstiftning som föreskriver lagring av sådana uppgifter.[38] Detta får emellertid inte bli huvudregeln, eftersom ”det system som inrättats genom direktiv 2002/58 kräver att sådan lagring ska vara ett undantag”.[39]

46. Det förelåg dessutom två särdrag som berodde på att lagstiftningen i fråga inte föreskrev ”några åtskillnader, begränsningar eller undantag utifrån det eftersträvade syftet”[40] och ”inte [kräver] något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten”:[41]

– För det första berörde lagstiftningen ”på ett allomfattande sätt samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring … Den föreskriver inte heller några undantag, vilket innebär att den även är tillämplig på personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt.”[42]

– För det andra är den ”… 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.”[43]

47. Den nationella lagstiftningen i fråga överskred således gränserna för vad som var strängt nödvändigt. Den kunde således inte 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.[44]

b) Huruvida en riktad lagring får göras

48. Domstolen har slagit fast att lagstiftning ”som i förebyggande syfte tillåter en *riktad lagring* av trafikuppgifter och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet” är förenlig med unionsrätten.[45]

49. Villkoret för att en riktad lagring av uppgifter ska få göras är att lagringen ”vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt”.

50. De riktlinjer som domstolen gav i domen Tele2 Sverige och Watson för att avgöra när dessa villkor är uppfyllda var inte uttömmande (och kunde kanske heller inte vara det) utan snarast allmänt formulerade. För att uppfylla villkoren ska medlemsstaterna

38 *Ibidem*, punkt 102.
39 *Ibidem*, punkt 104.
40 *Ibidem*, punkt 105.
41 *Ibidem*, punkt 106.
42 *Ibidem*, punkt 105.
43 *Ibidem*, punkt 106.
44 *Ibidem*, punkt 107.
45 *Ibidem*, punkt 108. Min kursivering.

– föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd, [46]

– tillämpa ”objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet” [47] och

– ”grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet, på ett eller annat sätt bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten”. [48]

51. Vad beträffar dessa objektiva omständigheter anförde domstolen som exempel möjligheten att använda sig av ett geografiskt kriterium för att avgränsa personkretsen och de situationer som kan komma att beröras. Jag anser inte att hänvisningen till detta kriterium, vilken vissa medlemsstater har kritiserat, syftar till att det enbart är det som ska tillämpas för att avgöra när en riktad lagring är tillåten.

4. Proportionaliteten vid tillgång till personuppgifter

a) Domen Tele2 Sverige och Watson

52. Domstolen behandlar de nationella myndigheternas *tillgång* till uppgifterna oberoende av omfattningen av den skyldighet att *lagra* som leverantörer av elektroniska kommunikationstjänster åläggs, och oberoende av om lagringen av dessa uppgifter är generell eller riktad. [49]

53. Även om syftet med lagringen är att göra det möjligt att senare få tillgång till uppgifterna, kan de ge upphov till olika åsidosättanden av de grundläggande rättigheter som skyddas i stadgan. Denna differentiering hindrar emellertid inte att vissa av övervägandena rörande lagringen även är tillämpliga på tillgången till de lagrade uppgifterna.

54. Således måste tillgången

– ”vara faktiskt och strikt begränsad till de fall då tillgången krävs för ett av dessa syften” som anges i artikel 15.1 första meningen i direktiv 2002/58. Syftet med lagstiftningen måste också stå i proportion till hur allvarligt ingreppet är. Om ingreppet betecknas som allvarligt, får det endast användas för att bekämpa grov brottslighet. [50]

– Tillgång får inte ges utöver vad som är strängt nödvändigt. [51] Dessutom måste lagstiftningen föreskriva ”klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella

46 *Ibidem*, punkt 109. Den måste särskilt precisera ”under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt”.

47 *Ibidem*, punkt 110.

48 Ibidem, punkt 111.

49 *Ibidem*, punkt 113.

50 *Ibidem*, punkt 115.

51 *Ibidem*, punkt 116.

myndigheter tillgång till uppgifterna. En åtgärd av detta slag måste också vara rättsligt bindande i nationell rätt”. [52]

– Närmare bestämt måste den nationella lagstiftningen ”ange de materiella och formella villkoren för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna”. [53]

55. Härav följer att ”en allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det eftersträvade syftet, inte kan anses vara begränsad till vad som är strängt nödvändigt”. [54]

56. Enligt domstolen ”måste den berörda nationella lagstiftningen således vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter om abonnenter eller registrerade användare”. [55] ”Tillgång kan i princip bara beviljas, i samband med bekämpning av brott, *till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott*.” [56]

57. Med andra ord ska den nationella lagstiftning som ger de nationella myndigheterna tillgång till de lagrade uppgifterna ha en tillräckligt begränsad räckvidd. Det ska finnas ett samband mellan de berörda personerna och det eftersträvade syftet, vilket innebär att tillgången inte får omfatta ett stort antal personer, eller till och med alla personer, alla elektroniska kommunikationsmedel och alla lagrade uppgifter.

58. Dessa villkor får emellertid modereras under vissa omständigheter. Domstolen beaktar ”särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism”. I sådana situationer ”skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism”. [57]

59. Detta klargörande från domstolens sida innebär att medlemsstaterna i undantagsfall får införa ett särskilt system för en mer omfattande tillgång till uppgifter, när det är nödvändigt för att bekämpa hot mot statens grundläggande intressen (nationell säkerhet, försvar och allmän säkerhet), [58] så att det även innefattar personer som bara har en indirekt anknytning till dessa risker.

60. För att de nationella myndigheterna ska få tillgång till lagrade uppgifter, oavsett av vilket slag de är, måste tre villkor vara uppfyllda:

– Tillgången ska ”i princip, utom i vederbörligen motiverade brådskande fall, [vara] underkastad förhandskontroll av en domstol eller en oberoende myndighet”. Domstolen ska meddela sitt avgörande eller myndigheten fatta sitt beslut ”efter det att de behöriga nationella

52 *Ibidem*, punkt 117.

53 *Ibidem*, punkt 118.

54 *Ibidem*, punkt 119.

55 *Idem.*

56 *Idem*. Min kursivering.

57 *Idem.*

58 Utöver vid terrorism skulle en sådan mer omfattande tillgång kunna motiveras vid ett IT-angrepp i stor skala mot känslig statlig infrastruktur eller ett hot med anknytning till kärnvapenspridning.

myndigheterna framställt en motiverad ansökan, vilket kan ske bland annat inom ramen för ett förfarande för förebyggande, avslöjande eller lagföring av brott”. [59]

– Det ”krävs att de behöriga nationella myndigheter som beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta, enligt tillämpliga nationella förfaranden, så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar”. [60]

– Medlemsstaterna måste anta bestämmelser om säkerhet och skydd för de uppgifter som finns hos leverantörer av elektroniska kommunikationstjänster, för att förhindra missbruk och otillåten tillgång till uppgifterna. [61]

b) Domen Ministerio Fiscal

61. I det målet prövades frågan huruvida en nationell lagstiftning som föreskriver att de behöriga myndigheterna ska få tillgång till identitetsuppgifter för vissa innehavare av SIM-kort var förenlig med artikel 15.1 i direktiv 2002/58, tolkad mot bakgrund av artiklarna 7 och 8 i stadgan.

62. Domstolen slog fast att artikel 15.1 första meningen i direktiv 2002/58 inte begränsar syftet att förebygga, utreda, upptäcka och lagföra brott till kampen mot allvarlig brottslighet, utan hänvisar till ”brott” i allmänhet. [62]

63. Den fann vidare att det, för att det ska vara motiverat att de behöriga nationella myndigheterna får tillgång till uppgifterna, måste finnas en överensstämmelse mellan hur allvarligt ingreppet är och hur allvarliga brotten i fråga är. Följaktligen

– ”kan ett allvarligt ingrepp … endast motiveras av syftet att bekämpa brottslighet, vilken då också måste kvalificeras som ’allvarlig’”. [63]

– ”När det ingrepp som en sådan tillgång innebär däremot inte är allvarligt, kan det emellertid motiveras av syftet att förebygga, utreda, upptäcka och lagföra ’brott’ i allmänhet.” [64]

64. Mot bakgrund av detta och till skillnad från vad som var fallet i domen Tele2 Sverige och Watson, betecknade domstolen inte ingreppet i de rättigheter som skyddas genom artiklarna 7 och 8 i stadgan som ”allvarligt”, eftersom begäran om tillgång enbart syftade ”till att identifiera innehavarna av de SIM-kort som under en tolvdagarsperiod aktiverats med den stulna mobiltelefonens IMEI-kod”. [65]

65. För att betona att ingreppet var mindre allvarligt förklarade domstolen att ”[d]e uppgifter som begäran avser … bara [tycks] koppla samman det eller de SIM-kort som under en viss tidsperiod aktiverats genom den stulna mobiltelefonen med SIM-kortsinnehavarnas identitet. Om man inte

[59] Domen Tele2 Sverige och Watson, punkt 120.

[60] *Ibidem*, punkt 121.

[61] *Ibidem*, punkt 122.

[62] Domen Ministerio Fiscal, punkt 53.

[63] *Ibidem*, punkt 56.

[64] *Ibidem*, punkt 57.

[65] *Ibidem*, punkt 59. Det rörde sig om tillgång ”till de telefonnummer som svarar mot SIM-korten samt identitetsuppgifter för innehavarna av dessa kort, såsom deras för- och efternamn och eventuellt adress. Dessa uppgifter rör däremot inte, vilket såväl den spanska regeringen som åklagarmyndigheten bekräftat vid förhandlingen, den kommunikation som ägt rum med den stulna mobiltelefonen eller telefonens geografiska position.”

stämmer av dessa uppgifter med uppgifterna om den kommunikation som skett med SIM-korten och med lokaliseringsuppgifterna, går det inte att av dessa uppgifter utläsa vare sig datum, tidpunkt, varaktighet eller mottagare för den kommunikation som skett med SIM-kortet eller SIM-korten i fråga eller var denna kommunikation ägt rum eller hur ofta med vissa personer under en viss tidsperiod. Dessa uppgifter gör det således inte möjligt att dra några mer precisa slutsatser om privatlivet för de personer vars uppgifter berörs.” [66]

66. Det mål som avgjordes genom domen Ministerio Fiscal handlade inte om huruvida de personuppgifter som tillgången avsåg hade lagrats av leverantörer av elektroniska kommunikationstjänster i enlighet med de villkor som anges i artikel 15.1 i direktiv 2002/58, mot bakgrund av artiklarna 7 och 8 i stadgan. [67] Inte heller behandlades frågan huruvida de uppfyllde de övriga villkoren för tillgång enligt den artikeln.

67. Det går därför inte att utifrån lydelsen av domen Ministerio Fiscal dra slutsatsen att domstolen ändrat den praxis som innebär att ett nationellt system som medger en generell och odifferentierad lagring av uppgifter, i den mening som avses i domen Tele2 Sverige och Watson, är oförenligt med unionsrätten.

68. Jag anser emellertid att när domstolen fann att det var tillåtet med ett system för tillgång som begränsade sig till vissa personuppgifter (identitetsuppgifter för innehavare av SIM-kort), godtog den underförstått att samma uppgifter fick lagras av leverantörerna av tjänsten.

C. Den viktigaste kritiken mot domstolens praxis

69. Såväl den hänskjutande domstolen som merparten av de medlemsstater som har yttrat sig i målet uppmanar domstolen att klargöra, nyansera eller till och med ompröva flera aspekter av sin praxis inom detta område, vilka de riktar kritik mot.

70. Merparten av denna, förtäckta eller öppna, kritik har redan framförts med anledning av domen Digital Rights och tillbakavisats i domen Tele2 Sverige och Watson. Nu dyker den upp på nytt för att, kortfattat uttryckt, betona att det skulle räcka med stränga bestämmelser om tillgång till sådana uppgifter som leverantörerna av elektroniska kommunikationstjänster förfogar över, för att i viss mån kompensera för det allvarliga ingrepp som en generell och odifferentierad lagring av dessa uppgifter innebär.

71. I flera fall betonas det även att det är nödvändigt att vidta åtgärder som verkligen är effektiva för att bekämpa de allvarliga säkerhetshoten och brottsligheten i allmänhet, och domstolen uppmanas att beakta rätten till personlig säkerhet (artikel 6 i stadgan) och medlemsstaternas utrymme för skönsmässig bedömning för att skydda den nationella säkerheten. I något fall har det även påpekats att domstolen inte har beaktat den preventiva verkan av säkerhets- och underrättelsetjänsternas ingripanden.

66 *Ibidem*, punkt 60.

67 Domen Ministerio Fiscal, punkt 49.

D. Min bedömning av denna kritik och av de nyanseringar som skulle kunna göras i domstolens praxis

72. Jag anser att domstolen bör hålla fast vid den principiella ståndpunkt som den intagit i sina tidigare domar, nämligen att en generell och odifferentierad skyldighet att lagra alla trafik- och lokaliseringsuppgifter avseende alla abonnenter och registrerade användare, på ett orimligt sätt åsidosätter de grundläggande rättigheter som skyddas genom artiklarna 7, 8 och 11 i stadgan.

73. E contrario skulle en nationell lagstiftning som föreskriver lämpliga restriktioner för lagring av vissa av dessa uppgifter, som genererats i samband med tillhandahållande av elektroniska kommunikationstjänster, kunna vara förenlig med unionsrätten. Det centrala här är således den *begränsade lagringen* av dessa uppgifter.

74. Av nedan angivna skäl bör denna begränsade lagring inte bara avse ett visst geografiskt område eller en viss kategori av personer. Diskussionerna kring dessa lagringskriterier visar att de antingen skulle kunna vara omöjliga att genomföra eller att de inte skulle vara verkningsfulla med avseende på syftena, eller till och med skulle kunna ge upphov till diskriminering.

75. Till att börja med instämmer jag inte med de kritiker som förespråkar ”mer omfattande lagring i utbyte mot mer begränsad tillgång”. Domstolens resonemang, som jag instämmer i, går ut på att lagring och tillgång till uppgifter är två olika typer av ingrepp. Även om en lagring av uppgifter har betydelse för en eventuell senare tillgång för de behöriga myndigheterna, bör dessa ingrepp motiveras vart och ett för sig, genom en särskild prövning som bygger på det eftersträvade syftet.

76. Ett nationellt system som föreskriver en generell och odifferentierad lagring av uppgifter kan således inte motiveras av att bestämmelserna i fråga samtidigt föreskriver stränga materiella och processuella villkor för tillgång till dessa uppgifter.

77. Det måste således finnas bestämmelser som särskilt har samband med lagringen av uppgifterna och som underkastar den vissa villkor för att förhindra att den är generell och odifferentierad. Det är endast på det sättet som det kan säkerställas att bestämmelserna är förenliga med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan.

78. Detta är för övrigt det synsätt som antogs av de arbetsgrupper som sammanträdde inom rådet för att fastställa regler för lagring och tillgång som är förenliga med domstolens praxis, där de två typerna av ingrepp granskades parallellt. [68]

79. Genom att tillämpa begränsningar för var och en av dessa två typer av ingrepp, kan en bedömning göras av om deras kumulativa verkan, kombinerad med gedigna skyddsmekanismer, är sådan att den dämpar den verkan som lagringen av uppgifterna har på de grundläggande rättigheter som skyddas genom artiklarna 7, 8 och 11 i stadgan, samtidigt som den säkerställer att utredningarna blir effektiva.

80. För att skydda dessa rättigheter måste systemet

– föreskriva en lagring av uppgifter som innehåller vissa begränsningar och skillnader beroende på vilket syfte som eftersträvas, och

[68] Medlemsstaterna deltar sedan år 2017 i en arbetsgrupp som har till syfte att anpassa deras lagstiftningar till de kriterier som fastställts i domstolens praxis inom detta område (Arbetsgruppen för informationsutbyte och uppgiftsskydd (DAPIX)).

– reglera tillgången till dessa uppgifter så, att tillgång enbart medges i den mån det är strängt nödvändigt för det syfte som eftersträvas, och under kontroll av en domstol eller en oberoende förvaltningsmyndighet.

81. Kraven på leverantörerna av elektroniska kommunikationstjänster att lagra vissa uppgifter, inte bara för att sköta sina avtalsförpliktelser gentemot användarna, ökar i takt med den tekniska utvecklingen. Om det medges att denna lagring är till nytta för att förebygga och bekämpa brottslighet (vilket är svårt att förneka [69]), är det inte logiskt att begränsa dess räckvidd till att enbart omfatta hantering av sådana uppgifter som operatörerna använder för att bedriva sin affärsverksamhet och enbart den tid som är nödvändig för denna verksamhet.

82. Om det medges att en skyldighet att lagra uppgifter är användbar för att skydda den nationella säkerheten och bekämpa brottslighet, är det nödvändigt att definiera gränserna för denna skyldighet, utöver den lagring som operatörerna kan göra för att tillgodose sina tekniska och affärsmässiga behov.

83. Varje system för lagring måste vara strängt anpassat till det syfte som eftersträvas och det får inte omvandlas till en odifferentierad lagring. [70] Det måste också utesluta att summan av dessa uppgifter ger en *bild* av den berörda personen (det vill säga av hans eller hennes normala aktiviteter och sociala relationer) som ligger nära eller liknar den bild man skulle få fram om man kände till innehållet i kommunikationerna.

84. För att klargöra missförstånd och viss bristande förståelse, är det viktigt att beakta vad domstolen *inte slog fast* i sina domar Digital Rights och Tele2 Sverige och Watson. I dessa domar förkastade domstolen inte i sig ett system för lagring av uppgifter som ett användbart instrument för att bekämpa brottslighet. Tvärtom slog domstolen fast att syftet att förebygga och bekämpa brott var legitimt och att ett system för lagring av uppgifter kan vara användbart för att uppnå detta syfte.

85. Det som domstolen, som jag tidigare nämnt, bestämt vände sig mot där var att unionen eller dess medlemsstater genom att hänvisa till detta syfte föreskriver en odifferentierad lagring av *alla* uppgifter som genereras i samband med tillhandahållande av elektroniska kommunikationstjänster och en allmän tillgång till dessa uppgifter.

86. Det är således nödvändigt att hitta former för lagring av uppgifter som inte kan betecknas på ett sådant sätt (”generell och odifferentierad”) att den är oförenlig med det skydd som krävs enligt artiklarna 7, 8 och 11 i stadgan.

87. En av dessa former är *riktad* lagring av uppgifter, som antingen rör en viss personkrets (i teorin den som har viss, mer eller mindre direkt, anknytning till allvarligare hot) eller ett visst geografiskt område.

88. Det finns emellertid vissa svårigheter med detta upplägg:

– Det räcker sannolikt inte att identifiera en grupp potentiella angripare, om dessa använder sig av anonymiseringsteknik eller förfalskar sina identiteter. Ett val att inrikta sig på sådana grupper skulle dessutom kunna leda till att det införs ett system med allmänna misstankar

[69] Under alla förhållanden omfattas fastställandet av dessa undersökningstekniker och bedömningen av deras effektivitet av medlemsstaternas utrymme för skönsmässig bedömning.

[70] Domen Digital Rights, punkt 57, och domen Tele2 Sverige och Watson, punkt 105.

mot vissa befolkningsgrupper som skulle kunna betecknas som diskriminerande och som bygger på vilken algoritm som används.

– Ett system med geografiska kriterier (som för att vara effektivt inte får avse alltför små områden) ger upphov till samma problem och fler därtill, vilket Europeiska datatillsynsmannen påpekade vid förhandlingen, eftersom det skulle kunna stigmatisera dessa områden.

89. Dessutom skulle det kunna finnas en viss motsättning mellan den preventiva karaktären hos en lagring som riktar sig mot en särskild personkrets eller ett visst geografiskt område och den omständigheten att det inte på förhand är känt vilka gärningsmännen är eller var och när brotten kommer att begås.

90. Under alla förhållanden kan det inte uteslutas att det går att hitta former för riktad lagring som bygger på dessa kriterier och som är användbara för att uppnå de ovannämnda syftena. Det ankommer på den lagstiftande makten, i varje medlemsstat eller för hela unionen, att fastställa dessa former så, att de iakttar skyddet för de grundläggande rättigheter som domstolen värnar om.

91. Det skulle vara ett misstag att tro att en riktad lagring av uppgifter som rör en viss personkrets eller ett visst geografiskt område, är den enda formen som domstolen anser är förenlig med artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7 och 8 i stadgan.

92. Det är som sagt möjligt att hitta andra former för riktad lagring än dem som är inriktade på särskilda grupper av personer eller särskilda geografiska områden. Detta anser också de ovannämnda arbetsgrupperna inom rådet. De har bland annat pekat på möjligheterna till begränsning av de kategorier av uppgifter som lagras,[71] pseudoanonymisering av uppgifter,[72] införande av begränsade lagringsperioder,[73] uteslutande av vissa kategorier av leverantörer av elektroniska kommunikationstjänster,[74] förnybara tillstånd för lagring,[75] och skyldighet att lagra de lagrade uppgifterna inom unionen eller en systematisk och regelbunden kontroll av en oberoende förvaltningsmyndighet av de garantier som leverantörerna av elektroniska kommunikationstjänster lämnar mot en otillbörlig användning av uppgifterna.

93. Jag anser att en tillfällig lagring av vissa *kategorier* av trafik- eller lokaliseringsuppgifter, som begränsar sig till vad som är strängt nödvändigt för säkerheten och som sammantaget inte gör det möjligt att skaffa sig en exakt och detaljerad bild av de berörda personernas liv, är att föredra för att det ska vara förenligt med domstolens praxis.

71 Uppgifter som inte är helt oumbärliga och objektivt nödvändiga för att förebygga och bekämpa brott och skydda den allmänna säkerheten undantas från lagringsskyldigheten. Det bör bland annat anges, beroende på vilket syfte som eftersträvas, vilken typ av abonnentuppgifter, trafikuppgifter och lokaliseringsuppgifter som måste lagras för att uppnå detta syfte. Bland annat undantas uppgifter som inte anses oumbärliga för utredning och lagföring av brott.

72 En metod där namnen byts ut mot alias så att uppgifterna inte längre kan knytas till ett namn. Till skillnad från vid anonymisering, innebär pseudoanonymisering att uppgifterna åter kan knytas till den berörda personens namn.

73 Man skulle kunna undersöka möjligheten att anpassa lagringsperioderna till den kategori av uppgifter det rör sig om, med beaktande av hur allvarligt intrånget i personernas privatliv är. Det bör dessutom föreskrivas att uppgifterna ska utplånas permanent i slutet av lagringsperioden.

74 Man skulle kunna överväga möjligheten att inte ålägga alla leverantörer av elektroniska kommunikationstjänster en lagringsskyldighet, utan basera skyldigheten på leverantörernas storlek och vilken typ av tjänster de erbjuder och till exempel undanta sådana leverantörer som erbjuder högspecialiserade tjänster.

75 Tillståndssystemen skulle kunna bygga på periodiska utvärderingar av hoten i varje medlemsstat. Det bör säkerställas att kopplingen mellan de lagrade uppgifterna och det eftersträvade syftet görs och anpassas efter den särskilda situation som föreligger i varje medlemsstat. De lagringstillstånd som beviljats leverantörerna skulle således kunna medföra att vissa typer av uppgifter lagras under en viss tid, beroende på utvärderingen av hotet. Sådana tillstånd skulle kunna beviljas av en domstol eller en oberoende förvaltningsmyndighet och de skulle kunna medföra periodiska kontroller av om lagringen är nödvändig.

94. I praktiken innebär det att i de två huvudkategorierna (trafikuppgifter och lokaliseringsuppgifter) ska genom användning av lämpliga filter bara den *minimala* mängd uppgifter lagras som anses absolut nödvändig för att på ett effektivt sätt kunna förebygga och kontrollera brottslighet och skydda nationell säkerhet.

95. Det ankommer på medlemsstaterna eller på unionens institutioner att genom lagstiftning (med hjälp av sina egna experter) göra detta urval och undvika varje försök att ålägga en skyldighet att generellt och odifferentierat lagra alla trafik- och lokaliseringsuppgifter.

96. Förutom denna begränsning till vissa kategorier, bör uppgifterna bara få lagras under en viss period, för att det inte ska gå att få fram en detaljerad bild av de berörda personernas liv. Denna lagringsperiod bör dessutom vara anpassad till uppgifternas karaktär, så att de uppgifter som ger närmare information om dessa personers livsstil och vanor lagras under en kortare tidsperiod. [76]

97. Med andra ord är en differentiering av lagringsperioden för var och en av uppgiftskategorierna, som bygger på hur viktiga de är för att uppnå säkerhetsmålen, ett alternativ som bör undersökas. Genom att begränsa den tid under vilken de båda kategorierna av uppgifter lagras samtidigt (och därmed kan användas för att hitta samband som avslöjar de berörda personernas livsstil), utökas skyddet av den rättighet som värnas genom artikel 8 i stadgan.

98. I denna riktning uttalade sig Europeiska datatillsynsmannen vid förhandlingen: ju fler kategorier av metadata som lagras och ju längre lagringstiden är, desto lättare är det att få fram en detaljerad profil av en person och vice versa. [77]

99. Det är för övrigt svårt att dra en gräns mellan vissa metadata vid elektronisk kommunikation och själva innehållet i denna kommunikation, vilket även framkom vid förhandlingen. Vissa metadata kan vara minst lika avslöjande som själva innehållet i kommunikationen. Så kan exempelvis vara fallet med adresserna (URL) till de webbplatser som besökts. [78] Det är därför särskild uppmärksamhet bör ägnas åt den typen av uppgifter och andra liknande, för att maximalt begränsa behovet av att lagra dem och den tid under vilken de lagras.

100. Att hitta en balanserad lösning är inte lätt, eftersom tekniken för att kontrollera uppgifter mot varandra och koppla samman uppgifter gör det möjligt för de utredande och övervakande myndigheterna att identifiera en misstänkt person eller ett hot. Trots det finns det en gradskillnad mellan lagring av uppgifter för att upptäcka sådana misstänkta personer eller hot och lagring som leder till att man får en detaljerad bild av en persons liv.

101. I avvaktan på en gemensam reglering för hela unionen inom just detta område, anser jag inte att man kan begära att domstolen ska utföra lagstiftande uppgifter och noga precisera vilka kategorier av uppgifter som får lagras och under hur lång tid. Det ankommer på unionens och medlemsstaternas institutioner att, när väl de gränser har fastställts som enligt domstolen följer av stadgan, sätta markören på rätt plats för att åstadkomma en balans mellan upprätthållandet av säkerheten och de grundläggande rättigheter som skyddas genom stadgan.

[76] Detta tycks vara det system som tillämpas i Förbundsrepubliken Tyskland, vars regering vid förhandlingen påpekade att lagringstiden för trafikuppgifter enligt tysk lagstiftning är tio veckor, medan lagringstiden för lokaliseringsuppgifter bara är fyra veckor. Republiken Frankrike anser däremot att det är nödvändigt med en period på ett år för lagring av trafikuppgifter och lokaliseringsuppgifter. Enligt den medlemsstaten skulle en kortare lagringsperiod än ett år medföra att kriminalpolisens arbete blev mindre effektivt.

[77] Det ska naturligtvis säkerställas att leverantörerna av elektroniska kommunikationstjänster raderar uppgifterna permanent vid lagringsperiodens slut (med undantag av de uppgifter som får fortsätta att lagras för affärsmässigt bruk enligt direktiv 2002/58).

[78] Vid förhandlingen uppgav den franska regeringen att uppgifter om URL var undantagna från de uppkopplingsuppgifter för vilka lagen föreskriver en allmän lagringsskyldighet.

102. Att avstå från information som kan fås fram från en större mängd lagrade uppgifter skulle visserligen i en del fall kunna göra det svårare att bekämpa potentiella hot. Det är dock ett pris, bland andra, som myndigheterna får betala när de ålägger sig själva en skyldighet att skydda de grundläggande rättigheterna.

103. På samma sätt som att ingen skulle förespråka en skyldighet på förhand att generellt och odifferentierat lagra *innehållet* i privat elektronisk kommunikation (inte ens när lagarna säkerställer en begränsad tillgång till detta innehåll senare), bör metadata från denna kommunikation, vilka kan innehålla lika känslig information som själva innehållet, kunna bli föremål för en odifferentierad och generell lagring.

104. Den omständigheten att det är svårt (vilken jag medger att det är) att i lagstiftning noga ange i vilka fall och under vilka villkor som riktad lagring ska få göras, rättfärdigar inte att medlemsstaterna gör ett undantag till huvudregel och omvandlar en generell lagring av personuppgifter till den centrala principen i sina lagstiftningar. Om så hade varit fallet, skulle en allvarlig kränkning av rätten till skydd av personuppgifter på obestämd tid ha godtagits.

105. Jag vill tillägga att ovanstående reflektioner inte hindrar att det i verkligt *exceptionella* situationer, där det föreligger ett överhängande hot eller en extraordinär risk som motiverar en officiell förklaring om nödläge i en medlemsstat, under en begränsad tid i den nationella lagstiftningen föreskrivs en möjlighet att införa en så omfattande och allmän skyldighet att lagra uppgifter som anses nödvändig.

106. Det skulle i sådana fall kunna införas en lagstiftning som särskilt medger en mer omfattande lagring av (och tillgång till) uppgifter, i enlighet med villkor och förfaranden som säkerställer att dessa åtgärder är av extraordinär karaktär när det gäller deras materiella räckvidd och deras utsträckning i tiden, samt de erforderliga rättsliga garantierna.

107. En jämförelse mellan de olika regelverken för grundlagsstadgade nödsituationer visar att det inte är omöjligt att avgränsa faktiska omständigheter som kan utlösa en tillämpning av ett visst regelverk och föreskriva vilken myndighet som ska fatta beslutet, på vilka villkor det ska ske och hur tillsynen ska se ut.[79]

E. De specifika svaren på de tre tolkningsfrågorna

1. Inledande anmärkning

108. Den hänskjutande domstolen efterfrågar en tolkning av artikel 15.1 i direktiv 2002/58 mot bakgrund av flera rättigheter som säkerställs i stadgan, nämligen rätten till respekt för privatlivet och familjelivet (artikel 7), rätten till skydd av personuppgifter (artikel 8) och rätten till yttrandefrihet och informationsfrihet (artikel 11).

109. Som jag påpekar i mitt förslag till avgörande i målen C-511/18 och C-512/18, är det dessa rättigheter som enligt domstolen kan beröras i dessa fall.

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

110. Cour constitutionnelle (Författningsdomstolen) hänvisar emellertid även till artiklarna 4 och 6 i stadgan, vilka den andra respektive den första tolkningsfrågan handlar om.

111. Vad beträffar artikel 6 i stadgan, vilken säkerställer rätten till frihet och säkerhet, så har det även hänvisats till den i målen C-511/18 och C-512/18. Jag har uttalat mig om dess relevans i mitt förslag till avgörande i de målen, vilket jag hänvisar till. [80]

112. Vad beträffar artikel 4 i stadgan, anser jag att det är lämpligt att besvara frågan om den först, eftersom svaret på den i mindre grad bygger på en bedömning av den nationella lagstiftningen – för att kunna jämföra den med unionsrätten – än på en tolkning av den bestämmelsen.

2. Den andra tolkningsfrågan

113. Hänvisningen till förbudet mot tortyr och omänsklig eller förnedrande bestraffning och behandling, som garanteras av artikel 4 i stadgan, gäller enbart denna begäran om förhandsavgörande, vilket gör att den behöver tas upp här.

114. Genom att hänvisa till artikel 4 i stadgan vill den hänskjutande domstolen visa att den nationella bestämmelsen även har till syfte att uppfylla den *positiva skyldighet* som åligger myndigheterna att inrätta ”en rättslig ram som möjliggör effektiv brottsutredning och verkningsfulla straff för sexuella övergrepp mot minderåriga och som gör det möjligt att på ett effektivt sätt identifiera gärningsmannen, även när elektroniska kommunikationstjänster används”. [81]

115. Jag anser att just denna *positiva skyldighet* inte skiljer sig så mycket från var och en av de särskilda förpliktelser som för staten tar sig uttryck i tillkännagivandet av en rad grundläggande rättigheter. Rätten till liv (artikel 2 i stadgan), till integritet (artikel 3 i stadgan) eller till skydd av personuppgifter (artikel 8 i stadgan), liksom yttrandefriheten (artikel 11 i stadgan) och tankefriheten, samvetsfriheten och religionsfriheten (artikel 10 i stadgan), medför en skyldighet för staten att utarbeta rättsliga ramar som garanterar att dessa rättigheter faktiskt kan åtnjutas, vid behov med hjälp av myndigheternas tvångsmonopol, till skydd mot den som försöker förhindra eller försvåra detta. [82]

116. Vad beträffar sexuella övergrepp mot minderåriga anser Europadomstolen att barn och andra utsatta personer har en kvalificerad rätt till skydd av staten, genom att den antar straffrättsliga bestämmelser som på ett effektivt sätt bestraffar sådana brott och har en avskräckande verkan. [83]

117. Denna kvalificerade rätt till skydd omfattas inte bara av artikel 4 i stadgan, utan här skulle även artikel 1 (människans värdighet) eller artikel 3 (rätten till fysisk och mental integritet) utan vidare kunna åberopas.

[80] Förslag till avgörande i de förenade målen C-511/18 och C-512/18, punkt 95 och följande punkter.

[81] Denna formulering är hämtad från den andra tolkningsfrågan, *in fine*. Hänvisningen till elektroniska kommunikationsmedel förklarar varför frågan tar upp ytterligare en *positiv skyldighet* som åvilar staterna, nämligen den som följer av artikel 8 i stadgan när det gäller skydd av personuppgifter. Den dubbla hänvisningen till artikel 8 i stadgan visar att den hänskjutande domstolen anser att rättigheterna i stadgan, beroende på deras art, har en dubbel uppgift: som *gräns* för den omtvistade skyldigheten och som *motivering* till denna skyldighet.

[82] Denna skyldighet att säkerställa ett faktiskt åtnjutande tar sig uttryck i ett påbud rörande resultat för myndigheterna i välfärdsstaten, där det inte bara är det formella erkännandet av rättigheterna som har betydelse utan även det praktiska genomförandet av deras materiella innehåll.

[83] Europadomstolen, dom av den 2 december 2008, K.U. mot Finland (CE:ECHR:2008:1202JUD000287202), § 46.

118. Även om man inte kan bortse från myndigheternas positiva skyldighet att garantera skydd för barn och andra utsatta personer när man överväger de rättsliga intressen som berörs av den nationella lagstiftningen,[84] får den heller inte medföra en ”orimlig belastning” för myndigheterna[85] eller uppfyllas utan lagligt stöd och utan att de övriga grundläggande rättigheterna iakttas.[86]

3. Den första tolkningsfrågan

119. Den hänskjutande domstolen vill i korthet veta om unionsrätten utgör hinder för den nationella lag som den ska uttala sig om inom ramen för en talan om grundlagsstridighet.

120. Eftersom domstolen redan har tillhandahållit en tolkning av direktiv 2002/58 som överensstämmer med motsvarande bestämmelser i stadgan, bör svaret på tolkningsfrågan beakta den rättspraxis som följer av domen Tele2 Sverige och Watson, eventuellt med de nyanseringar som läggs till här.

121. Mot bakgrund av detta måste de tolkningsriktlinjer som domstolen kan erbjuda Cour constitutionnelle (Författningsdomstolen) när den själv ska pröva om den nationella lagstiftningen är förenlig med unionsrätten, handla om lagring av uppgifter och tillgång till uppgifter, var och en för sig, så som de regleras i den nationella lagstiftningen.

a) Villkoren för lagring av personuppgifter

122. Den belgiska regeringen har betonat att den avsåg att införa en tydlig rättslig ram som innefattade de garantier som krävs för att skydda privatlivet och som inte byggde på praxis hos leverantörerna av elektroniska kommunikationstjänster rörande lagring av uppgifter för fakturering och hantering av informationsförfrågningar från kunderna.

123. Enligt den belgiska regeringen syftar den allmänna och preventiva skyldigheten att lagra uppgifter inte bara till att utreda och lagföra allvarliga brott, utan även till att skydda nationell säkerhet, landets försvar och allmän säkerhet, samt till att utreda, avslöja och lagföra andra brott än grova brott och förebygga otillåten användning av de elektroniska kommunikationssystemen,[87] eller något av de andra syften som anges i artikel 23.1 i förordning 2016/679.

124. Den belgiska regeringen har anfört följande:

– Lagringen av uppgifter som sådan innebär inte att det går att dra mycket precisa slutsatser rörande de berörda personernas privatliv. Den möjligheten finns bara om det även ges tillgång till de lagrade uppgifterna.

84 I detta sammanhang anser jag att till de rättigheter som den hänskjutande domstolen hänvisar till (som *gränser* för den omtvistade skyldigheten, inte som en *motivering* av den) skulle kunna läggas rätten till ett effektivt rättsmedel (artikel 47 i stadgan) eller rätten till försvar (artikel 48 i stadgan), vars eventuella åsidosättande också har varit föremål för debatt i de nationella målen. I själva beslutsdelen i beslutet att begära förhandsavgörande nämns emellertid bara artiklarna 7, 8, 11 och 52.1 i stadgan.

85 Europadomstolen, dom av den 28 oktober 1998, Osman mot Förenade kungariket (CE:ECHR:1998:1028JUD002345294), § 116.

86 *Ibidem*, punkt 116 *in fine*. ”Det måste säkerställas att polisen utövar sin befogenhet att bekämpa och förebygga brott med fullt iakttagande av lagliga metoder och de andra garantier som på ett berättigat sätt begränsar omfattningen av dess brottsutredande handlingar.” Se även Europadomstolens dom av den 2 december 2008, K.U. mot Finland (CE:ECHR:2008:1202JUD000287202), § 48. På liknande sätt har domstolen i punkt 49 i dom av den 29 juli 2019, Gambino och Hyka (C-38/18, EU:C:2019:628) slagit fast att den rättighet som föreskrivs till förmån för ett brottsoffer inte kan påverka möjligheten för den tilltalade att faktiskt åtnjuta sina rättigheter.

87 Det är även motiverat för att svara på ett samtal till en räddningstjänst eller för att hitta en försvunnen person, när det föreligger en överhängande fara för personens hälsa.

– Lagen innehåller mekanismer för att skydda integriteten. Bland annat påverkar lagringen av uppgifterna inte kommunikationernas innehåll; garantierna vad beträffar motiveringen till lagringen, rätten till tillgång och rätten till rättelse m.fl. är fullt tillämpliga; leverantörerna och operatörerna måste underkasta de lagrade uppgifterna samma skyldigheter och säkerhets- och skyddsåtgärder som de som är tillämpliga på uppgifter på internet och förhindra att de oavsiktligt eller rättsstridigt förstörs, förloras eller oavsiktligt ändras.

– Uppgifterna får lagras i tolv månader (därefter ska de utplånas) och bara inom unionens territorium.

– Leverantörerna och operatörerna ska använda sig av tekniska skyddsåtgärder som gör att de lagrade uppgifterna så snart de registreras blir oläsliga och oanvändbara för alla personer som inte har rätt att få tillgång till dem.

– Under alla förhållanden sker dessa operationer under tillsyn av den belgiska tillsynsmyndigheten för post och telekommunikation och dataskyddsmyndigheten.

125. Trots dessa garantier stämmer det att den belgiska lagstiftningen ålägger operatörer och leverantörer av elektroniska kommunikationstjänster en allmän och odifferentierad skyldighet att lagra trafik- och lokaliseringsuppgifter, i den mening som avses i direktiv 2002/58, som behandlas i samband med att sådana tjänster tillhandahålls. Lagringstiden är som nämnts i allmänhet tolv månader, och det föreskrivs ingen tidsbegränsning beroende på vilka kategorier av uppgifter som lagras.

126. Denna allmänna och odifferentierade skyldighet gäller varaktigt och fortlöpande. Även om syftet är att förebygga, utreda och lagföra alla sorters brott (från sådana som har samband med nationell säkerhet, försvar eller särskilt allvarliga brott, till sådana brott för vilka det föreskrivs högst ett års fängelse), är en skyldighet av det här slaget inte förenlig med domstolens praxis, vilket innebär att den inte kan anses vara förenlig med stadgan.

127. För att anpassa sig till denna rättspraxis behöver den belgiska lagstiftaren utforska andra vägar (som dem jag tidigare har nämnt) som innebär begränsade lagringsmetoder. Dessa metoder, som kan variera beroende på vilken kategori av uppgifter det rör sig om, måste iaktta principen att det bara får lagras ett *minimalt* antal uppgifter som är nödvändiga, beroende på risk eller hot, och under en begränsad tid, vilken är beroende av den lagrade informationens art. Under alla förhållanden får lagringen inte medföra en noggrann *kartläggning* av de berörda personernas privatliv, vanor, beteende eller sociala relationer.

b) Villkoren för myndigheternas tillgång till de lagrade uppgifterna

128. Jag anser att de villkor som domstolen angav i domen Tele2 Sverige och Watson [88] även är relevanta när det gäller tillgången. Den nationella lagstiftningen ska föreskriva de materiella och processuella villkoren för att de behöriga myndigheterna ska få tillgång till de lagrade uppgifterna. [89]

88 Se punkt 60 i detta förslag till avgörande.

89 Domen Tele2 Sverige och Watson, punkt 118.

129. Enligt den belgiska regeringen föreskriver artikel 126.2 i 2005 års lag (om elektronisk kommunikation) [90] på ett restriktivt sätt vilka nationella myndigheter som kan få tillgång till de uppgifter som lagras i enlighet med punkt 1 i samma artikel.

130. Bland dessa myndigheter återfinns domstolarna och åklagarmyndigheten, statens säkerhetstjänst, den allmänna underrättelse- och säkerhetstjänsten, vilka står under kontroll av var sin oberoende kommission, polistjänstemän vid det belgiska institutet för post- och teletjänster, räddningstjänsterna, polistjänstemän vid den federala polisens enhet för försvunna personer, medlingstjänsten för telekommunikationer och finansinspektionen.

131. Generellt gör den belgiska regeringen gällande att den nationella lagstiftningen inte medger att de olika organen får tillgång till uppgifter för att aktivt bekämpa hot som inte har identifierats eller där det inte finns några konkreta indicier. De nationella myndigheterna kan således inte utan vidare få tillgång till rådata om kommunikation och behandla den automatiskt för att få fram information och aktivt förebygga hot mot säkerheten.

132. Enligt den belgiska regeringen är tillgången till uppgifterna underkastad stränga villkor som är beroende av den ställning som var och en av de behöriga nationella myndigheterna har.

133. Jag anser inte att svaret på den första tolkningsfrågan kräver att domstolen gör en uttömmande analys av de villkor som gäller för att var och en av dessa myndigheter ska få tillgång till de lagrade uppgifterna. Denna uppgift faller snarast på den hänskjutande domstolen, som bör utföra den mot bakgrund av den vägledning som domstolen tillhandahållit i domarna Tele2 Sverige och Watson och Ministerio Fiscal.

134. För övrigt finns det enligt den information som den belgiska regeringen har tillhandahållit betydande skillnader mellan villkoren för att domstolarna och åklagarmyndigheten [91] ska få tillgång till uppgifter för att utreda och lagföra brott, enligt artiklarna 46 *bis* [92] och 88 *bis* [93] i straffprocesslagen, och de villkor som gäller för andra myndigheter.

135. Vad beträffar underrättelse- och säkerhetstjänsterna, måste enligt 1998 års lag en begäran om tillgång till trafik- och lokaliseringsuppgifter som finns hos operatörerna bygga på objektiva kriterier för att säkerställa att den begränsas till vad som är strängt nödvändigt, på grundval av ett på förhand identifierat hot. [94] Det föreskrivs olika tidsgränser (sex, nio eller tolv månader) för

90 Artikel 126, i dess lydelse enligt lagen av den 29 maj 2016.

91 Huruvida åklagarmyndigheten är lämpad att besluta om åtgärder av det här slaget är omtvistat i målet C-746/18, HK/Prokuratur, vilket ännu inte har avgjorts.

92 Åklagarmyndigheten är behörig att begära ut identitetsuppgifter från operatörer, genom ett motiverat skriftligt beslut (det får vara muntligt i brådskande fall) som visar att åtgärden är proportionerlig med hänsyn till respekten för privatlivet och subsidiär till andra utredningsskyldigheter. Vid brott på vilka inte kan följa fängelse i ett år eller mer, får åklagarmyndigheten bara begära ut uppgifter för en period av sex månader före beslutet.

93 Det är undersökningsdomaren som är behörig att ålägga operatörerna spårning av elektronisk kommunikation eller av lagrade trafik- eller lokaliseringsuppgifter, och denne får besluta om en sådan åtgärd om det finns allvarliga indicier på att ett brott har begåtts på vilket vissa straff kan följa, genom ett motiverat skriftligt beslut (det får vara muntligt i brådskande fall) som omfattas av samma krav på proportionalitet och subsidiaritet som de som gäller för åklagarmyndigheten. Det finns vissa undantag när åtgärden riktar sig mot vissa skyddade yrkesgrupper (till exempel advokater eller läkare).

94 Beslutet ska, alltefter omständigheterna, innehålla uppgifter om vilka fysiska eller juridiska personer, sammanslutningar eller de facto-grupper, föremål, platser eller händelser eller vilken information som omfattas av den särskilda metoden. Det bör även anges vilket samband som finns mellan syftet med de begärda uppgifterna och det potentiella hot som motiverar just denna metod.

tillgång beroende på det potentiella hotet, och begäran måste iaktta principerna om proportionalitet och subsidiaritet. Det har dessutom införts en kontrollmekanism, som handhas av en oberoende myndighet. [95]

136. Vad beträffar polistjänstemän vid det belgiska institutet för post- och teletjänster (BIPT), är det möjligt för dem att få tillgång till uppgifter som finns hos telekommunikationsoperatörerna, under tillsyn av åklagarmyndigheten, i vissa mycket begränsade fall, [96] och enligt den belgiska regeringen omfattar deras verksamhet inte personer vilkas uppgifter lagras.

137. Vad beträffar räddningstjänsterna, som tillhandahåller hjälp på plats, får de begära uppgifter om den som ringt ett nödsamtal när de efter ett sådant samtal inte kan få uppgifter, eller endast får ofullständiga eller felaktiga uppgifter, om den uppringandes identitet från den berörda leverantören eller operatören.

138. Vad beträffar polistjänstemän vid den federala polisens enhet med ansvar för sökande efter försvunna personer, får de från operatören begära att få de uppgifter som krävs för att hitta en försvunnen person när det föreligger en överhängande fara för personens hälsa. Tillgången, som omfattas av stränga villkor, inskränker sig till de uppgifter som krävs för att identifiera användaren samt uppgifter om tillgång och anslutning till nätterminaler och om tjänsten, samt uppgifter om var utrustningen finns, och de omfattar bara uppgifter som lagrats under 48 timmar före begäran.

139. Vad beträffar Medlingstjänsten för telekommunikationer, får den bara begära uppgifter för att identifiera en person som gjort en felaktig användning av ett nät eller av elektroniska kommunikationstjänster. Det finns i sådana fall inte någon föregående kontroll av en domstol eller oberoende förvaltningsmyndighet (som är fristående från själva tjänsten).

140. Avslutningsvis får Finansinspektionen i syfte att bekämpa ekonomisk brottslighet ges tillgång till trafik- och lokaliseringsuppgifter, vilken först måste godkännas av undersökningsdomaren.

141. Redogörelsen för dessa former och villkor för tillgång till lagrade uppgifter, som gäller för var och en av de myndigheter som har tillstånd att begära ut dem, visar att det finns en rad olika situationer och skyddsmekanismer, och det ankommer på den hänskjutande domstolen att pröva om dessa strikt följer de kriterier som domstolen har använt sig av i sin praxis. [97]

142. Jag noterar till exempel att det i samband med den omtvistade lagstiftningen inte finns någon uppgift om att de behöriga nationella myndigheterna är skyldiga att systematiskt informera de berörda personerna (under förutsättning att det inte riskerar att skada pågående utredningar) om att deras uppgifter har begärts ut. Inte heller förefaller det föreskrivas några på förhand bestämda regler för hur allvarliga brotten ska vara för att det ska motivera en tillgång till uppgifterna i fråga,

[95] Förvaltningskommittén för tillsyn över särskilda och extraordinära metoder för insamling av uppgifter som används av underrättelse-och säkerhetstjänsterna (BIM-kommittén) och Ständiga kommittén för kontroll av underrättelsetjänsterna (R-kommittén). Den belgiska regeringen har uppgett att BIM-kommittén har ansvar för uppföljningen av de sökmetoder som underrättelse- och säkerhetstjänsterna använder, över vilka den utövar en kontroll i första ledet. Denna kommitté, som är sammansatt av domare, utför sina uppgifter helt självständigt. Det finns även en oberoende kontroll i andra ledet, som utövas av R-kommittén.

[96] Det är tillåtet för utredning och lagföring av brott enligt artiklarna 114 (nätsäkerhet), 124 (konfidentialitet för elektronisk kommunikation) och 126 (lagring av uppgifter och tillgång) i lagen av den 13 juni 2005 om elektronisk kommunikation.

[97] Jag hänvisar till punkt 60 i detta förslag till avgörande.

utom i vissa fall, exempelvis rörande ekonomiska brott. Sambandet mellan ingreppets omfattning och det utredda brottets svårighetsgrad, i den mening som avses i domen Ministerio Fiscal, är inte uppenbart i samtliga fall.

143. Under alla förhållanden anser jag att övervägandena rörande myndigheternas tillgång till uppgifterna av ovannämnda skäl får en underordnad betydelse och att det är själva den generella och odifferentierade lagringen av dessa uppgifter som är huvudskälet till att den nationella lagstiftning som begäran om förhandsavgörande avser inte är förenlig med unionsrätten.

4. Den tredje tolkningsfrågan

144. Cour constitutionnelle (Författningsdomstolen) vill veta huruvida rättsverkningarna av den nationella lagstiftningen tills vidare kan bestå, för det fallet att det mot bakgrund av domstolens praxis slås fast att denna lagstiftning är oförenlig med unionsrätten. På så sätt skulle rättsosäkerhet kunna undvikas och tidigare insamlade och lagrade uppgifter fortfarande kunna användas för de ändamål som anges i lagen.

145. Det följer av fast rättspraxis att ”endast domstolen undantagsvis och av tvingande rättssäkerhetshänsyn kan tillåta att det företräde som en regel i unionsrätten har i förhållande till nationell rätt som strider mot denna skjuts upp. Om de nationella domstolarna hade kunnat ge nationella bestämmelser företräde framför den unionsrätt som strider mot dem, om än tillfälligt, skulle det nämligen äventyra den enhetliga tillämpningen av unionsrätten”. [98]

146. Kommissionen anser att eftersom domstolen inte har begränsat rättsverkningarna i tiden av tolkningen av artikel 15.1 i direktiv 2002/58, bör svaret på denna fråga från den hänskjutande domstolen vara nekande. [99]

147. Domstolen slog emellertid i domen av den 28 februari 2012, Inter-Environnement Wallonie och Terre wallonne, [100] fast att det undantagsvis kan tillåtas att en nationell domstol, när det föreligger tvingande miljöskyddshänsyn, tillämpar den nationella bestämmelse som ger den instansen behörighet att förordna att vissa rättsverkningar av en nationell rättsakt som ogiltigförklarats på grund av åsidosättande av direktivet om strategiska miljöbedömningar ska bestå. [101]

148. Denna rättspraxis har bekräftats genom dom av den 29 juli 2019, Inter-Environnement Wallonie och Bond Beter Leefmilieu Vlaanderen. [102] Även om denna praxis rörde området miljöskydd eller byggde på säkerställandet av elförsörjningen, ser jag inga skäl till varför den inte skulle kunna tillämpas inom andra unionsrättsliga områden, bland annat det här aktuella.

98 Dom av den 28 juli 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, punkt 33).

99 Punkt 100 i kommissionens skriftliga yttrande.

100 Mål C-41/11, EU:C:2012:103.

101 Dom av den 28 februari 2012, Inter-Environnement Wallonie och Terre wallonne (C-41/11, EU:C:2012:103, punkt 58). I punkt 34 i sin dom av den 28 juli 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603), drog domstolen slutsatsen av det konstaterandet att ”domstolen avser att utifrån varje enskilt fall och undantagsvis ge en nationell domstol möjlighet att anpassa verkningarna av att en nationell bestämmelse som befunnits strida mot unionsrätten ogiltigförklaras”.

102 Mål C-411/17, EU:C:2019:622, punkt 178.

149. Att ”tvingande miljöskyddshänsyn” i undantagsfall kan motivera att de nationella domstolarna bibehåller vissa rättsverkningar av en nationell bestämmelse som är oförenlig med unionsrätten beror på att miljöskyddet är ”ett av unionens huvudsakliga mål som är av tvärgående och grundläggande karaktär”. [103]

150. Bland unionens mål finns även skapandet av ett område med säkerhet (artikel 3 FEU), vilket innefattar att respektera väsentliga statliga funktioner, särskilt funktioner vars syfte är att upprätthålla lag och ordning och skydda den nationella säkerheten (artikel 4.2 FEU). Det är ett mål som inte är mindre ”tvärgående och grundläggande” än miljöskyddet, eftersom uppnåendet av det är en nödvändig förutsättning för att kunna införa ett rättsligt ramverk som kan säkerställa det faktiska åtnjutandet av de grundläggande rättigheterna och friheterna.

151. Jag anser att tvingande skäl som har samband med skyddet av nationell säkerhet i detta fall skulle kunna motivera att domstolen, som ett undantagsfall, tillåter den hänskjutande domstolen att bibehålla åtminstone några av rättsverkningarna av den omtvistade lagen.

152. Ett sådant bibehållande förutsätter att den hänskjutande domstolen, mot bakgrund av domstolens uttalande, anser att den nationella lagstiftningen är oförenlig med unionsrätten och att verkningarna av ett omedelbart upphävande av den, eller en underlåtenhet att tillämpa den, skulle vara synnerligen skadligt för den allmänna säkerheten eller för statens säkerhet (om upphävandet skulle vara konsekvensen av denna oförenlighet enligt den nationella rätten).

153. Ett tillfälligt bibehållande (helt eller delvis) av rättsverkningarna av den nationella lagstiftningen skulle dessutom kräva att

– syftet med detta tillfälliga bibehållande är att undvika ett rättsligt tomrum med verkningar som är lika skadliga som en tillämpning av den omtvistade lagstiftningen skulle vara, och att det skulle vara omöjligt att fylla detta tomrum på något annat sätt och frånta de nationella myndigheterna ett värdefullt instrument för att garantera statens säkerhet, och att

– rättsverkningarna bara består under den tid som är absolut nödvändig för att vidta de åtgärder som avhjälper den konstaterade oförenligheten med unionsrätten. [104]

154. För en sådan lösning talar dessutom svårigheten att anpassa de nationella lagstiftningarna till den rättspraxis som följer av domen Tele2 Sverige och Watson [105] och att den belgiska lagstiftarens avsikt visat sig genom att den godtagit domen Digital Rights och ändrat sin egen lagstiftning. Det innebär att det kan förväntas att den även kommer att anpassa lagen av den 29 maj 2016 (som antogs innan domen Tele2 och Watson hade offentliggjorts) till den rättspraxis som följer av den sistnämnda domen.

[103] Dom av den 28 februari 2012, Inter-Environnement Wallonie och Terre wallonne (C-41/11, EU:C:2012:103, punkt 57).

[104] Dom av den 28 februari 2012, Inter-Environnement Wallonie och Terre wallonne (C-41/11, EU:C:2012:103, punkt 62).

[105] Punkt 45 i den danska regeringens skriftliga yttrande.

V. Förslag till avgörande

155. Mot bakgrund av vad som ovan anförts föreslår jag att domstolen ska ge Cour constitutionnelle (Författningsdomstolen, Belgien) följande svar:

”1) Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), jämförd med artiklarna 7, 8 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas så, att den

– utgör hinder för en nationell lagstiftning som ålägger operatörer och leverantörer av elektroniska kommunikationstjänster en generell och odifferentierad skyldighet att lagra trafik- och lokaliseringsuppgifter rörande alla abonnenter och användare avseende alla elektroniska kommunikationsmedel.

– Ovanstående svar påverkas inte av att målet med den nationella lagstiftningen inte bara är att utreda, avslöja och lagföra brott, grova eller mindre grova, utan även att skydda nationell säkerhet, försvaret och allmän säkerhet eller förebygga otillåten användning av elektroniska kommunikationssystem eller något annat mål enligt artikel 23.1 i 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).

– Svaret påverkas inte heller av att tillgången till de lagrade uppgifterna åtföljs av närmare angivna skyddsmekanismer. Det ankommer på den hänskjutande domstolen att pröva om den nationella lagstiftning som reglerar villkoren för de behöriga myndigheternas tillgång till uppgifterna begränsar den till särskilda fall som är så allvarliga att det är nödvändigt med ett ingripande, ställer som villkor att det sker en förhandskontroll (utom i brådskande fall) av en domstol eller en oberoende myndighet samt föreskriver att de berörda personerna ska informeras om att tillgång lämnats till uppgifterna, under förutsättning att det inte är skadligt för myndigheternas verksamhet att informera om detta.

2) Artiklarna 4 och 6 i Europeiska unionens stadga om de grundläggande rättigheterna påverkar inte tolkningen av artikel 15.1 i direktiv 2002/58, jämförd med de övriga ovannämnda artiklarna i stadgan, på ett sätt som förhindrar att det slås fast att en nationell lagstiftning som den som är aktuell i det nationella målet är oförenlig med unionsrätten.

3) En nationell domstol får, om den nationella rätten medger det, i undantagsfall och under en begränsad tid bibehålla rättsverkningarna av en lagstiftning, som den som är aktuell i det nationella målet, trots att den är oförenlig med unionsrätten, om ett sådant bibehållande är motiverat av tvingande skäl som har samband med hot mot allmän säkerhet eller nationell säkerhet som inte kan bemötas med andra metoder eller på andra sätt. Ett sådant bibehållande får endast omfatta den tidsrymd som är absolut nödvändig för att avhjälpa denna oförenlighet med unionsrätten.”