



Samling af Afgørelser

DOMSTOLENS DOM (plenum)

30. april 2024*

Indhold

Retsforskrifter	5
EU-retten	5
De almindelige bestemmelser om beskyttelse af personoplysninger	5
– Direktiv 95/46/EF	5
– Databeskyttelsesforordningen	6
De sektorspecifikke bestemmelser om beskyttelse af personoplysninger	7
– Direktiv 2002/58	7
– Direktiv (EU) 2016/680	10
Bestemmelserne om beskyttelse af intellektuelle ejendomsrettigheder	11
Fransk ret	12
CPI	12
Dekret 2010/236	16
Lov om postvæsen og elektronisk kommunikation	18
Twisten i hovedsagen og de præjudicielle spørgsmål	19
Om de præjudicielle spørgsmål	21
Indledende bemærkninger	21

* Processprog: fransk.

Spørgsmålet, om en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse, der er lagret af udbydere af elektroniske kommunikationstjenester, med henblik på bekæmpelse af immaterialretskrænkelser begået online, kan begrundes i henhold til artikel 15, stk. 1, i direktiv 2002/58 23

Kravene i forbindelse med lagring af identitetsdata og de hertil knyttede IP-adresser, der foretages af udbydere af elektroniske kommunikationstjenester 23

Kravene i forbindelse med adgang til identitetsdata knyttet til en IP-adresse lagret af udbydere af elektroniske kommunikationstjenester 28

Kravet om kontrol ved en domstol eller en uafhængig administrativ enhed forud for en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse 33

De krav vedrørende de materielle og processuelle betingelser samt vedrørende garantierne mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data, der gælder for en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse 38

Sagsomkostninger 41

»Præjudiciel forelæggelse – behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor – direktiv 2002/58/EF – fortrolighed af elektronisk kommunikation – beskyttelse – artikel 5 og artikel 15, stk. 1 – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 7, 8 og 11 samt artikel 52, stk. 1 – national lovgivning med henblik på bekæmpelse af immaterialretskrænkelser på internettet ved en offentlig myndigheds indgriben – procedure med såkaldte »gradvise foranstaltninger« – rettighedsorganisationernes forudgående indsamling af IP-adresser, der er anvendt til aktiviteter, som krænker ophavsrettigheder eller beslægtede rettigheder – efterfølgende adgang for den offentlige myndighed, der har til opgave at beskytte ophavsrettigheder og beslægtede rettigheder, til identitetsdata knyttet til disse IP-adresser, der er lagret af udbyderne af elektroniske kommunikationstjenester – automatiseret behandling – krav om forudgående kontrol ved en domstol eller en uafhængig administrativ enhed – materielle og processuelle betingelser – garantier mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data«

I sag C-470/21,

angående en anmodning om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) ved afgørelse af 5. juli 2021, indgået til Domstolen den 30. juli 2021, i sagen

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

mod

Premier ministre,

Ministre de la Culture,

har

DOMSTOLEN (plenum),

sammensat af præsidenten, K. Lenaerts, vicepræsidenten, L. Bay Larsen, afdelingsformændene A. Arabadjiev, A. Prechal (refererende dommer), K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra og Z. Csehi samt dommerne M. Ilešič, J.-C. Bonichot, S. Rodin, P.G. Xuereb, L.S. Rossi, I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl, I. Ziemele, J. Passer, D. Gratsias, M.L. Arastey Sahún og M. Gavalec,

generaladvokat: M. Szpunar,

justitssekretærer: fuldmægtige V. Giacobbo og M. Krausenböck,

på grundlag af den skriftlige forhandling og efter retsmødet den 5. juli 2022,

efter at der er afgivet indlæg af:

- La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net og French Data Network ved avocat A. Fitzjean Ó Cobhthaigh,
- den franske regering ved A. Daniel, A.-L. Desjonquères og J. Illouz, som befuldmægtigede,
- den danske regering ved J.F. Kronborg og V. Pasternak Jørgensen, som befuldmægtigede,
- den estiske regering ved M. Kriisa, som befuldmægtiget,
- den finske regering ved H. Leppo, som befuldmægtiget,
- den svenske regering ved H. Shev, som befuldmægtiget,
- den norske regering ved F. Bergsjø, S.-E. Dahl, J.T. Kaasin og P. Wennerås, som befuldmægtigede,
- Europa-Kommissionen ved S.L. Kalèda, H. Kranenborg, P.-J. Loewenthal og F. Wilman, som befuldmægtigede,

efter at generaladvokaten har fremsat forslag til afgørelse i retsmødet den 27. oktober 2022,

på grundlag af kendelsen af 23. marts 2023 om genoptagelse af den mundtlige forhandling og efter retsmødet den 15. maj 2023,

efter at der er afgivet indlæg af:

- La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net og French Data Network ved avocat A. Fitzjean Ó Cobhthaigh,
- den franske regering ved R. Bénard, J. Illouz og T. Stéhelin, som befuldmægtigede,

- den tjekkiske regering ved T. Suchá og J. Vlácil, som befuldmægtigede,
 - den danske regering ved J.F. Kronborg og C. A.-S. Maertens, som befuldmægtigede,
 - den estiske regering ved M. Kriisa, som befuldmægtiget,
 - Irland ved Chief State Solicitor M. Browne samt A. Joyce og D. O'Reilly, som befuldmægtigede, bistået af D. Fenelly, BL,
 - den spanske regering ved A. Gavela Llopis, som befuldmægtiget,
 - den cypriotiske regering ved I. Neophytou, som befuldmægtiget,
 - den lettiske regering ved J. Davidoviča og K. Pommere, som befuldmægtigede,
 - den nederlandske regering ved E.M.M. Besselink, M.K. Bultermann og A. Hanje, som befuldmægtigede,
 - den finske regering ved A. Laine og H. Leppo, som befuldmægtigede,
 - den svenske regering ved F.-D. Göransson og H. Shev, som befuldmægtigede,
 - den norske regering ved S.-E. Dahl og P. Wennerås, som befuldmægtigede,
 - Europa-Kommissionen ved S.L. Kalèda, H. Kranenborg, P.-J. Loewenthal og F. Wilman, som befuldmægtigede,
 - Den Europæiske Tilsynsførende for Databeskyttelse ved V. Bernardo, C.-A. Marnier, D. Nardi og M. Pollmann, som befuldmægtigede,
 - Den Europæiske Unions Agentur for Cybersikkerhed ved A. Bourka, som befuldmægtiget,
- og efter at generaladvokaten har fremsat forslag til afgørelse i retsmødet den 28. september 2023, afsagt følgende

Dom

- 1 Anmodningen om præjudiciel afgørelse vedrører fortolkningen af Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT 2002, L 201, s. 37), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EUT 2009, L 337, s. 11) (herefter »direktiv 2002/58«), sammenholdt med Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«).
- 2 Anmodningen er blevet indgivet i forbindelse med en tvist mellem på den ene side foreningerne La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net og French Data Network og på den anden side Premier ministre (premierministeren, Frankrig)

og Ministre de la Culture (kulturministeren, Frankrig) vedrørende lovligheden af décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé »Système de gestion des mesures pour la protection des œuvres sur internet« (dekret 2010-236 af 5.3.2010 om den automatiserede behandling af personoplysninger, der er tilladt i medfør af artikel L. 331-29 i lov om intellektuel ejendomsret og benævnt »System til håndtering af foranstaltninger til beskyttelse af værker på internettet«) (JORF nr. 56 af 7.3.2010, tekst nr. 19), som ændret ved décret n° 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (dekret 2017-924 af 6.5.2017 om forvaltning af ophavsret og beslægtede rettigheder gennem en forvaltningsorganisation og om ændring af lov om intellektuel ejendomsret) (JORF nr. 109 af 10.5.2017, tekst nr. 176) (herefter »dekret 2010-236«).

Retsforskrifter

EU-retten

De almindelige bestemmelser om beskyttelse af personoplysninger

– Direktiv 95/46/EF

- 3 I afdeling II med overskriften »Principper vedrørende grundlaget for behandling af oplysninger« i kapitel II i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31) var artikel 7 affattet som følger:

»Medlemsstaterne fastsætter bestemmelser om, at behandling af personoplysninger kun må finde sted, hvis:

[...]

- f) behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1, i dette direktiv, går forud herfor.«

- 4 Dette direktivs artikel 13, stk. 1, bestemte følgende:

»Medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk. 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:

[...]

- g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder.«

– Databeskyttelsesforordningen

- 5 Artikel 2 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT 2016, L 119, s. 1, herefter »databeskyttelsesforordningen«), der har overskriften »Materielt anvendelsesområde«, bestemmer følgende i stk. 1 og 2:

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

2. Denne forordning gælder ikke for behandling af personoplysninger:

[...]

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

- 6 I databeskyttelsesforordningens artikel 4, der har overskriften »Definitioner«, er følgende angivet:

»I denne forordning forstås ved:

1) »personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«) [...]

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

[...]«

- 7 Denne forordnings artikel 6 med overskriften »Lovlig behandling« fastsætter følgende i stk. 1:

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

[...]

f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor [...].

Første afsnit, litra f), gælder ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.«

8 Databeskyttelsesforordningens artikel 9, der har overskriften »Behandling af særlige kategorier af personoplysninger«, fastsætter i stk. 2, litra e) og f), at forbuddet mod behandling af visse typer personoplysninger vedrørende bl.a. oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering ikke finder anvendelse, hvis behandlingen vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede, eller er nødvendig, bl.a. for at retskrav kan fastlægges, gøres gældende eller forsvares.

9 Databeskyttelsesforordningens artikel 23, der har overskriften »Begrænsninger«, bestemmer følgende i stk. 1:

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

[...]

i) beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder

j) håndhævelse af civilretlige krav.«

De sektorspecifikke bestemmelser om beskyttelse af personoplysninger

– *Direktiv 2002/58*

10 I 2., 6., 7., 11., 26. og 30. betragtning til direktiv 2002/58 er følgende anført:

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

[...]

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

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

[...]

- (11) Ligesom direktiv [95/46] finder dette direktiv ikke anvendelse på beskyttelse af grundlæggende rettigheder og frihedsrettigheder, der er forbundet med aktiviteter, der ikke er omfattet af fællesskabsretten. Det ændrer derfor ikke den nuværende balance mellem enkeltpersoners ret til privatlivets fred og medlemsstaternes mulighed for, jf. artikel 15, stk. 1, i dette direktiv, at træffe de foranstaltninger, der er nødvendige til beskyttelse af den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område. Dette direktiv berører derfor ikke medlemsstaternes mulighed for lovligt at opfange elektronisk kommunikation eller træffe andre foranstaltninger, hvis det er nødvendigt med et af disse formål for øje og i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder[, undertegnet i Rom den 4. november 1950,] som fortolket i Den Europæiske Menneskerettighedsdomstols retspraksis. Sådanne foranstaltninger skal være passende, stå i åbenbart rimeligt forhold til det mål, der forfølges, og være nødvendige i et demokratisk samfund, og foranstaltningerne bør omfattes af passende beskyttelsesordninger i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

[...]

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

[...]

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

- 11 Artikel 2 i direktiv 2002/58, der har overskriften »Definitioner«, har følgende ordlyd:

»[...]

Følgende definitioner anvendes også:

- a) »bruger«: en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste
- b) »trafikdata«: data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf

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

[...]«

- 12 Dette direktivs artikel 3, der har overskriften »Omfattede tjenester«, fastsætter følgende:

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

- 13 Direktivets artikel 5, der har overskriften »Kommunikationshemmelighed«, har følgende ordlyd:

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

[...]

3. Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv [95/46] at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. [...]«

- 14 Samme direktivs artikel 6, der har overskriften »Trafikdata«, bestemmer følgende:

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

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

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

[...]

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

- 15 Artikel 15 i direktiv 2002/58, der har overskriften »Anvendelsesområdet for visse bestemmelser i direktiv [95/46]«, fastsætter følgende:

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

[...]

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

[...]«

– *Direktiv (EU) 2016/680*

- 16 Artikel 1 i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2016, L 119, s. 89), der har overskriften »Genstand og formål«, fastsætter følgende i stk. 1:

»I dette direktiv fastsættes regler om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.«

- 17 Dette direktivs artikel 3, der har overskriften »Definitioner«, bestemmer følgende:

»I dette direktiv forstås ved:

[...]

7. »kompetent myndighed«:

- a) enhver offentlig myndighed, der er kompetent med hensyn til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed, eller
- b) ethvert andet organ eller enhver anden enhed, som i henhold til medlemsstaternes nationale ret udøver offentlig myndighed og offentlige beføjelser med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed

[...]«

Bestemmelserne om beskyttelse af intellektuelle ejendomsrettigheder

- 18 Artikel 8 i Europa-Parlamentets og Rådets direktiv 2004/48/EF af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder (EUT 2004, L 157, s. 45, berigtiget i EUT 2004, L 195, s. 16), der har overskriften »Ret til information«, bestemmer følgende:

»1. Medlemsstaterne sikrer, at de kompetente retslige myndigheder i forbindelse med sager om krænkelse af en intellektuel ejendomsrettighed og som svar på en velbegrundet og forholdsmæssig afpasset begæring fra rekvirenten[...] kan pålægge den krænkende part [...] at give oplysninger om oprindelsen af og distributionskanalerne for de varer eller tjenesteydelser, der krænker en intellektuel ejendomsrettighed [...]

2. De i stk. 1 nævnte oplysninger omfatter i givet fald:

- a) navn og adresse på producenter, fremstillere, distributører, leverandører og andre tidligere indehavere af varer eller tjenesteydelser samt på engros- og detailhandelsled

[...]

3. Stk. 1 og 2 finder anvendelse med forbehold af andre lovbestemmelser, der:

- a) tillægger rettighedshaveren en mere vidtgående ret til information
- b) regulerer brugen af oplysninger meddelt i henhold til denne artikel i civilretlige eller strafferetlige sager
- c) omhandler erstatningsansvaret ved misbrug af retten til information
- d) danner grundlag for at nægte at meddele oplysninger, som ville tvinge den i stk. 1 omhandlede person til at indrømme, at vedkommende selv eller en nær slægtning har deltaget i en krænkelse af en intellektuel ejendomsrettighed, eller
- e) omhandler beskyttelsen af fortrolige kilder til information eller behandlingen af personoplysninger.«

Fransk ret

CPI

- 19 Artikel L. 331-12 i code de la propriété intellectuelle (lov om intellektuel ejendomsret) i den affattelse, der var gældende på datoen for den afgørelse, som anfægtes af sagsøgerne i hovedsagen (herefter »CPI«), bestemmer følgende:

»La Haute autorité pour la diffusion des œuvres et la protection des droits sur internet [den høje myndighed for spredning af værker og beskyttelse af rettigheder på internettet (Hadopi)] er en uafhængig offentlig myndighed. [...]«

- 20 Denne lovs artikel L. 331-13 fastsætter følgende:

»[Hadopi] varetager:

1° En opgave bestående i fremme af udviklingen af det lovlige udbud og observation af den lovlige og den ulovlige brug af værker og andre frembringelser, der er beskyttet af en ophavsret eller en beslægtet rettighed, på de elektroniske kommunikationsnet, der anvendes til levering af offentlige onlinekommunikationstjenester.

2° En opgave bestående i beskyttelse af disse værker og frembringelser mod krænkelse af disse rettigheder, der begås på de elektroniske kommunikationsnet, der anvendes til levering af offentlige onlinekommunikationstjenester.

[...]«

- 21 Den nævnte lovs artikel L. 331-15 har følgende ordlyd:

»[Hadopi] er sammensat af et kollegium og en kommission for beskyttelse af rettigheder. [...]«

[...]

Medlemmerne af kollegiet og af kommissionen for beskyttelse af rettigheder modtager under udøvelsen af deres beføjelser ikke instruks fra nogen myndighed.«

- 22 Samme lovs artikel L. 331-17, stk. 1, bestemmer følgende:

»Kommissionen for beskyttelse af rettigheder har til ansvar at træffe de foranstaltninger, der er omhandlet i artikel L. 331-25.«

- 23 CPI's artikel L 331-21 har følgende ordlyd:

»Med henblik på udøvelsen af de beføjelser, der tilkommer kommissionen for beskyttelse af rettigheder, råder [Hadopi] over edsvorne embedsmænd, som er bemyndiget af [præsidenten for Hadopi] på de betingelser, der er fastsat i et dekret efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager, Frankrig)]. [...]«

Medlemmerne af kommissionen for beskyttelse af rettigheder og de i stk. 1 nævnte embedsmænd modtager de henvendelser, der rettes til kommissionen i overensstemmelse med artikel L. 331-24. De bedømmer de faktiske omstændigheder.

De kan af hensyn til proceduren indhente alle dokumenter, uanset hvilket medie de er lagret på, herunder data, der er lagret og behandlet af operatører inden for elektronisk kommunikation i henhold til artikel L. 34-1 i code des postes et des communications électroniques [(lov om postvæsen og elektronisk kommunikation)] og de tjenesteydere, der er nævnt i artikel 6, stk. 1, nr. 1 og 2, i loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(lov 2004-575 af 21.6.2004 om tillid til den digitale økonomi)].

De kan ligeledes indhente en kopi af de dokumenter, der er nævnt i det foregående stykke.

Fra operatørerne inden for elektronisk kommunikation kan de navnlig indhente oplysninger om navn, postadresse, e-mailadresse og telefonnummer på abonnenter, hvis adgang til offentlige onlinekommunikationstjenester er blevet anvendt til reproduktion, fremførelse, tilrådighedsstillelse eller overføring til almenheden af beskyttede værker eller andre frembringelser uden tilladelse fra rettighedshaverne [...], når en sådan er påkrævet.«

24 Denne lovs artikel L. 331-24 bestemmer følgende:

»Kommissionen for beskyttelse af rettigheder optager en sag til behandling på anmodning af edsvorne, befuldmægtigede embedsmænd [...], der udpeges af:

- faglige interesseorganisationer, der er forskriftsmæssigt oprettet
- kollektive forvaltningsorganisationer
- Centre national du cinéma et de l'image animée [(det nationale center for filmproduktion og animerede billeder)].

Kommissionen for beskyttelse af rettigheder kan ligeledes optage en sag til behandling på grundlag af oplysninger, der videregives til den af procureur de la République [(anklagemyndighed, Frankrig)].

Kommissionen kan ikke optage en sag til behandling vedrørende faktiske forhold, der ligger mere end seks måneder tilbage i tiden.«

25 Den nævnte lovs artikel L. 331-25, der regulerer proceduren med såkaldte »gradvise foranstaltninger«, har følgende ordlyd:

»Når kommissionen for beskyttelse af rettigheder skal træffe afgørelse om faktiske forhold, der kan udgøre en tilsidesættelse af den forpligtelse, der er fastsat i [CPI's] artikel L. 336-3, kan den rette en henstilling til abonnenten [...], hvori denne mindes om bestemmelserne i artikel L. 336-3, pålægges at overholde den forpligtelse, der er fastlagt i disse bestemmelser, og bliver gjort opmærksom på, hvilke sanktioner der kan bringes i anvendelse i medfør af artikel L. 335-7 og L. 335-7-1. Henstillingen indeholder ligeledes oplysning til abonnenten om lovligt udbud af kulturelt onlineindhold, om sikringsmidler, der gør det muligt at forebygge tilsidesættelser af den forpligtelse, der er fastsat i artikel L. 336-3, og om de farer, som praksis, der ikke overholder ophavsretten og de beslægtede rettigheder, indebærer for fornyelsen af den kunstneriske frembringelse og for økonomien i den kulturelle sektor.

I tilfælde af, at de faktiske forhold, der kan udgøre en tilsidesættelse af den forpligtelse, der er fastsat i artikel L. 336-3, gentages inden for seks måneder regnet fra det tidspunkt, hvor der er rettet henstilling som omhandlet i stk. 1, kan kommissionen rette en ny elektronisk henstilling med samme oplysninger som i den foregående henstilling [...]. Kommissionen påser, at denne henstilling ledsages af en

anbefalet skrivelse eller en skrivelse, hvorved det på anden vis er muligt at godtgøre datoen for fremsættelsen af henstillingen.

I henstillinger, der fremsættes på grundlag af denne artikel, anføres dato og tidspunkt for konstateringen af de faktiske forhold, der kan udgøre en tilsidesættelse af den forpligtelse, der er fastsat i artikel L. 336-3. Indholdet af de beskyttede værker eller frembringelser, der er berørt af en sådan tilsidesættelse, meddeles derimod ikke heri. Der anføres kontaktoplysninger – telefonnummer, postadresse og e-mailadresse – som modtageren, såfremt denne måtte ønske det, kan benytte til at fremsætte bemærkninger til kommissionen for beskyttelse af rettigheder, og til – ved udtrykkeligt at anmode herom – at opnå nærmere oplysninger om indholdet af de beskyttede værker eller frembringelser, der er berørt af den tilsidesættelse, som foreholdes modtageren.«

26 CPI's artikel L. 331-29 bestemmer følgende:

»[Hadopi] kan vedtage bestemmelse om en automatiseret behandling af oplysninger om personer, der er genstand for en procedure som omhandlet i dette underafsnit.

Formålet med denne behandling er at gøre det muligt for kommissionen for beskyttelse af rettigheder at gennemføre de foranstaltninger, der er fastsat i dette underafsnit, alle hermed forbundne proceduremæssige skridt og den nærmere ordning for fremsendelse af meddelelse til faglige interesseorganisationer og kollektive forvaltningsorganisationer om eventuelle indbringelser af sager for den retslige myndighed samt underretninger som omhandlet i artikel L. 335-7, stk. 5.

Gennemførelsesbestemmelserne til denne artikel fastsættes ved dekret [...]. Dekretet skal bl.a. fastsætte nærmere bestemmelser om:

- kategorierne af registrerede oplysninger og opbevaringsperioden
- de modtagere, der er berettigede til at modtage meddelelse om disse oplysninger, heriblandt personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester
- betingelserne for, at de berørte personer over for [Hadopi] kan udøve deres ret til indsigt i oplysninger om dem [...]

27 I lovens artikel L. 335-2, stk. 1 og 2, er følgende angivet:

»Enhver udgivelse af skrifter, musikkompositioner, design, malerier eller andre frembringelser, helt eller delvist trykt eller indspillet, i strid med lovene og forskrifterne om ophavsmænds ejendomsret, udgør en immaterialretskrænkelser, og enhver sådan krænkelse er en strafbar handling.

Ophavsretskrænkelser i Frankrig af værker, der er udgivet i Frankrig eller i udlandet, straffes med tre års fængsel og en bøde på 300 000 EUR.«

28 Den nævnte lovs artikel L. 335-4, stk. 1, bestemmer følgende:

»Optagelse, reproduktion, videregivelse, tilrådighedsstillelse for offentligheden, mod eller uden vederlag, TV-spredning af en ydelse, et fonogram, et videogram, et program eller en pressepublikation, foretaget uden den udøvende kunstners, fonogram- eller videofremstillerens, den audiovisuelle formidlingsvirksomheds, presseudgiverens eller nyhedsbureauets tilladelse, når en sådan kræves, straffes med tre års fængsel og en bøde på 300 000 EUR.«

29 CPI's artikel L. 335-7 fastsætter reglerne om pålæggelse af supplerende straf i form af inddragelse af adgang til en offentlig onlinekommunikationstjeneste i højst et år over for personer, der er skyldige i strafbare handlinger som omhandlet i bl.a. denne lovs artikel L. 335-2 og L. 335-4.

30 Denne lovs artikel 335-7-1, stk. 1, har følgende ordlyd:

»For forseelser af femte grad, der er omhandlet i denne lov, kan der på de samme betingelser, når forskrifterne hjemler det, ved alvorlig forsømmelighed pålægges en supplerende straf som fastsat i artikel L. 335-7 over for indehaveren af en adgang til en offentlig onlinekommunikationstjeneste, til hvem kommissionen for beskyttelse af rettigheder i medfør af artikel L. 331-25 forudgående, ved en anbefalet skrivelse eller en skrivelse, hvorved det på anden vis er muligt at godtgøre fremsættelsesdatoen, har rettet en henstilling med opfordring til at iværksætte midler til sikring af vedkommendes internetadgang.«

31 Samme lovs artikel L. 336-3 har følgende ordlyd:

»Indehaveren af en adgang til offentlige onlinekommunikationstjenester har pligt til at sikre, at denne adgang ikke anvendes til reproduktion, fremførelse, tilrådighedsstillelse eller overføring til almenheden af værker eller andre frembringelser, der er beskyttet af en ophavsret eller en beslægtet rettighed uden tilladelse fra rettighedshaverne [...], når en sådan er påkrævet.

Indehaverens manglende opfyldelse af den forpligtelse, der er fastsat stk. 1, medfører ikke, at den pågældende ifalder strafansvar [...].«

32 CPI's artikel R. 331-37, stk. 1, fastsætter følgende:

»Operatører inden for elektronisk kommunikation [...] og tjenesteudbydere [...] skal ved samkøring af den automatiserede behandling af personoplysninger, der er nævnt i artikel L. 331-29, eller ved brug af et lagringsmedium, der sikrer oplysningernes integritet og sikkerhed, videregive de personoplysninger og andre oplysninger, der er nævnt i nr. 2 i bilaget til dekret [2010-236], inden for otte dage efter kommissionen for beskyttelse af rettigheders videregivelse af de tekniske data, der er nødvendige til identificering af den abonnent, hvis adgang til offentlige onlinekommunikationstjenester er blevet anvendt til reproduktion, fremførelse, tilrådighedsstillelse eller overføring til almenheden af beskyttede værker eller frembringelser uden tilladelse fra rettighedshaverne [...], når en sådan er påkrævet.«

33 Denne lovs artikel L. 331-40 har følgende ordlyd:

»Såfremt kommissionen for beskyttelse af rettigheder inden for et år efter fremsættelsen af en henstilling som nævnt i artikel L. 335-7-1, stk. 1, forelægges nye faktiske forhold, der kan udgøre en alvorlig forsømmelse som defineret i artikel R. 335-5, meddeler den ved anbefalet skrivelse abonnenten, at disse forhold kan forfølges. I skrivelsen opfordres den pågældende til at fremsætte sine bemærkninger inden for en frist på 15 dage. Det præciseres, at vedkommende inden for samme frist kan anmode om at blive hørt i henhold til artikel L. 331-21-1 og har ret til at lade sig bistå af en advokat. I skrivelsen opfordres abonnenten ligeledes til at angive sine udgifter til forsørgelse og sine økonomiske midler.

Kommissionen for beskyttelse af rettigheder kan på eget initiativ indkalde den pågældende til høring. I indkaldelsen skal det angives, at vedkommende har ret til at lade sig bistå af en advokat.«

34 CPI's artikel R. 335-5 bestemmer følgende:

»I. – Der foreligger en alvorlig forsømmelse, der straffes med bøde som fastsat for forseelser af femte grad, såfremt indehaveren af en adgang til offentlige onlinekommunikationstjenester uden gyldig grund, og når de betingelser, der er fastsat i stk. II, er opfyldt,

1° ikke har iværksat noget middel til sikring af denne adgang eller

2° ikke har udvist agtpågivenhed ved iværksættelsen af et sådant middel.

II. – Bestemmelserne i stk. I finder alene anvendelse, når følgende to betingelser er opfyldt:

1° Kommissionen for beskyttelse af rettigheder har i henhold til artikel L. 331-25 og i de former, der er fastsat ved denne artikel, henstillet til indehaveren af adgangen at iværksætte et middel til sikring af sin adgang, som gør det muligt at forebygge en fornyet anvendelse heraf til reproduktion, fremførelse, tilrådighedsstillelse eller overføring til almenheden af værker eller frembringelser, der er beskyttet af en ophavsret eller en beslægtet rettighed uden tilladelse fra rettighedshaverne [...], når en sådan er påkrævet.

2° Denne adgang benyttes i løbet af året efter fremsættelsen af denne henstilling på ny til de formål, der er nævnt i stk. II, nr. 1.«

35 Med virkning fra den 1. januar 2022 blev Hadopi i henhold til loi n° 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (lov 2021-1382 af 25.10.2021 om regulering og beskyttelse af adgang til kulturelle værker i den digitale tidsalder, JORF nr. 250 af 26.10.2021, tekst nr. 2), lagt sammen med Conseil supérieur de l'audiovisuel (øverste råd for audiovisuelle anliggender, CSA), der er en anden uafhængig offentlig myndighed, til Autorité de régulation de la communication audiovisuelle et numérique (tilsynsmyndighed for audiovisuel og digital kommunikation, ARCOM).

36 Den procedure med gradvise foranstaltninger, som er nævnt i denne doms præmis 25, er dog i det væsentlige forblevet uændret, selv om den nu ikke gennemføres af Hadopis kommission for beskyttelse af rettigheder, der var sammensat af tre medlemmer udpeget af henholdsvis Conseil d'État (øverste domstol i forvaltningsretlige sager), Cour des comptes (revisionsret, Frankrig) og Cour de cassation (kassationsdomstol, Frankrig), men af to medlemmer af ARCOM's kollegium, hvoraf det ene udpeges af Conseil d'État (øverste domstol i forvaltningsretlige sager) og det andet af Cour de cassation (kassationsdomstol).

Dekret 2010/236

37 Dekret 2010-236, der bl.a. er vedtaget på grundlag af CPI's artikel L. 331-29, fastsætter følgende i artikel 1:

»Formålet med den behandling af personoplysninger, der benævnes »System til håndtering af foranstaltninger til beskyttelse af værker på internettet«, er at gøre det muligt for [Hadopis] kommission for beskyttelse af rettigheder at gennemføre:

1° De foranstaltninger, der er omhandlet i bog III i [CPI's] lovgivningsmæssige del (afsnit III, kapitel I, afdeling 3, underafdeling 3) og bog III i samme lovs forskriftsmæssige del (afsnit III, kapitel I, afdeling 2, underafdeling 2).

2° Indbringelser af sager for anklagemyndigheden vedrørende faktiske forhold, der kan udgøre strafbare handlinger i henhold til samme lovs artikel L. 335-2, L. 335-3, L. 335-4 og R. 335-5, og fremsendelse af meddelelse til faglige interesseorganisationer og kollektive forvaltningsorganisationer om sådanne indbringelser.

[...]«

38 Dette dekrets artikel 4 bestemmer følgende:

»I. – Direkte adgang til personoplysninger og til de oplysninger, der er nævnt i bilaget til dette dekret, har edsvorne embedsmænd, som er bemyndiget af præsidenten for [Hadopi] i henhold til [CPI's] artikel L. 331-21, og medlemmerne af den kommission for beskyttelse af rettigheder, der er nævnt i artikel 1.

II – Operatørerne inden for elektronisk kommunikation og de tjenesteudbydere, der er nævnt i nr. 2 i bilaget til dette dekret, modtager følgende:

- de tekniske data, der er nødvendige til identificering af abonnenten
- de henstillinger, der er omhandlet i [CPI's] artikel L. 331-25, med henblik på, at disse rettes elektronisk til abonnenterne
- de oplysninger, der er nødvendige for at iværksætte de supplerende straffe i form af inddragelse af adgang til en offentlig onlinekommunikationstjeneste, som anklagemyndigheden har gjort kommissionen for beskyttelse af rettigheder bekendt med.

III – De faglige interesseorganisationer og de kollektive forvaltningsorganisationer modtager meddelelse om indbringelse af en sag for anklagemyndigheden.

IV – De retslige myndigheder modtager rapporter om fastslåelse af faktiske forhold, der kan udgøre strafbare handlinger i henhold til [CPI's] artikel L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 og R. 335-5.

Det automatiserede strafferegister tilføres oplysning om fuldbyrdelsen af straf, der består i inddragelse af adgang.»

39 Bilaget til det nævnte dekret fastsætter følgende:

»Følgende personoplysninger og andre oplysninger registreres i forbindelse med den behandling, der benævnes »System til håndtering af foranstaltninger til beskyttelse af værker på internettet«:

1° Personoplysninger og andre oplysninger, der hidrører fra faglige interesseorganisationer, som er forskriftsmæssigt oprettet, fra kollektive forvaltningsorganisationer og fra det nationale center for filmproduktion og animerede billeder, samt oplysninger, der hidrører fra anklagemyndigheden:

Hvad angår faktiske forhold, der kan udgøre en tilsidesættelse af den forpligtelse, der er fastsat i [CPI's] artikel L. 336-3:

dato og tidspunkt for de faktiske forhold

de berørte abonnenters IP-adresse

anvendt peer-to-peer-protokol

pseudonym anvendt af abonnenten

oplysninger om de beskyttede værker og frembringelser, som de faktiske forhold vedrører

filnavnet, således som dette forekommer på abonnentens apparat (efter omstændighederne)

den udbyder af internetadgang, hos hvilken der er tegnet abonnement på adgang, eller som har leveret den tekniske IP-ressource.

[...]

2° Personoplysninger og andre oplysninger, der vedrører abonnenten, og som er indsamlet hos operatørerne inden for elektronisk kommunikation [...] og hos tjenesteudbyderne [...]:

for- og efternavne

postadresse og e-mailadresser

telefonnummer

installationsadresse for abonnentens telefonudstyr

den udbyder af internetadgang, der anvender de tekniske ressourcer fra den internetudbyder, der er nævnt i nr. 1, og med hvem abonnenten har tegnet kontrakt, samt sagsnummer

startdatoen for inddragelsen af en adgang til en offentlig onlinekommunikationstjeneste.

[...]«

Lov om postvæsen og elektronisk kommunikation

40 Artikel L. 34-1, stk. IIa, i lov om postvæsen og elektronisk kommunikation bestemmer følgende:

»Operatører inden for elektronisk kommunikation skal lagre:

1° Med henblik på straffesager, forebyggelse af trusler mod den offentlige sikkerhed og beskyttelse af den nationale sikkerhed lagres data vedrørende brugerens identitet i fem år efter udløbet af kontraktens gyldighed.

2° Til de samme formål som angivet i stk. IIa, nr. 1, lagres andre oplysninger, der er afgivet af brugeren ved indgåelsen af en kontrakt eller ved oprettelsen af en konto, og betalingsoplysninger i et år, efter at gyldigheden af brugerens kontrakt er udløbet, eller vedkommendes konto er blevet lukket.

3° Med henblik på bekæmpelse af grov kriminalitet og alvorlige forbrydelser, forebyggelse af alvorlige trusler mod den offentlige sikkerhed og beskyttelse af den nationale sikkerhed lagres tekniske data, som gør det muligt at identificere kilden til en forbindelse, eller data vedrørende det anvendte terminaludstyr i et år efter forbindelsen eller anvendelsen af terminaludstyret.«

Twisten i hovedsagen og de præjudicielle spørgsmål

- 41 Efter et stiltiende afslag fra Premier ministre (premierministeren) på sagsøgerne i hovedsagens anmodning om ophævelse af dekret 2010-236 har de ved stævning af 12. august 2019 anlagt sag ved Conseil d'État (øverste domstol i forvaltningsretlige sager) med påstand om annulation af denne afgørelse om stiltiende afslag. De har i det væsentlige gjort gældende, at CPI's artikel L. 331-21, stk. 3-5, der er en del af retsgrundlaget for dette dekret, dels er i strid med retten til respekt for privatlivet som fastsat i den franske forfatning, dels tilsidesætter EU-retten, navnlig artikel 15 i direktiv 2002/58 og chartrets artikel 7, 8, 11 og 52.
- 42 Med hensyn til det aspekt af søgsmålet, der vedrører den hævdede tilsidesættelse af forfatningen, har Conseil d'État (øverste domstol i forvaltningsretlige sager) forelagt Conseil constitutionnel (forfatningsråd, Frankrig) et forudgående spørgsmål om forfatningsmæssighed.
- 43 Ved afgørelse 2020-841 QPC af 20. maj 2020, La Quadrature du Net m.fl. (Ret til videregivelse til Hadopi), fastslog Conseil constitutionnel (forfatningsråd), at CPI's artikel L. 331-21, stk. 3 og 4, var forfatningsstridige, men at samme artikels stk. 5 var i overensstemmelse med forfatningen, undtagen hvad angår ordet »navnlig« heri.
- 44 Hvad angår det aspekt af søgsmålet, der vedrører den hævdede tilsidesættelse af EU-retten, har sagsøgerne i hovedsagen navnlig gjort gældende, at dekret 2010-236 og de bestemmelser, der udgør retsgrundlaget for dette, for mindre, ophavsretlige lovovertrædelser, som er begået på internettet, i uforholdsmæssig grad tillader adgang til forbindelsesdata uden forudgående kontrol foretaget af en domstol eller en myndighed, der frembyder garantier for uafhængighed og upartiskhed. Navnlig hører disse overtrædelser ikke til »grov kriminalitet« som omhandlet i dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970).
- 45 I denne henseende har Conseil d'État (øverste domstol i forvaltningsretlige sager) for det første anført, at Domstolen ved dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), bl.a. har fastslået, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke er til hinder for retsforbud, der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af data vedrørende identiteten på brugerne af elektroniske kommunikationsmidler. Hvad angår data vedrørende identiteten på brugerne af elektroniske kommunikationsmidler er en sådan lagring dermed mulig, uden en særlig tidsbegrænsning, med henblik på efterforskning, afsløring og retsforfølgning i straffesager i almindelighed. Direktiv 2002/58 er heller ikke til hinder for, at der gives adgang til disse data til sådanne formål.
- 46 Den forelæggende ret har heraf udledt, at hvad angår adgang til data vedrørende identiteten på brugerne af elektroniske kommunikationsmidler skal sagsøgerne i hovedsagens anbringende om, at dekret 2010-236 er ulovligt, for så vidt som det er vedtaget i forbindelse med bekæmpelse af mindre lovovertrædelser, forkastes.

- 47 Den forelæggende ret har for det andet mindet om, at Domstolen ved dom af 21. december 2016, *Tele2 Sverige og Watson m.fl.* (C-203/15 og C-698/15, EU:C:2016:970), bl.a. har fastslået, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der regulerer beskyttelsen af og sikkerheden vedrørende trafikdata og lokaliseringsdata, og navnlig de kompetente nationale myndigheders adgang til de lagrede data, uden at undergive den nævnte adgang en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed.
- 48 Den forelæggende ret har nærmere bestemt henvist til ovennævnte doms præmis 120, hvori Domstolen præciserede, at det er afgørende, at en sådan adgang til de lagrede data principielt, undtagen i behørigt begrundede hastende tilfælde, er undergivet kravet om en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne domstols eller denne enheds afgørelse træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af disse myndigheder inden for rammerne af procedurer med henblik på forebygelse, afsløring eller strafferetlig forfølgning.
- 49 Domstolen henviste igen til dette krav i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), for så vidt angår efterretningstjenesters indsamling i realtid af forbindelsesdata og i dom af 2. marts 2021, *Prokuratuur* (Betingelser for adgang til oplysninger om elektronisk kommunikation) (C-746/18, EU:C:2021:152), hvad angår nationale myndigheders adgang til forbindelsesdata.
- 50 Den forelæggende ret har ligeledes anført, at Hadopi siden oprettelsen i 2009 har rettet mere end 12,7 mio. henstillinger til abonnenter på grundlag af den procedure med gradvise foranstaltninger, der er fastsat i CPI's artikel L. 331-25, heraf 827 791 henstillinger alene i 2019. Denne omstændighed indebærer, at embedsmændene i Hadopis kommission for beskyttelse af rettigheder hvert år nødvendigvis har måttet indsamle et betydeligt antal data vedrørende de pågældende brugeres identitet. Hvis denne indsamling underlægges en forudgående kontrol, er der efter den forelæggende rets opfattelse en risiko for, at det i betragtning af det store antal henstillinger bliver umuligt at gennemføre disse.
- 51 Under disse omstændigheder har Conseil d'État (øverste domstol i forvaltningsretlige sager) besluttet at udsætte sagen og forelægge Domstolen følgende præjudicielle spørgsmål:
- »1) Er [identitetsdata knyttet til] en IP-adresse blandt de trafik- eller lokaliseringsdata, der principielt skal gøres til genstand for en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser?
 - 2) Såfremt det første spørgsmål besvares bekræftende, ønskes det oplyst, om direktiv [2002/58], sammenholdt med [chartret], i betragtning af den lave følsomhed af data, der vedrører den civile identitet på brugerne, herunder deres kontaktoplysninger, skal fortolkes således, at det er til hinder for en national lovgivning, hvorefter en administrativ myndighed skal indsamle disse data [knyttet til] de pågældende brugeres IP-adresse uden en forudgående kontrol foretaget af en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser?
 - 3) Såfremt det andet spørgsmål besvares bekræftende, ønskes det oplyst, om direktiv [2002/58] – i betragtning af den lave følsomhed af data, der vedrører den civile identitet [på brugerne], af den omstændighed, at disse data alene kan indsamles med henblik på at forhindre tilsidesættelser af forpligtelser, der i national ret er præcist, indskrænkende og udtømmende

defineret, og af den omstændighed, at en systematisk kontrol af adgangen til data om hver enkelt bruger foretaget af en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, vil skade opfyldelsen af den samfundsopgave, der er overdraget den uafhængige administrative myndighed, der [foretager] denne indsamling – er til hinder for, at denne kontrol foretages i overensstemmelse med hensigtsmæssige retningslinjer, såsom en automatisk kontrol, i givet fald under tilsyn af en intern enhed i det pågældende organ, hvis embedsmænd, der foretager indsamlingen, er uafhængige og upartiske?»

Om de præjudicielle spørgsmål

- 52 Med de tre præjudicielle spørgsmål, der skal behandles samlet, ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der tillader, at den offentlige myndighed, der har til opgave at beskytte ophavsrettigheder og beslægtede rettigheder mod krænkelse af disse rettigheder, der begås på internettet, får adgang til identitetsdata, som er lagret af udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og som er knyttet til IP-adresser, der forudgående er indsamlet af rettighedsorganisationer, for at denne offentlige myndighed kan identificere indehaverne af disse adresser, som er blevet anvendt til aktiviteter, der kan udgøre sådanne krænkelse, og efter omstændighederne træffe foranstaltninger over for dem, uden at denne adgang er underlagt et krav om en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed.

Indledende bemærkninger

- 53 Hovedsagen vedrører to særskilte og på hinanden følgende behandlinger af personoplysninger, der foretages i forbindelse med den virksomhed, der udøves af Hadopi, som er en uafhængig offentlig myndighed, hvis opgave i henhold til CPI's artikel L. 331-13 bl.a. består i at beskytte værker og andre frembringelser, der er omfattet af en ophavsret eller en beslægtet rettighed, mod krænkelse af disse rettigheder, der begås på elektroniske kommunikationsnet, som anvendes til levering af offentlige onlinekommunikationstjenester.
- 54 Den første behandling, der foretages forudgående af befuldmægtigede, edsvorne embedsmænd i rettighedsorganisationer, foregår i to etaper. Først indsamles IP-adresser, der tilsyneladende er blevet anvendt til aktiviteter, der kan udgøre en krænkelse af en ophavsret eller en beslægtet rettighed, fra peer-to-peer-netværk. Dernæst stilles en række personoplysninger og andre oplysninger til rådighed for Hadopi i form af rapporter. Ifølge listen i punkt 1 i bilaget til dekret 2010/236 er der tale om oplysninger om datoen og tidspunktet for de faktiske forhold, de pågældende abonnenters IP-adresse, den anvendte peer-to-peer-protokol, det pseudonym, der er anvendt af abonnenten, oplysninger om de beskyttede værker eller frembringelser, som de faktiske forhold vedrører, navnet på filen, således som dette forekommer på abonnentens apparat (efter omstændighederne), og den udbyder af internetadgang, hos hvilken der er tegnet abonnement på adgang, eller som har leveret den tekniske IP-ressource.
- 55 Den anden behandling, som efterfølgende foretages af internetudbydere efter anmodning fra Hadopi, foregår ligeledes i to etaper. Først forbindes de IP-adresser, der forudgående er indsamlet, med indehaverne af disse adresser. Dernæst stilles en række personoplysninger og oplysninger om de nævnte indehavere, der i det væsentlige vedrører deres identitet, til rådighed

for denne offentlige myndighed. Ifølge listen i punkt 2 i bilaget til dekret 2010/236 er der i det væsentlige tale om for- og efternavn, postadresse og e-mailadresser, telefonnummer og installationsadresse for abonnentens telefonudstyr.

- 56 I sidstnævnte henseende fastsætter CPI's artikel L. 331-21 i stk. 5, i den affattelse, der følger af den afgørelse fra Conseil constitutionnel (forfatningsråd), der er nævnt i denne doms præmis 43, at medlemmerne af Hadopis kommission for beskyttelse af rettigheder og denne myndigheds edsvorne embedsmænd, som er bemyndiget af præsidenten for Hadopi, fra operatørerne inden for elektronisk kommunikation kan indhente oplysninger om identitet, postadresse, e-mailadresse og telefonnummer på abonnenter, hvis adgang til offentlige onlinekommunikationstjenester er blevet anvendt til reproduktion, fremførelse, tilrådighedsstillelse eller overføring til almenheden af beskyttede værker eller andre frembringelser uden tilladelse fra rettighedshaverne, når en sådan er påkrævet.
- 57 Disse forskellige behandlinger af personoplysninger tager sigte på at gøre det muligt for Hadopi at træffe foranstaltninger som fastsat i forbindelse med den administrative procedure med såkaldte »gradvise foranstaltninger«, der er reguleret ved CPI's artikel L. 331-25, over for de således identificerede indehavere af IP-adresser. Disse foranstaltninger er først fremsættelse af »henstillinger«, der ligner advarsler, dernæst, såfremt sagen indbringes for Hadopis rettighedskommission inden for et år efter fremsættelsen af endnu en henstilling vedrørende faktiske forhold, der kan udgøre en gentagelse af den konstaterede tilsidesættelse, meddelelse til abonnenten, jf. CPI's artikel R. 331-40, om, at de faktiske forhold kan udgøre en strafbar handling i form af en såkaldt »alvorlig forsømmelse« som defineret i CPI's artikel R. 335-5, der kan straffes med bøde på op til 1 500 EUR og 3 000 EUR i gentagelsestilfælde, og endelig, efter forhandling, henvisning af sagen til anklagemyndigheden hvad angår faktiske forhold, der kan udgøre en sådan forseelse eller, efter omstændighederne, en immaterialretskrænkelser som omhandlet i CPI's artikel L. 335-2 eller L. 335-4, der kan straffes med tre års fængsel og bøde på 300 000 EUR.
- 58 Når dette er sagt, vedrører de spørgsmål, som den forelæggende ret har stillet, alene den efterfølgende behandling, der er beskrevet i denne doms præmis 55, og ikke den forudgående behandling, hvis væsentligste elementer er beskrevet i præmis 54.
- 59 Det bemærkes imidlertid, at såfremt de berørte rettighedsorganisationers forudgående indsamling af IP-adresser er i strid med EU-retten, vil EU-retten ligeledes være til hinder for, at udbyderne af elektroniske kommunikationstjenester kan udnytte disse data i forbindelse med den efterfølgende behandling, der består i at forbinde IP-adresserne med dataene vedrørende identiteten på indehaverne af disse adresser.
- 60 I denne forbindelse bemærkes indledningsvis, at IP-adresser ifølge Domstolens praksis både udgør trafikdata som omhandlet i direktiv 2002/58 og personoplysninger som omhandlet i databeskyttelsesforordningen (jf. i denne retning dom af 17.6.2021, M.I.C.M., C-597/19, EU:C:2021:492, præmis 102 og 113 og den deri nævnte retspraksis).
- 61 Rettighedsorganisationers indsamling af IP-adresser, der er offentlige og synlige for alle, er imidlertid ikke omfattet af anvendelsesområdet for direktiv 2002/58, eftersom det er åbenbart, at en sådan behandling ikke sker »i forbindelse med, at [...] elektroniske kommunikationstjenester stilles til rådighed«, som omhandlet i dette direktivs artikel 3.

- 62 En sådan indsamling af IP-adresser – der, således som det fremgår af sagsakterne for Domstolen, med visse kvantitative begrænsninger og på visse betingelser tillades af Commission nationale de l'informatique et des libertés (den nationale kommission for databehandling og frihedsrettigheder, CNIL, Frankrig) med henblik på videregivelse til Hadopi til eventuel brug i senere administrative eller retslige procedurer med sigte på at bekæmpe aktiviteter, der krænker ophavsrettigheder og beslægtede rettigheder – udgør derimod en »behandling« som omhandlet i databeskyttelsesforordningens artikel 4, nr. 2), hvis lovlighed afhænger af, om betingelserne i denne forordnings artikel 6, stk. 1, første afsnit, litra f), er opfyldt, i lyset af den praksis, som Domstolen har udviklet i bl.a. dom af 17. juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, præmis 102 og 103), og af 4. juli 2023, Meta Platforms m.fl. (Almindelige betingelser for anvendelse af et socialt netværk) (C-252/21, EU:C:2023:537, præmis 106-112 og den deri nævnte retspraksis).
- 63 Hvad angår den efterfølgende behandling, der er beskrevet i denne doms præmis 55, er denne for sin del omfattet af anvendelsesområdet for direktiv 2002/58, eftersom den sker »i forbindelse med, at [...] elektroniske kommunikationstjenester stilles til rådighed«, som omhandlet i dette direktivs artikel 3, for så vidt som de omhandlede data indhentes fra udbydere af elektroniske kommunikationstjenester i overensstemmelse med CPI's artikel L. 331-21.

Spørgsmålet, om en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse, der er lagret af udbydere af elektroniske kommunikationstjenester, med henblik på bekæmpelse af immaterialretskrænkelser begået online, kan begrundes i henhold til artikel 15, stk. 1, i direktiv 2002/58

- 64 Henset til ovenstående indledende bemærkninger opstår spørgsmålet – som også den forelæggende ret ønsker besvaret – om den begrænsning af de grundlæggende rettigheder som sikret ved chartrets artikel 7, 8 og 11, der følger af, at en offentlig myndighed, såsom Hadopi, har adgang til identitetsdata knyttet til en IP-adresse, som den allerede kender, kan begrundes i henhold til artikel 15, stk. 1, i direktiv 2002/58.
- 65 Adgang til sådanne personoplysninger kan kun gives, for så vidt som de er blevet lagret i overensstemmelse med direktiv 2002/58 (jf. i denne retning dom af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 29).

Kravene i forbindelse med lagring af identitetsdata og de hertil knyttede IP-adresser, der foretages af udbydere af elektroniske kommunikationstjenester

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

forbundne data, og navnlig af det forbud mod at lagre disse data, der udtrykkeligt er fastsat i dette direktivs artikel 5, bliver hovedreglen (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, præmis 110 og 111).

- 67 En retsforskrift, der er vedtaget i henhold til denne bestemmelse, skal derfor faktisk og præcist opfylde et af de formål, der er nævnt i den foregående præmis, idet opregningen af disse formål i artikel 15, stk. 1, første punktum, i direktiv 2002/58 er udtømmende, og være i overensstemmelse med EU-rettens generelle principper, som bl.a. omfatter proportionalitetsprincippet, og de grundlæggende rettigheder, der er sikret ved chartret. Domstolen har i denne henseende allerede fastslået, at den pligt, som en medlemsstat i henhold til en national lovgivning har pålagt udbydere af elektroniske kommunikationstjenester, til at lagre trafikdata med henblik på i påkommende tilfælde at gøre dem tilgængelige for de kompetente nationale myndigheder, ikke blot rejser en række spørgsmål vedrørende overholdelsen af chartrets artikel 7 og 8, der vedrører henholdsvis respekten for privatlivet og beskyttelsen af personoplysninger, men ligeledes vedrørende artikel 11, der omhandler ytringsfriheden (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 112 og 113).
- 68 I forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 skal der således tages hensyn til betydningen af såvel retten til respekt for privatlivet, der er sikret ved chartrets artikel 7, som retten til beskyttelse af personoplysninger, der er sikret ved dette charters artikel 8, således som denne betydning fremgår af Domstolens praksis, og retten til ytringsfrihed, idet denne grundlæggende rettighed, der er sikret ved chartrets artikel 11, udgør et af de væsentlige grundlag for et demokratisk og pluralistisk samfund og er en del af de værdier, som Unionen i overensstemmelse med artikel 2 TEU er støttet på (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 114 og den deri nævnte retspraksis).
- 69 Det skal i denne henseende fremhæves, at lagring af trafikdata og lokaliseringsdata i sig selv udgør dels en undtagelse fra det forbud mod at lagre disse data, der er fastsat i artikel 5, stk. 1, i direktiv 2002/58, og som gælder for alle andre end brugerne, dels et indgreb i den grundlæggende ret til respekt for privatlivet og til beskyttelse af personoplysninger, der er sikret ved chartrets artikel 7 og 8, idet det ikke er afgørende, om de pågældende oplysninger vedrørende privatlivet er følsomme, eller om dette indgreb har medført eventuelle ubehageligheder for de berørte. Det er desuden ikke afgørende, om de lagrede data efterfølgende anvendes, idet adgangen til sådanne data, uanset hvorledes de efterfølgende anvendes, udgør et særskilt indgreb i de grundlæggende rettigheder, der er nævnt i den foregående præmis (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 115 og 116).
- 70 Når dette er sagt, afspejler artikel 15, stk. 1, i direktiv 2002/58, for så vidt som den giver medlemsstaterne mulighed for at indføre visse undtagelser, således som anført i denne doms præmis 66, det forhold, at de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, ikke er absolutte rettigheder, men skal ses i sammenhæng med deres funktion i samfundet. Som det fremgår af chartrets artikel 52, stk. 1, tillader dette charter nemlig begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen og respekterer de nævnte rettigheders væsentligste indhold, og for så vidt som disse begrænsninger under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af EU, eller et behov for beskyttelse af andres rettigheder og friheder (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 120 og 121).

- 71 I det foreliggende tilfælde bemærkes, at selv om Hadopi formelt kun er bemyndiget til at få adgang til de identitetsdata, der er knyttet til en IP-adresse, er det karakteristisk for denne adgang, at den forudsætter, at IP-adressen og dataene vedrørende identiteten på indehaveren af denne adresse forudgående er blevet forbundet af de pågældende udbydere af elektroniske kommunikationstjenester. Adgangen forudsætter således nødvendigvis, at udbyderne råder over både IP-adresserne og dataene vedrørende deres indehaveres identitet.
- 72 Desuden ønsker denne offentlige myndighed adgang til disse data alene med det formål at identificere indehaveren af en IP-adresse, der er blevet anvendt til aktiviteter, som kan krænge ophavsrettigheder eller beslægtede rettigheder, eftersom den pågældende ulovligt har stillet beskyttede værker til rådighed på internettet, for at de kan downloades af andre. Under disse omstændigheder skal identitetsdata anses for at være tæt knyttet til både IP-adressen og de oplysninger, som Hadopi råder over, vedrørende det værk, der er stillet til rådighed på internettet.
- 73 Der kan ikke ses bort fra en sådan særlig sammenhæng i forbindelse med undersøgelsen af, om en foranstaltning vedrørende lagring af personoplysninger i henhold til artikel 15, stk. 1, i direktiv 2002/58, fortolket i lyset af chartrets artikel 7, 8 og 11, eventuelt kan begrundes (jf. analogt Menneskerettighedsdomstolen, 24.4.2018, Benedik mod Slovenien, CE:ECHR:2018:0424JUD006235714, § 109).
- 74 Det er derfor i lyset af de krav vedrørende lagring af IP-adresser, der følger af nævnte artikel 15, stk. 1, fortolket i lyset af chartrets artikel 7, 8 og 11, at det skal undersøges, om det er muligt at begrunde det indgreb i de grundlæggende rettigheder, som er sikret ved sidstnævnte artikler i chartret, der følger af, at udbydere af offentligt tilgængelige elektroniske kommunikationstjenester lagrer oplysninger, som Hadopi har beføjelse til at få adgang til.
- 75 I denne forbindelse skal det fremhæves, at det følger af Domstolens praksis, at selv om IP-adresser som anført i denne doms præmis 60 udgør trafikdata som omhandlet i direktiv 2002/58, adskiller disse adresser sig fra andre kategorier af trafikdata og fra lokaliseringsdata.
- 76 I denne henseende har Domstolen anført, at IP-adresser genereres uden at være knyttet til en bestemt kommunikation og hovedsageligt tjener til gennem udbydere af elektroniske kommunikationstjenester at identificere ejeren af det terminaludstyr, hvorfra en kommunikation via internettet foretages. Hvad angår e-mail og IP-telefoni afslører IP-adresser, for så vidt som det kun er IP-adresserne på kilden til kommunikationen og ikke IP-adresserne på modtageren af kommunikationen, der lagres, således ikke som sådan nogen oplysninger om de tredjemænd, der har været i kontakt med den person, som har foretaget kommunikationen. I denne henseende er denne kategori af data mindre følsomme end andre former for trafikdata (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 152).
- 77 Domstolen har ganske vist i præmis 156 i dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), fastslået, at på trods af konstateringen af, at oplysninger om IP-adresser er mindre følsomme, når de udelukkende tjener til at identificere brugeren af en elektronisk kommunikationstjeneste, er artikel 15, stk. 1, i direktiv 2002/58 til hinder for generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, til andre formål end bekæmpelse af grov kriminalitet, forebyggelse af alvorlige trusler mod den offentlige sikkerhed og beskyttelse af den nationale sikkerhed. Domstolen støttede

imidlertid udtrykkeligt denne konklusion på den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8 og 11, som en sådan lagring af IP-adresser kan indebære.

- 78 Domstolen fastslog nemlig i samme doms præmis 153, at i det omfang IP-adresser, når de anvendes til at foretage en »udtømmende sporing af en internetbrugers søgemønstre« og dermed af den pågældendes onlineaktiviteter, bl.a. kan gøre det muligt at fastlægge en »detaljeret profil« af denne internetbruger, udgør den lagring og analyse af de nævnte IP-adresser, som en sådan sporing kræver, alvorlige indgreb i den pågældendes grundlæggende rettigheder, som er sikret ved chartrets artikel 7 og 8, og som ligeledes kan have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved chartrets artikel 11.
- 79 Det skal imidlertid fremhæves, at enhver generel og udifferentieret lagring af en, eventuelt omfattende, samling af statiske og dynamiske IP-adresser, der er anvendt af en person i en given periode, ikke nødvendigvis udgør et alvorligt indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7, 8 og 11.
- 80 I denne henseende vedrørte de sager, der gav anledning til dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), først og fremmest nationale lovgivninger, som indebar en forpligtelse til at lagre en række data, der var nødvendige for at fastslå en kommunikations dato, tidspunkt, varighed og type, identificere det anvendte kommunikationsudstyr og foretage lokalisering af terminaludstyret og kommunikationerne, dvs. data, der navnlig omfattede navn og adresse på brugeren, telefonnummer på den, der foretog opkaldet, og det kaldte nummer samt for internettjenester en IP-adresse. Desuden syntes de omhandlede nationale lovgivninger i to af disse sager også at omfatte data vedrørende overføring af elektronisk kommunikation via netværk, således at disse ligeledes gjorde det muligt at identificere arten af de oplysninger, der blev tilgået online (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 82 og 83).
- 81 Den lagring af IP-adresser, der blev foretaget inden for rammerne af sådanne nationale lovgivninger, kunne således, henset til de andre oplysninger, som i henhold til disse lovgivninger skulle lagres, og muligheden for at kombinere disse forskellige oplysninger, gøre det muligt at drage præcise slutninger om privatlivet for de personer, hvis data var omhandlet, og dermed føre til et alvorligt indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8 om beskyttelse af disse personers privatliv og personoplysninger samt ved chartrets artikel 11 om deres ytringsfrihed.
- 82 Derimod kan en forpligtelse for udbydere af elektroniske kommunikationstjenester til at foretage generel og udifferentieret lagring af IP-adresser, som de er pålagt ved en retsforordning vedtaget i medfør af artikel 15, stk. 1, i direktiv 2002/58, efter omstændighederne være begrundet i formålet om at bekæmpe strafbare handlinger i almindelighed, når det faktisk er udelukket, at denne lagring kan medføre alvorlige indgreb i den berørte persons privatliv som følge af muligheden for at drage præcise slutninger om vedkommende, bl.a. ved at koble disse IP-adresser sammen med en række trafik- eller lokaliseringsdata, der ligeledes er blevet lagret af disse udbydere.
- 83 En medlemsstat, der påtænker at pålægge udbyderne af elektroniske kommunikationstjenester en forpligtelse til at foretage generel og udifferentieret lagring af IP-adresser med henblik på at nå et mål, der er knyttet til bekæmpelse af strafbare handlinger i almindelighed, skal derfor sikre, at

måden, hvorpå disse data lagres, garanteret udelukker enhver kombination af disse IP-adresser med andre data, der er lagret under overholdelse af direktiv 2002/58, som gør det muligt at drage præcise slutninger om privatlivet for de personer, hvis data således vil blive lagret.

- 84 Med henblik på at sikre, at en sådan kombination af data, der gør det muligt at drage præcise slutninger om den omhandlede persons privatliv, er udelukket, skal lagringsmåden vedrøre selve strukturen af lagringen, som i det væsentlige skal være tilrettelagt således, at det sikres, at de forskellige kategorier af lagrede data faktisk er hermetisk adskilte.
- 85 I denne henseende tilkommer det ganske vist den medlemsstat, der påtænker at pålægge udbyderne af elektroniske kommunikationstjenester en forpligtelse til generel og udifferentieret lagring af IP-adresser med henblik på at nå et mål, der er knyttet til bekæmpelse af strafbare handlinger i almindelighed, i sin lovgivning at fastsætte klare og præcise regler vedrørende den nævnte lagringsmåde, idet denne skal opfylde strenge krav. Domstolen kan imidlertid give nærmere oplysninger om lagringsmåden.
- 86 For det første skal de nationale regler, der er nævnt i den foregående præmis, sikre, at hver kategori af data, herunder identitetsdataene og IP-adresserne, opbevares fuldstændig adskilt fra de øvrige kategorier af lagrede data.
- 87 For det andet skal disse regler sikre, at adskillelsen af de forskellige kategorier af lagrede data, bl.a. identitetsdataene, IP-adresserne, de forskellige andre trafikdata, som ikke er data vedrørende IP-adresser, og de forskellige lokaliseringsdata, på det tekniske plan faktisk er hermetisk tæt, ved hjælp af et sikkert og pålideligt IT-system.
- 88 For det tredje må de nævnte regler, for så vidt som de giver mulighed for at koble de lagrede IP-adresser sammen med den berørte persons identitet under overholdelse af de krav, der følger af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11, kun tillade en sådan sammenkobling ved anvendelse af en effektiv teknisk fremgangsmåde, der ikke skader effektiviteten af den hermetiske adskillelse af disse datakategorier.
- 89 For det fjerde skal pålideligheden af denne hermetiske adskillelse kontrolleres regelmæssigt af en anden offentlig myndighed end den, der søger at få adgang til de personoplysninger, der er lagret af udbyderne af elektroniske kommunikationstjenester.
- 90 For så vidt som der i den gældende nationale lovgivning er fastsat sådanne strenge krav vedrørende den måde, hvorpå der foretages generel og udifferentieret lagring af IP-adresser og andre data, der lagres af udbyderne af elektroniske kommunikationstjenester, kan det indgreb, der følger af denne lagring af IP-adresser, på grund af selve strukturen af lagringen ikke kvalificeres som »alvorligt«.
- 91 Såfremt sådanne lovbestemmelser er indført, udelukker den således foreskrevne lagringsmåde for IP-adresser nemlig, at disse data kan kombineres med andre data, der er lagret under overholdelse af direktiv 2002/58, således at der kan drages præcise slutninger om den berørte persons privatliv.
- 92 Såfremt der findes lovbestemmelser, der opfylder de krav, der er angivet i denne doms præmis 86-89, og som garanterer, at ingen kombination af data vil kunne gøre det muligt at drage præcise slutninger om den omhandlede persons privatliv, er artikel 15, stk. 1, i direktiv

2002/58, sammenholdt med chartrets artikel 7, 8 og 11, følgelig ikke til hinder for, at den pågældende medlemsstat indfører en forpligtelse til generel og udifferentieret lagring af IP-adresser med henblik på et formål om bekæmpelse af strafbare handlinger i almindelighed.

- 93 Endelig skal sådanne lovbestemmelser, således som det fremgår af præmis 168 i dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), fastsætte en varighed af lagringen, der er begrænset til det strengt nødvendige, og ved klare og præcise regler sikre, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og processuelle betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data.
- 94 Det tilkommer den forelæggende ret at efterprøve, om den nationale lovgivning, der er omhandlet i hovedsagen, overholder de krav, der er angivet i denne doms præmis 85-93.

Kravene i forbindelse med adgang til identitetsdata knyttet til en IP-adresse lagret af udbydere af elektroniske kommunikationstjenester

- 95 Det følger af Domstolens praksis, at det på området for bekæmpelse af strafbare handlinger kun er bekæmpelse af grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde det alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, som følger af offentlige myndigheders adgang til en samling af trafikdata eller lokaliseringsdata, der kan tilvejebringe oplysninger om den kommunikation, som en bruger har foretaget ved hjælp af et elektronisk kommunikationsmiddel, eller om placeringen af det terminaludstyr, som den pågældende gør brug af, og som kan gøre det muligt at drage præcise slutninger vedrørende de berørte personers privatliv, uden at andre faktorer vedrørende forholdsmæssigheden af en anmodning om adgang, såsom varigheden af den periode, for hvilken der anmodes om adgang til sådanne data, kan føre til, at formålet om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed kan begrunde en sådan adgang (dom af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 35).
- 96 Når det indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, som følger af de offentlige myndigheders adgang til identitetsdata lagret af udbyderne af elektroniske kommunikationstjenester, uden at disse data kan kædes sammen med oplysninger om den foretagne kommunikation, ikke er alvorligt, eftersom disse data tilsammen ikke gør det muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis data er omhandlet, kan den nævnte adgang begrundes i et formål om forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 54, 57 og 60).
- 97 Det skal ligeledes tilføjes, at ifølge et princip, der er fastslået i Domstolens faste praksis, kan adgang til trafikdata og lokaliseringsdata kun begrundes i henhold til artikel 15, stk. 1, i direktiv 2002/58 i det mål af almen interesse, med henblik på hvilket udbyderne af elektroniske kommunikationstjenester er blevet pålagt at foretage lagringen, medmindre denne adgang er begrundet i et mål af almen interesse, som er vigtigere. Det følger bl.a. af dette princip, at der under ingen omstændigheder kan gives en sådan adgang med henblik på bekæmpelse af strafbare handlinger i almindelighed, når lagringen af de nævnte data er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 166).

- 98 Et sådant formål om bekæmpelse af strafbare handlinger i almindelighed kan derimod begrunde, at der gives adgang til trafikdata og lokaliseringsdata, der er blevet lagret og dermed opbevaret i det omfang og tidsrum, der er nødvendigt af hensyn til markedsføringen og faktureringen af tjenesterne samt leveringen af værdiforøgende tjenester som tilladt i henhold til artikel 6 i direktiv 2002/58 (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 108 og 167).
- 99 I det foreliggende tilfælde fremgår det for det første af den nationale lovgivning, der er omhandlet i hovedsagen, at Hadopi ikke har adgang til »en samling af trafikdata eller lokaliseringsdata« som omhandlet i den retspraksis, der er nævnt i denne doms præmis 95, således at Hadopi principielt ikke kan drage præcise slutninger om de berørte personers privatliv. En adgang, der ikke gør det muligt at drage sådanne slutninger, udgør ikke et alvorligt indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8.
- 100 Det følger nemlig af denne lovgivning og af de forklaringer, som den franske regering har givet herom, at denne offentlige myndigheds adgang er strengt begrænset til visse data vedrørende identiteten på indehaveren af en IP-adresse og alene tilladt med det formål at kunne identificere denne indehaver, der mistænkes for at have udøvet en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, idet den pågældende ulovligt har stillet beskyttede værker til rådighed på internettet, for at de kan downloades af andre. Adgangen tager sigte på, at der, efter omstændighederne, over for denne indehaver kan træffes en af de pædagogiske eller repressive foranstaltninger, der er fastsat i forbindelse med proceduren med gradvise foranstaltninger, nemlig fremsættelse af en første og en anden henstilling, dernæst en skrivelse til den pågældende om, at denne aktivitet kan udgøre en strafbar handling i form af en alvorlig forsømmelse, og endelig indbringelse af sagen for anklagemyndigheden med henblik på retsforfølgning af denne overtrædelse eller immaterialretskrænkelsen.
- 101 Den nationale lovgivning skal desuden fastsætte klare og præcise regler, der sikrer, at IP-adresser, der lagres i overensstemmelse med direktiv 2002/58, udelukkende kan anvendes til at identificere den person, som en bestemt IP-adresse er blevet tildelt, og samtidig forhindrer anvendelse, der gør det muligt, ved hjælp af en eller flere af disse adresser, at overvåge denne persons onlineaktiviteter. Når en IP-adresse således anvendes alene med det formål at identificere indehaveren af denne i forbindelse med en specifik administrativ procedure, der kan føre til strafferetlig forfølgning af den pågældende, og ikke med henblik på f.eks. at afsløre indehaverens kontakter eller lokalisering, vedrører adgangen til denne adresse med dette ene formål den nævnte adresse som identitetsdata snarere end som trafikdata.
- 102 Det følger endvidere af det princip, der er fastslået i den faste retspraksis, der er henvist til i denne doms præmis 97, at en adgang som den, Hadopi har i medfør af den lovgivning, der er omhandlet i hovedsagen, eftersom den forfølger et formål om bekæmpelse af strafbare handlinger i almindelighed, kun kan begrundes, hvis den gælder IP-adresser, der skal lagres af udbyderne af elektroniske kommunikationstjenester med henblik på samme formål og ikke med henblik på et formål, der er vigtigere, såsom bekæmpelse af grov kriminalitet, uden at dette dog berører adgang begrundet i et sådant formål om bekæmpelse af strafbare handlinger i almindelighed, når den er rettet mod IP-adresser, der lagres og dermed opbevares på de betingelser, der er fastsat i artikel 6 i direktiv 2002/58.
- 103 Som det fremgår af denne doms præmis 85-92, kan lagring af IP-adresser, der er baseret på en retsforordning vedtaget i medfør af artikel 15, stk. 1, i direktiv 2002/58 med henblik på formålet om bekæmpelse af strafbare handlinger i almindelighed, være begrundet, når den lagringsmåde, der er

indført ved de pågældende lovbestemmelser, opfylder en række krav, der i det væsentlige skal sikre, at de forskellige kategorier af lagrede data faktisk er hermetisk adskilte, således at kombination af data, der tilhører forskellige kategorier, faktisk er udelukket. Når en sådan lagringsmåde pålægges udbyderne af elektroniske kommunikationstjenester, udgør generel og uddifferentieret lagring af IP-adresser nemlig ikke et alvorligt indgreb i indehavernes privatliv, eftersom disse data ikke gør det muligt at drage præcise slutninger om deres privatliv.

- 104 I lyset af den retspraksis, der er anført i denne doms præmis 95-97, kan adgang til IP-adresser, der er lagret med henblik på at bekæmpe strafbare handlinger i almindelighed, når sådanne lovbestemmelser er indført, følgelig være begrundet henset til artikel 15, stk. 1, i direktiv 2002/58, når den alene er tilladt med henblik på at identificere en person, der mistænkes for at være involveret i sådanne strafbare handlinger.
- 105 I øvrigt er det forhold, at en offentlig myndighed som Hadopi gives adgang til identitetsdata knyttet til en offentlig IP-adresse, som rettighedsorganisationer har videregivet til denne myndighed alene med det formål at identificere indehaveren af denne adresse, der er blevet anvendt til onlineaktiviteter, som kan krænke ophavsrettigheder eller beslægtede rettigheder, således at denne indehaver kan pålægges en af de foranstaltninger, der er fastsat i forbindelse med proceduren med gradvise foranstaltninger, i overensstemmelse med Domstolens praksis vedrørende »retten til information« i forbindelse med sager om krænkelse af en intellektuel ejendomsrettighed som fastsat i artikel 8 i direktiv 2004/48 (jf. i denne retning dom af 29.1.2008, *Promusicae* (C-275/06, EU:C:2008:54, præmis 47 ff.).
- 106 I denne retspraksis har Domstolen nemlig, alt imens den har fremhævet, at anvendelse af foranstaltningerne i direktiv 2004/48 ikke kan påvirke hverken databeskyttelsesforordningen eller direktiv 2002/58, fastslået, at artikel 8, stk. 3, i direktiv 2004/48, sammenholdt med artikel 15, stk. 1, i direktiv 2002/58 og artikel 7, litra f), i direktiv 95/46, ikke er til hinder for, at medlemsstaterne fastsætter en forpligtelse for udbyderne af elektroniske kommunikationstjenester til overførsel af personoplysninger til privatpersoner med henblik på retsforfølgelse af krænkelse af ophavsretten ved de civile domstole, men omvendt heller ikke tvinger dem til at fastsætte en sådan forpligtelse (jf. i denne retning dom af 17.6.2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, præmis 124 og 125 og den deri nævnte retspraksis).
- 107 Når dette er sagt, kan der ved den konkrete bedømmelse af graden af det indgreb i privatlivet, som en offentlig myndigheds adgang til personoplysninger indebærer, for det andet ikke ses bort fra de særlige kendetegn ved den sammenhæng, hvori denne adgang indgår, og navnlig hele det sæt af data og oplysninger, der videregives til denne myndighed i medfør af den gældende nationale lovgivning, herunder allerede eksisterende data og oplysninger, der afslører indholdet (jf. analogt *Menneskerettighedsdomstolen*, 24.4.2018, *Benedik mod Slovenien*, CE:ECHR:2018:0424JUD006235714, § 109).
- 108 I det foreliggende tilfælde skal der således med henblik på den nævnte bedømmelse tages hensyn til den omstændighed, at Hadopi, før denne myndighed fik adgang til de omhandlede identitetsdata, som den har ret til, modtog bl.a. »oplysninger om de beskyttede værker og frembringelser, som de faktiske forhold vedrører«, og efter omstændighederne »filnavnet, således som dette forekommer på abonnentens apparat«, fra rettighedsorganisationerne i overensstemmelse med punkt 1 i bilaget til dekret 2010-236.

- 109 Med forbehold for den forelæggende rets efterprøvelse fremgår det af sagsakterne for Domstolen, at oplysningerne om det værk, som forholdene vedrører, således som angivet i en rapport, hvis indhold blev fastlagt ved CNIL's afgørelser af 10. juni 2010, i det væsentlige er begrænset til det pågældende værks titel og til et uddrag benævnt »chunk«, der fremstår som en alfanumerisk sekvens og ikke som en lyd- eller videooptagelse af værket.
- 110 I denne henseende kan det ganske vist ikke generelt udelukkes, at en offentlig myndigheds adgang til et begrænset antal data vedrørende identiteten på indehaveren af en IP-adresse, som er blevet videregivet til denne myndighed af en udbyder af elektroniske kommunikationstjenester alene med det formål at identificere denne indehaver i tilfælde, hvor IP-adressen er blevet anvendt til aktiviteter, der kan krænke ophavsrettigheder eller beslægtede rettigheder, kombineret med en analyse af selv begrænsede oplysninger, som rettighedsorganisationer forudgående har videregivet til den offentlige myndighed, om indholdet af det værk, der ulovligt er stillet til rådighed på internettet, kan give denne myndighed oplysninger om visse aspekter af denne indehavers privatliv, herunder følsomme oplysninger, såsom oplysninger om seksuel orientering, politiske anskuelser, samfundsmæssige, filosofiske, religiøse og andre overbevisninger samt oplysninger om helbredstilstand, selv om sådanne oplysninger i øvrigt nyder en særlig beskyttelse i EU-retten.
- 111 I det foreliggende tilfælde er det imidlertid, henset til karakteren af dataene og de begrænsede oplysninger, som Hadopi råder over, kun i atypiske situationer, at disse kan afsløre – eventuelt følsomme – oplysninger om aspekter af den omhandlede persons privatliv, der samlet set kan gøre det muligt for denne offentlige myndighed at drage præcise slutninger om dennes privatliv, f.eks. ved at fastlægge en detaljeret profil af vedkommende.
- 112 Dette kunne f.eks. være tilfældet med hensyn til en person, hvis IP-adresse gentagne gange, eller i stor målestok, er blevet anvendt til aktiviteter, der krænker ophavsrettigheder eller beslægtede rettigheder i peer-to-peer-netværk i forbindelse med bestemte typer beskyttede værker, der kan kategoriseres på grundlag af ord i deres titel, som kan afsløre – eventuelt følsomme – oplysninger om aspekter af vedkommendes privatliv.
- 113 Når dette er sagt, gør forskellige forhold det muligt i det foreliggende tilfælde at lægge til grund, at det indgreb i privatlivet for en person, der mistænkes for at have udøvet en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, som en lovgivning som den, der er omhandlet i hovedsagen, tillader, ikke nødvendigvis har en høj grad af alvor. Først og fremmest er Hadopis adgang til de omhandlede personoplysninger i henhold til denne lovgivning forbeholdt et begrænset antal befuldmægtigede, edsvorne embedsmænd ved denne offentlige myndighed, som i øvrigt er uafhængig i henhold til CPI's artikel L. 331-12. Dernæst har denne adgang alene til formål at identificere en person, der mistænkes for at have udøvet en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, når det konstateres, at et beskyttet værk ulovligt er blevet stillet til rådighed fra vedkommendes internetadgang. Endelig er Hadopis adgang til de omhandlede personoplysninger strengt begrænset til de data, der er nødvendige med henblik herpå (jf. analogt Menneskerettighedsdomstolen, 17.10.2019, López Ribalda m.fl. mod Spanien, CE:ECHR:2019:1017JUD000187413, §§ 126 og 127).
- 114 Et andet element, der yderligere kan mindske alvoren af indgrebet i den grundlæggende ret til beskyttelse af privatlivet og personoplysninger som følge af Hadopis adgang, og som synes at fremgå af sagsakterne for Domstolen, hvilket dog skal efterprøves af den forelæggende ret, vedrører det forhold, at de embedsmænd i Hadopi, der har adgang til de pågældende data og oplysninger, efter den gældende nationale lovgivning er underlagt en tavshedspligt, der forbyder

dem at udbrede disse data og oplysninger i nogen som helst form – undtagen med henblik på indbringelse af sagen for anklagemyndigheden – og at anvende dem til andre formål end identificering af indehaveren af en IP-adresse, der mistænkes for at have udøvet en aktivitet, der krænker ophavsret eller en beslægtet rettighed, for at den pågældende kan pålægges en af de foranstaltninger, der er fastsat i forbindelse med proceduren med gradvise foranstaltninger (jf. analogt Menneskerettighedsdomstolen, 17.12.2009, Gardel mod Frankrig, CE:ECHR:2009:1217JUD001642805, § 70).

- 115 For så vidt som en national lovgivning opfylder de betingelser, der er nævnt i denne doms præmis 101, gør de IP-adresser, der videregives til en offentlig myndighed såsom Hadopi, det således ikke muligt at spore deres indehaveres søgemønstre, hvilket synes at bekræfte, at det indgreb, som denne myndigheds adgang til de i hovedsagen omhandlede identifikationsdata indebærer, ikke kan kvalificeres som alvorligt.
- 116 For det tredje bemærkes, at ved den nødvendige afvejning af de berørte rettigheder og interesser, som er pålagt ved kravet om proportionalitet i artikel 15, stk. 1, første punktum, i direktiv 2002/58, er disse grundlæggende rettigheder – selv om ytringsfriheden og fortroligheden af personoplysninger er yderst vigtige hensyn, og selv om brugerne af telekommunikation og internettjenester skal have sikkerhed for, at deres privatliv og ytringsfrihed respekteres – dog ikke absolutte. I forbindelse med en afvejning af de omhandlede rettigheder og interesser må disse til tider vige for andre grundlæggende rettigheder og tvingende almene hensyn, såsom beskyttelsen af den offentlige orden og forebyggelsen af strafbare handlinger eller beskyttelsen af andres rettigheder og friheder. Dette er navnlig tilfældet, når den afgørende vægt, der tillægges disse yderst vigtige hensyn, kan hindre effektiviteten af en strafferetlig efterforskning, bl.a. ved at gøre det umuligt eller uforholdsmæssigt vanskeligt faktisk at identificere gerningsmanden til en strafbar handling og pålægge vedkommende en sanktion (jf. analogt Menneskerettighedsdomstolen, 2.3.2009, K.U. mod Finland, CE:ECHR:2008:1202JUD000287202, § 49).
- 117 I denne sammenhæng skal der tages behørigt hensyn til det forhold, at med hensyn til lovovertrædelser, der er begået online, kan IP-adressen, således som Domstolen allerede har fastslået, udgøre det eneste efterforskningsmiddel, der gør det muligt faktisk at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 154).
- 118 Dette forhold synes, således som generaladvokaten ligeledes i det væsentlige har anført i punkt 59 i forslaget til afgørelse af 28. september 2023, at godtgøre, at lagring af og adgang til disse adresser hvad angår bekæmpelsen af strafbare handlinger såsom handlinger, der krænker ophavsrettigheder eller beslægtede rettigheder, og som begås online, er strengt nødvendig for virkeliggørelsen af det formål, der forfølges, og dermed opfylder det proportionalitetskrav, som er fastsat i artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med 11. betragtning til dette direktiv og chartrets artikel 52, stk. 2.
- 119 Ikke at tillade en sådan adgang ville i øvrigt, således som generaladvokaten i det væsentlige har fremhævet i punkt 78-80 i forslaget til afgørelse af 27. oktober 2022 og i punkt 80 og 81 i forslaget til afgørelse af 28. september 2023, indebære en reel risiko for systemisk straffrihed, ikke blot for strafbare handlinger, der krænker ophavsrettigheder eller beslægtede rettigheder, men også for andre former for strafbare handlinger, der begås online, eller som internettets særlige kendetegn gør det lettere at begå eller forberede. Eksistensen af en sådan risiko er en relevant

omstændighed, når det i forbindelse med en afvejning af de forskellige foreliggende rettigheder og interesser bedømmes, om et indgreb i de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, er en forholdsmæssig foranstaltning i forhold til formålet om at bekæmpe strafbare handlinger.

- 120 Det er korrekt, at adgang for en offentlig myndighed som Hadopi til identitetsdata knyttet til den IP-adresse, hvorfra en onlineovertrædelse er blevet begået, ikke nødvendigvis er det eneste mulige efterforskningsmiddel med henblik på at identificere den person, der var indehaver af denne adresse på det tidspunkt, hvor overtrædelsen blev begået. En sådan identificering kan nemlig også a priori være mulig ved at undersøge alle den pågældende persons onlineaktiviteter, bl.a. gennem en analyse af de »spor«, som vedkommende kan have efterladt på de sociale medier, såsom den anvendte identifikator eller personens kontaktoplysninger.
- 121 Som generaladvokaten har anført i punkt 83 i forslaget til afgørelse af 28. september 2023, ville et sådant efterforskningsmiddel imidlertid være særligt indgribende, eftersom det ville kunne afsløre præcise oplysninger om de berørte personers privatliv. Det ville således indebære et mere alvorligt indgreb i de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, for disse personer end det indgreb, der følger af en lovgivning som den, der er omhandlet i hovedsagen.
- 122 Det følger af det ovenstående, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse principielt ikke er til hinder for en national lovgivning, der tillader, at en offentlig myndighed, der har til opgave at beskytte ophavsrettigheder og beslægtede rettigheder mod krænkelse af disse rettigheder, der begås på internettet, får adgang til identitetsdata knyttet til IP-adresser, som forudgående er indsamlet af rettighedsorganisationer og lagret af udbydere af elektroniske kommunikationstjenester særskilt og på en sådan måde, at dataene er hermetisk adskilte, alene med det formål, at denne myndighed kan identificere indehaverne af disse adresser, der mistænkes for at være ansvarlige for krænkelse, og efter omstændighederne træffe foranstaltninger over for dem. I et sådant tilfælde skal den nationale lovgivning, der finder anvendelse, forbyde de embedsmænd, der har en sådan adgang, for det første at udbrede oplysninger i nogen som helst form om indholdet af de filer, som disse indehavere har konsulteret, undtagen med henblik på indbringelse af sagen for anklagemyndigheden, for det andet at foretage sporing af nogen art af indehavernes søgemønstre og for det tredje at anvende disse IP-adresser til andre formål end at træffe disse foranstaltninger.

Kravet om kontrol ved en domstol eller en uafhængig administrativ enhed forud for en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse

- 123 Spørgsmålet er imidlertid, om den offentlige myndigheds adgang til identitetsdata knyttet til en IP-adresse desuden skal være underlagt en forudgående kontrol, der foretages af en domstol eller af en uafhængig administrativ enhed.
- 124 I denne henseende er det med henblik på i praksis at sikre fuld iagttagelse af de betingelser, som medlemsstaterne har pligt til at fastsætte for at sikre, at adgangen er begrænset til det strengt nødvendige, at Domstolen har fastslået, at det er »afgørende«, at de kompetente nationale myndigheds adgang til trafikdata og lokaliseringsdata er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed (jf. i denne retning dom af 21.12.2016, Tele2 Sverige og Watson m.fl., C-203/15 og C-698/15, EU:C:2016:970, præmis 120, af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791,

præmis 189, af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 51, og af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 106).

- 125 Denne forudgående kontrol kræver for det første, at den domstol eller uafhængige administrative enhed, der har til opgave at foretage den, har alle de beføjelser og frembyder alle de garantier, der er nødvendige for at sikre en afvejning af de forskellige berørte legitime interesser og rettigheder. Hvad nærmere bestemt angår en strafferetlig efterforskning kræver en sådan kontrol, at denne domstol eller denne enhed er i stand til at sikre en rimelig ligevægt mellem dels de legitime interesser, der er forbundet med, hvad der er nødvendigt af hensyn til efterforskningen i forbindelse med bekæmpelsen af kriminalitet, dels den grundlæggende ret til respekt for privatlivet og beskyttelsen af personoplysninger for så vidt angår de personer, hvis oplysninger er berørt af adgangen (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 107 og den deri nævnte retspraksis).
- 126 Når denne kontrol ikke foretages af en domstol, men af en uafhængig administrativ enhed, skal denne for det andet have en status, der gør det muligt for den at udføre sine opgaver på en objektiv og upartisk måde og i denne forbindelse at handle uden udefrakommende indflydelse. Det krav om uafhængighed, som den enhed, der har til opgave at udføre den forudgående kontrol, skal opfylde, indebærer således, at denne enhed skal være udenforstående i forhold til den myndighed, der anmoder om adgang til dataene, således at den nævnte enhed er i stand til at foretage denne kontrol på en objektiv og upartisk måde uden nogen form for udefrakommende indflydelse. Navnlig inden for det strafferetlige område indebærer kravet om uafhængighed, at den myndighed, der har til opgave at foretage denne forudgående kontrol, for det første ikke må være involveret i den pågældende strafferetlige efterforskning og for det andet skal være neutral i forhold til parterne i straffesagen (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 108 og den deri nævnte retspraksis).
- 127 For det tredje skal den uafhængige kontrol, som kræves i henhold til artikel 15, stk. 1, i direktiv 2002/58, foretages forud for enhver adgang til de omhandlede data, undtagen i behørigt begrundede hastende tilfælde, i hvilket tilfælde kontrollen skal foretages hurtigst muligt. En senere kontrol vil nemlig ikke gøre det muligt at opfylde formålet med den forudgående kontrol, der består i at forhindre, at der gives adgang til de omhandlede data på en måde, der går ud over, hvad der er strengt nødvendigt (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 110).
- 128 Selv om Domstolen, således som det fremgår af den retspraksis, der er nævnt i denne doms præmis 124, har fastslået, at det er »afgørende«, at de kompetente nationale myndigheders adgang til trafikdata og lokaliseringsdata er undergivet en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed, er denne retspraksis imidlertid blevet udviklet i forbindelse med nationale foranstaltninger, som med henblik på et formål, der er knyttet til bekæmpelse af grov kriminalitet, tillader en generel adgang til alle lagrede trafikdata og lokaliseringsdata, uafhængigt af om der foreligger nogen forbindelse, selv indirekte, til det forfulgte mål, og som således indebærer alvorlige og endda »særligt alvorlige« indgreb i de berørte grundlæggende rettigheder.
- 129 Når der derimod har været tale om de betingelser, hvorunder adgang til identitetsdata kunne være begrundet henset til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11, har Domstolen ikke udtrykkeligt nævnt kravet om en sådan forudgående kontrol (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 59, 60

og 62, af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 157 og 158, og af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 34).

- 130 Det følger imidlertid af Domstolens praksis vedrørende proportionalitetsprincippet, som i henhold til artikel 15, stk. 1, første punktum, i direktiv 2002/58 skal overholdes, og særligt af den praksis, hvorefter medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der bl.a. er fastsat i dette direktivs artikel 5, 6 og 9, skal vurderes ved at bedømme alvoren af det indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 131), at alvoren af det indgreb i de berørte grundlæggende rettigheder, som adgangen til de omhandlede personoplysninger indebærer, og disses grad af følsomhed, ligeledes skal have indvirkning på de materielle og processuelle betingelser i forbindelse med denne adgang, herunder kravet om en forudgående kontrol foretaget af en domstol eller en uafhængig administrativ enhed.
- 131 Henset til dette proportionalitetsprincip skal det derfor fastslås, at kravet om en forudgående kontrol foretaget af en domstol eller en uafhængig administrativ enhed gælder, når en national myndighed i medfør af en national lovgivning har adgang til personoplysninger, og denne adgang medfører risiko for et alvorligt indgreb i den berørte persons grundlæggende rettigheder i den forstand, at den kan gøre det muligt for den offentlige myndighed at drage præcise slutninger om denne persons privatliv og efter omstændighederne fastlægge en detaljeret profil af vedkommende.
- 132 Omvendt skal dette krav om en forudgående kontrol ikke finde anvendelse, når det indgreb i de berørte grundlæggende rettigheder, som en offentlig myndigheds adgang til personoplysninger indebærer, ikke kan kvalificeres som alvorligt.
- 133 Dette er tilfældet for adgang til data vedrørende identiteten på brugerne af elektroniske kommunikationsmidler alene med henblik på at identificere den pågældende bruger, og uden at disse data kan kædes sammen med oplysninger om den foretagne kommunikation, eftersom det indgreb, som en sådan behandling af de nævnte data indebærer, ifølge Domstolens praksis principielt ikke kan kvalificeres som alvorligt (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 157 og 158).
- 134 Det følger heraf, at såfremt en lagringsordning som den, der er beskrevet i denne doms præmis 86-89, er indført, er den offentlige myndigheds adgang til identitetsdata knyttet til IP-adresser, der således er lagret, principielt ikke underlagt kravet om en forudgående kontrol foretaget af en domstol eller en uafhængig administrativ enhed.
- 135 Når dette er sagt, kan det som allerede anført i denne doms præmis 110 og 111 ikke udelukkes, at de begrænsede data og oplysninger, der stilles til rådighed for en offentlig myndighed i forbindelse med en procedure som den i hovedsagen omhandlede med gradvise foranstaltninger, i atypiske situationer kan afsløre – eventuelt følsomme – oplysninger om aspekter af den berørte persons privatliv, der samlet set kan gøre det muligt for denne offentlige myndighed at drage præcise slutninger om denne persons privatliv og efter omstændighederne fastlægge en detaljeret profil af vedkommende.

- 136 Som det fremgår af denne doms præmis 112, kan en sådan risiko for privatlivet bl.a. opstå, når en person gentagne gange, eller i stor målestok, beskæftiger sig med aktiviteter, der krænker ophavsrettigheder eller beslægtede rettigheder i peer-to-peer-netværk i forbindelse med bestemte typer beskyttede værker, der kan kategoriseres på grundlag af ord i deres titel, som afslører – eventuelt følsomme – oplysninger om vedkommendes privatliv.
- 137 I det foreliggende tilfælde kan en indehaver af en IP-adresse i forbindelse med proceduren med gradvise foranstaltninger således være særligt udsat for en sådan risiko for sit privatliv, når denne procedure når til det stadium, hvor Hadopi skal træffe afgørelse om, hvorvidt sagen skal indbringes for anklagemyndigheden med henblik på retsforfølgning af denne indehaver på grund af forhold, der kan kvalificeres som en alvorlig forsømmelse eller en immaterialretskrænkelse.
- 138 Indbringelse for anklagemyndigheden forudsætter nemlig, at indehaveren af en IP-adresse allerede har modtaget to henstillinger og en skrivelse med meddelelse om, at vedkommendes aktiviteter kan give anledning til strafferetlig forfølgning, hvilke foranstaltninger indebærer, at Hadopi hver gang har haft adgang til data vedrørende identiteten på denne indehaver, hvis IP-adresse er blevet anvendt til aktiviteter, der krænker ophavsrettigheder eller beslægtede rettigheder, og til en fil vedrørende det pågældende værk, der i det væsentlige indeholder dets titel.
- 139 Det kan ikke udelukkes, at de data, der således tilvejebringes i de forskellige faser af denne procedure, samlet set og efterhånden som den administrative procedure med gradvise foranstaltninger skrider frem, kan afsløre samstemmende og eventuelt følsomme oplysninger om aspekter af den berørte persons privatliv, der efter omstændighederne gør det muligt at udarbejde en profil af vedkommende.
- 140 Voldsomheden af indgrebet i retten til respekt for privatlivet kan således stige, efterhånden som proceduren med gradvise foranstaltninger, der forløber i trin, når igennem de forskellige faser, som den består af.
- 141 I det foreliggende tilfælde kan Hadopis adgang til det sæt af data, der vedrører den berørte person, og som er kumuleret i de forskellige faser af denne procedure, ved en sammenkobling af disse data muliggøre, at der drages præcise slutninger om vedkommendes privatliv. I forbindelse med en procedure som den i hovedsagen omhandlede med gradvise foranstaltninger skal det derfor i den nationale lovgivning ligeledes være fastsat, at der på et bestemt stadium af denne procedure skal foretages en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed, der opfylder de krav, der er angivet i denne doms præmis 125-127, med henblik på at udelukke risici for uforholdsmæssige indgreb i den berørte persons grundlæggende ret til beskyttelse af sit privatliv og personoplysninger. Dette betyder, at en sådan kontrol i praksis skal finde sted, før Hadopi kan sammenkoble en persons identitetsdata, der er knyttet til en IP-adresse og indhentet fra en udbyder af elektroniske kommunikationstjenester – idet denne person allerede har modtaget to henstillinger – med filen vedrørende det værk, som er blevet stillet til rådighed på internettet, for at det kan downloades af andre. Kontrollen skal således ske før den eventuelle fremsendelse af den meddelelse, der er omhandlet i CPI's artikel R-331-40, hvori det konstateres, at denne person har begået forhold, der kan udgøre en strafbar handling i form af en alvorlig forsømmelse. Det er først efter en sådan forudgående kontrol ved en domstol eller en uafhængig administrativ myndighed og dennes godkendelse, at Hadopi kan fremsende en sådan skrivelse og derefter efter omstændighederne indbringe sagen for anklagemyndigheden med henblik på retsforfølgning af denne strafbare handling.

- 142 Hadopi bør have mulighed for at identificere de tilfælde, hvor indehaveren af den pågældende IP-adresse når til denne tredje fase i en sådan procedure med gradvise foranstaltninger. Denne procedure skal derfor tilrettelægges og struktureres på en sådan måde, at en persons identitetsdata, der er knyttet til IP-adresser, der forudgående er indsamlet på internettet, og som er indhentet fra udbydere af elektroniske kommunikationstjenester, ikke af de personer i Hadopi, der har til opgave at undersøge de faktiske omstændigheder, automatisk kan sammenkobles med de filer med oplysninger, der gør det muligt at få kendskab til titlerne på de beskyttede værker, hvis tilrådighedsstillelse på internettet har begrundet denne indsamling.
- 143 Denne sammenkobling til brug for den tredje fase i proceduren med gradvise foranstaltninger skal således udsættes, når indsamlingen af de nævnte identitetsdata i forbindelse med et tilfælde af anden mulige gentagelse af en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, udløser det krav om en forudgående kontrol ved en domstol eller en uafhængig administrativ enhed, der er beskrevet i denne doms præmis 141.
- 144 Udformningen af kravet om den forudgående kontrol, der er beskrevet i denne doms præmis 141-143, muliggør i øvrigt – for så vidt som denne kontrol er begrænset til den tredje fase i proceduren med gradvise foranstaltninger og ikke finder anvendelse på procedurens tidligere faser – hensyntagen til argumentet om, at det er nødvendigt at sikre gennemførligheden af denne procedure, som – især i de faser af denne, der går forud for en eventuel fremsendelse af meddelelsen og efter omstændighederne indbringelsen af sagen for anklagemyndigheden – er karakteriseret ved det store antal anmodninger om adgang fra den offentlige myndighed, der følger af det lige så store antal rapporter, som denne modtager fra rettighedsorganisationerne.
- 145 Hvad endvidere angår genstanden for den forudgående kontrol, der er omhandlet i denne doms præmis 141-143, følger det af den retspraksis, der er nævnt i præmis 95 og 96, at i de tilfælde, hvor den berørte person mistænkes for at have begået en »alvorlig forsømmelse« som defineret i CPI's artikel R. 335-5, der hører under strafbare handlinger i almindelighed, skal den domstol eller uafhængige administrative enhed, der skal foretage kontrollen, nægte adgang, når denne ville gøre det muligt for den offentlige myndighed, der har anmodet herom, at drage præcise slutninger om den nævnte persons privatliv.
- 146 Derimod skal selv adgang, der gør det muligt at drage sådanne præcise slutninger, tillades i de tilfælde, hvor de oplysninger, der bringes til denne domstols eller denne uafhængige administrative enheds kendskab, giver anledning til mistanke om, at den berørte person har begået en immaterialretskrænkelse som omhandlet i CPI's artikel L. 335-2 eller denne lovs artikel L. 335-4, eftersom en medlemsstat har mulighed for at anse en sådan strafbar handling for at høre under de alvorlige former for kriminalitet, for så vidt som den er til skade for en grundlæggende samfundsinteresse.
- 147 Hvad endelig angår de nærmere regler for denne forudgående kontrol er den franske regering af den opfattelse, at det, henset til de særlige kendetegn ved Hadopis adgang til de omhandlede data, navnlig det store omfang heraf, vil være hensigtsmæssigt, at en forudgående kontrol, hvis den er nødvendig, er fuldstændig automatiseret. En sådan kontrol, der har en rent objektiv karakter, tager nemlig grundlæggende sigte på at efterprøve, om den rapport, der forelægges Hadopi, indeholder alle de nødvendige oplysninger og data, uden at denne myndighed er nødt til at vurdere disse.

- 148 En forudgående kontrol kan imidlertid i intet tilfælde være fuldstændig automatiseret, for hvad angår en strafferetlig efterforskning kræver en sådan kontrol, således som det fremgår af den retspraksis, der er nævnt i denne doms præmis 125, under alle omstændigheder, at den pågældende domstol eller uafhængige administrative enhed er i stand til at sikre en rimelig ligevægt mellem på den ene side de legitime interesser, der er forbundet med, hvad der er nødvendigt af hensyn til efterforskningen i forbindelse med bekæmpelse af kriminalitet, og på den anden side den grundlæggende ret til respekt for privatlivet og beskyttelse af personoplysninger for de personer, hvis oplysninger er berørt af adgangen.
- 149 En sådan afvejning af de forskellige legitime interesser og omhandlede rettigheder kræver nemlig en fysisk persons medvirken, idet en sådan er så meget desto mere nødvendig, som automatikken i og det store omfang af den omhandlede databehandling indebærer risici for privatlivet.
- 150 Desuden kan en fuldstændig automatiseret kontrol principielt ikke sikre, at adgangen ikke overskrider grænserne for det strengt nødvendige, og at de personer, hvis personoplysninger er berørt, råder over effektive garantier mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse oplysninger.
- 151 Selv om automatiserede kontroller kan gøre det muligt at efterprøve visse af de oplysninger, der er indeholdt i rapporterne fra rettighedsorganisationerne, skal sådanne kontroller således under alle omstændigheder ledsages af kontroller foretaget af fysiske personer, der fuldt ud opfylder de krav, der er angivet i denne doms præmis 125-127.

De krav vedrørende de materielle og processuelle betingelser samt vedrørende garantierne mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data, der gælder for en offentlig myndigheds adgang til identitetsdata knyttet til en IP-adresse

- 152 Det fremgår af Domstolens praksis, at adgang til personoplysninger kun kan være i overensstemmelse med det proportionalitetskrav, som er fastsat i artikel 15, stk. 1, i direktiv 2002/58, hvis den retsforordning, der tillader adgangen, ved klare og præcise regler fastsætter, at adgangen er underlagt overholdelse af de materielle og processuelle betingelser herfor, og at de berørte personer råder over effektive garantier mod risikoen for adgang til og anvendelse af disse oplysninger, som er ulovlig eller udtryk for misbrug (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 132 og 173, og af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 49 og den deri nævnte retspraksis).
- 153 Som Domstolen har fremhævet, er nødvendigheden af at råde over sådanne garantier så meget desto større, når personoplysningerne er undergivet en automatiseret behandling (dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 176 og den deri nævnte retspraksis).
- 154 I denne henseende har den franske regering som svar på et spørgsmål fra Domstolen med henblik på retsmødet den 5. juli 2022 bekræftet, at Hadopis adgang til identitetsdata i forbindelse med proceduren med gradvise foranstaltninger, således som det også fremgår af CPI's artikel L. 331-29, hidrører fra en i det væsentlige automatiseret behandling af data, der skyldes det store omfang af immaterialretskrænkelser, som rettighedsorganisationerne konstaterer, og som de fremsender underretning til Hadopi om i form af rapporter.

- 155 Det fremgår navnlig af sagsakterne for Domstolen, at Hadopi embedsmænd i forbindelse med denne databehandling ved en i det væsentlige automatiseret fremgangsmåde og uden som sådan at vurdere de omhandlede faktiske forhold kontrollerer, om de rapporter, som myndigheden er blevet forelagt, indeholder alle de oplysninger og data, der er nævnt i punkt 1 i bilaget til dekret 2010-236, navnlig de pågældende omstændigheder vedrørende ulovlig tilrådighedsstillelse på internettet og de IP-adresser, der er anvendt til dette formål. Sådanne behandlinger skal imidlertid ledsages af kontroller foretaget af fysiske personer.
- 156 Eftersom en sådan automatiseret behandling kan medføre et vist antal falsk positive tilfælde og, især, risiko for, at et potentielt meget stort antal personoplysninger misbruges af tredjemand til uberettigede eller ulovlige formål, er det vigtigt, at det databehandlingssystem, som en offentlig myndighed anvender, i henhold til en retsforskrift med jævne mellemrum kontrolleres af et uafhængigt organ, der er udenforstående i forhold til denne myndighed, med henblik på at efterprøve systemets integritet, herunder de effektive garantier mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data, som dette system skal sikre, samt systemets effektivitet og pålidelighed med hensyn til at afsløre overtrædelser, der ved gentagelse kan kvalificeres som alvorlige forsømmelser eller immaterialretskrænkelser.
- 157 Endelig skal det tilføjes, at en offentlig myndigheds behandling af personoplysninger som den, Hadopi foretager i forbindelse med proceduren med gradvise foranstaltninger, skal overholde de særlige regler om beskyttelse af disse oplysninger, der er fastsat i direktiv 2016/680, hvis formål ifølge artikel 1 er at fastsætte regler om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.
- 158 Selv om Hadopi i det foreliggende tilfælde i henhold til gældende national ret ikke har selvstændige beslutningsbeføjelser, skal denne myndighed nemlig, når den i forbindelse med proceduren med gradvise foranstaltninger behandler personoplysninger og træffer foranstaltninger i form af f.eks. en henstilling eller meddelelse til den berørte person om, at de omhandlede faktiske forhold kan forfølges strafferetligt, kvalificeres som en »offentlig myndighed« som omhandlet i artikel 3 i direktiv 2016/680, der er involveret i forebyggelse og afsløring af strafbare handlinger, nemlig alvorlige forsømmelser eller immaterialretskrænkelser, og den hører dermed under dette direktivs anvendelsesområdet i overensstemmelse med dets artikel 1.
- 159 I denne henseende har den franske regering som svar på et spørgsmål fra Domstolen med henblik på retsmødet den 5. juli 2022 anført, at eftersom de foranstaltninger, som Hadopi vedtager i forbindelse med gennemførelsen af proceduren med gradvise foranstaltninger, »har en præpønal karakter, der er direkte forbundet med den retslige procedure«, er det system til håndtering af foranstaltninger til beskyttelse af værker på internettet, som Hadopi har indført, således som det fremgår af den forelæggende rets praksis, underlagt de bestemmelser i national ret, der tager sigte på at gennemføre direktiv 2016/680.
- 160 Derimod er en sådan databehandling foretaget af Hadopi ikke omfattet af databeskyttelsesforordningens anvendelsesområde. Databeskyttelsesforordningens artikel 2, stk. 2, litra d), bestemmer nemlig, at denne forordning ikke gælder for behandling af personoplysninger, som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

- 161 Som generaladvokaten har anført i punkt 104 i forslaget til afgørelse af 27. oktober 2022, skal personer, der er involveret i en sådan procedure, eftersom Hadopi følgelig skal overholde direktiv 2016/680 i forbindelse med proceduren med gradvise foranstaltninger, være omfattet af en række sammenhængende materielle og processuelle garantier, der omfatter retten til indsigt i samt berigtigelse og sletning af de personoplysninger, som Hadopi behandler, såvel som muligheden for at indgive en klage til en uafhængig tilsynsmyndighed, efter omstændighederne efterfulgt af en adgang til retsmidler, der udøves i henhold til de almindelige regler.
- 162 I denne sammenhæng fremgår det af den nationale lovgivning, der er omhandlet i hovedsagen, at i forbindelse med proceduren med gradvise foranstaltninger, nærmere bestemt i forbindelse med fremsendelsen af den anden henstilling og den efterfølgende meddelelse om, at de konstaterede faktiske forhold kan kvalificeres som en strafbar handling, er adressaten for disse skrivelser omfattet af visse processuelle garantier, såsom retten til at fremsætte bemærkninger, retten til at få nærmere oplysninger om den overtrædelse, som vedkommende foreholdes, samt, hvad angår den nævnte meddelelse, retten til at anmode om at blive hørt og til at lade sig bistå af en advokat.
- 163 Under alle omstændigheder tilkommer det den forelæggende ret at efterprøve, om denne nationale lovgivning fastsætter alle de materielle og processuelle garantier, som direktiv 2016/680 foreskriver.
- 164 Henset til samtlige ovenstående betragtninger skal de tre præjudicielle spørgsmål besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse ikke er til hinder for en national lovgivning, der tillader, at den offentlige myndighed, der har til opgave at beskytte ophavsrettigheder og beslægtede rettigheder mod krænkelse af disse rettigheder, der begås på internettet, får adgang til identitetsdata, som er lagret af udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og som er knyttet til IP-adresser, der forudgående er indsamlet af rettighedsorganisationer, for at denne myndighed kan identificere indehaverne af disse adresser, som er blevet anvendt til aktiviteter, der kan udgøre sådanne krænkelse, og efter omstændighederne træffe foranstaltninger over for dem, forudsat at det i henhold til denne lovgivning gælder, at
- disse data skal lagres på betingelser og efter tekniske fremgangsmåder, der sikrer, at det er udelukket, at lagringen kan gøre det muligt at drage præcise slutninger om disse indehaveres privatliv, f.eks. ved at fastlægge en detaljeret profil af dem, hvilket navnlig kan opnås ved at pålægge udbyderne af elektroniske kommunikationstjenester en pligt til lagring af de forskellige kategorier af personoplysninger, såsom identitetsdata, IP-adresser samt trafikdata og lokaliseringsdata, der sikrer, at disse forskellige kategorier af data faktisk er hermetisk adskilte, således at enhver kombineret udnyttelse af disse forskellige kategorier af data forhindres på lagringsstadiet, og at lagringen kun sker i et tidsrum, der ikke overstiger det strengt nødvendige
 - denne offentlige myndigheds adgang til sådanne data, der er lagret særskilt og på en sådan måde, at dataene er hermetisk adskilte, alene må tjene til at identificere den person, der mistænkes for at have begået en strafbar handling, og at adgangen skal være ledsaget af de nødvendige garantier med henblik på at udelukke, at den, undtagen i atypiske situationer, kan gøre det muligt at drage præcise slutninger om privatlivet for indehaverne af IP-adresserne, f.eks. ved at fastlægge en detaljeret profil af dem, hvilket navnlig indebærer, at det skal være forbudt for denne myndigheds embedsmænd med bemyndigelse til en sådan adgang at udbrede oplysninger i nogen som helst form om indholdet af de filer, som disse indehavere har

konsulteret, undtagen med henblik på indbringelse af sagen for anklagemyndigheden, at foretage sporing af indehavernes søgemønstre og mere generelt at anvende disse IP-adresser til andre formål end at identificere indehaverne med henblik på vedtagelse af eventuelle foranstaltninger over for dem

- muligheden for de personer i den nævnte offentlige myndighed, der har til opgave at undersøge de faktiske omstændigheder, for at koble sådanne data sammen med de filer med oplysninger, der gør det muligt at få kendskab til titlen på de beskyttede værker, hvis tilrådighedsstillelse på internettet har begrundet rettighedsorganisationernes indsamling af IP-adresserne, i tilfælde af samme persons gentagelse af en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, skal være undergivet en kontrol ved en domstol eller en uafhængig administrativ enhed, der ikke må være fuldstændig automatiseret, og som skal foretages forud for en sådan sammenkobling af data, idet denne i sådanne tilfælde kan gøre det muligt at drage præcise slutninger om privatlivet for denne person, hvis IP-adresse er blevet anvendt til aktiviteter, der kan krænke ophavsrettigheder eller beslægtede rettigheder
- det databehandlingssystem, som den offentlige myndighed anvender, med jævne mellemrum skal kontrolleres af et uafhængigt organ, der er udenforstående i forhold til denne myndighed, med henblik på at efterprøve systemets integritet, herunder de effektive garantier mod risikoen for uberettiget eller ulovlig adgang til og anvendelse af disse data, samt systemets effektivitet og pålidelighed med hensyn til at afsløre eventuelle overtrædelser.

Sagsomkostninger

- 165 Da sagens behandling i forhold til hovedsagens parter udgør et led i den sag, der verserer for den forelæggende ret, tilkommer det denne at træffe afgørelse om sagsomkostningerne. Bortset fra de nævnte parters udgifter kan de udgifter, som er afholdt i forbindelse med afgivelse af indlæg for Domstolen, ikke erstattes.

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

Artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i chartret om grundlæggende rettigheder,

skal fortolkes således, at

denne bestemmelse ikke er til hinder for en national lovgivning, der tillader, at den offentlige myndighed, der har til opgave at beskytte ophavsrettigheder og beslægtede rettigheder mod krænkelse af disse rettigheder, der begås på internettet, får adgang til identitetsdata, som er lagret af udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og som er knyttet til IP-adresser, der forudgående er indsamlet af rettighedsorganisationer, for at denne myndighed kan identificere indehaverne af disse adresser, som er blevet anvendt til aktiviteter, der kan udgøre sådanne krænkelse, og efter omstændighederne træffe foranstaltninger over for dem, forudsat at det i henhold til denne lovgivning gælder, at

- disse data skal lagres på betingelser og efter tekniske fremgangsmåder, der sikrer, at det er udelukket, at lagringen kan gøre det muligt at drage præcise slutninger om disse indehaveres privatliv, f.eks. ved at fastlægge en detaljeret profil af dem, hvilket navnlig kan opnås ved at pålægge udbyderne af elektroniske kommunikationstjenester en pligt til lagring af de forskellige kategorier af personoplysninger, såsom identitetsdata, IP-adresser samt trafikdata og lokaliseringsdata, der sikrer, at disse forskellige kategorier af data faktisk er hermetisk adskilte, således at enhver kombineret udnyttelse af disse forskellige kategorier af data forhindres på lagringsstadiet, og at lagringen kun sker i et tidsrum, der ikke overstiger det strengt nødvendige
- denne offentlige myndigheds adgang til sådanne data, der er lagret særskilt og på en sådan måde, at dataene er hermetisk adskilte, alene må tjene til at identificere den person, der mistænkes for at have begået en strafbar handling, og at adgangen skal være ledsaget af de nødvendige garantier med henblik på at udelukke, at den, undtagen i atypiske situationer, kan gøre det muligt at drage præcise slutninger om privatlivet for indehaverne af IP-adresserne, f.eks. ved at fastlægge en detaljeret profil af dem, hvilket navnlig indebærer, at det skal være forbudt for denne myndigheds embedsmænd med bemyndigelse til en sådan adgang at udbrede oplysninger i nogen som helst form om indholdet af de filer, som disse indehavere har konsulteret, undtagen med henblik på indbringelse af sagen for anklagemyndigheden, at foretage sporing af indehavernes søgemønstre og mere generelt at anvende disse IP-adresser til andre formål end at identificere indehaverne med henblik på vedtagelse af eventuelle foranstaltninger over for dem
- muligheden for de personer i den nævnte offentlige myndighed, der har til opgave at undersøge de faktiske omstændigheder, for at koble sådanne data sammen med de filer med oplysninger, der gør det muligt at få kendskab til titlen på de beskyttede værker, hvis tilrådighedsstillelse på internettet har begrundet rettighedsorganisationernes indsamling af IP-adresserne, i tilfælde af samme persons gentagelse af en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, skal være undergivet en kontrol ved en domstol eller en uafhængig administrativ enhed, der ikke må være fuldstændig automatiseret, og som skal foretages forud for en sådan sammenkobling af data, idet denne i sådanne tilfælde kan gøre det muligt at drage præcise slutninger om privatlivet for denne person, hvis IP-adresse er blevet anvendt til aktiviteter, der kan krænke ophavsrettigheder eller beslægtede rettigheder
- det databehandlingssystem, som den offentlige myndighed anvender, med jævne mellemrum skal kontrolleres af et uafhængigt organ, der er udenforstående i forhold til denne myndighed, med henblik på at efterprøve systemets integritet, herunder de effektive garantier mod risikoen for uberettiget eller ulovlig adgang til og anvendelse af disse data, samt systemets effektivitet og pålidelighed med hensyn til at afsløre eventuelle overtrædelser.

Underskrifter