

**Sag C-140/20**

**Sammen drag af anmodning om præjudiciel afgørelse i henhold til artikel 98, stk. 1, i Domstolens procesreglement**

**Dato for indlevering:**

25. marts 2020

**Forelæggende ret:**

Supreme Court (Irland)

**Afgørelse af:**

25. marts 2020

**Sagsøger:**

G.D.

**Sagsøgte:**

The Commissioner of the Garda Síochána

Minister for Communications, Energy and Natural Resources

Attorney General

---

**Hovedsagens genstand**

Den foreliggende sag vedrører den retlige ordning, der er indført i Irland i henhold til Communications (Retention of Data) Act 2011 (kommunikationsloven (datalagring) af 2011), som regulerer de irske myndigheders lagring af og adgang til metadata fra telekommunikation, herunder navnlig det irske politi («An Garda Síochána») i forbindelse med afsløring, efterforskning og retsforfølgning af grov kriminalitet.

**Genstand og retsgrundlag for anmodningen om præjudiciel afgørelse**

Er kommunikationsloven (datalagring) af 2011, navnlig lovens artikel 6, stk. 1, uforenelig med artikel 15, stk. 1, i direktiv 2002/58/EF?

## Præjudicielle spørgsmål

(1) Er en generel/universel ordning for lagring af data – selv om den er undergivet strenge begrænsninger med hensyn til lagring og adgang – i sig selv i strid med artikel 15 i direktiv 2002/58/EF som fortolket i lyset af chartret?

(2) Kan den nationale ret i forbindelse med undersøgelsen af, om en national foranstaltning, der er gennemført i henhold til direktiv 2006/24/EF, og som fastsætter en generel ordning for lagring af data (med forbehold af den nødvendige strenge kontrol med hensyn til lagring og/eller adgang), skal anses for uforenelig med EU-retten, og navnlig ved vurderingen af, om en sådan ordning er forholdsmæssig, tage hensyn til den omstændighed, at tjenesteudbydere lovligt kan lagre data til deres egne kommercielle formål, og kan det kræves, at de lagrer data af hensyn til den nationale sikkerhed, som ikke er omfattet af bestemmelserne i direktiv 2002/58/EF?

(3) Hvilke kriterier skal den nationale ret anvende i forbindelse med vurderingen af, om en national foranstaltning om adgang til lagrede data er forenelig med EU-retten, og navnlig chartret, når den undersøger, om en sådan adgangsordning sikrer den krævede forudgående og uafhængige kontrol, som Domstolen har fastlagt i sin praksis? Kan en national ret i denne sammenhæng ved en sådan bedømmelse tage hensyn til, om der foreligger en efterfølgende eller uafhængig domstolsprøvelse?

(4) Er en national ret under alle omstændigheder forpligtet til at erklære en national foranstaltning uforenelig med artikel 15 i direktiv 2002/58/EF, når den nationale foranstaltning fastsætter en generel ordning for lagring af data med henblik på bekæmpelse af grov kriminalitet, og når den nationale ret på grundlag af alle de foreliggende beviser har fastslået, at en sådan lagring er både nødvendig og absolut påkrævet for at opfylde målet om bekæmpelse af grov kriminalitet?

(5) Såfremt en national ret må fastslå, at en national foranstaltning ikke er i overensstemmelse med artikel 15 i direktiv 2002/58/EF, som fortolket i lyset af chartret, kan den da begrænse de tidsmæssige virkninger af en sådan afgørelse, når den er overbevist om, at en unkladelse heraf ville medføre »kaos og indgreb i den offentlige interesse« (i overensstemmelse med den tilgang, som f.eks. blev anvendt i R (National Council for Civil Liberties) mod Secretary of State for Home Department and Secretary of State for Foreign Affairs (2018) EWHC 975, præmis 46)?

(6) Kan en national ret, som er blevet anmodet om at fastslå, at den nationale lovgivning er uforenelig med artikel 15 i direktiv 2002/58/EF, og/eller at unklade at anvende denne lovgivning, og/eller at fastslå, at anvendelsen af en sådan lovgivning har krænket en borgers rettigheder, uanset om det sker inden for rammerne af en procedure, der er indledt for at muliggøre et anbringende om anerkendelse af bevismidler i forbindelse med en straffesag eller på anden vis, være berettiget til at nægte at tillade brugen af dette retsmiddel for så vidt angår

data, der lagres i henhold til den nationale bestemmelse, der er vedtaget i henhold til forpligtelsen i artikel 288 TEUF om at gennemføre et direktivs bestemmelser i national ret, eller til at begrænse en sådan konstatering til tidsrummet efter datoen, hvor Domstolen erklærede direktiv 2006/24/EF for ugyldigt, hvilket skete den 8. april 2014?

### **Anførte EU-retlige forskrifter**

Traktaten om Den Europæiske Union, artikel 5, stk. 4, og artikel 6, stk. 1, samt protokol nr. 21.

Den Europæiske Unions charter om grundlæggende rettigheder, artikel 7, 8 og 52, stk. 1.

Europa-Parlamentet 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).

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).

Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006, L 105, s. 54).

Dom af 10. februar 2009, Irland mod Parlamentet og Rådet (C-301/06, ECLI:EU:C:2009:68).

Dom af 26. november 2009, Kommissionen mod Irland (C-202/09, ECLI:EU:C:2009:736).

Dom af 8. april 2014, Digital Rights Ireland Limited mod Minister for Communications, Marine and Natural Resources m.fl. og Kärntner Landesregierung m.fl. (C-293/12 og C-594/12, ECLI:EU:C:2014:238).

Dom af 21. december 2016, Tele2 Sverige AB mod Post- och telestyrelsen og Secretary of State for the Home Department mod Tom Watson m.fl. (forenede sager C-203/15 og C-698/15, ECLI:EU:C:2016:970).

### **Anførte nationale retsforskrifter**

Communications (Retention of Data) Act 2011 (kommunikationsloven (datalagring) af 2011) (»loven af 2011«).

Loven af 2011 blev vedtaget med det udtrykkelige formål at gennemføre direktivet fra 2006. I henhold til lovens section 3 pålægges alle tjenesteudbydere at lagre »data vedrørende fastnettelefoni og mobiltelefoni« i en periode på to år. Det drejer sig om data, der gør det muligt at identificere kilden, bestemmelsesstedet, datoen og tidspunktet for en kommunikations begyndelse og afslutning, den pågældende kommunikationstype samt arten og den geografiske placering af det anvendte kommunikationsudstyr. Kommunikationens indhold er ikke omfattet af denne type data.

Der kan gives adgang til de lagrede data, og de kan videregives som følge af en anmodning om udlevering. I section 6 i loven af 2011 fastsættes de betingelser, hvorunder en anmodning om udlevering kan indgives, og subsection (1) bestemmer, at et medlem af An Garda Síochána, som mindst skal have rang af chief superintendent (vicepolitimester), kan indgive en anmodning om udlevering, hvis den pågældende har fastslået, at oplysningerne er nødvendige for bl.a. forebyggelse, afsløring, efterforskning eller retsforfølgning af grov kriminalitet. Ved »grov kriminalitet« forstås lovovertrædelser, der straffes med frihedsstraf i fem år eller derover, samt de øvrige lovovertrædelser, der er opregnet i schedule 1 til loven.

Blandt de tilsynsmekanismer, der er fastsat i loven af 2011, er klageprocedurerne i section 10 og funktionerne for en »udpeget dommer«, som fastsat i section 12, der har til opgave at føre tilsyn med, hvordan lovens bestemmelser fungerer.

For så vidt angår den interne politik besluttede chefen for An Garda Síochána, Commissioner of the Garda, at anmodninger om videregivelse af telefondata, der var indgivet i henhold til loven af 2011, skulle behandles centralt af en enkelt chief superintendent. Den detective chief superintendent, der fik overdraget ansvaret for videregivelse af data, var lederen af An Garda Síochána's afdeling for sikkerhed og efterretningsvirksomhed, og han eller hun beslutter i sidste instans, hvorvidt der skal fremsendes en anmodning om videregivelse til udbydere af kommunikationstjenester i henhold til bestemmelserne i loven af 2011. Der blev oprettet en lille uafhængig enhed, Telecommunications Liason Unit (enhed for telekommunikationsforbindelser, herefter »TLU«), som skulle bistå denne detective chief superintendent i dennes opgaver og fungere som eneste kontaktpunkt i forhold til tjenesteudbyderne.

I perioden for denne efterforskning skulle alle anmodninger om videregivelse af data godkendes i første instans af en superintendent (politiinspektør) (eller af en inspector (overbetjent), der optrådte i denne egenskab) og blev derefter sendt videre til behandling i TLU. Efterforskerne fik besked på at medtage tilstrækkeligt præcise angivelser i anmodningen, således at det var muligt at træffe en beslutning på et velinformeret grundlag, og på at være opmærksomme på, at den pågældende chief superintendent senere ville skulle begrunde beslutningen i retten eller over for den udpegede dommer ved High Court (ret i første instans). TLU og den pågældende detective chief superintendent har pligt til at efterprøve lovligheden, forholdsmæssigheden og nødvendigheden af de anmodninger om udlevering af

data, som medlemmer af An Garda Síochána indgiver. Anmodninger, som ikke blev anset for at være i overensstemmelse med kravene i Gardas interne protokoller, blev returneret med henblik på at få præciseringer eller yderligere oplysninger. I henhold til et aftalememorandum, der blev vedtaget i maj 2011, behandler tjenesteudbydere ikke anmodninger om oplysninger vedrørende opkald, der ikke er indgivet i henhold til denne procedure. TLU er ligeledes underlagt kontrol af den tilsynsførende for databeskyttelse.

### **Kort fremstilling af de faktiske omstændigheder og retsforhandlingerne i hovedsagen**

- 1 I marts 2015 blev sagsøgeren (herefter »G.D.«) af en jury kendt skyldig i drabet på fr. O'H. og idømt livsvarigt fængsel. Han har hele tiden erklæret sig ikke skyldig. G.D. appellerede denne dom til Court of Appeal (appeldomstol i straffesager). Under retssagen nedlagde G.D. forgæves påstand om, at visse af anklagemyndighedens beviser baseret på lagrede telefondata ikke kunne antages som gyldige bevismidler.
- 2 Sideløbende hermed anlagde G.D. et civilt søgsmål, hvorved han anfægtede visse bestemmelser i loven af 2011, i henhold til hvilke telefoni-metadata blev lagret og tilgået. Han har nedlagt påstand om, at den relevante lovbestemmelse erklæres ugyldig med henblik på i forbindelse med appelsagen til prøvelse af sin dom at gøre gældende, at telefondata ikke burde have været tilladt som bevisførelse under retssagen, hvilket således medfører, at det er usikkert, om hans domfældelse er korrekt. De sagsøgte (herefter »staten«) har nedlagt påstand om, at lovgivningens gyldighed bekræftes.
- 3 Ved dom af 6. december 2018, Dwyer mod Commissioner of An Garda Síochána m.fl. (2018) IEHC 685, gav High Court (ret i første instans) G.D. medhold i, at section 6(1)(a) i loven af 2011 ikke er i overensstemmelse med artikel 15, stk. 1, i direktiv 2002/58/EF, sammenholdt med artikel 7, 8 og 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder.
- 4 Staten har iværksat appel til prøvelse af denne afgørelse ved Supreme Court (øverste domstol), som har indgivet den foreliggende anmodning om præjudiciel afgørelse.
- 5 Supreme Court har angivet, at den var klar over, at afsløringen af visse kategorier af alvorlig kriminalitet og retsforfølgningen af disse i stadig højere grad påvirkes af beviser af den type, der var blevet fremlagt i straffesagen mod G.D. Det er Supreme Courts erfaring, at visse sager af denne type kun blevet opklaret på grund af adgangen til den type oplysninger, der er omfattet af den foreliggende sag.
- 6 Supreme Court har anført, at sådanne sager ofte indebærer alvorlige forbrydelser mod kvinder, børn og andre sårbare personer, og at det ikke ville være muligt at afsløre eller retsforfølge gerningsmanden uden beviser af den pågældende art.

Supreme Court har faktisk bemærket, at telefoni, som i G.D.'s tilfælde, anvendes til at groome eller på anden måde udnytte sårbare personer.

- 7 Supreme Court har fremhævet, at det ikke er muligt at få adgang til data, der ikke er blevet lagret. Hvis universel lagring af metadata ikke var tilladt, uanset hvor robust ordningen for adgang er, ville mange af disse alvorlige forbrydelser ikke blive opklaret eller føre til retsforfølgning.
- 8 Supreme Court har fastslået følgende faktiske omstændigheder:
  - (i) Andre former for lagring af data ved hjælp af geografisk sporing eller på anden vis er ineffektive med henblik på at opfylde målene om forebyggelse, efterforskning, afsløring og retsforfølgning af i det mindste visse former for grov kriminalitet, og kan desuden medføre en potentiel krænkelse af andre af den pågældendes rettigheder.
  - (ii) Målet om lagring af data ved hjælp af mindre indgribende midler end en generel ordning for lagring af data med forbehold af de nødvendige garantier er uigennemførligt i praksis, og
  - (iii) målene om forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet ville blive bragt i alvorlig fare, hvis der ikke fandtes en generel ordning for datalagring.

#### **De væsentligste argumenter fremsat af parterne i hovedsagen**

- 9 Sagsøgeren har gjort gældende, at section 6(1)(a) i loven af 2011, hvorefter telefoni-metadata blev lagret og tilgået og anerkendt som bevismidler i forbindelse med den straffesag, der var indledt mod ham, er ugyldig, idet den er uforenelig med artikel 15, stk. 1, i direktiv 2002/58.
- 10 Han har gjort gældende, at universel lagring af data er uacceptabel, uanset hvilke sikkerhedsforanstaltninger der indføres for adgangen til disse data. Han har endvidere anført, at adgangsordningen yder utilstrækkelig selvstændig beskyttelse mod uhensigtsmæssig adgang til data. Han har gjort gældende, at sikkerhedsforanstaltningerne i loven af 2011 er minimale, og at denne lovgivning ikke fastsætter klare og præcise regler, der angiver, under hvilke omstændigheder og på hvilke betingelser tjenesteudbydere skal give de nationale myndigheder adgang til data, således som Den Europæiske Unions Domstol kræver. Den nuværende ordning med selvcertificering af anmodninger om videregivelse af data, som anvendes af An Garda Síochána, opfylder navnlig ikke kravet om, at anmodninger om adgang skal være undergivet forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, således som det er fastsat i præmis 120 i Tele2 Sverige-dommen.
- 11 De sagsøgte (herefter »staten«) har gjort gældende, at lovgivningen er gyldig. De har gjort gældende, at der bør anlægges en overordnet tilgang med henblik på at

afgøre, om den retlige ordning beskytter retten til respekt for privatlivets fred på en forholdsmæssig måde.

- 12 De sagsøgte har gjort gældende, at loven af 2011 fastsatte en detaljeret ramme for adgangen til de lagrede data. Staten har desuden gjort gældende, at TLU, der er funktionelt uafhængig af An Garda Síochána ved udførelsen af sine opgaver, opfylder kravet om en »uafhængig administrativ myndighed«, der foretager en forudgående gennemgang af anmodninger om adgang, og at dette system er forstærket af flere yderligere niveauer af retsligt tilsyn i form af den udpegede dommer, den fastsatte klageprocedure og domstolsprøvelsen.
- 13 De sagsøgte har desuden gjort gældende, at hvis loven af 2011 i sidste ende anses for at være uforenelig med EU-retten, bør den tidsmæssige virkning af enhver afgørelse, som Domstolen måtte træffe, kun gælde fremadrettet. De har gjort gældende, at dette er passende under hensyntagen til de særlige omstændigheder i den foreliggende sag, hvor staten på det tidspunkt i slutningen af 2013, hvor der blev givet adgang til de relevante data i hovedsagen, i henhold til EU-retten var forpligtet til at gennemføre bestemmelserne i direktivet af 2006 og opretholde en datalagringsordning som den, der er fastsat i loven af 2011. Endvidere har staten gjort gældende, at dette er hensigtsmæssigt under omstændigheder, hvor en afgørelse om uforenelighed uden nogen begrænsning af virkningen ville få betydelige konsekvenser for efterforskning og retsforfølgning af grov kriminalitet i Irland, både hvad angår de personer, der er blevet retsforfulgt og dømt, og for igangværende efterforskninger og retsforfølgning.

### **Kort fremstilling af begrundelsen for forelæggelsen**

- 14 Den foreliggende anmodning om præjudiciel afgørelse har til formål at få præciseret de EU-retlige krav vedrørende lagring af data med henblik på bekæmpelse af grov kriminalitet og de nødvendige sikkerhedsforanstaltninger ved adgang til disse data, henset til en medlemsstats kompetence på det strafferetlige område. Den forelæggende ret ønsker ligeledes at få præciseret rækkevidden og de tidsmæssige virkninger af det eventuelle anerkendelsessøgsmaal, som kunne indrømmes under de foreliggende omstændigheder i denne sag.
- 15 Supreme Court har anført, at loven af 2011 foreskrev lagring af alle de metadata, der var underlagt dens bestemmelser, hvilket tilsyneladende på daværende tidspunkt var et krav i medfør af EU-retten. Men hvis universel lagring som sådan er ulovlig, således som G.D. har gjort gældende, er loven af 2011 ikke i overensstemmelse med EU-retten. Hvis det på den anden side er hensigtsmæssigt med en bredere tilgang, således som staten har gjort gældende, skal formålet med ordningen i dens helhed og de omstændigheder, hvorunder adgangen er tilladt, undersøges, og det skal afgøres, om loven af 2011 udgør et forholdsmæssigt indgreb i retten til privatlivets fred, der er sikret ved EU-retten og chartret.
- 16 Supreme Court har anerkendt, at spørgsmålet om anerkendelse af bevismidler i en straffesag henhører under national ret. Spørgsmålet om gyldigheden af visse dele

af loven af 2011 er imidlertid et spørgsmål, der kan rejses ved en civil retssag. Desuden skal selve spørgsmålet om anerkendelse af bevismidler behandles i lyset af en (eventuel) konstatering af ugyldighed og dennes præcise karakter, rækkevidde, formål, anvendelsesområde og tidsmæssige virkning.

- 17 Under disse omstændigheder finder retten det nødvendigt at forelægge Den Europæiske Unions Domstol de ovenstående spørgsmål.

ARBEJDSDOKUMENT