Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
MACIEJ SZPUNAR
föredraget den 27 oktober 2022 [1]

Mål C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'access à Internet associatifs,
Franciliens.net,
French Data Network
mot
Premier ministre,
Ministère de la Culture

(begäran om förhandsavgörande från Conseil d'État (Frankrike))

”Begäran om förhandsavgörande – Behandling av personuppgifter inom sektorn för elektronisk kommunikation – Direktiv 2002/58/EG – Artikel 15.1 – Medlemsstaternas rätt att begränsa omfattningen av vissa rättigheter och skyldigheter – Förpliktelse om förhandskontroll av en domstol eller av ett oberoende förvaltningsorgan vars avgöranden har bindande verkan – Uppgifter om den fysiska identitet som motsvarar en IP-adress”

I. Inledning

1. Frågan om lagring av och åtkomst till vissa uppgifter om internetanvändare är en ständigt aktuell fråga som redan hunnit bli föremål för en ny men riklig praxis från domstolen.

2. Det nu aktuella målet ger domstolen ännu ett tillfälle att behandla denna fråga, nu i sammanhanget av bekämpandet av intrång i immateriella rättigheter som enbart begås på internet.

[1] Originalspråk: franska.

II. Tillämpliga bestämmelser

A. Unionsrätt

3. I skälen 2, 6, 7, 11, 22, 26 och 30 i direktiv 2002/58/EG [2] anges följande:

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

…

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

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

…

(11) I likhet med direktiv 95/46/EG[3] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av gemenskapslagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna [undertecknad i Rom den 4 november 1950] i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

…

[2] Europaparlamentets och rådets direktiv 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).

[3] Europaparlamentets och rådets direktiv 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).

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

…

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

…

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

4. I artikel 2 i direktivet, som har rubriken ”Definitioner”, anges följande:

”…

Dessutom skall följande definitioner gälla:

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

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

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

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

…”

5. I artikel 3 i direktivet, som har rubriken ”Berörda tjänster”, föreskrivs följande:

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

6. I artikel 5 i samma direktiv, som har rubriken ”Konfidentialitet vid kommunikation”, föreskrivs följande:

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

…

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

7. Artikel 6 i direktiv 2002/58, som har rubriken ”Trafikuppgifter”, har följande lydelse:

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

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

…”

8. Artikel 15 i direktiv 2002/58 har rubriken ”Tillämpningen av vissa bestämmelser i direktiv [95/46]”. I artikel 15.1 anges följande:

”Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv [95/46]. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i [union]slagstiftningen, inklusive principerna i artikel 6.1 och 6.2 [FEU].”

B. Fransk rätt

1. Lagen om immateriella rättigheter

9. I artikel L. 331–12 i Code de la propriété intellectuelle (lagen om immateriella rättigheter), i den lydelse som är tillämplig i det nationella målet (nedan kallad CPI), föreskrivs följande:

”Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (central myndighet för spridning av verk och rättighetsskydd på internet) [(nedan kallad Hadopi)] är en oberoende offentlig myndighet.”

10. I artikel L. 331–13 CPI föreskrivs följande:

”Hadopi ska sörja för följande:

…

2° Ett uppdrag att skydda [verk och alster som omfattas av upphovsrätt eller en närstående rättighet i elektroniska kommunikationsnät] mot rättighetsintrång som begås i elektroniska kommunikationsnät som används för tillhandahållande av allmänt tillgängliga kommunikationstjänster på internet; …”

11. I artikel L. 331–15 i denna lag anges följande:

”[Hadopi] består av ett kollegium och en kommitté för rättighetsskydd. …

…

Kollegiets ledamöter och ledamöterna av kommittén för rättighetsskydd ska utföra sina uppgifter utan att ta emot instruktioner från någon myndighet.”

12. I artikel L. 331–17 i nämnda lag anges följande:

”Kommittén för rättighetsskydd är ansvarig för att vidta åtgärder enligt artikel L. 331–25.”

13. I artikel L. 331–21 i samma lag anges följande:

”För att kommittén för rättighetsskydd ska kunna utöva sina befogenheter förfogar [Hadopi] över auktoriserade tjänstemän som bemyndigats av [Hadopis] ordförande i enlighet med ett dekret meddelat efter yttrande av Conseil d’État [(Högsta förvaltningsdomstolen, Frankrike)]. …

Kommitténs ledamöter och de tjänstemän som avses i första stycket ska ta emot ärenden som hänskjuts till kommittén i enlighet med artikel L. 331–24. De ska granska de faktiska omständigheterna.

För att kunna genomföra förfarandet får de begära in alla former av handlingar, inbegripet uppgifter som lagras och behandlas av operatörer av elektronisk kommunikation med tillämpning av artikel L. 34–1 i Code des postes et des communications électroniques (lag om elektronisk post och kommunikation) och av de leverantörer som avses i artikel 6 I leden 1 och 2 i Loi n° 2004–575 du 21 juin 2004 pour la confiance dans l’économie numérique (lag nr 2004–575 av den 21 juni 2004 om förtroendet för den digitala ekonomin).

De får också begära in kopior av de handlingar som avses i föregående stycke.

De kan bland annat begära att operatörer av elektronisk kommunikation lämnar ut namn, postadress, e-postadress och telefonnummer till en abonnent vars tillgång till allmänt tillgängliga elektroniska kommunikationstjänster på internet, utan tillstånd från [rättsinnehavarna], har använts för mångfaldigande, återgivning, tillgängliggörande eller överföring av skyddade verk eller alster, om ett sådant tillstånd krävs.”

14. I artikel L. 331–24 CPI föreskrivs följande:

”Kommittén för rättighetsskydd ska agera efter det att ett ärende har hänskjutits av certifierade och auktoriserade ombud … som ska utses av

– lagenligt konstituerade organ som tillvaratar branschintressen,

– kollektiva förvaltningsorgan,

– Centre national du cinéma et de l’image animée (nationellt centrum för film och animerade bilder).

Kommittén för rättighetsskydd kan även agera på grundval av upplysningar som erhålls från allmän åklagare.

Kommittén får inte ta upp ärenden om faktiska omständigheter som är äldre än sex månader.”

15. I artikel L. 331-25 CPI, som reglerar det så kallade ”förfarandet för *graduated response*”, anges följande:

”Om ett ärende avseende gärningar som kan utgöra åsidosättande av skyldigheten enligt artikel L. 336-3 [CPI] hänskjuts till kommittén för rättighetsskydd kan den översända … en rekommendation till abonnenten med en erinran om bestämmelserna i artikel L. 336-3 och en anmodan om att iaktta skyldigheten enligt dessa bestämmelser samt upplysa abonnenten om de påföljder som han eller hon kan påföras enligt artiklarna L. 335-7 och L. 335-7-1. Denna

rekommendation ska även innehålla information till abonnenten om det lagenliga kulturutbudet på internet, säkerhetsåtgärder som finns att tillgå för att förhindra åsidosättande av skyldigheten enligt artikel L. 336-3 och om hotet mot det konstnärliga skapandet och ekonomin i kultursektorn från förfaringssätt ägnade att kringgå upphovsrätten och närstående rättigheter.

För det fall att gärningar som kan utgöra åsidosättande av skyldigheten enligt artikel L. 336-3 upprepas under en period av sex månader efter översändande av rekommendationen enligt första stycket får kommittén översända en ny rekommendation med e-post med samma innehåll som den föregående … Kommittén ska se till att rekommendationen åtföljs av en skrivelse som överlämnas mot underskrift eller på något annat sätt som kan styrka dagen för överlämnandet av rekommendationen.

Rekommendationer enligt denna artikel ska innehålla uppgift om datum och klockslag då gärningar som kan utgöra åsidosättande av skyldigheten enligt artikel L. 336-3 fastställts. Innehållet i de skyddade verk eller alster som berörs av åsidosättandet ska däremot inte anges. En rekommendation ska innehålla telefonnummer, postadress och elektroniska kontaktuppgifter som mottagaren kan använda sig av om han eller hon vill yttra sig till kommittén för rättighetsskydd och, om mottagaren uttryckligen begär det, erhålla klargöranden om innehållet i de skyddade verk eller alster som berörs av det åsidosättande som han eller hon klandrats för.”

16. I artikel L. 331-29 i nämnda lag föreskrivs följande:

”[Hadopi] får upprätta en automatisk behandling av personuppgifter för personer som är föremål för ett förfarande enligt detta underavsnitt.

Ändamålet med denna behandling ska vara att kommittén för rättighetsskydd ska kunna vidta de åtgärder som föreskrivs i detta underavsnitt, upprätta alla handlingar i ärendet, fastställa villkoren för att underrätta organ som tillvaratar branschintressen och kollektiva förvaltningsorgan om ärenden som hänskjutits till rättsliga myndigheter samt för delgivningar enligt vad som föreskrivs i artikel L. 335-7 femte stycket.

Närmare bestämmelser om tillämpningen av denna artikel ska fastställas i ett dekret … Dekretet ska i synnerhet klargöra

– vilka kategorier av uppgifter som ska registreras och hur länge de ska lagras,

– vilka mottagare som har rätt att ta del av uppgifterna, i synnerhet personer vars verksamhet består i att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster,

– under vilka förutsättningar berörda personer kan utöva sin rätt att få tillgång till sina uppgifter hos [Hadopi] …”

17. I artikel R. 331-37 i samma lag föreskrivs följande:

”Operatörer av elektronisk kommunikation … och … leverantörer … är skyldiga att, genom uppkoppling till den automatiska behandlingen av personuppgifter enligt artikel L. 331-29 eller genom att använda sig av ett lagringsmedium som garanterar personuppgifternas integritet och säkerhet, lämna ut personuppgifter och den information som anges i punkt 2 i bilagan till [dekret nr 2010-236 av den 5 mars 2010 om den automatiska behandling av personuppgifter i enlighet med artikel L. 331-29 [CPI] som benämns ’System för förvaltning av åtgärder för skydd av verk på

internet'[4]] inom åtta dagar, räknat från den dag då kommittén för rättighetsskydd lämnar ut de tekniska uppgifter som krävs för att identifiera den abonnent vars tillgång till allmänt tillgängliga elektroniska kommunikationstjänster, utan tillstånd från [rättsinnehavarna], har använts för mångfaldigande, återgivning, tillgängliggörande eller kommunikation av skyddade verk eller alster, om ett sådant tillstånd krävs.

…"

18. I artikel R. 335-5 CPI föreskrivs följande:

"I.- Den som har en anslutning till allmänt tillgängliga kommunikationstjänster på nätet gör sig skyldig till grov oaktsamhet, vilket är förenat med böter i enlighet med vad som föreskrivs för överträdelser av femte graden, om han eller hon utan legitimt skäl, och om villkoren i II är uppfyllda,

1° inte har installerat ett hjälpmedel för att säkra denna anslutning, eller

2° har brustit i aktsamhet vid användningen av detta hjälpmedel.

II.- Bestämmelserna i I är endast tillämpliga om följande två villkor är uppfyllda:

1° Kommittén för rättighetsskydd ska i enlighet med artikel L. 331-25 och på det sätt som föreskrivs i denna artikel ha rekommenderat innehavaren av anslutningen att installera ett hjälpmedel för att säkra sin anslutning som gör det möjligt att förhindra att anslutningen återigen används för mångfaldigande, återgivning, tillgängliggörande eller kommunikation till allmänheten av verk eller alster som skyddas av upphovsrätt eller närstående rättigheter utan tillstånd från [rättsinnehavarna], om ett sådant tillstånd krävs.

2° Anslutningen används på nytt för de ändamål som anges i 1° i denna II under en period av ett år efter det att rekommendationen lämnades."

19. I artikel L. 336-3 i lagen anges följande:

"Den som har en anslutning till allmänt tillgängliga elektroniska kommunikationstjänster ska se till att denna anslutning inte används för mångfaldigande, återgivning, tillgängliggörande eller kommunikation till allmänheten av verk eller alster som skyddas av upphovsrätt eller närstående rättigheter utan tillstånd från [rättsinnehavarna], om ett sådant tillstånd krävs.

Den person som innehar anslutningen blir inte straffrättsligt ansvarig på grund av åsidosättande av skyldigheten enligt första stycket …"

2. Dekret av den 5 mars 2010

20. I artikel 1 i dekretet av den 5 mars 2010, i den lydelse som är tillämplig på omständigheterna i det nationella målet, föreskrivs följande:

"Syftet med behandlingen av personuppgifter i 'System för förvaltning av åtgärder för att skydda verk på internet' är att [Hadopis] kommitté för rättighetsskydd ska

4 JORF av den 7 mars 2010, text nr 19.

1° vidta åtgärder enligt del III i lagstiftningsdelen [CPI] (avdelning III, kapitel I, avsnitt 3, underavsnitt 3 och del III i regleringsdelen av samma lag (avdelning III, kapitel I, avsnitt 2, underavsnitt 2),

2° anmäla faktiska omständigheter som kan utgöra brott enligt artiklarna L. 335-2, L. 335-3, L. 335-4 och R. 335-5 i samma lag till allmän åklagare och informera organ som tillvaratar branschintressen och kollektiva förvaltningsorgan om dessa anmälningar,

…”

21. I artikel 4 i dekretet anges följande:

”I. De auktoriserade offentliga tjänstemän som bemyndigats av [Hadopis] ordförande i enlighet med artikel L. 331-21 [CPI] och ledamöterna i den kommitté för rättighetsskydd som anges i artikel 1 ska ha direkt tillgång till personuppgifter och den information som anges i bilaga till detta dekret.

II. De operatörer av elektronisk kommunikation och de leverantörer som anges i 2° i bilagan till detta dekret ska erhålla

– de tekniska uppgifter som krävs för att identifiera abonnenten,

– de rekommendationer som föreskrivs i artikel L. 331-25 [CPI] för elektronisk vidarebefordran till abonnenterna,

– de uppgifter som behövs för att genomföra kompletterande straff i form av avstängning av anslutningen till en allmänt tillgänglig kommunikationstjänst på internet som allmän åklagare underrättat kommittén för rättighetsskydd om.

III. Organ som tillvaratar branschintressen och kollektiva förvaltningsorgan ska erhålla information om en anmälan till allmän åklagare.

IV. De rättsliga myndigheterna ska erhålla protokoll från fastställande av faktiska omständigheter som kan utgöra överträdelser enligt artiklarna L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 och R. 335-5 [CPI].

Det automatiska belastningsregistret ska underrättas om verkställighet av ett avstängningsstraff.”

22. I bilagan till dekretet av den 5 mars 2010 föreskrivs följande:

”Följande personuppgifter och information ska registreras i systemet för förvaltning av åtgärder för skydd av verk på internet:

1° Personuppgifter och information som härrör från lagligt konstituerade organ som tillvaratar branschintressen, kollektiva förvaltningsorgan, Nationella centrumet för film och animerade bilder samt från allmän åklagare.

Beträffande omständigheter som kan utgöra åsidosättande av skyldigheten enligt artikel L. 336-3 [CPI]:

Datum och klockslag för omständigheterna.

Berörda abonnenters IP-adress.

Använt peer-to-peer-protokoll.

Pseudonym som använts av abonnenten.

Information om skyddade verk eller alster som berörs av omständigheterna.

Filens namn på abonnentens dator (i förekommande fall).

Internetleverantör som åtkomsten erhållits från eller som tillhandahållit den tekniska IP-resursen.
…

2° Personuppgifter och information om abonnenten som inhämtats från operatörer av elektronisk kommunikation … och leverantörer …:

För- och efternamn.

Postadress och e-postadresser.

Telefonnummer.

Adress till abonnentens telefoninstallation.

Internetleverantör som använder de tekniska resurserna från den leverantör som anges i 1°, hos vilken abonnenten har tecknat avtal, kundnummer.

Datum då åtkomsten till en allmänt tillgänglig kommunikationstjänst på internet stängs av.

…”

3. Post- och telekommunikationslagen

23. Artikel L. 34-1 i Code des postes et des communications électroniques (post- och telekommunikationslagen), i dess lydelse enligt artikel 17 i lag nr 2021-998 av den 30 juli 2021[5] (nedan kallad CPCE), föreskriver, i punkt II bis, att ”operatörer av elektronisk kommunikation är skyldiga att lagra följande:

1° Information om användarens fysiska identitet, upp till fem år efter det att vederbörandes avtal har upphört att gälla, för att möjliggöra genomförande av straffrättsliga förfaranden, förebyggande av hot mot den allmänna säkerheten förebyggas och skydd av den nationella säkerheten.

2°Annan information som användaren lämnat i samband med tecknandet av ett avtal eller skapandet av ett konto samt betalningsinformation, upp till ett år efter det att vederbörandes avtal har upphört att gälla eller dennes konto har avslutats, för samma ändamål som de som avses i punkt 1 i denna bestämmelse.

3° Tekniska uppgifter som gör det möjligt att identifiera källan till en uppkoppling eller den terminalutrustning som använts, upp till ett år efter uppkopplingen eller användningen av terminalutrustningen, för att möjliggöra bekämpande av grov brottslighet, förebyggande allvarliga hot mot den allmänna säkerheten och skydd av den nationella säkerheten.”

III. Det nationella målet, tolkningsfrågorna och förfarandet vid domstolen

24. La Quadrature du Net, Fédération des fournisseurs d’accès à Internet associatifs, Franciliens.net och French Data Network har genom ansökan av den 12 augusti 2019, och två kompletterande inlagor av den 12 november 2019 och den 6 maj 2021, yrkat att Conseil d’État (Högsta förvaltningsdomstolen, Frankrike) ska ogiltigförklara det indirekta beslutet genom vilket Premier ministre (premiärministern, Frankrike) avslog deras ansökan om upphävande av dekretet av den 5 mars 2010, trots att detta dekret och de bestämmelser som utgör dess rättsliga grund utgör ett orimligt ingrepp i rättigheter som garanteras genom den franska konstitutionen och dessutom strider mot artikel 15 i direktiv 2002/58 samt mot artiklarna 7, 8, 11, och 52 i stadgan.

25. Sökandena i det nationella målet har i synnerhet gjort gällande att dekretet av den 5 mars 2010 och de bestämmelser som utgör dess rättsliga grund tillåter en oproportionerlig åtkomst till anslutningsuppgifter för brott som avser upphovsrätt som begås på internet och inte är grova, utan att någon förhandskontroll görs av en domstol eller en myndighet för vilken det finns garantier för dess oberoende och opartiskhet.

[5] JORF av den 31 juli 2021, text nr 1. Denna version av artikel L. 34-1 CPCE, som varit i kraft sedan den 31 juli 2021, antogs till följd av ett beslut av Conseil d’État (Högsta förvaltningsdomstolen, Frankrike) av den 21 april 2021, nr 393099 (JORF av den 25 april 2021), genom vilket denna förvaltningsdomstol underkände den tidigare versionen av bestämmelsen, vilken föreskrev en skyldighet att lagra personuppgifter ”när det behövs för att utreda, avslöja och lagföra brott eller åsidosättanden av skyldigheten enligt artikel L. 336-3 [CPI]” i det enda syftet att vid behov kunna ställa dessa uppgifter till förfogande för bland annat Hadopi. Genom beslut nr 2021-976–977 QPC av den 25 februari 2022 (Habib A. m.fl.) förklarade Conseil constitutionnel (Författningsdomstolen, Frankrike) att denna tidigare version av artikel L. 34-1 CPCE var författningsstridig huvudsakligen på grund av att ”de angripna bestämmelserna genom att medge en generell och odifferentierad lagring av uppkopplingsuppgifter medför ett oproportionerligt ingrepp i respekten för privatlivet” (punkt 13). Författningsdomstolen ansåg nämligen att de uppkopplingsuppgifter som skulle lagras enligt dessa bestämmelser avsåg både identifiering av användarna av de elektroniska kommunikationstjänsterna och andra uppgifter som ”med hänsyn till sin beskaffenhet och sin mångfald och vilka behandlingar de kan bli föremål för … ger omfattande och utförlig information om användarna och i förekommande fall om tredje man som särskilt inkräktar på deras privatliv” (punkt 11).

26. Den hänskjutande domstolen har först och främst understrukit att domstolen i sin senaste dom om La Quadrature du Net m.fl.[6], slog fast att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11, och artikel 52.1 i stadgan, inte utgör hinder för lagstiftningsåtgärder som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring *av uppgifter om den fysiska identiteten för användare av elektroniska kommunikationsmedel*. Det är således möjligt att lagra dessa uppgifter utan någon särskild tidsgräns för att brott i allmänhet ska kunna utredas, avslöjas och lagföras.

27. Den hänskjutande domstolen har av detta dragit slutsatsen att den grund som anförts av sökandena i det nationella målet för att göra gällande att dekretet av den 5 mars 2010 är rättsstridigt i den del det antagits i ett sammanhang som avser bekämpande av ringa brott, ska underkännas.

28. Den hänskjutande domstolen har sedan erinrat om att domstolen i dom Tele2 Sverige och Watson[7] fastställde att artikel 15.1 i direktiv 2002/58/EG, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters åtkomst till lagrade uppgifter och som inte föreskriver att åtkomsten ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet.

29. Den hänskjutande domstolen har framhållit att EU-domstolen i Tele2-domen[8] angav att det är väsentligt, för att säkerställa att dessa villkor uppfylls fullt ut i praktiken, att behöriga nationella myndigheters åtkomst till de lagrade uppgifterna i princip, utom i vederbörligen motiverade brådskande fall, är underkastad ett krav på förhandskontroll av en domstol eller en oberoende myndighet och att domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att de behöriga nationella myndigheterna framställt en motiverad ansökan, vilket kan ske bland annat inom ramen för ett förfarande för förebyggande, avslöjande eller lagföring av brott.

30. Den hänskjutande domstolen har understrukit att EU-domstolen erinrade om detta krav i domen La Quadrature du Net m.fl.,[9] som avsåg en underrättelsemyndighets insamling i realtid av uppkopplingsuppgifter, och i domen Prokuratuur (Villkor för att ge tillgång till uppgifter avseende elektronisk kommunikation),[10] som avsåg nationella myndigheters åtkomst till uppkopplingsuppgifter.

31. Den hänskjutande domstolen har slutligen påpekat att Hadopi sedan myndigheten inrättades 2009 har lämnat över 12,7 miljoner rekommendationer till abonnenter enligt förfarandet för *graduated response* i artikel L 331-25 CPI, varav 827 791 rekommendationer enbart under 2019. För detta ändamål måste de ansvariga vid Hadopis kommitté för rättighetsskydd kunna samla in ett avsevärt antal uppgifter varje år om de berörda användarnas fysiska identitet. Den hänskjutande domstolen anser att det med hänsyn till det stora antalet rekommendationer finns en risk att ett krav på förhandskontroll av denna insamling leder till att rekommendationerna omöjliggörs.

6 Se dom av den 6 oktober 2020 (C-511/18, C-512/18 och C-520/18, nedan kallad domen Quadrature du Net m.fl., EU:C:2020:791, domslut).

7 Se dom av den 21 december 2016 (C-203/15 och C-698/15, nedan kallad Tele2-domen, EU:C:2016:970, domslut).

8 Punkt 120 i den domen.

9 Punkt 189 i den domen.

10 Se dom av den 2 mars 2021, Prokuratuur (C-746/18, EU:C:2021:152) (nedan kallad domen Prokuratuur).

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

”1) Ingår de uppgifter om den fysiska identitet som är knuten till en IP-adress bland de trafik- och lokaliseringsuppgifter som i princip är underkastade förhandskontroll av en domstol eller en oberoende myndighet vars avgöranden har bindande verkan?

2) Om fråga 1 besvaras jakande, och med beaktande av att uppgifter om användarnas fysiska identitet, inklusive deras kontaktuppgifter, är föga känsliga, ska [direktiv 2002/58], jämfört med [stadgan], tolkas så, att det utgör hinder för en nationell lagstiftning som föreskriver att en myndighet ska samla in uppgifter om användarnas IP-adresser, utan någon förhandskontroll av en domstol eller av ett oberoende förvaltningsorgan, vars avgöranden har bindande verkan?

3) Om fråga 2 besvaras jakande, och med beaktande av att uppgifterna om den fysiska identiteten är föga känsliga, att dessa uppgifter endast får samlas in i syfte att förebygga underlåtenhet att uppfylla skyldigheter som i nationell rätt blivit definierat på ett precist, uttömmande och restriktivt sätt, och att en systematisk kontroll av åtkomsten till respektive användares uppgifter som utförs av en domstol eller ett utomstående förvaltningsorgan, vars avgöranden har bindande verkan, skulle kunna äventyra fullgörandet av det allmännyttiga uppdrag som anförtrotts den oberoende myndighet som samlar in uppgifterna, utgör [direktiv 2002/58] hinder för att denna kontroll utförs på ett anpassat sätt, såsom genom automatiserad kontroll, vilken, i förekommande fall, sker under överinseende av en intern avdelning inom förvaltningsorganet som uppfyller krav på oavhängighet och opartiskhet i förhållande till de tjänstemän som ansvarar för insamlingen?”

33. Skriftliga yttranden har inkommit från sökandena i målet vid den nationella domstolen, den franska regeringen, den estniska regeringen, den svenska regeringen och den norska regeringen samt från Europeiska kommissionen. Dessa parter, med undantag av den estniska regeringen, samt den danska och den finska regeringen var företrädda vid förhandlingen den 5 juli 2022.

IV. Bedömning

A. Den första och den andra tolkningsfrågan

34. Den hänskjutande domstolen har ställt de första två tolkningsfrågorna, som jag anser ska prövas tillsammans, för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan, ska tolkas så, att den utgör hinder för en nationell lagstiftning som innebär att en förvaltningsmyndighet som har till uppgift att skydda upphovsrätten och närstående rättigheter mot rättighetsintrång på internet kan få åtkomst till fysiska identitetsuppgifter som motsvarar IP-adresser så att myndigheten kan identifiera innehavarna till adresserna, som är misstänkta för att ha begått intrången och vid behov vidta åtgärder mot dem, utan att denna åtkomst är underkastad någon förhandskontroll av en domstol eller ett oberoende förvaltningsorgan.

1. Avgränsning av tolkningsfrågorna

a) Upphovsrättsorganisationers föregående insamling av IP-adresser

35. Det framgår av beslutet om hänskjutande att det förfarande för *graduated response* som är aktuellt i det nationella målet omfattar två på varandra följande databehandlingar. Den första behandlingen består i att upphovsrättsorganisationer först samlar in IP-adresser i peer-to-peer-nätverk som används för upphovsrättsintrång. Den andra består i att Hadopi efter att ta tagit emot en anmälan parar ihop IP-adressen med den berördes fysiska identitet i syfte att översända en rekommendation till de vars tillgång till allmänt tillgängliga kommunikationstjänster på internet har använts i strid med reglerna om upphovsrätt.

36. Den första och den andra tolkningsfrågan gäller enbart den andra behandlingen, som utförs av Hadopi.

37. Sökandena i det nationella målet har emellertid anfört att domstolen borde granska den första behandlingen, eftersom det ofrånkomligen strider mot bestämmelserna i direktiv 2002/58 att utnyttja IP-adresserna om de erhållits i strid med dessa bestämmelser.

38. Resonemanget övertygar inte. Tillämpningsområdet för direktiv 2002/58 begränsas genom artikel 3.1 i direktivet till ”behandling av personuppgifter i samband med att. elektroniska kommunikationstjänster tillhandahålls”. Såsom den franska regeringen anförde vid förhandlingen erhåller inte upphovsrättsorganisationerna de aktuella IP-adresserna genom leverantörer av elektroniska kommunikationstjänster utan direkt på internet, genom att söka bland allmänt tillgängliga uppgifter.

39. Jag kan alltså bara konstatera att upphovsrättsorganisationernas föregående insamling av IP-adresser inte omfattas av bestämmelserna i direktiv 2002/58 och att den därför, såsom kommissionen har framhållit, skulle kunna bedömas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.[11] En sådan bedömning tycks därför falla utanför ramen för de tolkningsfrågor som ställts till EU-domstolen, i synnerhet som den hänskjutande domstolen inte har lämnat några klargöranden om insamlingen som skulle kunna göra det möjligt för EU-domstolen att lämna ett ändamålsenligt svar.

40. Under dessa förutsättningar ska min bedömning ägnas åt frågan om Hadopis åtkomst till uppgifter om fysisk identitet som motsvarar en IP-adress.

b) Kopplingen mellan IP-adresser och uppgifter om fysisk identitet

41. De två första tolkningsfrågorna avser ”de uppgifter om den fysiska identitet som är knuten till en IP-adress”, vilka enligt den hänskjutande domstolen är av låg känslighet. Den domstolen hänför sig i sitt beslut enbart till de punkter i domen Quadrature du Net m.fl. som avser lagring av uppgifter om fysisk identitet.

[11] Europaparlamentets och rådets förordning 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).

42. Det är riktigt att EU-domstolen i sin praxis gör en skillnad mellan regelverket för lagring av och åtkomst till IP-adresser och regelverket för lagring och åtkomst till uppgifter om den fysiska identiteten på användare av elektroniska kommunikationsmedel, varvid den sistnämnda ordningen inte är lika sträng som den förstnämnda. [12]

43. Trots formuleringen av dessa två tolkningsfrågor tycks det emellertid i det nu aktuella fallet inte endast vara fråga om själva åtkomsten till uppgifterna om den fysiska identiteten på användarna av de elektroniska kommunikationsmedlen, utan om att dessa uppgifter paras ihop med de IP-adresser som Hadopi förfogar över sedan de samlats in och översänts av upphovsrättsorganisationerna. Syftet med att ge Hadopi åtkomst till uppgifterna om fysisk identitet är nämligen, såsom kommissionen har framhållit, att frigöra en större mängd uppgifter, däribland IP-adresser och utdrag ur filer som har konsulterats, och att göra det möjligt att utnyttja dessa uppgifter, eftersom uppgifter om fysisk identitet och IP-adresser var för sig saknar intresse för de nationella myndigheterna då varken fysisk identitet eller IP-adress i sig kan ge information om fysiska personers aktivitet på nätet om de inte är sammankopplade.

44. Jag menar att de två första tolkningsfrågorna följaktligen bör förstås så, att de inte avser endast uppgifterna om den fysiska identiteten hos användare av ett elektroniskt kommunikationsmedel, utan även åtkomsten till de IP-adresser som gör det möjligt att identifiera källan till en anslutning.

c) Lagring av IP-adresser hos leverantörer av kommunikationstjänster

45. Det är riktigt att tolkningsfrågorna till domstolen, såsom den franska regeringen och kommissionen har framhållit, formellt inte avser den datalagring som leverantörer av elektroniska kommunikationstjänster företar, utan endast den omständigheten att Hadopi får åtkomst till uppgifter om fysisk identitet som motsvarar IP-adresser.

46. Som jag ser det kan frågan om Hadopis åtkomst till dessa uppgifter emellertid inte skiljas från den föregående frågan om lagringen av dessa uppgifter hos leverantörerna av kommunikationstjänster. Såsom domstolen har understrukit sker datalagringen endast för det ändamålet att, i förekommande fall, kunna ge behöriga nationella myndigheter åtkomst till uppgifterna. [13] Datalagringen och åtkomsten till uppgifter kan med andra ord inte ses separat, i och med att den sistnämnda är beroende av den förstnämnda.

47. Domstolen har förvisso redan prövat huruvida artikel 15.1 i direktiv 2002/58 är förenlig med en nationell lagstiftning om behöriga nationella myndigheters själva åtkomst till vissa personuppgifter, oberoende av frågan om den aktuella datalagringen är förenlig med denna bestämmelse. [14] De nu aktuella tolkningsfrågorna skulle därmed kunna besvaras med bortseende från frågan om de aktuella uppgifterna har lagrats i enlighet med unionsbestämmelserna.

48. Jag vill emellertid först och främst framhålla att domstolens prövning i domen Ministerio Fiscal [15] av frågan huruvida de nationella myndigheternas åtkomst till vissa personuppgifter var förenlig med unionsrätten i strikt bemärkelse gjordes enligt samma principer som domstolens prövning av frågan huruvida datalagringen var förenlig med unionsrätten. Domstolen hänvisade nämligen enbart till den rättspraxis som utvecklats i det sistnämnda avseendet för att överföra

12 Se domen La Quadrature du Net m.fl. (punkterna 155 och 159).

13 Se dom Tele2 (punkt 79).

14 Se dom av den 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punkt 49).

15 Dom av den 2 oktober 2018 (C-207/16, EU:C:2018:788).

den på frågan om åtkomst till personuppgifter. För det fall frågan om en viss datalagrings förenlighet med unionsrätten inte har prövats skjuts denna prövning med andra ord upp till prövningen av frågan om åtkomsten till dessa uppgifter, vilket innebär att frågan om denna åtkomst är förenlig med unionsrätten till syvende och sist blir beroende av lagringens förenlighet.

49. Domstolen har också klart och tydligt angett att åtkomst till personuppgifter endast får beviljas såvitt dessa uppgifter har lagrats av leverantörerna av de elektroniska kommunikationstjänsterna på ett sätt som är förenligt med artikel 15.1 i direktiv 2002/58 [16] och att privatpersoners åtkomst till personuppgifter för att göra det möjligt att väcka talan vid allmänna domstolar om upphovsrättsintrång endast är förenlig med unionsrätten på villkor att dessa uppgifter lagras på ett sätt som är förenligt med denna bestämmelse. [17]

50. Domstolens fasta praxis är att åtkomst till trafik- och lokaliseringsuppgifter som lagrats av leverantörer med tillämpning av en åtgärd som vidtagits med stöd av artikel 15.1 i direktiv 2002/58, vilken ska ske med iakttagande av de villkor som följer av rättspraxis avseende tolkningen av direktiv 2002/58, i princip endast kan motiveras av det mål av allmänt samhällsintresse som ligger till grund för leverantörernas skyldighet att lagra uppgifterna. [18] Frågan om nationella myndigheters åtkomst till vissa personuppgifter är förenlig med unionsrätten är med andra ord helt beroende av huruvida lagringen av dessa uppgifter är förenlig med unionsrätten.

51. Jag menar att det följaktligen är en förutsättning för bedömningen av huruvida en nationell lagstiftning som föreskriver att en nationell myndighet ska ha åtkomst till personuppgifter är förenlig med unionsrätten att det först är fastställt att lagringen av samma uppgifter är förenlig med unionsrätten.

52. Under dessa förutsättningar inleder jag min bedömning med att erinra om domstolens praxis i fråga om lagring av IP-adresser som tilldelats källan till en anslutning för att visa på dess gränser och föreslå en anpassad tolkning av regelverket i fråga.

2. Domstolens praxis om tolkningen av artikel 15.1 i direktiv 2002/58/EG när det gäller åtgärder avseende lagring av IP-adresser som tilldelats källan till en anslutning

53. I artikel 5.1 i direktiv 2002/58 fastställs principen om konfidentialitet för såväl elektronisk kommunikation som därmed förbundna trafikuppgifter. Detta innebär bland annat ett principiellt förbud för andra personer än användarna att, utan användarnas samtycke, lagra sådan kommunikation och sådana uppgifter. [19]

54. När det gäller trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantörer av elektroniska kommunikationstjänster föreskrivs i artikel 6.1 i direktiv 2002/58 att dessa uppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation. I artikel 6.2 anges att trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter endast får behandlas fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. I fråga om andra

[16] Se dom Prokuratuur (punkt 29).

[17] Se dom av den 17 juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, punkterna 127–130).

[18] Se dom La Quadrature du Net m.fl., punkt 166), dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl. (C-140/20, EU:C:2022:258, punkt 98) (nedan kallad dom Commissioner of An Garda Síochána m.fl.), och dom av den 20 september 2022, SpaceNet (C-793/19 och C-794/19, EU:C:2022:702, punkt 131) (nedan kallad dom SpaceNet).

[19] Se dom La Quadrature du Net m.fl. (punkt 107), Commissioner of An Garda Síochána m.fl. (punkt 35), och SpaceNet (punkt 52).

lokaliseringsuppgifter än trafikuppgifter föreskrivs i artikel 9.1 i direktivet att dessa endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke. [20]

55. Genom att anta direktiv 2002/58 har unionslagstiftaren således konkretiserat de rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan, vilket innebär att användarna av elektroniska kommunikationsmedel i princip har rätt att förvänta sig att deras kommunikationer och därmed förbundna uppgifter förblir anonyma och inte kan registreras, såvida de inte har samtyckt till detta. [21] Direktivet reglerar således inte bara åtkomsten till sådana uppgifter genom att föreskriva garantier i syfte att förhindra missbruk utan innehåller även, i synnerhet, ett förbud mot att de lagras av tredje part.

56. I och med att artikel 15.1 i direktiv 2002/58 tillåter medlemsstaterna att genom lagstiftning vidta åtgärder för att ”begränsa omfattningen” av rättigheter och skyldigheter enligt bland annat artiklarna 5, 6 och 9 i direktivet, såsom de som följer av principerna om konfidentialitet vid kommunikation och om förbud mot lagring av därmed förbundna uppgifter, föreskriver den under dessa förutsättningar ett undantag från huvudregeln i bland annat artiklarna 5, 6 och 9 i direktivet. Enligt fast rättspraxis ska de således tolkas restriktivt. En sådan bestämmelse kan alltså inte motivera att undantaget från den principiella skyldigheten att garantera konfidentialitet för elektronisk kommunikation och därmed förbundna uppgifter, i synnerhet förbudet i artikel 5 i direktivet mot att lagra dessa uppgifter, görs till huvudregel. Det skulle förta verkan av den sistnämnda bestämmelsen. [22]

57. Vad gäller de mål som kan motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58, har domstolen redan slagit fast att uppräkningen av mål i artikel 15.1 första meningen i detta direktiv är uttömmande. En lagstiftningsåtgärd som har vidtagits med stöd av denna bestämmelse måste därför faktiskt och strikt avse ett av dessa mål. [23]

58. Det framgår dessutom av artikel 15.1 tredje meningen i direktiv 2002/58 att de åtgärder som medlemsstaterna vidtar enligt denna bestämmelse ska vara förenliga med de allmänna principerna i unionsrätten, däribland proportionalitetsprincipen, och säkerställa att de grundläggande rättigheter som garanteras i stadgan iakttas. Domstolen har tidigare slagit fast att när en medlemsstat i nationell lagstiftning ålägger leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra trafikuppgifter i syfte att, i förekommande fall, göra dem tillgängliga för behöriga nationella myndigheter väcker detta frågor om en sådan lagstiftnings förenlighet inte bara med artiklarna 7 och 8 i stadgan, vilka rör skyddet för privatlivet respektive skyddet av personuppgifter, utan även med artikel 11 i stadgan, som rör yttrandefriheten, en frihet som utgör en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som unionen enligt artikel 2 FEU bygger på. [24]

[20] Se dom Tele2 (punkt 86), La Quadrature du Net m.fl. (punkt 108), Commissioner of An Garda Síochána m.fl. (punkt 38), och SpaceNet (punkt 55).

[21] Se dom La Quadrature du Net m.fl. (punkt 109), dom Commissioner of An Garda Síochána m.fl. (punkt 37), och dom SpaceNet (punkt 54).

[22] Se dom La Quadrature du Net m.fl. (punkterna 110 och 111), dom Commissioner of An Garda Síochána m.fl. (punkt 40), och dom SpaceNet (punkt 57).

[23] Se dom La Quadrature du Net m.fl. (punkt 112), dom Commissioner of An Garda Síochána m.fl. (punkt 41), och dom SpaceNet (punkt 58).

[24] Se dom La Quadrature du Net m.fl. (punkterna 113 och 114), dom Commissioner of An Garda Síochána m.fl. (punkt 42), och dom SpaceNet (punkt 60).

59. Eftersom artikel 15.1 i direktiv 2002/58 ger medlemsstaterna möjlighet att begränsa de rättigheter och skyldigheter som föreskrivs i artiklarna 5, 6 och 9 i direktivet, avspeglar denna bestämmelse emellertid den omständigheten att de rättigheter som är stadfästa i artiklarna 7, 8 och 11 i stadgan inte är några absoluta rättigheter, utan måste bedömas utifrån deras funktion i samhället. Såsom framgår av artikel 52.1 i stadgan är det nämligen enligt stadgan tillåtet att begränsa utövandet av dessa rättigheter, under förutsättning att begränsningarna föreskrivs i lag, att de är förenliga med det väsentliga innehållet i dessa rättigheter och att de, med beaktande av proportionalitetsprincipen, är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter. En tolkning av artikel 15.1 i direktiv 2002/58, jämförd med stadgan, kräver således även att det tas hänsyn till den betydelse som målen att skydda nationell säkerhet och bekämpa grov brottslighet har genom att bidra till skyddet för andra människors rättigheter och friheter och betydelsen av de rättigheter som är stadfästa i artiklarna 3, 4, 6 och 7 i stadgan, [25] av vilka kan följa positiva skyldigheter för myndigheterna. [26]

60. Mot bakgrund av dessa olika positiva skyldigheter är det således nödvändigt att göra en avvägning mellan de olika intressen och de rättigheter som är i fråga. Det föreskrivs i artikel 15.1 första meningen i direktiv 2002/58 att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet när en sådan åtgärd är ”nödvändig, lämplig och proportionerlig … i ett demokratiskt samhälle”. I skäl 11 i direktivet anges att en åtgärd av detta slag ska vara i ”strikt” proportion till det avsedda ändamålet. [27]

61. Det framgår av domstolens praxis att medlemsstaternas möjlighet att motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58 ska bedömas med hänsyn till hur allvarligt det ingrepp är som en sådan begränsning medför. Det ska också kontrolleras att betydelsen av det mål av allmänt samhällsintresse som eftersträvas med denna begränsning står i proportion till hur allvarligt ingreppet är. [28]

62. Jag vill också framhålla att domstolen i sin praxis har gjort skillnad mellan å ena sidan ingrepp som följer av åtkomsten till uppgifter som i sig ger exakt information om de aktuella kommunikationerna och alltså om personens privatliv, för vilka lagringsordningen är restriktiv, och, å andra sidan, ingrepp som följer av åtkomsten till uppgifter som endast kan ge sådan information i den mån de är parade med andra uppgifter, såsom IP-adresser. [29]

63. När det närmare bestämt gäller IP-adresser har domstolen således framhållit att de genereras utan anknytning till en viss kommunikation och huvudsakligen har till syfte att, via leverantörer av elektroniska kommunikationstjänster, identifiera den fysiska person som äger den terminalutrustning från vilken en kommunikation sker via internet. Såvitt endast IP-adresser till kommunikationskällan lagras och inte adresserna till kommunikationsmottagaren, har denna kategori av uppgifter därmed en lägre grad av känslighet än andra trafikuppgifter. [30]

[25] Se dom La Quadrature du Net m.fl. (punkterna 120–122), dom Commissioner of An Garda Síochána m.fl. (punkt 48), och dom SpaceNet (punkt 63).

[26] Se dom La Quadrature du Net m.fl. (punkterna 120–122), dom Commissioner of An Garda Síochána m.fl. (punkt 49), och dom SpaceNet (punkt 64).

[27] Se dom La Quadrature du Net m.fl. (punkterna 127–129), dom Commissioner of An Garda Síochána m.fl. (punkterna 50 och 51), och dom SpaceNet (punkterna 65 och 66).

[28] Se dom La Quadrature du Net m.fl. (punkt 131), dom Commissioner of An Garda Síochána m.fl. (punkt 53), och dom SpaceNet (punkt 68).

[29] Se ovan punkt 41och följande punkter.

[30] Se dom La Quadrature du Net m.fl. (punkt 152).

64. Domstolen har dock samtidigt understrukit att i och med att IP-adresser kan användas för att bland annat på ett uttömmande sätt kartlägga en internetanvändares hela klickström, och därmed dennes online-aktivitet, är det emellertid möjligt att med användning av dessa adresser utförligt kartlägga internetanvändaren och dra exakta slutsatser om användarens privatliv. Lagring och analys av dessa IP-adresser utgör alltså *allvarliga* ingrepp i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan och kan ha en avhållande inverkan på utövandet av den yttrandefrihet som garanteras i artikel 11 i stadgan. [31]

65. Vid avvägningen mellan rättigheter och de berättigade intressen som är i fråga ska emellertid enligt fast rättspraxis det faktum beaktas att, när det är fråga om brott som begåtts på internet, kan IP-adressen utgöra den enda utredningsmetod som gör det möjligt att identifiera den person, till vilken denna adress var tilldelad vid den tidpunkt då brottet begicks. [32]

66. Domstolen har följaktligen slagit fast att en lagstiftningsåtgärd som föreskriver en generell och odifferentierad lagring enbart av IP-adresser som har tilldelats källan till en internetanslutning i princip inte strider mot artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan, och att denna möjlighet måste vara strikt underkastad de materiella och processuella villkor som reglerar behandlingen av dessa uppgifter, eftersom det med hänsyn till det allvarliga ingrepp i de grundläggande rättigheter som denna lagring innebär endast är bekämpning av *grov* brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som, i likhet med skyddet av nationell säkerhet, kan motivera detta ingrepp. [33]

67. Domstolen har vidare klargjort att lagringstiden inte får överstiga den tid som är strängt nödvändig med hänsyn till det eftersträvade målet och att en åtgärd av denna art måste föreskriva strikta villkor och garantier för utnyttjandet av dessa uppgifter. [34]

3. De begränsningar som följer av rättspraxis angående tolkningen av artikel 15.1 i direktiv 2002/58 med avseende på åtgärder för lagring av IP-adresser som tilldelats källan till en anslutning

68. Den lösning som domstolen kommit fram till i fråga om nationella åtgärder avseende lagring av IP-adresser som tilldelats källan till en anslutning, tolkade mot bakgrund av artikel 15.1 i direktiv 2002/58, tycks emellertid förenad med två huvudsakliga svårigheter.

a) Sammanjämkningen med rättspraxis om utlämnande av IP-adresser som tilldelats källan till en anslutning inom ramen för en talan om skydd för immateriella rättigheter

69. Såsom jag angav redan i mitt förslag till avgörande i målet M.I.C.M. [35], finns det en tydlig spänning mellan denna linje i rättspraxis och den rättspraxis som avser utlämnande av IP-adresser inom ramen för en talan om skydd för immateriella rättigheter för innehavare av dessa

[31] Se dom La Quadrature du Net m.fl. (punkt 153), dom Commissioner of An Garda Síochána m.fl. (punkt 73), och dom SpaceNet (punkt 103). Min kursivering.

[32] Se dom La Quadrature du Net m.fl. (punkt 154), dom Commissioner of An Garda Síochána m.fl. (punkt 73), och dom SpaceNet (punkt 103).

[33] Se dom La Quadrature du Net m.fl. (punkterna 155 och 156), dom Commissioner of An Garda Síochána m.fl. (punkt 74), och dom SpaceNet (punkterna 104 och 105).

[34] Se dom La Quadrature du Net m.fl. (punkt 156) och SpaceNet (punkt 105).

[35] C-597/19, EU:C:2020:1063, punkt 98.

rättigheter, i vilken betonas medlemsstaternas skyldighet att säkerställa att innehavare av immateriella rättigheter verkligen har möjlighet att yrka ersättning för den skada de lidit till följd av intrång i dessa rättigheter. [36]

70. Vad beträffar den andra linjen i rättspraxis har domstolen nämligen vidhållit att unionsrätten inte hindrar att medlemsstaterna föreskriver en skyldighet att lämna ut personuppgifter till enskilda för att dessa ska kunna väcka talan vid allmän domstol angående upphovsrättsintrång. [37]

71. Domstolen har i detta avseende framhållit att möjligheten för medlemsstaterna att föreskriva en skyldighet att lämna ut personuppgifter i tvistemål i första hand följer av möjligheten att föreskriva ett sådant utlämnande i samband med lagföring av brott, [38] vilken senare har utvidgats till tvistemål.

72. I fråga om IP-adresser har domstolen emellertid samtidigt slagit fast att dessa uppgifter endast får lagras inom ramen för bekämpande av grov brottslighet och förebyggande av allvarliga hot mot den allmänna säkerheten. [39]

73. Att försöka förena dessa två linjer i rättspraxis leder enligt min mening till otillräckliga och föga övertygande resultat.

74. Bekämpande av intrång i immateriella rättigheter kan i motsats till vad den franska regeringen anförde vid förhandlingen inte hänföras till bekämpande av grov brottslighet. Begreppet grov brottslighet ska enligt min mening tolkas fristående. Det får inte göras beroende av varje enskild medlemsstat uppfattning, såvida inte kraven i artikel 15.1 i direktiv 2002/58 ska få kringgås beroende på huruvida medlemsstaterna betraktar bekämpande av grov brottslighet i vid bemärkelse eller inte. Såsom jag redan har framhållit får intressen som är knutna till skyddet för immateriella rättigheter inte blandas ihop med de intressen som ligger bakom bekämpandet av grov brottslighet. [40]

75. Att medge överföring av IP-adresser till innehavare av immateriella rättigheter inom ramen för förfaranden som syftar till att skydda dessa rättigheter, trots att de bara får lagras inom ramen för bekämpande av grov brottslighet, skulle stå i uppenbar strid med domstolens praxis om lagring av anslutningsuppgifter. Villkoren för sådan datalagring skulle också förlora sin ändamålsenliga verkan, eftersom det i vart fall skulle vara möjligt att få åtkomst till dem på olika grunder.

76. Jag menar att det följaktligen skulle kunna strida mot artikel 15.1 direktiv 2002/58, såsom den har tolkats i domstolens praxis, att lagra IP-adresser i syfte att skydda immateriella rättigheter och lämna ut dessa adresser till rättsinnehavarna i samband med processer som rör skyddet av dessa rättigheter. Skyldigheten att överföra personuppgifter till privatpersoner för att göra det möjligt att väcka talan om upphovsrättsintrång vid allmän domstol, något som EU-domstolen själv har möjliggjort, omintetgörs således genom samma domstols praxis om lagring av IP-adresser hos leverantörer av elektroniska kommunikationstjänster.

[36] Se mitt förslag till avgörande i målet M.I.C.M. (C-597/19, EU:C:2020:1063, punkt 97).

[37] Se dom av den 19 april 2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219, punkt 55), dom av den 4 maj 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, punkt 34), och dom av den 17 juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, punkterna 47–54).

[38] Se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae (C-275/06, EU:C:2008:54, punkterna 50–52).

[39] Se punkt 65 i detta förslag till avgörande.

[40] Se mitt förslag till avgörande i målet M.I.C.M. (C-597/19, EU:C:2020:1063, punkt 103).

77. Detta är emellertid ingen tillfredsställande lösning, eftersom den undergräver den jämvikt mellan de olika intressen som står på spel som EU-domstolen har försökt upprätthålla, genom att innehavarna av immateriella rättigheter fråntas det främsta, om inte det enda, medlet för att identifiera dem som gör intrång i dessa rättigheter på internet. Detta övervägande föranleder en redogörelse för den andra svårigheten som EU-domstolens praxis i fråga om nationella åtgärder avseende lagring av IP-adresser som tilldelats källan till en anslutning, tolkad mot bakgrund av artikel 15.1 i direktiv 2002/58, enligt min mening kan ge upphov till.

b) Risken för generell straffrihet för brott som enbart begås på internet

78. Jag anser således att denna lösning också ger upphov till praktiska svårigheter. Såsom domstolen själv har understrukit kan IP-adressen, om ett brott begås uteslutande online, vara den enda utredningsmetod som gör det möjligt att identifiera den person som hade denna adress vid den tidpunkten då det aktuella brottet begicks.

79. Det förefaller mig som om denna aspekt inte beaktas fullt ut i avvägningen mellan de berörda intressena. I och med att domstolen trots allt har begränsat möjligheten att lagra IP-adresser till bekämpande av grov brottslighet, har den samtidigt uteslutit att dessa uppgifter får lagras för att bekämpa brott i allmänhet, trots att vissa av dessa brott inte kan förebyggas, avslöjas eller beivras utan nämnda uppgifter.

80. Domstolens praxis skulle med andra ord kunna leda till att nationella myndigheter fråntas det enda medlet för att identifiera gärningsmän som begår brott på internet som emellertid inte kan hänföras till grov brottslighet, såsom till exempel intrång i immateriella rättigheter. Följden av detta skulle i praktiken bli en generell straffrihet för brott som enbart begås på internet, vilka för övrigt omfattar mer än bara intrång i immateriella rättigheter. Jag tänker bland annat på förtalsbrott som begås på internet. I unionsrätten föreskrivs det visserligen att förelägganden får meddelas mot de mellanhänder vars tjänster används för att begå sådana brott,[41] men det skulle kunna följa av domstolens praxis att gärningsmännen aldrig lagförs.

81. För att inte medge att en rad brottsliga gärningar aldrig kan bli föremål för lagföring, anser jag att avvägningen mellan de olika aktuella intressena bör bli föremål för en ny bedömning.

82. Mot bakgrund av dessa olika överväganden föreslår jag att domstolen i viss mån ska justera sin praxis om nationella åtgärder avseende lagring av IP-adresser, tolkade mot bakgrund av artikel 15.1 i direktiv 2002/58.

4. Förslag till justering av domstolens praxis om tolkningen av artikel 15.1 i direktiv 2002/58/EG i fråga om åtgärder avseende lagring av IP-adresser som tilldelas källan till en anslutning

83. Med hänsyn till vad som anförs ovan anser jag att artikel 15.1 i direktiv 2002/58 ska tolkas så, att den inte utgör hinder för åtgärder som föreskriver en generell och odifferentierad lagring av IP-adresser som tilldelats källan till en anslutning under en tidsperiod som är begränsad till vad som är strikt nödvändigt, i syfte att förebygga, utreda, avslöja och lagföra brott som begås på internet för vilka IP-adresser utgör *den enda utredningsmetoden* som gör det möjligt att identifiera den person som var tilldelad denna adress då brottet begicks.

[41] Se artikel 15.1 i Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 2000, s. 1).

84. Jag vill i detta avseende understryka att ett sådant förslag enligt min mening inte undergräver kravet på proportionalitet som gäller för datalagring, med hänsyn till det allvarliga ingrepp i de grundläggande rättigheterna enligt artiklarna 7 och 8 i stadgan som detta ingrepp innebär.[42] Tvärtom uppfyller det till fullo detta krav.

85. Den begränsning av rättigheterna och skyldigheterna enligt artiklarna 5, 6 och 9 i direktiv 2002/58 som lagringen av IP-adresser utgör syftar till att uppnå ett mål av allmänt samhällsintresse i förhållande till allvaret i detta ingrepp, det vill säga att förebygga, utreda, avslöja och lagföra brott som avses i rättsakter som annars skulle bli verkningslösa.

86. Begränsningen görs också inom ramen för vad som är strikt nödvändigt. Lagringen är nämligen begränsad till vissa specifika fall, det vill säga när det gäller brott som begås på internet och för vilka en gärningsman inte kan identifieras på annat sätt än med hjälp av den IP-adress som han eller hon tilldelats. Det är med andra ord inte fråga om att tillåta en generell och odifferentierad datalagring utan några andra villkor, utan endast om att möjliggöra lagföring av brott, inte i allmänhet utan i vissa specifika fall.

87. Artikel 15.1 i direktiv 2002/58 hindrar visserligen inte en generell och odifferentierad lagring av IP-adresser som tilldelats källan till en anslutning i syfte att säkerställa förebyggande, utredning, avslöjande och lagföring av brott på internet för vilka IP-adressen utgör den enda utredningsmetoden som gör det möjligt att identifiera den person som var tilldelad denna adress då brottet begicks. Det ska emellertid också klargöras att denna möjlighet enligt rättspraxis ska användas ”med beaktande av de stränga materiella och formella villkor *som måste styra användningen av dessa uppgifter*.”[43] Domstolen har också angett att en sådan åtgärd måste ”föreskriva stränga villkor och garantier vad gäller *utnyttjandet av dessa uppgifter*”.[44]

88. Såsom jag understryker ovan kan lagring av uppgifter och åtkomst till dessa uppgifter med andra ord inte betraktas isolerat. Även om det i princip inte strider mot artikel 15.1 i direktiv 2002/58 att Hadopi kan få åtkomst till IP-adresser, såvitt uppgifterna har lagrats i enlighet med kraven i denna bestämmelse, är det under dessa förutsättningar fortfarande nödvändigt, för att besvara tolkningsfrågorna till domstolen, att undersöka huruvida villkoren för Hadopis åtkomst till IP-adresser som tilldelats källan till en anslutning i sig är förenliga med nämnda bestämmelse, särskilt med avseende på frågan huruvida en sådan åtkomst först måste kontrolleras av en domstol eller av en oberoende förvaltningsmyndighet.

89. Efter bedömningen av den inledande frågan om lagring av IP-adresser som tilldelats källan till en anslutning ska jag nu granska Hadopis åtkomst till dessa uppgifter mot bakgrund av artikel 15.1 i direktiv 2002/58.

42 Se punkterna 60 och 61 ovan.

43 Se dom La Quadrature du Net m.fl. (punkt 155). Min kursivering.

44 Se dom La Quadrature du Net m.fl. (punkt 156). Min kursivering.

5. Hadopis åtkomst till uppgifter om fysisk identitet som motsvarar IP-adresser

90. Det framgår av domstolens praxis i fråga om syften som kan motivera en nationell åtgärd som frångår principen om konfidentialitet för elektroniska kommunikationer, att åtkomsten till uppgifterna strikt och objektivt måste motsvara något av dessa syften och att syftet med en lagstiftning måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna i fråga åtgärden innebär. [45]

91. Såsom anges ovan [46] kan åtkomst till uppgifter som lagrats av leverantörer med stöd av en åtgärd som vidtagits i enlighet med artikel 15.1 i direktiv 2002/58 i princip endast motiveras av det mål av allmänt samhällsintresse som ligger till grund för leverantörernas skyldighet att lagra uppgifterna. [47]

92. Domstolen har således slagit fast att i enlighet med proportionalitetsprincipen kan ett allvarligt ingrepp i samband med förebyggande, utredning, avslöjande och lagföring av brott nämligen endast motiveras av syftet att bekämpa brottslighet som också måste kvalificeras som grov. [48]

93. Jag vill i detta avseende framhålla att Hadopis åtkomst till uppgifter om fysisk identitet som motsvarar en IP-adress tvärtemot vad den franska regeringen och kommissionen har anfört faktiskt utgör ett allvarligt ingrepp i de grundläggande rättigheterna. Det rör sig nämligen inte endast om att få åtkomst till uppgifter om fysisk identitet, vilka i sig inte är av hög känslighet, utan om att para ihop dessa uppgifter med en större mängd uppgifter, nämligen IP-adressen, och även, som sökandena i det nationella målet har anfört, ett utdrag ur en fil som laddats ned i strid med upphovsrätten. Det handlar alltså om att koppla en persons fysiska identitet till innehållet i den fil som konsulterats och till den IP-adress där konsultationen ägde rum.

94. På samma sätt som jag anser att sådan lagring av uppgifter som utgör ett allvarligt ingrepp i de grundläggande rättigheterna även bör tillåtas i syfte att förebygga, utreda, avslöja och lagföra brott på internet där IP-adressen utgör den enda utredningsmetoden som gör det möjligt att identifiera den person till vilken adressen var tilldelad då brottet begicks, [49] tror jag emellertid att det också måste vara möjligt att få åtkomst till dessa uppgifter i syfte att uppnå samma mål, för att inte godta en generell straffrihet för brott som enbart begås på internet.

95. Hadopis åtkomst till uppgifter om fysisk identitet parade med en IP-adress tycks alltså berättigad av det mål av allmänt samhällsintresse för vilket denna lagring har ålagts leverantörer av elektroniska kommunikationstjänster.

96. I domstolens praxis anges emellertid att nationell lagstiftning som reglerar behöriga myndigheters åtkomst till lagrade trafik- och lokaliseringsuppgifter inte kan vara begränsad till att kräva att åtkomst till uppgifterna svarar mot det ändamål som eftersträvas med lagstiftningen, utan den måste även fastställa de materiella och formella villkor som gäller för behöriga nationella myndigheters åtkomst till de berörda uppgifterna. [50]

45 Se dom av den 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punkt 55), och domen Prokuratuur (punkt 32).

46 Se ovan punkt 47.

47 Se dom SpaceNet, (punkt 131), La Quadrature du Net m.fl. (punkt 166), och dom Commissioner of An Garda Síochána m.fl. (punkt 98).

48 Se dom Tele2 (punkt 115), dom av den 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punkt 56), och dom Prokuratuur (punkt 33).

49 Se punkt 65 och följande punkter i detta förslag till avgörande.

50 Se dom Tele2 (punkt 118), Prokuratuur (punkt 49), och Commissioner of An Garda Síochána m.fl. (punkt 104).

97. Domstolen har i synnerhet slagit fast att eftersom en generell åtkomst till samtliga lagrade uppgifter, oberoende av om det finns någon koppling till det eftersträvade målet, inte kan anses vara begränsad till vad som är strängt nödvändigt, måste den nationella lagstiftningen således vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges åtkomst till uppgifter om användare, för att kontrollera att åtkomst endast beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. [51]

98. Enligt rättspraxis är det väsentligt, för att säkerställa att de villkoren uppfylls fullt ut i praktiken, att behöriga nationella myndigheters åtkomst till de lagrade uppgifterna i princip, utom i brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet. [52]

99. Jag konstaterar emellertid att domstolen, under andra omständigheter än dem i det nu aktuella fallet, har slagit fast att det krävs sådan förhandskontroll av åtkomsten till personuppgifter, vilken innebär *synnerligen allvarliga* ingrepp i privatlivet för användarna av elektroniska kommunikationstjänster.

100. I alla de domar i vilka detta krav underströks var det nämligen fråga om nationella åtgärder som tillät åtkomst till samtliga trafik- och lokaliseringsuppgifter om användarna med avseende på samtliga elektroniska kommunikationsmedel [53] eller, åtminstone, fast och mobil telefoni. [54] Det var närmare bestämt fråga om åtkomst till ”ett stort antal … uppgifter som kan ge information om den kommunikation som en användare av elektronisk kommunikationsutrustning har utfört eller om platsen där vederbörande har använt terminalutrustning, vilka gör det möjligt att dra mycket precisa slutsatser om de berörda personernas privatliv”. [55] Jag menar att det betyder att kravet på en förhandskontroll av åtkomsten till dessa uppgifter av en domstol eller ett oberoende förvaltningsorgan endast gäller under dessa förutsättningar.

101. Hadopi har endast åtkomst till uppgifter om fysisk identitet parade med den IP-adress som använts och den fil som konsulterats vid en viss tidpunkt, utan att det leder till att behöriga myndigheter kan rekonstruera den berörda användarens klickström, och därmed inte heller kan dra några precisa slutsatser om användarens privatliv utöver kunskapen om just den fil som konsulterades då brottet begicks. Det är alltså inte fråga om att tillåta spårning av allt som den berörda användaren gör på internet.

102. Vidare är det endast fråga om uppgifter om personer som, såsom fastställts i protokoll upprättade av upphovsrättsorganisationer, har ägnat sig åt gärningar som kan utgöra åsidosättande av skyldigheten enligt artikel L.336-3 CPI. Hadopis åtkomst till uppgifter om fysisk identitet parade med IP-adresser är alltså strikt begränsad till vad som är nödvändigt för att uppnå det eftersträvade målet, det vill säga att förebygga, utreda, avslöja och lagföra brott på internet – i vilket mekanismen för *graduated response* ingår – för vilka IP-adresserna utgör den enda utredningsmetoden som gör det möjligt att identifiera den person som var tilldelad adressen då brottet begicks.

[51] Se dom Tele2 (punkt 119), Prokuratuur (punkt 50), och Commissioner of An Garda Síochána m.fl. (punkt 105).

[52] Se dom Tele2 (punkt 120), Prokuratuur (punkt 51), och Commissioner of An Garda Síochána m.fl. (punkt 106).

[53] Se dom Tele2 och dom Commissioner of An Garda Síochána m.fl.

[54] Se dom Prokuratuur.

[55] Se dom Prokuratuur (punkt 45).

103. Under dessa förutsättningar anser jag att artikel 15.1 i direktiv 2002/58 inte kräver att en domstol eller ett oberoende förvaltningsorgan på förhand ska kontrollera Hadopis åtkomst till uppgifter om fysisk identitet parade med användarnas IP-adresser.

104. I övrigt vill jag i likhet med den franska regeringen framhålla att Hadopis åtkomst till dessa uppgifter, även om den inte är underkastad en förhandskontroll av en domstol eller ett oberoende förvaltningsorgan, ändå inte är undantagen all kontroll, i och med att den datafil som Hadopi översänder till operatörer av elektronisk kommunikation upprättas dagligen av en auktoriserad tjänsteman på grundval av anmälningar som tas emot och kontrolleras slumpmässigt genom stickprov innan de förs in i datafilen.[56] Framför allt ska det påpekas att förfarandet för *graduated response* fortfarande omfattas av bestämmelserna i direktiv (EU) 2016/680.[57] De fysiska personer som berörs av Hadopis verksamhet omfattas av en rad materiella och processuella garantier i enlighet med detta direktiv. Dessa garantier inbegriper rätt att begära tillgång till samt rättelse och radering av personuppgifter som behandlats av Hadopi, liksom en möjlighet att lämna in ett klagomål till en oberoende tillsynsmyndighet och därefter, i förekommande fall, väcka talan vid domstol enligt allmänna rättsregler.[58]

105. Jag föreslår följaktligen som svar på de två första tolkningsfrågorna att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan, ska tolkas så, att den inte utgör hinder för en nationell lagstiftning enligt vilken det är tillåtet för leverantörer av elektroniska kommunikationstjänster att lagra uppgifter om fysisk identitet som är kopplade till IP-adresser och enligt vilken en förvaltningsmyndighet som har till uppgift att skydda upphovsrätten och närstående rättigheter mot rättighetsintrång på internet ges rätt att få åtkomst till dessa uppgifter, så att myndigheten ska kunna identifiera innehavarna av adresserna, som är misstänkta för att ha begått sådana rättighetsintrång och, i förekommande fall, vidta åtgärder mot dem, utan att denna åtkomst är underkastad någon förhandskontroll av en domstol eller ett oberoende förvaltningsorgan, när dessa uppgifter utgör den enda utredningsmetoden som möjliggör identifiering av den person som var tilldelad denna adress när intrånget begicks.

B. Den tredje tolkningsfrågan

106. Den hänskjutande domstolen har ställt den tredje tolkningsfrågan, för det fall de två första frågorna besvaras jakande och med hänsyn till den låga känsligheten hos uppgifter om fysisk identitet, den strikta regleringen av åtkomsten till uppgifterna och kravet på att inte undergräva den aktuella förvaltningsmyndighetens allmännyttiga uppdrag, för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, och 11 samt med artikel 52.1 i stadgan, ska tolkas så, att den utgör hinder för att åtkomsten är föremål för förhandskontroll på ett anpassat sätt, till exempel genom en automatiserad kontroll, i förekommande fall under överinseende av en intern avdelning vid ett organ som garanterar oberoende och opartiskhet i förhållande till de tjänstemän som ansvarar för insamlingen.

[56] Jag vill tillägga att det finns genomförbarhetsargument som talar mot en skyldighet till systematisk förhandskontroll. En förutsättning för ett sådant organiserat system för att bekämpa upphovsrättsintrång på internet som det aktuella i det nationella målet är att det finns ett behov av att behandla stora mängder personuppgifter som står i proportion till antalet intrång som beivras. År 2019 hanterade Hadopi exempelvis, enligt den franska regeringens yttrande, 33 465 ansökningar om identifiering av IP-adress per dag. En skyldighet att på förhand kontrollera åtkomsten till dessa uppgifter skulle i praktiken innebära en risk att mekanismerna för organiserat bekämpande av intrång på internet inte kan fungera och att balansen mellan användarnas och upphovsmännens rättigheter rubbas.

[57] Europaparlamentets och rådets direktiv av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89).

[58] Alla dessa garantier föreskrivs genom bestämmelserna i kapitel III, avdelning III i Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (lag nr 78-17 av den 6 januari 1978 om datasystem, register och friheter) (JORF av den 7 januari 1978).

107. Det framgår av den tredje tolkningsfrågans lydelse och av den franska regeringens skriftliga svar på domstolens frågor att de villkor för den automatiserade kontroll som avses med frågan inte avser en befintlig kontrollmekanism i nationell rätt, utan vilka lösningar som skulle kunna undersökas för att vid behov anpassa det franska regelverket till unionsrätten.

108. Det är utrett i fast praxis att en begäran om förhandsavgörande syftar till att bidra till den faktiska lösningen av en tvist som rör unionsrätten och inte till att uttala sig om allmänna och hypotetiska frågor. [59]

109. Den tredje tolkningsfrågan är alltså enligt min mening hypotetisk och bör därför avvisas.

110. Mot bakgrund av det svar som jag föreslår på den första och den andra tolkningsfrågan finns det under alla omständigheter inte anledning att besvara den tredje tolkningsfrågan.

V. Förslag till avgörande

111. Mot bakgrund av det ovan anförda föreslår jag att domstolen besvarar de frågor som ställts av Conseil d'État (Högsta förvaltningsdomstolen, Frankrike) på följande sätt:

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 (direktivet om integritet och elektronisk kommunikation), jämförd med artiklarna 7, 8 och 11 samt artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna

ska tolkas så,

att den inte utgör hinder för en nationell lagstiftning enligt vilken det är tillåtet för leverantörer av elektroniska kommunikationstjänster att lagra uppgifter om fysisk identitet som är kopplade till IP-adresser och enligt vilken en förvaltningsmyndighet som har till uppgift att skydda upphovsrätten och närstående rättigheter mot rättighetsintrång på internet ges rätt att få åtkomst till dessa uppgifter, så att myndigheten ska kunna identifiera innehavarna av adresserna, som är misstänkta för att ha begått sådana rättighetsintrång och, i förekommande fall, vidta åtgärder mot dem, utan att denna åtkomst är underkastad någon förhandskontroll av en domstol eller ett oberoende förvaltningsorgan, när dessa uppgifter utgör den enda utredningsmetoden som möjliggör identifiering av den person som var tilldelad denna adress när intrånget begicks.

[59] Se dom av den 26 oktober 2017, Balgarska energiyna borsa (C-347/16, EU:C:2017:816, punkt 31), dom av den 31 maj 2018, Confetra m.fl. (C-259/16 och C-260/16, EU:C:2018:370, punkt 63), och dom av den 17 oktober 2019, Elektrorazpredelenie Yug (C-31/18, EU:C:2019:868, punkt 32).