Myndighetenes lagring og adgang til trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet.

En fremstilling og vurdering av norsk rett etter EU-domstolens tolkningsresultater

Kandidatnummer: 135

Antall ord: 14619

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

[1. juni 2018]

Innholdsfortegnelse

1. Innledende tema

1.1 Tema og aktualitet

Tema for avhandlingen er myndighetenes mulighet til *lagring av* og *adgang til* trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet. Problemstillingen er særlig aktuell etter at EU-domstolen i dommen *Tele2 Sverige og Watson og andre*[1] kom med klare retningslinjer for lagring og adgang av trafikk- og lokaliseringsdata. Oppgaven innebærer en fremstilling og vurdering av norsk rett etter EU-domstolens retningslinjer og praksis, med særlig vekt på Tele2 dommen. Overordnet vil forholdet mellom individers rett til personvern og myndighetenes inngrep overfor borgerne være sentralt.

Siden 90-tallet har den teknologiske utviklingen hatt en markant vekst. Dette har resultert i økt deling av personopplysninger i digitale forum, samt at kommunikasjon i større grad foregår ved bruk av digitale hjelpemidler. Som følge av dette er behovet for beskyttelse av personopplysninger større enn noen gang.

Ikke sjeldent hører man at digitale spor blir anvendt ved etterforskning av straffesaker og senere brukt som bevis i retten. Gjennom medias fremstilling er det lett å få inntrykk av at politi- og påtalemyndighetene har en nærmest ubegrenset adgang til de digitale spor vi etterlater oss. Som eksempel på myndighetenes bruk av trafikkdata- og lokaliseringsdata kan det vises til den høyt profilerte Jensen-saken fra 2017. Tiltalen mot Eirik Jensen er den mest alvorlige mot en politimann i norsk historie. Jensen ble av Oslo tingrett dømt til 21 års fengsel for å ha hjulpet Gjermund Cappelen med å innføre narkotika til Norge. I forbindelse med saken la Spesialenheten for politisaker frem en liste over etterforskingsskritt, hvor et av de viktigste skrittene var innhenting av trafikkdata.[2]

Myndighetenes mulighet for lagring og adgang til trafikk- og lokaliseringsdata har vært et omdiskutert tema i Norge i mange år. Dette ser man blant annet ved at forslag om lovendring for gjennomføring av EUs regelverk om lagring i alt fikk 130 skriftlige innspill, samt flere innlegg på Samferdselsdepartementets blogg.[3] Hvorvidt myndighetene skal ha en vid adgang til digitale spor kan diskuteres. På bakgrunn av samfunnsdebatten og den noe usikre rettstilstanden på

[1] C-203/15 og C-698/15, heretter Tele2 dommen
[2] NRK, https://www.nrk.no/norge/spesialenheten_-_-cappelen-var-jensens-kontantkilde-1.13313781
[3] Prop. 49 L (2010-2011) s. 8

området, er det utvilsomt behov for en avklaring av hvilke rett myndighetene har til lagring av og adgang til trafikk- og lokaliseringsdata.

Desember 2016 ga EU-domstolen i Tele2 dommen uttrykk for hvilke rettstilstand som gjelder i EU-retten for lagring og adgang til trafikk- og lokaliseringsdata. Domstolen kom med klare retningslinjer for henholdsvis lagring og adgang. Selv om Norge ikke er medlem av EU er vi en del av EUs indre marked gjennom EØS-samarbeidet. Tele2 dommen kan få betydning for norsk rett og vil følgelig være sentral for denne avhandlingen.

1.2 Definisjoner og avgrensninger

1.2.1 Trafikk- og lokaliseringsdata

For å få en bedre forståelse av avhandlingen er det hensiktsmessig å presentere hva begrepene trafikk- og lokaliseringsdata omfatter. Dette vil også bidra til de naturlige avgrensningene som er nødvendig for oppgaven.

Trafikkdata er data som er «*nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring*», jf. ekomforskriften § 7-1 første ledd.[4] Ut i fra en naturlig språklig forståelse innebærer trafikkdata informasjon som enkeltindivider etterlater seg ved bruk av elektronisk kommunikasjon. Slik data kan forstås som elektroniske spor. Dette vil typisk omfatte det telefonnummer som er brukt ved kommunikasjonen, når kommunikasjonen har oppstått og hvem som er sender og mottaker.

Lokaliseringsdata kan anses som en underkategori av trafikkdata. Etter ekomforskriften § 7-1 andre ledd er lokaliseringsdata informasjon om «*den geografiske plasseringen av terminalutstyr*» som fremkommer under elektronisk kommunikasjon. Dette kan for eksempel være informasjon om hvor sender ringer fra og hvor mottaker befinner seg.

Ekomlovens[5] forarbeider legger til grunn samme definisjon av trafikkdata som ekomforskriften.[6] Det er likevel verdt å presisere at forarbeidene på side 92 nevner at trafikkdata for eksempel kan være «*kommunikasjonens opphavssted, bestemmelsessted …»* med videre. En normal forståelse av ordlyden «*kommunikasjonens opphavssted*» og «*bestemmelsessted*» vil innebære en

[4] Ekomforskriften fra 2004
[5] Lov 4. juli 2003 nr. 83, heretter ekomloven eller ekoml.
[6] Ot.prp. nr. 58 (2002-2003) s. 92

beskrivelse av geografisk plassering knyttet til et bestemt fysisk sted. Ut i fra definisjonen som er gitt ovenfor vil dette omfattes av begrepet lokaliseringsdata. Lovens forarbeider skiller således ikke klart mellom trafikk- og lokaliseringsdata.

Begrepene «*kommunikasjonens opphavssted*» og «*bestemmelsessted*» kan også innebære et mer teknisk opphavs- og/eller bestemmelsessted. Dette kan for eksempel være en bestemt IP-adresse. En slik forståelse av begrepet vil ikke nødvendigvis være knyttet direkte til et fysisk geografisk sted og vil da ikke angi lokaliseringsdata ved å omhandle kommunikasjonens geografisk plassering. Likevel kan det vanskelig tenkes at lovgiver ved bruk av disse begrepene har tatt sikte på en slik teknisk og lite tilgjengelig forståelse av begrepene. Dersom en slik forståelse hadde vært tilfelle, er det nærliggende å anta at lovgiver uttrykkelig hadde nevnt dette i lovens forarbeider. Det legges dermed til grunn at begrepene som er brukt i lovens forarbeider gir uttrykk for en form for lokaliseringsdata som omhandler en stedlig geografisk plassering.

Etter dette skiller ikke lovens forarbeider klart mellom trafikkdata og lokaliseringsdata. Begge begrepene går innunder fellesbetegnelsen trafikkdata. Dette endrer likevel ikke begrepenes faktiske innhold. Hvorvidt man velger å skille mellom de to begrepene avhenger av den konkrete sammenhengen begrepene brukes i. Det sentrale vil uansett være at begrepene omhandler informasjon om faktiske omstendigheter ved kommunikasjonen.

For denne avhandlingen anses det som hensiktsmessig å holde begrepene trafikk- og lokaliseringsdata adskilt. Ved vurderingen av myndighetenes lagring og adgang kan det tenkes å være ulik vekt av personvernhensyn for henholdsvis trafikkdata og lokaliseringsdata. Lokaliseringsdata vil lettere kunne skape en profil av vedkommendes bevegelses- og handlingsmønster, og dermed være et større inngrep i retten til personvern.

Det er også verdt å nevne en form for lokaliseringsdata som betegnes som **signaleringsdata**. Signaleringsdata beskrives som «*data som genereres mellom terminal og tilgjengelig basestasjon og angir terminalens geografiske plassering når den er slått på, uten at trafikkdata formidles*», jf. ekomforskriften § 7-2. Bestemmelsens ordlyd beskriver ingen form for aktiv kommunikasjon. Signaleringsdata kan etter dette oppstå selv om man ikke aktivt kommuniserer. Ut i fra Justis- og beredskapsdepartementets beskrivelse anses signaleringsdata som

«*informasjon som genereres og lagres selv når telefonen ikke er i bruk*».[7] Dette innebærer at signaleringsdata er informasjon om telefonens geografiske plassering uten aktiv bruk og er dermed en form for lokaliseringsdata.

Videre i avhandlingen behandles signaleringsdata som en del av lokaliseringsdata. Dette begrunnes i det faktum at signaleringsdata innebærer informasjon om telefonens geografiske posisjon. Det er likevel viktig å være oppmerksom på at lagring av og adgang til signaleringsdata alene kan anses som et sterkere inngrep i retten til personvern. Dette fordi signaleringsdata omfatter lagring av informasjon ved at man har telefonen med seg, men uten aktiv bruk. Det er dermed ingenting enkeltindividet aktivt foretar seg, selv om det er teknisk mulig at opplysninger om vedkommende blir samlet inn. En slik forståelse kan også leses av Lysnesutvalgets utredning hvor det tas til ordet for at adgang til signaleringsdata er en «*meget personverninngripende metode*».[8]

Det er viktig å ha klart for seg at begrepene trafikk- og lokaliseringsdata avgrenses mot innholdet i kommunikasjonen. Hva som faktisk blir kommunisert omfattes ikke av begrepene. Oppgaven avgrenses i samsvar med dette.

Det er også verdt å merke seg at trafikk- og lokaliseringsdata kan anses som personopplysninger. Personopplysningsloven § 2 nr. 1 legger til grunn at en personopplysning innebærer «*opplysninger og vurderingen som kan knyttes til en enkeltperson».*[9] Ved kommunikasjon mellom individer vil informasjonen som fremkommer av trafikk- og lokaliseringsdata kunne knyttes til enkeltpersoner. Dette for eksempel ved å angi hvor vedkommende befinner seg og med hvem og hvordan vedkommende kommuniserer.

1.2.2 Kommunikasjonskontroll

For en bedre forståelse og en naturlig avgrensning av oppgavens problemstilling vil det være hensiktsmessig å se på hva som omfattes av begrepet kommunikasjonskontroll i norsk rett.

[7] NOU 2015:13 s. 113
[8] NOU 2015:13 s. 113
[9] Lov 14. april 2000 nr. 31, personopplysningsloven

Straffeprosessloven fjerde del regulerer myndighetenes mulighet for bruk av tvangsmidler.[10] Myndighetenes adgang til å foreta kommunikasjonskontroll fremgår av lovens kapittel 16 a og 16 b. Bestemmelsene i strpl. kapittel 16 a og 16 b omfatter kommunikasjonskontroll i form av avlytting eller annen form for kontroll av informasjon som oppstår ved kommunikasjon mellom to eller flere parter. En naturlig språklig forståelse av begrepet kommunikasjonskontroll omfatter både nåtidig og fremtidig kommunikasjon. Dette innebærer den kommunikasjonen som skjer akkurat nå, samt kommunikasjon som vil skje i fremtiden. Dette kan begrunnes ved at kontroll er noe som gjennomføres for å korrigere eller endre utfallet av en situasjon. Informasjon som allerede foreligger kan omtales som historisk data. Hvorvidt historisk data omfattes av begrepet kommunikasjonskontroll er noe uklart.

Strpl. § 216 b omhandler «*annen kontroll av kommunikasjonsanlegg*». Sett i sammenheng med lovens kapitteloverskrift vil dette innebære en form for kommunikasjonskontroll. Ut i fra det nevnte tilsier dette at bestemmelsen regulerer nåtidig og fremtidig data. Likevel er det uttrykkelig presisert i bestemmelsens andre ledd bokstav d at kontrollen også kan omfatte «*hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt…».* At kommunikasjonskontroll etter bestemmelsen også omfatter data som «*har vært satt*» innebærer at også historisk data kan omfattes av kommunikasjonskontroll etter bestemmelsen.

Lovens øvrige bestemmelser om kommunikasjonskontroll trekker ikke frem historisk data som en del av sitt anvendelsesområde. Hovedregelen vil dermed være at kommunikasjonskontroll fokuserer på nåtidig og fremtidig data. Strl. § 216 b andre ledd bokstav d regulerer slik sett ett unntak fra hovedregelen ved at bestemmelsen uttrykkelig også omfatter historisk data. Etter dette kan det sies at lovens systematikk rettes mot nåtidig og fremtidig data, men med innsalg av historisk data i § 216 b andre ledd bokstav d.

Det kan legges til grunn at fremtidig og sanntidig data er noe myndighetene har adgang til ved kommunikasjonskontroll dersom lovens vilkår er oppfylt. Myndighetenes adgang til slik data er ikke særlig problematisk. Oppgaven avgrenses i hovedsak mot kommunikasjonskontroll, med unntak av strpl. § 216 andre ledd bokstav d som vil kreve en videre vurdering.[11]

[10] Lov 22. mai 1981 nr. 25, heretter straffeprosessloven eller strpl.
[11] Se punkt 5.4.4

Siden fremtidig og sanntidig data syntes mindre problematisk er avhandlingen avgrenset til å omhandle myndighetens mulighet for lagring og adgang til historisk data.

1.2.3 Kriminalitetsbekjempende formål

Som det fremgår av problemstillingen vil avhandlingen konsentrere seg om myndighetenes mulighet til lagring og adgang av hensyn til bekjempelse av kriminalitet. Det vil ikke være rom for vurdering av lagring eller adgang ut i fra andre hensyn enn kriminalitetsbekjempelse. Det at avhandlingen konsentrer seg om kriminalitetsbekjempelse vil også medføre en naturlig avgrensning når det gjelder hvilke myndigheter som eventuelt vil få rett til lagring eller adgang til trafikk- og lokaliseringsdata. I Norge er politi- og påtalemyndigheten statens utøvende makt for bekjempelse av kriminalitet. Dette fremgår av politiloven, jf. §§ 1 og 2.[12] Spørsmål om myndighetenes lagring av og adgang til trafikk- og lokaliseringsdata vil omfatte hvilke muligheter politi- og påtalemyndigheter har til dette. Det kan likevel være verdt å merke seg at også andre myndigheter kan ha behov for slik data uten at dette blir nærmere behandlet i denne avhandlingen.

1.3 Metode

Avhandlingen bygger på vanlig juridisk metode.

Lagring og adgang til trafikk- og lokaliseringsdata er inngrep i borgernes grunnleggende rettigheter.[13] Dette innebærer at man er i kjernen av legalitetsprinsippets område og inngrep krever hjemmel i lov, jf. Grunnloven § 113.[14] Metodisk må man være bevisst at det innenfor legalitetsprinsippets område er viktig å være varsom med bruk av utvidende tolkning av hjemmelsgrunnlag.

En metodisk utfordring ved avhandlingen er at man befinner seg innenfor tre ulike rettssystemer, nemlig EU-/EØS-rett, EMK og norsk rett. Det er viktig å være bevisst på de til dels ulike tolkningsprinsippene for, og sammenhengen mellom rettssystemene, samt øvrige rettssystemers betydning for norsk rett. EU-domstolens betydning for norsk rett behandles utførlig i kapittel 4.

[12] Lov 4. august 1995 nr. 53, politiloven
[13] Se punkt 2 om vernet av personopplysninger, samt Grunnloven § 102
[14] Lov 17. mai 1814, Grunnloven eller Grl.

1.4 Fremstillingen videre

I det videre vil det først sies noe generelt om vernet av personopplysninger. Dette er nødvendig for å få en overordnet forståelse av hvilke krenkelse lagring og adgang til trafikk- og lokaliseringsdata kan innebære. Deretter vil EU-retten og dens betydning for norsk rett behandles, for så å se på hvilke krav EU stiller til lagring og adgang av trafikk- og lokaliseringsdata. Videre vil norske regler om lagring og adgang vurderes. Avslutningsvis vil det bli foretatt en vurdering av norsk rett i lys av statens positive forpliktelser, samt avsluttende bemerkninger om behovet for regler om lagring og adgang til trafikk- og lokaliseringsdata.

2. Vernet av personopplysninger

Som nevnt under punkt 1.2.1 kan trafikk- og lokaliseringsdata anses som personopplysninger. For en bedre forståelse av myndighetenes mulighet for lagring av og adgang til trafikk- og lokaliseringsdata er det hensiktsmessig å si noe generelt om personopplysningsvernet.

I Norge har retten til personvern eksistert i mange år. Vernet var tidligere beskyttet ved ulike bestemmelser i blant annet Grunnloven, se for eksempel den historisk versjonen av Grl. § 102 om forbudet mot husundersøkelser, samt § 100 fjerde ledd andre punktum som regulerte forbud mot brevsensur utenfor «*anstalter*».[15] Begge bestemmelsene inneholdt en begrenset rett til personvern. Vernet av personopplysninger var også regulert ved en rekke andre nasjonale bestemmelser som for eksempel personregisterloven, folkeregisterloven, helseregisterloven, arbeidsmiljøloven, åndsverkloven, straffeloven, mv.[16]

Beskyttelse av personvernet i norsk rett følger også av tidlig praksis. Dette fremgår blant annet av de to kjente dommene Rt.1896 s. 530 Aars-dommen og Rt.1952 s. 1217 To mistenkelige personer. I dommene fokuserte Høyesterett på retten til personvern ved henholdsvis slektsnavn, samt beskyttelse av personvernet ved filmatisering av en tidligere straffbar handling. Ved Grunnlovsrevisjonen i 2014 fikk Norges Grunnlov et eget kapittel om menneskerettigheter og personvernet fikk en generell konstitusjonell forankring i Grl. § 102.[17]

Etter Grl. § 102 reguleres «*rett til respekt for sitt privatliv og familieliv, sitt hjem og kommunikasjon*». Vern av personopplysninger omfattes som en naturlig del av retten til privatliv. Det er også utvilsomt lovgivers mening at bestemmelsen skal omfatte en beskyttelse av personvern og personopplysningsvern.[18]

Det er i denne sammenheng verdt å merke at Grl. § 102 også uttrykkelig omfatter retten til «*kommunikasjon*». Grunnet den teknologiske utviklingen ønsket lovgiver å tydeliggjøre at kommunikasjon har et generelt konstitusjonelt vern.[19] Det ble i denne sammenheng presisert at bestemmelsens vern av kommunikasjon innebærer «*systematisk innhenting, oppbevaring og bruk*

[15] Historisk versjon av Grl. før endring 13. mai 2014
[16] Dok. nr. 16 (2011-2012) s. 168
[17] Grunnlovens kapittel E om menneskerettigheter
[18] Innst. 186 S (2013-2014) s. 27
[19] Innst. 186 S (2013-2014) s. 27

av opplysninger om andres personlige forhold».[20] Trafikk- og lokaliseringsdata anses som personopplysninger som bygger på kommunikasjon og vernes utvilsomt av Grl. § 102.

Det grunnleggende vernet av ulike menneskerettigheter i Grl. kapittel E er ikke absolutt. Dette følger klart av praksis, se for eksempel Rt. 2014 s. 1105 avsnitt 28 og Hr-2016-1286-A avsnitt 25. Dommene omhandler henholdsvis bruk av ulovlige lagrede bevis når informasjonen er innhentet gjennom kommunikasjonskontroll og at tvangsmedisinering innenfor tvungent psykisk helsevern utgjør et inngrep i Grl. § 102 og EMK art. 8. Dommene er av prinsipiell betydning og viser at hvorvidt inngrep i retten til personvern etter Grl. § 102 anses som lovlig avhenger av konkrete vilkår.

For det første inneholder legalitetsprinsippet en grunnleggende ytre skranke ved inngrep i borgernes rettigheter. Etter legalitetsprinsippet kan det bare gjøres inngrep i borgernes rettigheter dersom et slikt inngrep har hjemmel i lov. Prinsippet bygger på konstitusjonell sedvanerett, men er nå også forankret i Grl. § 113. Dersom det skal gjøres inngrep i retten til personvern etter Grl. § 102 kreves det følgelig at det foreligger hjemmel i lov.

Videre presiserer Høyesterett i Rt. 2014 s. 1105 avsnitt 28 at lov som gjør inngrep i § 102 må ivareta et legitimt formål og være forholdsmessig. Det avgjørende for om et inngrep i retten til privatliv etter Grl. § 102 er lovlig, vil dermed avhenge av om «*inngrepet har hjemmel i lov, ivaretar et legitimt formål og er forholdsmessig*».[21] På et overordnet nasjonalt plan vil dette være avgjørende for myndighetenes mulighet for lagring og adgang til trafikk- og lokaliseringsdata.

Det er også andre rettssystemer som uttrykkelig verner om retten til respekt for privatliv, korrespondanse og dermed personvern og vern av personopplysninger. Av betydning kan nevnes vernet av privatliv og korrespondanse etter EMK art. 8. Også EMK art. 8 må forstås slik at bestemmelsen omfatter et personvern og vern av personopplysninger. Dette fremgår blant annet av praksis ved EMD. Som eksempel kan nevnes Amann mot Sveits hvor EMD la til grunn at myndighetenes lagring av personopplysninger knyttet til privatlivet utgjør et inngrep i den rett som fremgår av EMK art. 8.[22] Siden trafikk- og lokaliseringsdata er å anse som personopplysninger vernes lagring av denne type informasjon etter EMK art. 8.

[20] Innst. 186 S (2013-2014) s. 27
[21] HR-2016-1286-A avsnitt 25
[22] EMD dom 16. februar 2000, avsnitt 65

Myndighetenes adgang til trafikk- og lokaliseringsdata vernes også av EMK art. 8. I Copland mot Storbritannia la EMD til grunn at arbeidsgivers overvåking av blant annet arbeidstakers telefonlogger var et brudd på EMK art. 8.[23] Selv om det i dommen var snakk om arbeidsgivers overvåking og ikke myndighetenes adgang, er det naturlig å forstå dommen slik at også myndighetenes adgang til slike opplysninger er å anse som vernet etter EMK art. 8. Dette blant annet fordi inngrep fra myndighetene vil være vel så krenkende som arbeidsgivers inngrep. Det kan også nevnes at adgang til trafikk- og lokaliseringsdata vil være minst like inngripende, og i mange tilfeller mer inngripende, overfor borgerne enn lagring alene. Ut i fra dette vil også adgang til trafikk- og lokaliseringsdata være beskyttet av EMK art. 8.

Til forskjell fra Grl. § 102 åpner ordlyden i EMK art. 8 nr. 2 uttrykkelig opp for inngrep i rettigheten dersom *«dette er i samsvar med loven og er nødvendig i et demokratisk samfunn …»*. Vilkårene for inngrep i rettighetene etter EMK art. 8 og Grl. § 102 er tilsvarende lik.[24] Det kan i denne sammenheng nevnes at Justis- og beredskapsdepartementet har uttalt at Grl. § 102 og EMK art. 8 har klare likhetstrekk, samt at Grl. § 102 må tolkes i lys av EMK art. 8.[25] Som følge av EMK sin fortrinnsrett ville konvensjonen uansett gått foran norsk rett ved eventuell motstrid, jf. menneskerettsloven § 3.[26] Slik sett markerer konvensjonen en ytre ramme som gir myndighetene mulighet til å gjøre inngrep i individenes rett til personopplysninger dersom vilkårene for inngrep er oppfylt. Departementets oppfatning er imidlertid at Grl. § 102 ikke stiller strengere krav til behandling av personopplysninger enn EMK art. 8.[27]

[23] EMD dom 3. april 2007
[24] Prop. 56 LS (2017-2018) s. 34
[25] Prop. 56 LS (2017-2018) s. 34
[26] Lov 21. mai 1999 nr. 30, menneskerettsloven
[27] Prop. 56 LS (2017-2018) s. 34

3. EU-retten

3.1 Generelt

I kjølvannet av den teknologiske utviklingen kan det sies at EU de siste årene har hatt en stadig mer aktivistisk holdning til retten til personvern. Dette fremgår både av EU-domstolens praksis, samt den nylig vedtatte forordningen *General Data Protection Regulation*.[28]

Innføringen av GDPR innebærer økt beskyttelse av personvern ved et strengere vern av personopplysninger. Forordningen omfatter blant annet fire nye rettigheter for borgerne. Gjennom GDPR får borgerne rett til å få behandling av sine personopplysninger begrenset, det gis rett til å flytte data mellom ulike systemer og tjenester (dataportabilitet), rett til å motsette seg behandling og rett til å nekte at det foretas automatiserte avgjørelser og analysering av personopplysninger for å dekke adferd, preferanser, evner eller behov (personprofilering).[29]

Når det gjelder EU-domstolens praksis er det i denne sammenheng verdt å trekke frem Google-dommen fra 2014[30] og Safe Harbour-saken fra 2015.[31] Begge dommene viser at personvernet har fått en styrket stilling i EU. Førstnevnte dom gjaldt en persons rett til å ikke dukke opp i søk på nettstedet Google. EU-domstolen konkluderte med at retten til personvern veide tyngre enn offentlighetens interesse til innsyn i andres personopplysninger. I Safe- Harbour-saken kjente domstolen Safe Harbor avtalen med USA for ugyldig. Avtalen gjaldt deling av personopplysninger fra europeiske selskaper til USA. Domstolen kom til at avtalen var i strid med grunnleggende rettigheter etter EMK art.7 og 8 om retten til privatliv og personvern. I ettertid er avgjørelsen blitt sett på som et signal fra EU-domstolen om å styrke retten til privatliv, korrespondanse og databeskyttelse.[32]

Selv om den nevnte forordningen og praksis ikke direkte regulerer retten til lagring og adgang av trafikk- og lokaliseringsdata er kildene relevante da de viser den aktivistiske holdningen til personvern som har vokst frem i EU de siste årene. EUs aktivistiske holdning til personvern innebærer ikke automatisk at andre myndigheter har hatt en tilsvarende utvikling. Det er likevel

[28] Regulation 2016/679, heretter GDPR
[29] Datatilsynet, https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/hva-blir-nytt-med-forordningen/
[30] C-131/12, 13. mai 2014, Google-dommen
[31] C-362/14 6. oktober 2015, Safe Harbour-saken
[32] Se uttalelse fra Datatilsynets direktør Bjørn Erik Thon, https://www.datatilsynet.no/aktuelt/2015/safe-harbor-beslutningen-kjent-ugyldig2/

ikke utenkelig at også norske myndigheter og EMD vil følge denne utviklingen. Det at borgerne i større grad enn tidligere etterlater seg digitale spor gjør det nødvendig med klare regler når det gjelder personvern og myndighetenes inngrep i slike rettigheter.

3.2 Kommunikasjonsverndirektivet og Datalagringsdirektivet

Rettstilstanden i EU vedrørende myndighetenes lagring og adgang til trafikk- og lokaliseringsdata har vært i endring de siste årene. For å få en bedre forståelse av gjeldende rett er det nødvendig å se på hvilke utvikling EU-retten har hatt vedrørende lagring og adgang til slik informasjon.

Ved opprettelsen av Kommunikasjonsverndirektivet[33] hadde EU som formål å ivareta og sikre borgerne «*grunnleggende rettigheter og friheter, særlig retten til personvern, med hensyn til behandling av personopplysninger i sektoren for elektronisk kommunikasjon …*», jf. KVD art. 1 nr. 1. Behovet for beskyttelse av personopplysninger innenfor elektronisk kommunikasjon gjorde seg særlig gjeldende grunnet den stadig økende digitaliserte hverdagen. Hovedregelen etter KVD er at det skal sikres «*fortrolighet for kommunikasjon som foregår via offentlige kommunikasjonsnett og offentlig tilgjengelige elektroniske kommunikasjonstjenester samt fortrolighet for trafikkopplysninger knyttet til slik kommunikasjon»,* jf. art. 5 nr. 1. Fortrolighet vedrørende trafikkdata fremgår av art. 6 og fortrolighet vedrørende lokaliseringsdata av art. 9. Det er utvilsomt EU-komiteens ønske at borgernes kommunikasjon skal være beskyttet og uten fare for tilfeldig eller konstant overvåking.

Av hensyn til blant annet samfunnsinteresser og individenes egen sikkerhet er det utenkelig at all kommunikasjon skal være fortrolig til enhver tid og i ethvert tilfelle. Det kan lett tenkes tilfeller hvor det fra myndighetenes side vil være ønskelig at informasjon gjøres tilgjengelig for blant annet dem. Dette kan for eksempel være ved politiets arbeid for bekjempelse av kriminalitet.

KVD art. 15 åpner opp for at medlemslandene skal kunne vedta lovgivning som gjør inngrep i hovedregelen om kommunikasjonsfortrolighet. I medhold av bestemmelsen vedtok EUs medlemsland svært ulike regelverk om muligheten for lagring av trafikk- og lokaliseringsdata.[34]

[33] Directive 2002/58/EC, heretter KVD
[34] Rui (2017) s. 147

En slik utvikling var ikke forenelig med EUs mål om en helhetlig og ensartet rettstilstand for alle medlemslandene. Dette resulterte i vedtakelsen av Datalagringsdirektivet.[35]

DLD tok sikte på å harmonisere medlemslandene i EU sin lovgivning om lagring av trafikk- og lokaliseringsdata for å sikre adgang til opplysningene av hensyn til bekjempelse av kriminalitet, jf. DLD art. 1. Direktivets art. 3 påførte medlemslandene en plikt til å vedta lovgivning som sørget for lagring av trafikk- og lokaliseringsdata, jf. art. 5. Direktivet la således til grunn en lagringsplikt. En slik lagringsplikt ville i realiteten ført til at man gikk fra en hovedregel om konfidensiell kommunikasjon ved en sletteplikt, til en lagringsplikt for trafikk- og lokaliseringsdata, se særlig DLD art. 3 nr. 2.

Videre måtte medlemslandene gjennom lovgivning sørge for at de lagrede opplysningene i visse tilfeller kunne gis til nasjonale myndigheter dersom vilkårene for dette var oppfylt, jf. art. 4. Gjennom DLD ble det gitt vide rammer for når adgang til data kunne vært aktuelt.[36] Vilkår for adgang til opplysninger var etter art. 4 beskrevet som et krav om «*nødvendighet og rimelighet*», samt at det måtte være i samsvar med EUs regelverk, folkeretten og Den europeiske menneskerettighetskonvensjonen (EMK).

Den rettslige konsekvensen av DLD var at man gikk fra hovedregelen om kommunikasjonsfortrolighet etter KVD art. 5, til en ny hovedregel om at trafikk- og lokaliseringsdata skulle lagres med potensielt vide rammer for myndighetenes adgang til opplysningene, jf. DLD art. 3 og art. 4.

Når det gjelder DLD sin betydning for norsk rett bør det presiseres at direktivet aldri ble en del av EØS-avtalen. Ved innlemmelser av et EU-direktiv til EØS-avtalen kreves det enstemmighet i EFTA landene.[37] Under behandlingen av DLD benyttet Island sin vetorett, noe som resulterte i at direktivet aldri ble en del av EØS-avtalen. April 2011 vedtok Stortinget i Norge likevel å gjennomføre DLD i norsk rett. Innholdet ble forsøkt gjennomført i norsk rett ved endringer i ekomloven og straffeprosessloven mv.[38] Lovendringene er per dags dato ikke trådt i kraft.

[35] Directive 2006/24 EC, heretter DLD
[36] Rui (2017) s. 147
[37] Prop. 68 L (2015-2016) avsnitt 11.1.2.1
[38] Lov 15. april 2011 nr. 11

3.3 EU-domstolens praksis

Ved dommen *Digital Rights Irland og Kärnter Landesregierung* fra 2014 ble DLD kjent ugyldig av EU-domstolen.[39] EU-domstolen begrunnet direktivets ugyldighet ved at slike inngrep i grunnleggende rettigheter ikke var å tråd med proporsjonalitetsprinsippet.[40] I tillegg var ikke direktivet tilstrekkelig klart og presist, og krenket retten til privatliv og beskyttelse av personopplysninger i EU-charterets art. 7 og 8, samt art. 52 nr. 1.[41] Direktivet var for omfattende og ikke begrenset til det strengt nødvendige. Den rettslige konsekvensen av at domstolen erkjente DLD ugyldig er at man ser vekk i fra dette direktivet. Dette innebærer at KVD fremstår som gjeldende rett med tanke på lagring av og adgang til trafikk- og lokaliseringsdata. Dersom det skal foreligge unntak fra hovedregelen i KVD art. 5 om kommunikasjonsfortrolighet, må dette hjemles etter KVD art. 15.

Selv om EU-domstolen i Digital Rights dommen erkjente DLD ugyldig, ble sentrale spørsmål av betydning angående lagring og adgang til trafikk- og lokaliseringsdata ansett som ubesvart. Blant annet var det uavklart hvilke grenser som gjaldt i EU for nasjonale regler om lagring og adgang til slik data.[42] Det var dermed behov for en avklaring av hvilke grenser KVD oppstiller for datalagring etter nasjonal rett, sett i forhold til EU-rettens grunnleggende rettigheter og forpliktelser, her særlig charterets art. 7 og 8. Spørsmålet ble besvart av EU-domstolen i Tele2 dommen.

3.3.1 Tele2 dommen

Dagen etter Digital Rights dommen meddelte det svenske teleselskapet Tele2 at de ville stanse lagring av data slik de var pålagt etter LEK kap. 6, § 16 d.[43] LEK var vedtatt i medhold av DLD. Siden direktivet nå var kjent ugyldig hevdet Tele2 at loven ikke lengre var gjeldende rett. Svenske myndigheter benektet dette og hevdet at Tele2 var forpliktet til å lagre slik data. Tele2 anla sak for nasjonal domstol, men tapte. Etter anke fra Tele2 ba ankedomstolen EU-domstolen om en uttalelse.[44]

[39] C-293/12 og C-594/12, heretter Digital Rights dommen
[40] Digital Rights dommen avsnitt 69
[41] Charter of fundamental rights of the European Union, C 326/392
[42] Rui (2017) s. 147
[43] Svensk lovgivning: Lag (2003:389) av 12. juni 2003
[44] Rui (2017) s. 147-149

EU-domstolen foretok en vurdering av gjeldende rett vedrørende nasjonale myndigheters mulighet for lagring og adgang til trafikk- og lokaliseringsdata. Ved behandling av spørsmålet om lagring presiserer EU-domstolen at det andre spørsmålet angående adgang «*afhænger imidlertid ikke af spørsmålet om, hvorvidt en lagring af data er generel eller målrettet …*». Ut i fra en normal språklig forståelse siktet EU-domstolen til at de to spørsmålene må vurderes uavhengig av hverandre. Dette forsterkes ytterligere ved at domstolen videre i avsnittet har presisert at spørsmålet om adgang «*er forelagt uafhængigt af rækkevidden af den pligt til lagring af data*».[45] Ut i fra domstolens uttalelse er det naturlig å forstå de to spørsmålene som to uavhengige spørsmål. Det første spørsmålet i dommen var hvorvidt en udifferensiert plikt til å lagre data var forenelig med KVD art. 15 nr. 1, sett i lys av EU-charterets art. 7 og 8, samt art. 52 nr. 1.[46] Ved det andre spørsmålet vurderte domstolen vilkårene for myndighetenes adgang til slik data.[47]

En konsekvens av at domstolen behandler de to spørsmålene separat er at nasjonale regler om myndighetenes adgang ikke avhenger av teleselskapenes lagringsplikt, eller eventuelt andre muligheter for lagring av trafikk- og lokaliseringsdata. Selv om mange av vilkårene for lagring og adgang er like, vil det faktum at det er to uavhengige spørsmål innebære at det også kan foreligge selvstendige vilkår for henholdsvis lagring og adgang.

I det videre gis det en oversikt over de krav som domstolen stiller for henholdsvis lagring og adgang til trafikk- og lokaliseringsdata. Vilkårene for lagring og adgang er på en rekke punkter sammenfallende og vil behandles parallelt. Det gis ytterligere presiseringer når dommen gir ulike retningslinjer for lagring og adgang.

3.3.2 Tele2 dommens vilkår for lagring og adgang til trafikk- og lokaliseringsdata

EU-domstolen legger til grunn at KVD art. 15 nr. 1 gjør det mulig for medlemslandene å vedta unntak fra direktivets art. 5 nr. 1 om kommunikasjonsfortrolighet.[48] Videre presiseres det at en slik avgrensning av direktivets formål og hovedregel må fortolkes strengt.[49] Hovedregelen skal fremdeles innebære kommunikasjonsfortrolighet som nevnt i art. 5. En streng fortolkning av art.

[45] Tele2 dommen avsnitt 113
[46] Tele2 dommen avsnitt 50
[47] Tele2 dommen avsnitt 114 og Rui s. 149
[48] Tele2 dommen avsnitt 88
[49] Tele2 dommen avsnitt 89

15 nr. 1 vil dermed være nødvendig for å ikke uthule direktivets grunnleggende formål om kommunikasjonsfortrolighet.

Tiltak etter bestemmelsen skal også «*være i samsvar med de allmenne prinsippene i fellesskapsretten …»*, jf. KVD art. 15 nr. 1 siste punktum. Siden dette er et EU-direktiv er det naturlig å forstå bestemmelsens ordlyd slik at «*fellesskapsretten*» refererer til EU-retten. Etter dette må EU-charterets alminnelige bestemmelser være ivaretatt og respektert ved den nasjonale lovgivning medlemslandene gir om lagring og adgang til trafikk- og lokaliseringsdata. Som domstolen uttaler vil det særlig være EU-charterets art. 7 og 8, samt art. 11, som er sentrale for vurderingen av om en regel om lagring og adgang til trafikk- og lokaliseringsdata er gyldig.[50]

Etter KVD art. 15 nr. 1 må en begrensning fra direktivets hovedregel være «*nødvendig, egnet og rimelig i et demokratisk samfunn …»*. Det foreligger således et nødvendighetskrav ut i fra direktivets ordlyd. Videre presiserer EU-domstolen «*at undtagelserne fra og begrænsningerne af beskyttelsen av personopplysninger holdes inden for det strengt nødvendige*».[51] Beskyttelse av personopplysninger omfatter både lagring og adgang til trafikk- og lokaliseringsdata. Ut i fra dommens ordlyd presiseres det at nødvendighetskravet må anses som «*strengt*». Dette kan begrunnes i behovet for beskyttelse av personvernet og retten til privatliv. Det foreligger dermed et strengt nødvendighetskrav for lagring og adgang til trafikk- og lokaliseringsdata.

For å oppfylle det strenge nødvendighetskravet kreves det blant annet at inngrep i rettigheten fremmer et legitimt formål. Som det fremgår av KVD art. 15 nr. 1 må lovgivningstiltak kunne begrunnes i hensyn til «*nasjonal sikkerhet, forsvar, offentlig sikkerhet og forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger eller ulovlig bruk av det elektroniske kommunikasjonssystemet*». En slik oppramsing av ulike formål må anses som uttømmende. I dommen er det presisert at lovhjemmel om lagring og adgang til data alltid skal følge et objektivt formål, i dette tilfellet bekjempelse av grov kriminalitet.[52] Det stilles dermed krav til alvorlighetsgraden ved den kriminaliteten som skal bekjempes. Det er ikke rom for inngrep i retten til personvern ved lagring eller adgang for bekjempelse av mindre alvorlig kriminalitet. Hva som ligger i betegnelsen grov kriminalitet er omdiskutert. I forbindelse med spørsmål fra den regionale domstol i Tarragona har EUs generaladvokat Saugmandsgaard Øe

[50] Tele2 dommen avsnitt 92
[51] Tele2 dommen avsnitt 96
[52] Tele2 dommen avsnitt 110 og 115

nylig kommet med forslag til avgjørelse vedrørende spørsmål om begrepets betydning.[53] Saugmandsgaard Øe sitt forslag vil bli videre kommentert i del 5.4.4.

Videre fremgår det av Tele2 dommen at det kreves at nasjonal lovgivning «*fastsætter klare og præcise regler, der regulerer rekkevidden og anvendelsen af en sådan foranstaltning om lagring af data …».*[54] Tilsvarende angis ved at lovgivning om myndigheters adgang til data må «*fastsætte klare og præcise regler*».[55] Domstolens begrunnelse for kravet er å sikre enkeltindivider «*tilstrækkelige garanter, der gjør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug*».[56] Kravet til klarhet og presisjon skal ivaretas ved å sikre at nasjonale bestemmelser presist angir under hvilke omstendigheter og på hvilke betingelser lagring og adgang kan bli aktuelt.[57]

Når det gjelder svensk lovgivning om **lagring** og hvorvidt den oppfyller de krav som stilles, påpeker EU-domstolen at lovgivningen innebærer en «*generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation, og at den uden undtagelse forpligter udbyderne af elektroniske kommunikationstjenester til at lagre disse data systematisk og uafbrud.»* [58] Ved slik lagring samles det inn tilstrekkelig mengder opplysninger til å danne seg en profil av vedkommendes handle- og væremåte.[59] Domstolen var derfor av den oppfatning at en slik generell og udefinert lagring gikk utover det som var nødvendig og krenket dermed privatlivets fred i form av konstant overvåkning. En lagring som regulert i den svenske lovgivningen ville også kunne få betydning for personers kommunikasjonsmåte, og dermed være i strid med ytringsfriheten etter EU-charteret art. 11. I tillegg vil en slik regulering medføre at man får lagring som hovedregel, noe som strider mot grunnleggende målsettinger i KVD.[60]

For å oppfylle kravene til klare og presise regler angående myndighetenes **adgang**, oppstiller domstolen både materielle og prosessuelle regler. EU-domstolen trekker frem at det bare kan

[53] Sak C-207/16
[54] Tele2 dommen avsnitt 109
[55] Tele2 dommen avsnitt 117
[56] Tele2 dommen avsnitt 109
[57] Tele2 dommen avsnitt 109 og 117
[58] Tele2 dommen avsnitt 97
[59] Tele2 dommen avsnitt 100-101
[60] Tele2 dommen avsnitt 104

«*gives adgang til data vedrørende personer, der er mistænkt ...*».[61] Ved dette foreligger det imidlertid et unntak dersom adgangen til opplysningene skal anvendes i forbindelse med bekjempelse av terrorvirksomhet.[62] Videre kreves det prosessuelle regler i form av forutgående kontroll, underretning til mistenkte, effektiv beskyttelse av enkeltindivider og et uavhengig tilsyn med regelverket.[63]

[61] Tele2 dommen avsnitt 119
[62] Tele2 dommen avsnitt 119
[63] Tele2 dommen avsnitt 120, 121, 122, 125

4. EU-rettens betydning for norsk rett

4.1 Tele2 dommens betydning for norsk rett

Norge er som kjent ikke medlem av EU. Metodisk er det dermed nødvendig å gjøre rede for om EU-domstolens praksis, ved Tele2 dommen, får betydning for norsk rett.[64] Hvorvidt Tele2 dommen kan tillegges betydning i Norge har potensielt avgjørende betydning for norske myndigheters mulighet for lagring og adgang til trafikk- og lokaliseringsdata.

Selv om Norge ikke er medlem av EU er vi en del av det indre markedet gjennom EØS-avtalen. Et av formålene med EØS-samarbeidet er at det skal være ensartet rett for samtlige medlemsland innenfor avtalens område.[65] En slik målsetting om ensartethet omtales ofte som homogenitetsprinsippet.[66] Prinsippet legger til grunn at samme metode og tolkningsresultat skal være gjeldende i både EU og EØS, og dermed også norsk rett.[67] Å oppfylle kravet om like tolkningsresultater i samtlige medlemsland kan bare oppnås dersom EU-domstolen anses som den ledende prejudikatdomstol innenfor EØS.[68] Dette innebærer at EU-domstolens metode og tolkningsresultater som utgangspunkt får betydning for tolking og vurdering av EØS-rettslige spørsmål i Norge.

Som nevnt behandler Tele2 dommen muligheten for lagring og adgang til trafikk- og lokaliseringsdata etter KVD. Direktivet ble en del av EØS-avtalen i 2003,[69] og er gjennomført i norsk rett ved ekomloven med tilhørende forskrift.[70] Ut i fra homogenitetsprinsippet vil utgangspunktet være at norsk rett er bundet av de tolkningsresultater som gis av EU-domstolen i Tele2 dommen. Det kan likevel problematiseres hvorvidt Tele2 dommen får betydning for norsk rett da EU-domstolen tolket KVD art. 15 nr. 1 opp mot EU-charterets art. 7 og 8, samt art. 52 nr. 1.

EU-charteret er ikke gjort til en del av EØS-avtalen eller på annen måte implementert i norsk rett. I samsvar med norsk suverenitet innebærer dette at charteret ikke får rettsvirkning i Norge. Dersom Tele2 dommens tolkningsresultater gis fullstendig betydning i norsk rett vil dette

[64] Spørsmålet er også behandlet av Rui (2017) s. 151-154
[65] Se blant annet EØS-avtalens fortale femte avsnitt
[66] Fredriksen & Mathisen (2014) s. 40
[67] Fredriksen & Mathisen (2014) s. 247-248
[68] Arnesen og Stenvik (2015) s. 27
[69] EØS-komiteens beslutning nr. 80/2003 av 20. Juni 2003
[70] FOR 16. februar 2004 nr. 401

innebære at ikke vedtatt EU-lovgivning får en indirekte rettslig betydning i Norge. Dette kan fremstå som uheldig da Norge bevist har valgt å ikke slutte seg til EU og dermed ikke har implementert EU-charteret. En slik forståelse av EU-domstolens betydning for norsk rett vil være negativt for landets suverenitet. Dette taler for at Tele2 dommens utfall bør får noe begrenset betydning for norsk rett.

Det må videre presiseres at det vil stride mot homogenitetsprinsippet dersom EU-domstolens tolkning av KVD ikke gis fullstendig betydning i Norge. En slik forståelse av EØS-retten vil innebære at medlemslandene i EØS-avtalen, EFTA-landene, i mange tilfeller ikke fullt ut er bundet av EU-domstolens praksis vedrørende rettslige spørsmål innenfor EØS-avtalens område. Dette vil øke sannsynligheten for ulike tolkningsresultat innenfor fellesskapet, og vil svekke homogenitetsprinsippet og EØS-avtalens formål om en ensartet rettstilstand.

Det er i denne sammenheng verdt å nevne at flere er skeptiske til EØS-samarbeidet. [71] Dette kan blant annet begrunnes i at det vanskelig kan tenkes at Norge skal kunne ivareta sin absolutte suverenitet samtidig som EU- og EØS-retten skal være ensartet ved å bygge på et homogenitetsprinsipp. På bakgrunn av dette kan EØS-samarbeidet innebære at EUs regelverk får indirekte betydning i norsk rett innenfor EØS-avtalens område. Siden en ensartet rettstilstand står så sentralt for avtalens opprinnelse, fremstår en slik løsning som det eneste praktiske mulige. Dette kan også sees på som en av ulempene ved samarbeidet, og en av hovedgrunnene til at mange i utgangspunktet var skeptisk til et slikt delvis EU-medlemskap som EØS-samarbeidet i realiteten innebærer.[72] Selv om det å gi EU-domstolens tolkningsresultater avgjørende betydning kan innebære skår i norsk suverenitet, vil det være vanskelig å ivareta EØS-avtalens mål om ensartet rett dersom EU-domstolens praksis ikke gis fullstendig betydning. Dette trekker i retning av at Tele2 dommens tolkningsresultater får fullstendig betydning i Norge.

I tillegg kan det nevnes at KVD art. 15 nr. 1 siste punktum legger til grunn at *«Alle tiltak omhandlet i dette nummer skal være i samsvar med de allmenne prinsippene i fellesskapsretten …»*. Ordlyden «*tiltak omhandlet i dette nummer*» omfatter unntak fra hovedregel om kommunikasjonsfortrolighet etter art. 5, 6 og 9, herunder lagring og adgang til trafikk- og

[71] Blant annet har Eriksen og Fossum tar til ordet for at EØS-avtalen innebærer demokratisk selvskading for Norge, se særlig Eriksen & Fossum (2014) s. 19

[72] Ved vedtakelsen av EØS-avtalen i Norge var det bare KrF og Venstre som anså EØS-avtalen som den beste tilknytningen til EU. Øvrige partier, også flertallet, var enten for fullt medlemskap i EU eller imot både EU og EØS, se Sejersted, F. (2011), s. 40

lokaliseringsdata. En naturlig språklig forståelse av begrepet «*fellesskapsretten*» sikter til det fellesskap som KVD bygger på. Direktivet er som nevnt et EU-direktiv som er gjort til en del av EØS-avtalen. Slik sett vil de «*allmenne prinsippene i fellesskapsretten*» innebære EUs regelverk om grunnleggende rettigheter, herunder EU-charteret. En slik forståelse støttes også av professor Halvard H. Fredriksen.[73] Som eksempel på problemstillingen vedrørende EU-charterets betydning for tolkning og anvendelse av EØS-avtalen i Norge, nevner Fredriksen at Tjenestedirektivet[74] art. 1 nr. 7 første punktum henviser til fellesskapsretten. Fredriksen tar til ordet for at denne henvisningen må forstås som en henvisning til EUs grunnleggende rettigheter. Henvisningen i Tjenestedirektivet er tilsvarende lik som henvisningen i KVD art. 15 nr. 1. Dette taler for at Fredriksen sitt eksempel også vil være beskrivende for forståelsen av henvisningen i KVD. Ut i fra dette kan EU-charteret få avgjørende betydning for tolkning av EØS-rettslige spørsmål. For vårt tilfelle innebærer dette at Tele2 dommens tolkning av KVD art. 15 i lys av EU-charteret får fullstendig betydning for norsk rett.

Henvisningen som fremgår av KVD art. 15 nr. 1 siste punktum innebærer dermed en direkte henvisning til EU-retten. Slik sett har norske myndigheter ved implementeringen av KVD godtatt at direktivet skal forstås i lys av EUs grunnleggende rettigheter, selv om disse rettighetene ikke direkte er godkjent og implementert til norsk rett. Denne forståelse støttes også av norske myndigheter ved innføringen av Tjenestedirektivet. Tjenestedirektivet ble gjort til norsk rett ved vedtakelse av tjenesteloven.[75] I lovens forarbeider presiseres det at grunnleggende rettigheter etter § 2 må forstås som EUs pakt om grunnleggende rettigheter.[76] Som nevnt ovenfor er henvisningen i ordlyden i KVD og Tjenestedirektivet tilsvarende lik. Dette taler for at lovgivers forståelse av begrepet «*grunnleggende rettigheter*» etter Tjenesteloven bør forstås på samme måte ved henvisningen i KVD til allmenne prinsipper i fellesskapsretten. Det kan også i denne sammenheng trekkes frem at fortalen til KVD også uttrykkelig presiserer at direktivet har som mål å respektere grunnleggende rettigheter og prinsipper som anerkjennes av Den europeiske unions pakt om grunnleggende rettigheter. Ut fra dette er det naturlig å forstå forholdet slik at regler som vedtas i medhold av direktivet må ivareta EU-charterets grunnleggende rettigheter. Dette fører til at ikke vedtatt EU-lovgivning gis en indirekte

[73] Fredriksen (2013) s. 378-380
[74] Directive 2006/123/EC, Tjenestedirektivet
[75] Lov 19. juni 2009 nr. 103
[76] Ot.prp. nr. 70 (2008-2009) s. 130-131

betydning i norsk rett, og videre at EU-domstolens avgjørelse i Tele2 dommen får fullstendig betydning for norsk rett.

Det kan også nevnes at KVD art. 15 nr.1 siste punktum uttrykkelig trekker frem at de allmenne prinsippene i fellesskapsretten omfatter «*... herunder prinsippene i artikkel 6 nr. 1 og 2 i traktaten om Den europeiske union.*» En slik direkte henvisning til EUs regelverk vil trekke i retning av at norske myndigheter ved implementeringen av direktivet har godtatt EU-charteret som tolkningsfaktor ved forståelsen av KVD.

På bakgrunn av en naturlig språklig forståelse av KVD art. 15 nr. 1 sett i sammenheng med øvrige omstendigheter som homogenitetsprinsippet og uttalelser i juridisk litteratur, er det naturlig å forstå henvisningen i KVD art 15 nr. 1 slik at direktivet skal forstås i lys av EUs grunnleggende rettigheter, herunder EU-charteret. Dette innebærer at EU-charteret får en indirekte påvirkning i Norge. EU-domstolens tolkningsresultat i Tele2 dommen får dermed betydning for norsk rett ved spørsmålet om myndighetenes lagring og adgang til trafikk- og lokaliseringsdata.

I samsvar med Fredriksen og Rui vil det på bakgrunn av homogenitetsprinsippet og EØS-samarbeidets formål om en ensartet rettstilstand legges til grunn at EU-domstolens tolkningsresultat i Tele2 dommen får virkning for norsk rett. Den rettslige konsekvensen av dette er at norsk rett er bundet av EU-domstolens tolkningsresultat i Tele2 dommen om lagring og adgang til trafikk- og lokaliseringsdata.[77]

4.2 Tele2 dommens krav til nasjonal hjemmel

Som konkludert med vil EU-domstolens tolkningsresultat i Tele2 dommen få betydning for norsk rett ved vurderingen av myndighetenes lagring av og adgang til trafikk- og lokaliseringsdata. I det videre vil det kort presiseres hva dette konkret vil innebære for nasjonal lovgivning, før en videre vurdering av om norsk lovgivning er i samsvar med de krav som stilles.

Etter Tele2 dommen er det klart at EU-domstolen oppstiller klare krav for nasjonal lovgivning om lagring og adgang til trafikk- og lokaliseringsdata. EU-domstolen presiserer utvilsomt at KVD art. 15 nr. 1 gir adgang til nasjonal lovgivning om lagring og adgang til trafikk- og

[77] Fredriksen (2013) s. 380 og 398 og Rui (2017) s. 153

lokaliseringsdata. For at norsk lovgivning skal være i samsvar med de krav som stilles er det likevel viktig at hovedregelen om kommunikasjonsfortrolighet ivaretas, og at lagring og adgang anses som unntak. Ved dette foreligger det et strengt nødvendighetskrav ved slik regulering, og krav om at reglene er i samsvar med allmenne prinsipper i EU. I tillegg er det bare rom for klare og presise regler som uttrykker under hvilke omstendigheter lagring og adgang kan bli aktuelt. Nasjonale regler må også følge et legitimt formål, i dette tilfellet bekjempelse av grov kriminalitet. Det er ikke adgang til nasjonale regler om lagring og adgang dersom formålet er bekjempelse av mindre alvorlig kriminalitet. For myndighetenes mulighet for lagring presiseres det at det foreligger forbud mot en generell og udefinert lagring av hensyn til personvernet. I tillegg må reglene om myndighetenes adgang ha et krav om mistenkt, forutgående kontroll, underretning til vedkommende opplysningene omhandler, samt krav om effektiv beskyttelse av vedkommende.

5. Norske regler om lagring og adgang til trafikk- og lokaliseringsdata

5.1 Generelt

Trafikk- og lokaliseringsdata kan anses som personopplysninger og har konstitusjonelt vern etter Grl. § 102.[78] For å vurdere myndighetenes mulighet for lagring og adgang til trafikk- og lokaliseringsdata må det i første omgang vurderes hvorvidt inngrepet har hjemmel i lov. På bakgrunn av implementeringen av KVD og videre Tele2 dommens betydning for norsk rett, må nasjonale lovhjemler vurderes opp mot de krav som fremkommer av Tele2 dommen. For en mer pedagogisk fremstilling vil reglene om lagring og adgang behandles separat.

5.2 Hjemmel for lagring av trafikk- og lokaliseringsdata

Hovedregelen etter KVD er at det skal foreligge fortrolighet ved elektronisk kommunikasjon, jf. art. 5. Dette innebærer blant annet et forbud mot å lagre data, med mindre noe annet følger av lov, jf. art. 5 nr. 1 andre punktum. Hovedregelen er forsøkt ivaretatt gjennom ekoml. § 2-7 femte ledd ved at trafikk- og lokaliseringsdata skal slettes eller anonymiseres så snart de ikke lengre er nødvendig.

KVD art. 15 åpner for at medlemslandene ved nasjonal lovgivning kan vedta begrensninger i hovedregelen om kommunikasjonsfortroligheten. Bestemmelsen kan imidlertid ikke brukes som selvstendig grunnlag for myndighetenes mulighet til lagring av data, men hjemler myndighetenes adgang til lovregulering på området. Det avgjørende for myndighetenes lagringsadgang vil være hvorvidt det foreligger norsk lovgivning om mulighet for lagring av slik data, og videre om eventuell lov er i samsvar med de krav som fremkommer av Tele2 dommen.

Det foreligger flere unntak fra hovedregelen om kommunikasjonsfortrolighet og forbud mot lagring av data. Data kan for det første lagres dersom det foreligger samtykke, jf. art. 5, jf. ekoml. § 2-7 sjette ledd. Videre kan data lagres dersom det er snakk om «*teknisk lagring*» for å kunne gjennomføre kommunikasjonen, jf. KVD art. 5 nr. 1 siste ledd, jf. ekoml. § 2-7 femte ledd nr. 1, eller av hensyn til faktureringsformål, jf. KVD art. 6 nr. 2, jf. ekoml. § 2-7 femte ledd nr. 1. Etter dette gir ekomlovens bestemmelser tilbyder av elektronisk kommunikasjon en rett til å

[78] Se oppgaven punkt 2

lagre data frem til informasjonen ikke lengre er nødvendig av hensyn til «*kommunikasjons- eller faktureringsformål*.»

Etter dette kan det legges til grunn at det norske rettssystemet har nasjonal lovgivning om lagring av historisk trafikk- og lokaliseringsdata for kommunikasjons- og faktureringsformål, jf. ekoml. § 2-7 femte ledd. Ekoml. § 2-7 regulerer teleselskapenes lagring ut i fra deres egen interesse og formål. Oppgaven konsentrerer seg om myndighetenes lagringsmulighet for å bekjempe grov kriminalitet. Ekoml. § 2-7 kan ikke sies å hjemle myndighetenes mulighet for lagring av hensyn til kriminalitetsbekjempelse. En videre drøftelse av bestemmelsene om teleselskapenes lagring er følgelig ikke relevant.

I forbindelse med EUs vedtakelse av DLD ønsket norske myndigheter å forhåndsgodkjenne implementeringen av direktivet, samt vedta de lovendring som var nødvendig før direktivets ikrafttredelse i norsk rett.[79] I den forbindelse ble det fremmet lovforslag fra Justisdepartementet, [80] som senere ble vedtatt.[81] Lovendringen innebar blant annet en tilføyelse i ekoml., ny § 2-7 a om «*Plikt til lagring av data*». Bestemmelsen pålegger tilbydere av elektronisk kommunikasjonsnett å lagre trafikk- og lokaliseringsdata for å etterforske, oppklare og straffeforfølge alvorlige straffbare forhold. I likhet med svensk lovgivning innebærer bestemmelsen en lagringsplikt for teleselskapene. En slik lagringsplikt vil føre til at man går fra en hovedregel om kommunikasjonsfortrolighet, til en generell lagringsplikt for teleselskapene. På bakgrunn av likhetstrekkene mellom svensk lov og ekoml. § 2-7 a er det naturlig å anta at den norske bestemmelsen om lagringsplikt med stor sannsynlighet vil stride mot EUs tolkningsresultat etter Tele2 dommen.

Etter Digital Rights dommen besluttet norske myndigheter aldri ikrafttredelse av ekoml. § 2-7 a.[82] En videre drøftelse av gyldigheten ved ekoml. § 2-7 a sett i henhold til Tele2 dommen vil dermed ikke være relevant siden loven ikke er gjort til gjeldende rett i Norge. Vi står dermed ovenfor en situasjon i Norge hvor det ikke foreligger hjemmel for å lagre trafikk- og lokaliseringsdata for å bekjempe grov kriminalitet.

[79] Prop. 50 S (2010-2011) s. 1
[80] Prop. 49 L (2010-2011), særlig s. 1
[81] Lov 15. april 2011 nr. 11, særlig punkt III
[82] Se Rui (2017) s. 151

Norsk lovgivning om lagring av trafikk og lokaliseringsdata etter KVD art. 15 har uteblitt. Siden lagring av data er et inngrep i retten til personvern etter blant annet Grl. § 102 vil manglende lovhjemmel etter legalitetsprinsippet medføre at myndighetene ikke har mulighet til å lagre data for å bekjempe grov kriminalitet. Dette må også forstås slik at myndighetene med dagens lovgivning ikke kan pålegge teleselskapene å lagre data for kriminalitetsbekjempende formål. Dette begrunnes i det faktum at lagring ut i fra kriminalitetsbekjempende formål krever særskilt hjemmel i lov. Slik hjemmel foreligger ikke da teleselskapenes hjemmel for lagring utelukkende bygger på kommunikasjons- og faktureringsformål.

5.3 Myndighetenes adgang til opplysninger lagret ut i fra andre formål

Som det fremkommer av drøftelsen under punkt 5.2 har norske teleselskaper hjemmel for lagring av trafikk- og lokaliseringsdata for kommunikasjons- og faktureringsformål. I realiteten innebærer dette at teleselskapene med rette sitter på trafikk- og lokaliseringsdata. Før vurderingen av myndighetenes adgang til trafikk- og lokaliseringsdata må det tas stilling til om myndighetene kan gis adgang til data for å bekjempe grov kriminalitet når opplysningene er lagret ut i fra andre formål.

Det kan stilles spørsmål ved hvorvidt personvernhensynet ivaretas tilstrekkelig dersom myndighetene gis adgang til opplysninger for å bekjempe grov kriminalitet når opplysningene er lagret ut i fra andre formål. Dersom norske myndigheter gis adgang til opplysninger for å bekjempe kriminalitet når informasjonen er lagret av hensyn til kommunikasjons- eller faktureringsformål kan dette ses på som en omgåelse av regelverket. Dette kan begrunnes ved at det ikke vil være like nødvendig med lovhjemmel om lagring av trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet. Myndighetene vil ved et slikt tilfelle uansett kunne få tilgang til opplysningene som teleselskapene har lagret ut i fra andre formål. For å bedre ivareta enkeltindividers rett til personvern burde norske myndigheter ikke gis adgang til opplysninger lagret ut i fra andre formål.

På den annen side vil hensynet til kriminalitetsbekjempelse trekke i retning av at myndighetene gis adgang til trafikk- og lokaliseringsdata lagret for andre formål. Teleselskapene har lovlig hjemmel for lagring etter ekoml. § 2-7 femte ledd. Dersom myndighetene har hjemmel som samsvarer med de krav som stilles for adgang til slike opplysningene, vil ikke dette innebære et direkte brudd på retten til personvern etter Grl. § 102 eller EMK art. 8.

Også av hensyn til samfunnets interesser vil det være ønskelig at myndighetene ved behov får adgang til denne type informasjon. Det kan for eksempel tenkes at man står ovenfor en sak om grov vold, drap eller for eksempel grov gjengkriminalitet. Politiet kan i slike tilfeller være avhengig av trafikk- og lokaliseringsdata for å kunne sikre tilstrekkelige bevis og dermed kunne avklare slike alvorlige saker. Siden teleselskapene allerede sitter på opplysningene vil det særlig i grove saker virke urimelig dersom myndighetene ikke får tilgang til avgjørende opplysninger. Det kan for eksempel tenkes at en sak på grunn av manglende bevis blir henlagt på bevisets stilling fremfor at gjerningspersonen blir stilt til ansvar. I en slik situasjon vil det ut i fra rimelighetsbetraktninger være naturlig at myndighetene har en mulig adgang til viktig informasjon fremfor at kriminelle går fri.

Det kan i tillegg nevnes at domstolen behandler de to spørsmålene separat. Grunnlaget for lagring av trafikk- og lokaliseringsdata skal i utgangspunktet ikke få betydning for hvorvidt adgang kan gis. Dette trekker i retning av at myndighetene kan gis adgang til opplysninger lagret ut i fra andre formål.

Det er i denne sammenheng hensiktsmessig å vise til professor Jon Petter Rui sin oppfatning av spørsmålet.[83] Ut i fra Rui sin vurdering åpner Tele2 dommen for at myndighetene skal kunne gis adgang til trafikk- og lokaliseringsdata for å bekjempe kriminalitet selv om informasjonen er lagret ut fra andre formål. Av hensyn til kriminalitetsbekjempelse og samfunnets interesser anses Rui sin konklusjon som treffende.

For den videre drøftelsen legges det til grunn at myndighetene, for å bekjempe grov kriminalitet, kan gis adgang til trafikk- og lokaliseringsdata som er lagret ut i fra andre formål.

5.4 Hjemmel for adgang til trafikk- og lokaliseringsdata

5.4.1 Norske regler for myndighetenes adgang

I det videre vurderes det om norske regler for myndighetens adgang til trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet er i samsvar med KVD art. 15 og EU-domstolens krav etter Tele2 dommen.

[83] Rui (2017) s. 163

Ekoml. skal i hovedsak sikre brukere av elektronisk kommunikasjon ved å verne retten til elektronisk kommunikasjon. Det er i hovedsak straffeprosessloven som hjemler muligheten til innsyn og adgang til historisk lagret informasjon om elektronisk kommunikasjon, herunder trafikk- og lokaliseringsdata.

I dag anvendes for det meste strpl. §§ 203 og 210 som hjemmel for myndighetenes adgang til trafikk- og lokaliseringsdata for bekjempelse av kriminalitet.[84] Også strpl. § 216 b andre ledd anvendes for politiets adgang til trafikk- og lokaliseringsdata i tilfeller av kommunikasjonskontroll. Det må dermed vurderes hvorvidt bestemmelsene er i samsvar med de krav som fremkommer av Tele2 dommen.

5.4.2 Lovpålagt taushetsplikt

Det første spørsmålet som oppstår ved myndighetenes adgang til trafikk- og lokaliseringsdata er om det kreves unntak av lovpålagt taushetsplikt.

Etter ekoml. § 2-9 plikter tilbyder og installatør «*å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon»*. Ut i fra en normal forståelse av lovens ordlyd omfatter «*bruk av elektronisk kommunikasjo*n» all informasjon om den faktiske bruken ved kommunikasjonen. Dette kan for eksempel være tidspunkt for kommunikasjonen, samt hvem de kommuniserende parter er og hvilke geografiske posisjon de har. Dette er i samsvar med den definisjon som er gitt av både trafikk- og lokaliseringsdata under punkt 1.2.1.[85] Ut i fra dette omfattes trafikk- og lokaliseringsdata av taushetsplikten etter ekoml. § 2-9. En slik forståelse fremgår også av ekomforskriften § 7-1. Etter bestemmelsens første ledd nevnes det uttrykkelig at «*tilbyder skal bevare taushet om trafikkdata etter ekomloven § 2-9 (...)»*. Trafikkdata omfattes utvilsomt av den lovpålagt taushetsplikt.

Som nevnt definerer ekomforskriften lokaliseringsdata som en underkategori av trafikkdata, jf. § 7-1 andre ledd. Taushetsplikten etter ekoml. § 2-9 må dermed forstås slik at også lokaliseringsdata omfattes av taushetsplikten. En slik forståelse er også naturlig da det ofte er gode grunner for å verne sterkere om lokaliseringsdata enn trafikkdata. Dette kan begrunnes ved at lokaliseringsdata lettere skaper en profil av vedkommendes bevegelsesmønster og slik sett er mer beskyttelsesverdig.

---

[84] Rui (2017) s. 166

[85] Vedrørende lovpålagt taushetsplikt skilles det slik sett ikke mellom trafikk- og lokaliseringsdata

Etter dette har tilbyder av telekommunikasjon som hovedregel taushetsplikt vedrørende den trafikk- og lokaliseringsdata de har lagret, jf. ekoml. § 2-9, jf. ekomforskriften § 7-1 første ledd. Myndighetenes adgang til trafikk- og lokaliseringsdata krever dermed opphevelse av teleselskapenes taushetsplikt.

Strpl. § 118 regulerer rettens mulighet for å ta i mot forklaring fra vitner angående taushetsbelagte opplysninger. Etter bestemmelsens første ledd kan teleselskapene fritas fra sin taushetsplikt overfor retten ved samtykke fra departementet. Tilsvarende gjelder ved forklaring til politiet, jf. § 230 første og tredje ledd. Departementets kompetanse etter bestemmelser er delegert til Nasjonal Kommunikasjonsmyndighet (heretter Nkom) ved delegasjonsvedtak 15. september 1995.[86]

Dersom Nkom gir sitt samtykke vil ikke taushetsplikten være til hinder for myndighetenes adgang til trafikk- og lokaliseringsdata. Et slikt samtykke vil medføre en opphevelse av taushetsplikten og innebære dermed en forutsetning for myndighetenes adgang til trafikk- og lokaliseringsdata med hjemmel i for eksempel strpl. § 203 eller § 210. I denne sammenheng må det understrekes at strpl. § 230, jf. § 118 ikke kan anvendes som selvstendig grunnlag for myndighetenes adgang til trafikk- og lokaliseringsdata, men som et vilkår ved at taushetsplikten må oppheves for de aktuelle opplysningene.[87]

5.4.3 Straffeprosessloven §§ 203 og 210

Som nevnt er det i hovedsak strpl. §§ 203 og 210, om henholdsvis beslag og utleveringspålegg, som anvendes for myndighetenes adgang til trafikk- og lokaliseringsdata.

Det faktum at bestemmelsene omhandler beslag og utleveringspålegg taler ikke i seg selv for at bestemmelsene omfatter adgang til trafikk- og lokaliseringsdata. Forutberegneligheten ved bestemmelsene er følgelig noe svekket, noe som kan fremstå som lite heldig for borgernes rettssikkerhet.

---

[86] Nkom: https://www.nkom.no/teknisk/taushetsplikt-og-personvern/elektroniske-spor/begjæringer-om-fritak-fra-tilbyders-taushetsplikt

[87] Det er i denne sammenheng verdt å vise til Bruce (2010) s. 12. Tidligere hadde man en praksis hvor teletilbydere frivillig kunne utlevere opplysninger ved å oppheve taushetsplikten. En slik praksis foreligger ikke i dag, og adgang til trafikk- og lokaliseringsdata hjemles i hovedsak etter strpl. §§ 203 og 210. Se blant annet Prop. 49 L (2010-2011) s. 94

Etter lovens ordlyd regulerer §§ 203 og 210 beslag og utleveringspålegg av «*ting*». En normal forståelse av begrepet ting innebærer konkrete faste gjenstander, som for eksempel fast eiendom og løsøre. Trafikk- og lokaliseringsdata er digitale spor, og vil normalt ikke anses som en fast gjenstand. I henhold til Tele2 dommens krav om klare og presise regler taler dette for at bestemmelsene ikke kan anvendes for adgang til trafikk- og lokaliseringsdata.

Det fremgår imidlertid av straffeloven § 69 andre ledd at ting også omfatter «*elektronisk lagret informasjon*».[88] En slik forståelse fremgår også av Høyesteretts praksis, jf. Rt. 1992 s. 904 på side 906. Dommen omhandlet påtalemyndighetenes begjæring om beslag av Televerkets utskrift av telefonoppringninger til og fra siktede. I dommen presiserer Høyesterett at ting også omfatter «*opplysninger som lagres på data …*». Som følge av rettspraksis og av hensynet til en ensartet rettstilstand må denne forståelse av begrepet «*ting*» også legges til grunn for straffeprosesslovens bestemmelser. At elektronisk lagret informasjon, herunder trafikk- og lokaliseringsdata, omfattes av begrepet «*ting*» trekker i retning av at strpl. §§ 203 og 210 kan anvendes for myndighetenes adgang til trafikk- og lokaliseringsdata.

Det fremgår tydelig av Tele2 dommen at lovgiver klart og presist skal angi under hvilke omstendigheter og på hvilke betingelser adgang til trafikk- og lokaliseringsdata kan bli aktuelt.[89] Det kan vanskelig sies at §§ 203 eller 210 oppfyller dette kravet. Både §§ 203 og 210 legger til grunn at beslag eller utlevering kan bli aktuelt dersom tingen «*antas å ha betydning som bevis*». Forhold som kan antas å ha betydning som bevis omfatter mye. Det stilles dermed ikke strenge krav til når det er tilstrekkelig sikkerhet for at informasjonen har betydning, og heller ikke under hvilke omstendigheter eller i hvilke sakstyper. Dette kan vanskelig sies å oppfylle EU-domstolens krav til å angi under hvilke omstendigheter og på hvilke betingelser adgang kan bli aktuelt.

Det kan også trekkes frem at det i Tele2 dommen legges til grunn at adgang til trafikk- og lokaliseringsdata skal besluttes av retten.[90] Dette for å sikre en forutgående kontroll av inngrep i grunnleggende rettigheter som retten til privatliv. Etter strpl. § 203 kreves det ikke forutgående kontroll av domstolene for gjennomføring av beslag. Påtalemyndighetens adgang til å bestemme

[88] Lov 20. mai 2005 nr. 28, straffeloven
[89] Tele2 dommen avsnitt 117
[90] Tele2 dommen avsnitt 120

om det skal tas beslag vil ikke være i tråd med EU-domstolens retningslinjer. Bestemmelsen ivaretar ikke enkeltindividers rett til personvern på en tilfredsstillende måte.

Det er i tillegg verdt å nevne at § 206 går ytterligere lengre med tanke på beslutningskompetanse for beslag. Etter bestemmelsen kan den enkelte politimann ta beslag uten beslutning fra påtalemyndigheten. Slik sett åpner loven opp for en vid adgang til at personer uten tung faglig juridisk kompetanse kan avgjøre at det skal tas beslag fra personer. Dersom myndighetene skal gis adgang til trafikk- og lokaliseringsdata gjennom reglene om beslag, vil det foreligge manglende forutgående kontroll for å sikre vernet av personopplysninger. Ut i fra dette kan ikke regelen om beslag anvendes som grunnlag for adgang til trafikk- og lokaliseringsdata.

Strpl. § 210 skiller seg fra § 203 når det gjelder forutgående kontroll. Det fremgår av bestemmelsen at retten kan «*pålegge besitteren å utlevere …*». Kompetansen til å beslutte utleveringspålegg tillegges dermed retten. En slik praksis vil være i tråd med EU-domstolens krav. Det er i denne sammenheng verdt å merke unntaket i andre og tredje ledd. Etter § 210 andre ledd kan påtalemyndighetene beslutte utlevering dersom det er fare for at etterforskningen vil lide ved påvente av beslutning fra retten. En slik kompetanse tillegges påtalemyndighetene også etter tredje ledd. Det at andre og tredje ledd gjør unntak fra rettens kompetanse om å beslutte utleveringspålegg syntes å være i strid med EU-rettens krav. Det er imidlertid verdt å nevne at EU-domstolen tar forbehold om rettens forutgående kontroll «*i behørigt begrundede hastende tilfælde*».[91] Det er dermed rom for det unntaket som følger av § 210 andre og tredje ledd. Etter dette er bestemmelsen, hva angår forutgående kontroll, i tråd med de krav Tele2 dommen stiller.

Det kan i denne sammenheng være hensiktsmessig å nevne hvordan utleveringspålegg praktiseres. Ved etterforskning av straffesaker tar påtalemyndighetene i all hovedsak beslutning om utleveringspålegg etter andre ledd, før senere kontroll etter første ledd. Det er ikke vanskelig å begrunne at opphold i adgangen til utleveringspålegg kan skade etterforskningen, slik § 210 andre ledd regulerer. Det kan dermed stilles spørsmål ved hvorvidt unntaket fra forutgående kontroll er tilstrekkelig klart og presist ved å angi under hvilke omstendigheter og på hvilke betingelser rettens forutgående kontroll kan unntas. At hovedregelen i praksis har blitt at

[91] Tele2 dommen avsnitt 120

påtalemyndighetene selv tar slike beslutningene vil ikke være i tråd med de strenge retningslinjene og den økende beskyttelse av personvern som EU praktiserer.

I forbindelse med Tele2 dommens krav om forutgående kontroll kan vilkåret om oppheving av taushetsplikten nevnes. Som nevnt under punkt 5.4.2 kreves det at taushetsplikten etter ekoml. § 2-9 oppheves dersom adgang skal bli aktuelt. At oppheving av taushetsplikten fungerer som et selvstendig grunnlag for myndighetenes adgang innebærer en form for ekstern forutgående kontroll ved at Nkom tar stilling til hvorvidt adgang kan bli aktuelt. Dette kan syntes å være forenelig med Tele2 dommens krav om forutgående kontroll. Likevel må det nevne at EU-domstolen presiserer at adgang til opplysningene skal besluttes av retten.[92] Selv om Nkom er et uavhengig organ kan ikke dette sammenlignes med en rettslig instans. I tillegg avgjør Nkom bare spørsmål om oppheving av taushetsplikten, og ikke hvorvidt øvrige vilkår for beslag eller utleveringspålegg er oppfylt. Den forutgående kontroll som Nkom gjennomfører medfører ikke at Tele2 dommens krav til rettslig forutgående kontroll er oppfylt.

I denne sammenheng er det verdt å nevne at Nkom sine vedtak kan klages inn til retten etter strpl. § 118 andre ledd, jf. § 230 fjerde ledd. Det foreligger dermed en mulighet for domstolskontroll ved Nkom sine avgjørelser om opphevelse av taushetsplikten. Rettens mulighet til å overprøve Nkoms avgjørelser vil likevel ikke innebære at Tele2 dommens vilkår om forutgående domstolskontroll er oppfylt. Dette kan begrunnes ved at en slik domstolskontroll med Nkoms vedtak bare innebærer en rettslig prøving av spørsmålet om oppheving av taushetsplikten, samt at domstolskontroll bare vil bli aktuelt i de tilfeller hvor det fremmes klage.

EU-domstolen oppstiller også et materielt krav om at den personen informasjonen omhandler må anses som mistenkt i saken.[93] Status som mistenkt får vedkommende normalt dersom politiet har en konkret mistanke om at vedkommende har begått en straffbar handling. Både §§ 203 og 210 befinner seg i strpl. del 4 om tvangsmidler og anses dersom utvilsomt som tvangsmidler. Etter strpl. § 82 legges det til grunn at en mistenkt får stilling som siktet dersom det besluttes «*beslag eller lignende forholdsregler rettet mot ham*.» Dette innebærer at vedkommende det rettes beslag eller utleveringspålegg mot automatisk får stilling som siktet i saken. Dette trekker i retning av at §§ 203 og 210 oppfyller EU-domstolens krav om at vedkommende må være mistenkt.

[92] Tele2 dommen avsnitt 120
[93] Tele2 dommen avsnitt 119

Ved Rt. 2011 s. 423 om beslag av bankbeløp i bankboks sa Høyesteretts ankeutvalg seg enig i lagmannsrettens konklusjon om at det må foreligge skjellig grunn til mistanke for at vilkårene for beslag er oppfylt.[94] På bakgrunn av at vilkårene her er tilsvarende for § 210, må det sies at dette også vil få betydning for utleveringspålegg. Det er i denne sammenheng verdt å merke seg at lagmannsretten, med støtte av Høyesterett, kommer til at kravet om mistenkt ikke nødvendigvis må rette seg mot den personen som beslaget rettes mot. En slik forståelse vil ikke være i tråd med EU-domstolens krav om at adgang til data kun kan gis «*vedrørende personer, der er mistænkt*».[95] Norske regler om beslag og utleveringspålegg er ikke i samsvar med de krav EU-domstolen oppstiller når det gjelder krav om at opplysningene må omhandle en mistenkt.

Det kan også sies at verken §§ 203 eller 210 er begrenset til grov kriminalitet. Bestemmelsene åpner for en vid adgang til beslag og utleveringspålegg uavhengig av sakens omfang og strafferamme. En slik adgang vil ikke være i tråd med EU-domstolen krav om at unntak fra hovedregel om kommunikasjonsfortrolighet er begrenset til det strengt nødvendige og bare tilfeller av grov kriminalitet.[96]

Etter Tele2 dommens retningslinjer vil det være vanskelig å forsvare bruk av §§ 203 og 210 som hjemmel for myndighetenes adgang til trafikk- og lokaliseringsdata.

5.4.4 Straffeprosessloven § 216 b andre ledd bokstav d

Som nevnt under punkt 1.2.2 innebærer strpl. § 216 b andre ledd bokstav d et unntak fra hovedregelen om at kommunikasjonskontroll bare omhandler nåtidig og fremtidig data. Det vil dermed være behov for en vurdering av hvorvidt § 216 b andre ledd bokstav d om kommunikasjonskontroll av historisk data er i tråd med EU-domstolens retningslinjer.

Strpl. § 216 b andre ledd bokstav d regulerer blant annet politiets adgang til «*data knyttet til kommunikasjonen, og den geografiske posisjonen til et slikt anlegg».* Ut i fra ordlyden omfattes trafikk- og lokaliseringsdata av bestemmelsen. Denne forståelse fremgår også av lovens forarbeider.[97] Det kan dermed sies at lovgivers ønske ved bestemmelsen er å åpne opp for

[94] Tele2 dommen avsnitt 11 sammenholdt med avsnitt 16
[95] Tele2 dommen avsnitt 119
[96] Tele2 dommen avsnitt 115
[97] Ot.prp.nr. 64 (1998-1999) s. 159

myndighetenes adgang til historisk trafikk- og lokaliseringsdata dersom lovens øvrige vilkår er oppfylt.

Selv om lovgivers ønske med bestemmelsen er å åpne for politiets adgang til trafikk- og lokaliseringsdata innebærer ikke dette uten videre at bestemmelsen er i samsvar med etterfølgende praksis. Hvorvidt myndighetene har tilstrekkelig hjemmel etter § 216 b andre ledd bokstav d må vurderes ut i fra EU-domstolens krav etter Tele2 dommen.

Det fremgår av lovens ordlyd at kontroll etter § 216 b avhenger av rettens kjennelse og at det må foreligge skjellig grunn til mistanke. EU-domstolens krav om forutgående domstolskontroll og kravet om mistenkt er oppfylt. Det faktum at det foreligger en hastekompetanse etter § 216 d får ikke betydning. Det avgjørende vil være hvorvidt strpl. § 216 b ivaretar et legitimt formål ved bekjempelse av grov kriminalitet, samt er tilstrekkelig klar og presis for å ivareta EU-domstolens strenge nødvendighetskrav.[98]

Anvendelse av strpl. § 216 b andre ledd bokstav d avhenger av hvorvidt det foreligger skjellig grunn til mistanke for en handling som beskrevet etter bestemmelsens første ledd. Etter strpl. § 216 b første ledd bokstav a kan kontroll iverksettes dersom mistanken gjelder en handling som kan medføre straff med fengsel i 5 år eller mer. At det foreligger en begrensning ut i fra kriminalitetens strafferamme taler for at det bare er mulighet for adgang til trafikk- og lokaliseringsdata når det er snakk om grov kriminalitet. Kravet om at formålet må være å bekjempe grov kriminalitet syntes å være oppfylt.

Det er i denne sammenheng verdt å nevne generaladvokat Saugmandsgaard sin uttalelse i sak C-207/16. I forbindelse med uttalelsen er det viktig å presisere at uttalelsen ikke er rettslig bindende. Generaladvokatens uttalelse er et forslag til den sak som er forelagt for EU-domstolen. Det kan ikke tas for gitt at forslaget fra generaladvokaten tas til følge.[99] Metodisk kan forslaget likestilles med juridisk teori og vil ha vekt deretter.

Saken omhandler spanske myndigheters avslag på utlevering av sivilstandsopplysninger i forbindelse med etterforskning av en kriminell handling. Avslaget ble begrunnet ved at de

[98] Tele2 dommen avsnitt 115
[99] EU-opplysning, Danmark: http://www.eu.dk/da/spoergsmaal-og-svar-folder/hvad-er-en-generaladvokat

faktiske omstendigheter ikke ble ansett som en alvorlig forbrytelse.[100] Den regionale domstol i Tarragona rettet spørsmål til EU-domstolen om hvor grensen for alvorlig forbrytelse går i forbindelse med adgang til personopplysninger lagret av teleoperatør.[101] Ved spørsmål om hvorvidt spansk lov sin minimumsgrense på tre år var forenelig med de krav som fulgte av EU-retten i blant annet Tele2 dommen uttalte Saugmandsgaard at statene selv bestemmer minimumsgrensen for straff.[102] Det avgjørende vil være at forbudet mot å lagre og anvende personopplysninger ikke endrer karakter.[103]

Etter strpl. § 216 b første ledd bokstav a har norske myndigheter lagt til grunn en strafferamme på 5 år for adgang til trafikk- og lokaliseringsdata. Ut i fra Saugmandsgaard sin uttalelse vil myndighetene selv kunne avgjøre minimumsgrensen for straff. En slik forståelse trekker i retning av at bestemmelsen er i samsvar med Tele2 dommens krav om grov kriminalitet. Likevel kan det sies at en vesentlig andel av straffelovens bestemmelser inneholder en strafferamme på 5 år eller mer. Minimumsgrensen på 5 år vil innebære at det foreligger mulighet for adgang til trafikk- og lokaliseringsdata ved et stort antall straffesanksjonerte overtredelser. Dette kan tale for at forbudet mot adgang til personopplysninger til en viss grad endrer karakter, og slik sett ikke er forenelig med det grunnleggende utgangspunktet om kommunikasjonsfortrolighet.

Det er også verdt å merke at generaladvokat Saugmandsgaard tar til orde for at vurderingen av hvorvidt den kriminelle handling kan anses som tilstrekkelig alvorlig ikke alene avhenger av den aktuelle strafferammen.[104] Saugmandsgaard mener at straffen har en vesentlig betydning, men at det også må tas hensyn til andre objektive faktorer i det enkelte tilfellet. Dette kan for eksempel være forsett, skjerpede omstendigheter, gjentakelsestilfeller, samfunnsinteresse, skader eller strafferamme. Det presiseres at listen ikke er uttømmende.[105] Ut i fra dette vil reglene om hvorvidt forholdet er av tilstrekkelig alvorlig karakter måtte bedømmes konkret for hvert enkelt tilfelle ut i fra de konkrete omstendigheter som foreligger. At norske myndigheter har besluttet en strafferamme på 5 år for å tillate adgang kan etter dette ikke i seg selv tilsi at bestemmelsen er uforenelig med kravet om grov kriminalitet.

[100] C-207/16 avsnitt 2
[101] C-207/16 avsnitt 3
[102] C-207/16 avsnitt 121
[103] C-207/16 avsnitt 114
[104] C-207/16 avsnitt 104
[105] C-207/16 avsnitt 105

Det må også nevnes at § 216 c inneholder et generelt og alminnelig vilkår for kommunikasjonskontroll. Etter bestemmelsen kan kommunikasjonskontroll «*bare gis dersom det må antas at slik avlytting eller kontroll vil være av vesentlig betydning for å oppklare saken …*». Ved denne begrensningen avgrenses kommunikasjonskontroll til det strengt nødvendige. Etter dette syntes strpl. § 216 b første ledd bokstav a å være i samsvar med de krav som stilles til streng straff ved å angi en strafferamme på 5 år, samt at Tele2 dommens vilkår om nødvendighet ivaretas ved vilkåret etter § 216 c.

Som nevnt innebærer Tele2 dommen også et krav om klarhet og presisjon til de bestemmelser som skal anvendes for adgang til trafikk- og lokaliseringsdata.[106] Det kan her stilles spørsmål ved hvorvidt strpl. § 216 b første ledd bokstav a inneholder presise regler som angir under hvilke omstendigheter og på hvilke betingelser adgang kan bli aktuelt.[107] Etter bestemmelsen er det klart at samtlige handlinger med strafferamme på minimum 5 år kan være grunnlag for adgang til data, så sant øvrige vilkår er oppfylt. Det foreligger ingen begrensning i hvilke type kriminalitet som må foreligge. Dette kan vanskelig forenes med Tele2 dommens krav om klarhet og presisjon. Etter dette oppfyller strpl. § 216 b første ledd bokstav a ikke Tele2 dommens strenge retningslinjer ved klarhet og presisjon.

Det kan også nevnes at det ved lovendring i 1999 skjedde en utvidelse av anvendelsesområdet i strpl. kapittel 16 a.[108] Tidligere ga kapittelet hjemmel for telefonavlytting ved etterforskning av narkotikakriminalitet.[109] En presisering ved at bestemmelsene i kapittelet, herunder § 216 b, bare kan anvendes ved en type kriminalitet vil være mer forenelig med Tele2 dommens krav om klarhet og presisjon. En utvidelse ved å tillate generell kommunikasjonskontroll kan ikke sies å være i tråd med EU-domstolens ønske om klare og presise regler som angir under hvilke omstendigheter adgang kan gis.

Med tanke på manglende klarhet og presisjon oppfyller ikke strpl. § 216 b andre ledd bokstav d, jf. førte ledd bokstav a Tele2 dommens krav. Dette begrunnes ytterligere ved at man befinner seg i kjernen av legalitetsprinsippet og at inngrep dermed krever klar hjemmel i lov, samt at EU-

[106] Tele2 dommen avsnitt 117
[107] Tele2 dommen avsnitt 117
[108] Endringslov 3. desember 1999 nr. 82 punkt IV
[109] Ot.prp. nr. 64 (1998-1999) s. 155

domstolen uttrykkelig presiserer at unntak fra hovedregelen om kommunikasjonsfortrolighet må «*fortolkes strengt*».[110]

Når det gjelder strpl. § 216 b første ledd bokstav b inneholder bestemmelsen en oppramsing av konkrete bestemmelser hvor kommunikasjonskontroll kan bli aktuelt. En slik oppramsing av aktuelle straffebud vil være i tråd med kravet om klare og presise regler som angir under hvilke omstendigheter og betingelser adgang kan bli aktuelt. Ved dette alternativet vil det uansett være tvilsomt hvorvidt kravet til grov kriminalitet er oppfylt. Flere av bestemmelsene etter bokstav b har en øvre strafferamme på fengsel i inntil 1 år. Dette kan vanskelig forenes med kravet om grov kriminalitet. I denne sammenheng må det igjen vises til generaladvokat Saugmandsgaard sin uttalelse. Saugmandsgaard sin oppfatning er at det ikke bare er strafferammen som er avgjørende for hvorvidt forholdet er tilstrekkelig alvorlig. Dette tyder på at bestemmelsens strafferamme ikke hindrer at forholdene kan anses som grov kriminalitet.

Det må likevel presiseres at samtlige av de femten bestemmelsene som nevnes i § 216 b første ledd bokstav b har en øvre strafferamme på 6 år eller mindre. Dette i seg selv taler mot at bestemmelsen regulerer grov kriminalitet. Det kan også nevnes at de aktuelle bestemmelsene syntes å innebære mindre alvorlige forhold sett ut i fra straffelovens systematikk. Som eksempel kan nevens at av totalt tjue bestemmelser i strl. kapittel 17 er det totalt syv bestemmelser som har en strafferamme på 6 år eller mindre. Seks av disse er hjemlet i strpl. § 216 b første ledd bokstav b. Bestemmelsene med høyest strafferamme i strl. kapittel 17, og slik sett bestemmelsene av mest alvorlig karakter, er holdt utenfor anvendelsesområde til § 216 b. Etter dette er det vanskelig å forsvare at strpl. § 216 b første ledd bokstav b utelukkende regulerer forhold av alvorlig kriminalitet.

Ut i fra denne vurderingen vil strpl. § 216 b andre ledd bokstav d i større grad enn §§ 203 og 210 ivareta de krav som EU-domstolen stiller. Likevel er det tvilsomt hvorvidt bestemmelsen ivaretar det strenge nødvendighetskravet ved at det kreves klare og presise regler, samt formålet ved at inngrep bare er aktuelt av hensyn til grov kriminalitet. På bakgrunn av legalitetsprinsippet og som fremhevet av EU-domstolen kreves det at unntak fra hovedregelen må fortolkes strengt.[111] Dette forsterker ytterligere det faktum at bestemmelsen ikke kan anvendes for myndighetenes adgang til trafikk- og lokaliseringsdata.

[110] Tele2 dommen avsnitt 89
[111] Tele2 dommen avsnitt 89

Strpl. § 216 b andre ledd bokstav d oppfyller ikke Tele2 dommens krav for myndighetenes adgang til trafikk- og lokaliseringsdata.

5.4.5 Ekomloven § 2-9 tredje ledd

Det er også verdt å nevne at ekoml. § 2-9 tredje ledd gjør unntak fra hovedregelen om taushetsplikt.

Etter bestemmelsens ordlyd er taushetsplikten ikke til hinder for at det «*gis opplysninger til påtalemyndighetene eller politi om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse.*» Lovens ordlyd er noe uklar angående hva som menes med avtalebasert hemmelig telefonnummer og andre abonnementsopplysninger. Bruk av formuleringen «*andre abonnementsopplysninger*» tyder på at bestemmelsen fokuserer på abonnementsopplysninger alene. Dette vil medføre at man er utenfor definisjonen av trafikk- og lokaliseringsdata som konsentrerer seg om selve kommunikasjonen.

Ut i fra lovens forarbeider må lovens ordlyd forstås slik at avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger omfatter opplysninger om bruker av et abonnement, som for eksempel telefonnummer knyttet til en telefon, serienummer, opplysninger om SIM-kort og andre opplysninger om selve abonnementet. Slike opplysninger forutsetter imidlertid at politiet selv er klar over oppkoblingstidspunktet.[112] På bakgrunn av dette fokuserer begrepene i bestemmelsen på opplysninger om selve abonnementet. Dette vil falle utenfor trafikk- og lokaliseringsdata som omhandler opplysninger om den faktiske kommunikasjonen og trekker i retning av at unntaket etter § 2-9 tredje ledd ikke omfatter trafikk- og lokaliseringsdata.

Ekomlovens forarbeider kan også brukes som selvstendig grunnlag for vurderingen av hvorvidt trafikkdata omfattes av unntaket fra taushetsplikt etter § 2-9 tredje ledd. I forarbeidene presiseres det at «*Også annen informasjon som bare gir opplysninger om bruker av et abonnement eller en telefon omfattes av tredje ledd …*».[113] Det at bestemmelsen gjelder informasjon som bare gir opplysninger om bruker, innebærer en avgrensning mot informasjon om selve kommunikasjonen og følgelig trafikk- og lokaliseringsdata. Ut i fra dette omfatter ikke ekoml. § 2-9 tredje ledd

[112] Ot.prp.nr. 58 (2002-2003) s. 93-94
[113] Ot.prp. nr. 58 (2002-2003) s. 93-94

denne type data, og kan dermed ikke brukes som hjemmel for myndighetenes adgang til trafikk- og lokaliseringsdata.

Som nevnt inneholder ekoml. § 2-9 tredje ledd også unntak fra taushetsplikten ved «*elektronisk kommunikasjonsadresse*». Videre må det tas stilling til hvorvidt «*elektronisk kommunikasjonsadresse*» omfatter trafikk- og lokaliseringsdata.

Etter lovens forarbeider innebærer elektronisk kommunikasjonsadresse navn, adresse og telefonnummer knyttet til den elektroniske kommunikasjonsadressen.[114] Dette innebærer rene abonnementsopplysninger, det vil si opplysninger som knytter bruker av tjenesten opp mot et bestemt telefonnummer.[115] Når det gjelder trafikk- og lokaliseringsdata er disse opplysningene knyttet til den aktuelle kommunikasjonen. Slik sett anses ikke elektronisk kommunikasjonsadresse som en form for trafikk- og lokaliseringsdata. En slik forståelse fremgår også av rettspraksis. I Rt. 1999 s. 1944 på side 1950 uttalte Høyesterett at Teleloven § 9-3 tredje ledd ikke omfattet trafikkdata.[116] Saken gjaldt taushetspliktens rekkevidde ved anonym formidling av barnepornografiske bilder på internett. Det er her verdt å merke seg at dommen omfatter tidligere lov om telekommunikasjon, teleloven, nå opphevet og erstattet av ekomloven. Teleloven § 9-3 tredje ledd er nærmest tilsvarende lik ekoml. § 2-9 tredje ledd om taushetsplikt. Det er ingenting som tilsier en realitetsendring på dette området. Dette fremgår også av ekomlovens forarbeider som presiserer at «*bestemmelsen må sees på bakgrunn av Høyesteretts dom i RT-1999-1544.*»[117] Dommen får dermed avgjørende betydning ved tolkningen av ekoml. § 2-9 tredje ledd og trekker i retning av at trafikkdata ikke omfattes av unntaket fra taushetsplikten.

Det er også hensiktsmessig å se på unntaket i ekoml. § 2-9 tredje ledd i sammenheng med bestemmelsens øvrige innhold. Etter § 2-9 første ledd gjelder taushetsplikten for innholdet av kommunikasjonen og andres bruk. Trafikk- og lokaliseringsdata omfattes av taushetsplikten etter første ledd.[118] Unntaket i tredje ledd har ikke tilsvarende ordlyd. Det er nærliggende å anta at lovgiver ville brukt tilsvarende ordlyd som første ledd dersom meningen var at unntaket fra

[114] Ot.prp. nr. 58 (2002-2003) s. 93
[115] Hansen (2010) s. 4
[116] Lov 23. juni 1995 nr. 39 (opphevet)
[117] Ot.prp. nr. 58 (2002-20003) s. 93-94
[118] Se oppgaven punkt 5.4.2

taushetsplikten skulle omfatte trafikk- og lokaliseringsdata. Dette taler for at unntaket etter tredje ledd ikke omfatter denne type informasjon.

Ut i fra lovens vage ordlyd, forarbeidene og rettspraksis konkluderes det med at unntaket fra taushetsplikten etter ekoml. § 2-9 tredje ledd første punktum ikke omfatter trafikk- og lokaliseringsdata.

Det konkluderes med at de norske bestemmelsene om myndighetenes adgang til trafikk- og lokaliseringsdata ikke er i samsvar med de krav Tele2 dommen stiller. Norske myndigheter har følgelig ikke hjemmel for adgang til trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet.

6. Vurdering av norsk rett i forhold til statens positive forpliktelser

Debatten rundt hvorvidt myndighetene bør gis adgang til trafikk- og lokaliseringsdata bygger på mange ulike motstridende hensyn. Hensyn til personvernet bør trekkes frem som et grunnleggende hensyn mot å gi myndighetene en slik adgang. I tillegg foreligger det fare for konstant overvåkning og kontroll av befolkningen dersom adgang til trafikk- og lokaliseringsdata gis, noe som klart vil stride mot en rettsstats grunnleggende verdier. Det kan også sies at det ved en utstrakt adgang kan være fare for misbruk og at uskyldige tredjepersoner, som for eksempel ikke er mistenkt, blir rammet av den adgangen som gis. I motsatt retning trekker hensynet til kriminalitetsbekjempelse. Politiet har som hovedoppgave å bekjempe kriminaliteten i samfunnet. Ved adgang til flere opplysninger vil et slikt formål lettere og mer effektivt kunne oppnås. Det vil være i både enkeltpersoners og samfunnets interesse at kriminelle forhold blir avklart.

Det er mange og delte meninger om i hvilke grad myndighetene bør gis adgang til trafikk- og lokaliseringsdata. Motstridende hensyn er mange og debatten har pågått i flere år. En oppramsing av hensyn for og mot syntes dermed allerede å foreligge. Det vil være av større interesse å se på hvorvidt myndighetene har en positiv plikt til å legge til rette for myndighetenes mulighet for adgang til trafikk- og lokaliseringsdata.[119]

Grl. § 92 og EMK art. 1 pålegger staten å sikre og respektere grunnleggende menneskerettigheter. Denne sikringsplikten omfatter både en negativ og en positiv plikt. Den negative forpliktelsen innebærer en plikt til selv å avstå fra å krenke, mens den positive plikten omfatter en plikt til å aktivt motvirke at andre krenker grunnleggende rettigheter. I denne sammenheng er det interessant å stille spørsmål ved hvorvidt myndighetene har en positiv plikt til å aktivt motvirke at andres grunnleggende rettigheter blir krenket ved å legge til rette for adgang til trafikk- og lokaliseringsdata for å bekjempe kriminalitet.

Statens positive plikt til å sikre grunnleggende rettigheter ved å legge til rette for adgang til trafikk- og lokaliseringsdata har tidligere vært behandlet av EMD ved saken K.U mot Finland.[120] Dommen er relevant for Norsk rett siden Norge har ratifisert EMK.[121] EMD er etablert for å håndheve og kontrollere at konvensjonens bestemmelser blir oppfylt. Domstolens avgjørelser får dermed betydning for hvilke forståelse man skal legge til grunn ved tolkning av

[119] Spørsmålet er også behandlet av Bruce (2010) s. 23-26
[120] EMD dom 2. desember 2008
[121] Lov 21. mai 1999 nr. 30, § 2 nr. 1

konvensjonsbestemmelsene. I forbindelse med dommens relevans er det verdt å merke seg at det er likhetstrekk mellom finsk og norsk rett når det gjelder myndighetenes adgang til data for å bekjempe kriminalitet. Under saken fantes det ingen finsk lovhjemmel som påla tjenestetilbydere å gjøre unntak fra taushetsplikten for å gi politiet adgang til den informasjonen de trengte for å bekjempe grov kriminalitet. I Norge gis det stadig adgang til trafikk- og lokaliseringsdata med hjemmel i strpl. §§ 203, 210 og § 216 b andre ledd bokstav d. Som konkludert med under punkt 5.4 oppfyller ikke bestemmelsene Tele2 dommens krav. I likhet med Finland har heller ikke norsk rett hjemmel for adgang til trafikk- og lokaliseringsdata. Saken K.U mot Finland er dermed av klar relevans.

K.U mot Finland omhandler en finsk statsborger på 12 år som ble utsatt for at en fremmed mann spredte personopplysninger om han på internett i form av en kontaktannonse angående seksuell adferd. Forholdene krenket utvilsomt guttens rett til privatliv etter EMK art. 8.[122] På bakgrunn av den lovpålagte taushetsplikten ved telekommunikasjon i finsk lov, fikk ikke politiet identifisert vedkommende som la ut opplysningene om gutten. Finsk lov hadde ingen hjemmel som forpliktet tjenesteyteren til å gjøre unntak fra taushetsplikten for å avdekke informasjonen. Dette medførte at vedkommende som krenket guttens rett til privatliv ikke kunne identifiseres og gikk dermed fri. Guttens far tok saken inn for EMD med anførsel om at staten ikke hadde oppfylt sine positive forpliktelser ved å beskytte retten til privatliv etter EMK art. 8.[123]

I dommen presiserer EMD at staten er positivt forpliktet til å iverksette tiltak for å sikre respekt for privatlivet.[124] I denne sammenheng måtte det kunne kreves at staten foretok effektive grep for å kunne indentifisere og straffeforfølge den som la ut annonsen. Det er dermed naturlig å forstå dommen slik at det kreves at myndighetene sørger for lovhjemler for å effektivt ivareta og sikre borgernes grunnleggende rettigheter. Dette tilsvarer den positive siden av sikringsplikten etter EMK art. 1 og Grl. § 92 som krever at staten aktivt avverger krenkelser av grunnleggende rettigheter.

Som det fremgår av K.U mot Finland vil det å ikke kunne identifisere og straffeforfølge lovbrytere kunne medføre et brudd i statens positive forpliktelser til å ivareta andre enkeltindividers grunnleggende rettigheter. Selv om adgang til trafikk- og lokaliseringsdata kan

[122] K.U mot Finland avsnitt 41
[123] K.U mot Finland avsnitt 3
[124] K.U mot Finland avsnitt 46

innebære et inngrep i retten til personvern mot den mistenkte, vil et slik inngrep være lovlig dersom det foreligger hjemmel i lov, inngrepet ivaretar et legitimt formål og er forholdsmessig. Det vil av hensyn til offeret for den kriminelle handlingen være større beskyttelsesinteresse ovenfor vedkommende enn for den som er mistenkt i saken. Dette tilsier at det vil være i strid med statens sikringsplikt å ikke ha tilstrekkelige hjemler for myndighetenes adgang til trafikk- og lokaliseringsdata.

Dersom myndighetene står ovenfor en situasjon hvor de ikke har tilstrekkelig bevis for å avklare en alvorlig straffesak vil det å undersøke trafikk- og lokaliseringsdata kunne få avgjørende betydning for sakens utfall. For at staten skal kunne ivareta sine positive forpliktelser med tanke på å avverge og straffeforfølge alvorlig kriminalitet må det legges til rette for at myndighetene har lovlig hjemmel for adgang til trafikk- og lokaliseringsdata. På bakgrunn av dette kan det sies at staten er positivt forpliktet til å regulere myndighetenes adgang til trafikk- og lokaliseringsdata.

7. Avsluttende bemerkninger

7.1 Behov for regler om lagring

Som konkludert med har ikke norske myndigheter hjemmel for lagring av trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet. Dette syntes uproblematisk dersom myndighetene kan få adgang til informasjon lagret ut i fra andre formål. Det kan i denne sammenheng være interessant å se på teleselskapenes utvikling av abonnementer.[125]

De siste årene har det blitt stadig vanligere med mobilabonnementer med fastpris. En slik utvikling kan medføre at teleselskapenes grunnlag for lagring av hensyn til faktureringsformål blir redusert. Det kan da tenkes at teleselskapene lagrer færre opplysninger, og myndighetenes mulighet til adgang blir på den måten redusert. Gitt en slik utvikling kan det i denne sammenheng spørres hvorvidt myndighetene er positivt forpliktet til å vedta lovgivning om myndighetenes mulighet for lagring av trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet. Etter K.U mot Finland er det nærliggende å anta at staten har en positiv forpliktelse til å sørge for hjemmel om lagring for å kunne ivareta enkeltindividers grunnleggende rettigheter på en tilfredsstillende måte. Det er likevel verdt å merke seg at dommen omhandlet retten til adgang. Det kan dermed stiles spørsmål ved hvorvidt K.U mot Finland kan trekkes så langt at den også gjelder lagring.

I denne sammenheng kan det sies at teleselskapenes prisutvikling kan ha ført til at det er mindre behov for å lagre lokaliseringsdata enn trafikkdata av hensyn til faktureringsformål. Særlig innen EU og EØS er det ikke lengre ulike priser avhengig av geografisk plassering. Teleselskapene vil da ikke være avhengig av å lagre den geografiske posisjonen ved kommunikasjonen for å kunne fakturere brukerne riktig. Dette kan redusere teleselskapenes behov for lokaliseringsdata. Likevel er myndighetenes behov for lokaliseringsdata av kriminalitetsbekjempende formål like stort, om ikke større. Mennesker forflytter seg fortere og kriminalitet skjer i stadig større omfang på tvers av landegrensene. En slik utvikling forsterker det faktum at myndighetene innenfor visse rammer bør ha mulighet til å lagre lokaliseringsdata for å bekjempe grov kriminalitet.

Teleselskapenes grunnlag for lagring av data er i endring, noe som kan innebære at mindre data blir lagret. Likevel har denne informasjonen stor nytteverdi for myndighetene ved oppklaring av kriminelle forhold.

[125] Problemstillingen er også nevnt av Bruce (2010) s. 9

7.2 Behov for regler om adgang

Som konkludert med har ikke norske rett tilstrekkelige klare og presise regler om myndighetenes adgang til trafikk- og lokaliseringsdata for bekjempelse av grov kriminalitet. Som vi har sett ved K.U mot Finland kan statens positive forpliktelse i enkelte tilfeller bare ivaretas dersom det foreligger en mulighet for adgang til trafikk- og lokaliseringsdata for å forebygge, avverge eller oppklare alvorlig kriminalitet. Ut i fra dette vil dagens rettstilstand ikke være holdbar i henhold til våre konvensjons- og folkerettslige forpliktelser.

Det er her hensiktsmessig å ta frem igjen skillet mellom trafikk- og lokaliseringsdata. Siden lokaliseringsdata sier noe om en privatpersons geografiske plassering vil opplysningene lettere skape en personlig profil av vedkommende. Siden lagring og adgang skal begrenses til det strengt nødvendige, er det naturlig å forstå det slik at det bør være strengere regulering for lokaliseringsdata enn for trafikkdata.

For at myndighetene skal ivareta deres forpliktelser kreves det for det første at det ikke gis adgang til trafikk- og lokaliseringsdata med de mangelfulle bestemmelsene som anvendes i dag. Slik adgang vil være et brudd på retten til privatliv etter både EMK art. 8 og Grl. § 102.

Staten har også gjennom sine positive forpliktelser en plikt til å ivareta borgernes grunnleggende rettigheter ved å legge til rette for myndighetenes adgang til trafikk- og lokaliseringsdata. Det faktum at myndighetene har vedtatt lovregler som regulerer adgang til trafikk- og lokaliseringsdata uten at reglene har trådt i kraft er ikke tilstrekkelig.

8. Litteratur- og kildeliste

8.1 Lover

8.1.1 Norske lover

Lov 17. mai 1814 Grunnloven (Grl.)

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven, strpl.)

Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtalen om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)

Lov 23. juni 1995 nr. 39 om telekommunikasjon (teleloven)

Lov 4. august 1995 nr. 53 om politiet (politiloven, pl.)

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven, mrl.)

Lov 3. desember 1999 nr. 82 om endringer i straffeprosessloven og straffeloven m.v. (etterforskningsmetoder m.v.)

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven, popplyl.)

Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven, ekoml.)

Forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)

Lov 20. mai 2005 nr. 28 om straff (straffeloven, strl.)

Lov 19. Juni 2009 nr. 103 om tjenestevirksomhet (tjenesteloven)

Lov 15. april 2011 nr. 11 om endring av ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) – *ikke trådt i kraft*

8.1.2 Internasjonale regelverk

Convention for the Protection of Human Rights and Fundamental Freedoms, 4. Nov 1950, (EMK)

Svensk lovgivning: Lag (2003:389), 12. juni 2003 om elektronisk kommunikation

8.2 EU- og EØS-rettsakter

Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Kommunikasjonsverndirektivet, KVD)

EØS-komiteens beslutning nr. 80/2003 av 20. juni 2003 om endring av EØS-avtalens vedlegg XI

Directive 2006/24 EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EU (Datalagringsdirektivet, DLD)

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (Tjenestedirektivet)

Charter of fundamental right of the European Union, 2012, C 326/02

GDPR: Regulation 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU (General Data Protection Regulation)

8.3 Forarbeider og utredninger

Ot.prp. nr. 64 (1998-1999) Lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv.)

Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven)

Ot.prp. nr. 70 (2008-2009) Om tjenestevirksomhet (tjenesteloven)

Prop. 49 L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Prop. 50 S (2010-2011) Samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse i EØS-avtalen av direktiv 2006/24/EF om lagring av data fremkommet ved bruk av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett (datalagringsdirektivet)

Dok. nr. 16 (2011-2012) Rapports fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven

Innst. 186 S (2013-2014) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Foss, Kolberg, Nybakk, Christensen, Anundsen, Langeland, Lundteigen, Bekkevold og Grande om grunnlovfesting av sivile og politiske menneskerettigheter

NOU 2015: 13 Digital sårbarhet – sikkert samfunn, Beskyttelse av enkeltmennesker og samfunn i en digitalisert verden

Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Prop. 56 LS (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen

8.4 Rettspraksis

Norsk rettspraksis

Rt. 1896 s. 530 – Aars-dommen

Rt. 1952 s. 1217 – To mistenkelige personer

Rt. 1992 s. 904

Rt. 1999 s. 1944

Rt. 2011 s. 423

Rt. 2014 s. 1105

HR-2016-1286-A

Annen rettspraksis

Case Amann v. Switzerland, Menneskerettighetsdomstolen (EMD) 16. februar 2000, saksnummer 27798/95

Case of Copland v. The United Kingdom, 3. april 2007, Menneskerettighetsdomstolen (EMD), saksnummer 62617/00

Case of K.U v. Finland, 2. desember 2008, Menneskerettighetsdomstolen (EMD), saksnummer 2982/02

Digital Rights Irland og Kärnter Landesregierung, EU-domstolen, C-293/12 og C-594/12, storkammerdom 8. april 2014

Google-dommen, EU-domstolen, C-131/12, 13. mai 2014

Safe Harbor-dommen, EU-domstolen, C-362/14, 6. oktober 2015

Tele2 Sverige AB og Watson og andre, EU-domstolen, C-203/15 og C-698/15, storkammerdom 21. desember 2016

Forslag til avgjørelse fra generaladvokat H. Saugmandsgaard Øe, EU-domstolen, C-207/16, fremsatt 3. mai 2018 (1)

8.5 Artikler og bøker

Bruce, Ingvild, «Datalagringsdirektivet – en menneskerettskrenkelse eller –forpliktelse», *Lov Og Rett* (trykt Utg.)., Årg. 49, nr. 1-2, 2010, s. 6-26

Hansen, Eirik Trønnes, «Datalagringsdirektivet og politiets behov», *LoD, 2010 s. 102-126*, utgiver: Lovdata

Sejersted, F. (2011). *EØS-rett* (3. utg. ed.). Oslo: Universitetsforlaget

Fredriksen, Halvard H., «Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten». *Jussens Venner (trykt Utg.)., Vol.48, nr 9 (2013)*, s. 371-399

Fredriksen, H., & Mathisen, G. (2014). *EØS-rett* (2.utg.ed.). Bergen: Fagbokforl.

Fossum, Eriksen & Fossym, John Erik (2014). *Det Norske paradoks : Om Norges forhold til Den europeiske union*. Oslo: Universitetsforl.

Arnesen, F., & Stenvik, A. (2015), *Internasjonalisering og juridisk metode : Særlig om EØS-rettens betydning i norsk rett* (2. utg. ed.)

Rui, Jon Petter, "Fra EU-domstolen ; grenser for myndighetenes lagring av og tilgang til trafikk- og lokaliseringsdata : Tele2 Sverige AB og Watson og andre, C-203/15 og C-698/15, storkammerdom 21. desember 2016." *Tidsskrift for Strafferett*, 2017, 17 (2), s.146-168

8.6 Andre kilder:

Datatilsynet, «*Safe Harbor-beslutningen kjent ugyldig*», publisert 6. oktober 2015, sist sjekket 26. mai 2018, https://www.datatilsynet.no/aktuelt/2015/safe-harbor-beslutningen-kjent-ugyldig2/

Datatilsynet, *«Hva blir nytt med forordningen?»,* publisert 18. februar 2016, sist sjekket 26. mai 2018, https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/hva-blir-nytt-med-forordningen/

Nasjonal kommunikasjonsmyndighet, *«Begjæringer om fritak fra tilbyders taushetsplikt",* sist oppdatert 8. september 2017, sist sjekket 26. mai 2018, https://www.nkom.no/teknisk/taushetsplikt-og-personvern/elektroniske-spor/begjæringer-om-fritak-fra-tilbyders-taushetsplikt

Folkeregisterets EU-Oplysning, Danmark, *«Hvad er en generaladvokat?»,* sist sjekket 26. mai 2018, http://www.eu.dk/da/spoergsmaal-og-svar-folder/hvad-er-en-generaladvokat

Norsk rikskringkasting AS (NRK) , «*Spesialenheten: - Cappelen var Jensens kontantkilde*», sist sjekket 26. mai 2018, https://www.nrk.no/norge/spesialenheten_-_-cappelen-var-jensens-kontantkilde-1.13313781