UiT Norges arktiske universitet

Det juridiske fakultet

Pålegg om utlevering av trafikk- og lokaliseringsdata etter straffeprosessloven § 210

Tage Edvard Johannesen

Masteroppgave i Rettsvitenskap, JUR-3902, desember 2021

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Temaet for denne masteroppgaven er de rettslige rammene for statens adgang til å pålegge tilbydere av elektronisk kommunikasjonsmidler og utlevere «trafikk- eller lokaliseringsdata» av betydning for etterforsking av straffesaker, jf. straffeprosessloven § 210 første ledd.[1]

Kompetansen til å lede etterforsking av straffesaker ligger hos påtalemyndigheten, som er et uavhengig forvaltningsorgan.[2] Under etterforskingen av straffesaker vil påtalemyndigheten kunne ha behov for å benytte seg av straffeprosessuelle tvangsmidler. Et tvangsmiddel kan defineres som «et tiltak mot en person eller en eiendom, som har et straffeprosessuelt formål, kan gjennomføres uten personens eller eierens samtykke og er så inngripende at tiltaket krever hjemmel i lov».[3] Straffeprosesslovens del 4 omhandler tvangsmidler som kan gjennomføres under etterforsking av straffesaker. Strpl. § 210 første ledd er plassert i straffeprosessloven del 4 kapittel 16 om «[b]eslag og utleveringspålegg». Bestemmelsen hjemler en adgang for å staten til å pålegge besittere av ting med vitneplikt og utlevere det som antas å ha betydning som bevis.

Problemstillingen for avhandlingen er hvilke vilkår som må foreligge for at eiere eller tilbydere av nett eller tjenester som benyttes ved elektronisk kommunikasjon skal kunne pålegges å utlevere data. Et hovedelement i masteroppgaven vil være en klarlegging av hva som er gjeldende rett tilknyttet pålegg om utlevering av elektronisk bevismateriale, med utgangspunkt i vilkårene i straffeprosessloven. For å gi en helhetlig redegjørelse, vil det dermed være avgjørende å se på det overordnede menneskerettslige rammeverket som utgjør en skranke for tolkningen av strpl. § 210. I tillegg vil det være aktuelt å gi en oversikt over enkelte av Norges forpliktelser gjennom EØS-samarbeidet for å gi en dekkende behandling av problemstillingen.

[1] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven - strpl.).
[2] Jf. straffeprosessloven § 55. se Øyen 2019 s. 83.
[3] Øyen (2019) s. 195.

1.2 Bakgrunn og aktualitet

En stadig større andel av vårt privatliv utøves via elektroniske kommunikasjonsmidler, f.eks. via telefon eller internett. Trafikkdata er data som produseres for at slik kommunikasjon kan finne sted.[4] Dette medfører at tilbyderne av slike kommunikasjonsmidler potensielt sett har tilgang til mye data som sier noe om hva brukerne foretar seg. I tillegg til trafikkdata, produseres også lokaliseringsdata, som vil kunne si noe om hvor en telefon eller pc befinner seg når den benyttes til elektronisk kommunikasjon.[5] Trafikk- og lokaliseringsdata kan inkludere bl.a. hvor brukere befinner seg på et spesifikt tidspunkt, hvem de kommuniserer med, hvor lange telefonsamtaler de har, innholdet i tekstmeldinger, og hva de søker opp på internett.[6] Slik data kan være avgjørende for påtalemyndigheten under etterforsking av straffesaker. Av hensyn til personvernet, som er forankret i Grl. § 102 og EMK artikkel 8, vil det i en rettsstat være behov for klare rettslige rammer for når offentlige myndigheter kan tilegne seg slik data ved etterforsking av straffesaker.[7] Et overordnet formål for denne avhandlingen er å klargjøre disse rammene.

Problemstillinger tilknyttet til lagring av, og det offentlighets tilgang til, elektronisk kommunikasjon, har de siste årene vært behandlet i en rekke dommer, spesielt av EU-domstolen.[8] I tillegg foreligger det et lovforslag i Prop.167 L (2020–2021) endringer i ekomloven, hvor utlevering av elektronisk data og tilknyttede temaer i lys av utviklingen i EMK- og EØS-retten vurderes.[9] Et tilgrensende interessant tema knytter seg til dagens plikt for tilbydere av elektronisk kommunikasjonsmidler til å slette eller anonymisere data, herunder informasjon om hvilke IP-adresser personer har benyttet seg av, etter ekomloven § 2-7 femte ledd.[10] IP-adresser er elektroniske adresser som kan identifisere en enhet, eksempelvis en smarttelefon, et nettbrett eller en datamaskin.[11] I lovforslaget framkommer det et ønske fra departementet om å innføre en lagrinsplikt på tolv måneder for opplysninger om

---

[4] Forskrift 16. feb 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste – (ekomforskriften) § 7-1 første ledd annet punktum.
[5] Ekomforskriften § 7-1 annet ledd jf. § 7-2 første ledd annet punktum.
[6] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt.
[7] Kongeriket Norges Grunnlov 17. mai 1814 (Grunnloven – Grl.), og Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950 (entered into force 3 september 1953). (Den europeiske menneskerettighetskonvensjonen – EMK).
[8] Se bl.a. *Tele2 Sverige AB* [GC], *La Quadrature du Net og andre* [GC] og *H.K. v Prokuratuur* [GC] C-746/18.
[9] Prop.167 L (2020–2021).
[10] Lov 4 juni 2003 nr. 83 om elektronisk kommunikasjon (ekomloven).
[11] Prop.167 L (2020–2021) s. 13.

IP-adresser.[12] Dette vil medføre en betydelig utvidelse av den dataen som politi/påtalemyndigheten vil kunne tilegne seg gjennom strpl. § 210 i dag. I skrivende stund er lovforslaget tilknyttet disse problemstillingene vedtatt, og vil tre i kraft 1. januar 2022.[13] Disse momentene aktualiserer et behov for å klarlegge de rettslige rammene tilknyttet disse problemstillingene, og å undersøke det nasjonale hjemmelsgrunnlaget nærmere.

1.3 Avgrensning og presisering

Avhandlingens tema avgrenser mot en gjennomgang av strpl. § 210 generelt, men vil sette søkelys på bestemmelsen som hjemmelsgrunnlag for adgangen til å pålegge tilbydere av elektronisk kommunikasjonsmidler og utlevere trafikk- eller lokaliseringsdata. Dette gjør det nødvendig å se på enkelte bestemmelsen om vitneplikt og vitneforbud i straffeprosessloven kapittel 10 og ekomregelverket.[14] Disse vil imidlertid kun behandles i den utstrekning de er relevant for å pålegge tilbydere å utlevere trafikk- og lokaliseringsdata.

Avhandlingen vil avgrenses mot bestemmelser som tilrettelegger for innhenting av elektronisk kommunikasjon som transporteres over den norske grensen, som framkommer av etterretningstjenesteloven kapittel 7.[15] Det følger av etterretningstjenesteloven § 7-14 at informasjon innhentet etter de bestemmelsene generelt ikke skal brukes som bevis i straffesaker.

Hjemmelen for å beslaglegge bevis vil ikke bli behandlet nærmere.[16] De materielle vilkårene for å beslaglegge bevis og for å pålegge bevis utlevert, er i det vesentlige sammenfallende. Dette medfører at det som blir vurdert i tilknyttet til å pålegge tilbydere å utlevere trafikk- og lokaliseringsdata i det vesentlige også vil gjelde for beslagsadgangen.

Avhandlingen vil også bli avgrenset mot kommunikasjonskontroll og dataavlesing.[17] Kommunikasjonskontroll omhandler innhenting av informasjon i nåtid og framover i tid.[18]

---

[12] Prop.167 L (2020–2021) s. 47.
[13] Lov nr. 131/2021.
[14] Spesielt strpl. §§ 108 og 118, samt ekomloven og ekomforskriften.
[15] Lov av 19. juni 2020 nr. 77 om etterretningstjenesten (etterretningstjenesteloven). Se også ekomloven § 2-8 fjerde ledd.
[16] Se strpl. § 203 jf. 204.
[17] Strpl. kapitel 16 a. til d.
[18] Strpl. § 216 a tredje ledd.

Ved pålegg om utlevering av trafikk- eller lokaliseringsdata er det snakk om data som allerede foreligger hos tilbyderen av elektronisk kommunikasjon, altså historisk data. Det foreligger en viss hjemmel for å tilegne seg historisk data gjennom kommunikasjonskontroll i strpl. § 216 b tredje ledd bokstav d.[19] Kommunikasjonskontroll er likevel et mer inngripende tiltak, som medfører at vilkårene for å benytte et slik tvangsmiddel er strengere enn ved pålegging om utlevering av trafikk- eller lokaliseringsdata. Ettersom dette ligger utenfor oppgavens tema, gås det ikke nærmere inn på nevnte hjemmel.

1.4 Videre framstilling

I den videre framstillingen vil jeg først gjennomgå to metodiske problemstillinger. Den første knytter seg til gjennomføringen av Den europeiske menneskerettskonvensjonen og vektleggingen av praksis fra EMD. Den andre omhandler EØS-retten, hvor det vil redegjøres for gjennomføringen av kommunikasjonsverndirektivet med de endringer som følger av cookie-direktivet, og hvilken rettskildemessig vekt EU-domstolens avgjørelser har i norsk rett.[20] Deretter vil det overordnede rettslige rammeverket som utgjør skranker for tolkningen av hjemmelen til å pålegge utlevering av trafikk- og lokaliseringsdata gjennomgås. Det konstitusjonelle og menneskerettslige vernet av privatlivet setter grenser for inngrepsadgangen i lovgivningen. Etter dette vil kommunikasjonsverndirektivet med de endringer som ble gjennomført i cookie-direktivet behandles i den utstrekning reglene er relevante for problemstillingen i avhandlingen. Her vil det være nødvendig å se hvordan de er gjennomført i norsk rett, og hvordan EU-domstolens har tolket disse reglene. Deretter behandles vilkårene i det primære rettsgrunnlaget i strpl. § 210. Videre vil jeg se nærmere på tilbydere av elektronisk kommunikasjonsmidlers plikt til å vitne i straffesaker, jf. strpl. § 108 og 118, samt reglene for taushetsplikt i ekomloven § 2-9. Dette er spesielt aktuelt med tanke på at vitneplikt er et av de materielle vilkårene som må finne sted for å kunne pålegge utlevering av bevis. Avslutningsvis vil jeg sammenfalle hva jeg har kommet fram til.

[19] Rui (2017) s. 166-167.
[20] Direktiv 2002/58/EF om kommunikasjonsvern 2002 – (kommunikasjonsverndirektivet) og Direktiv 2009/136/EF om forbrukerrettigheter ved elektronisk kommunikasjon – (cookie-direktivet).

2 Metodiske spørsmål

2.1 EMK og EMD-praksis stilling i norsk rett

Den europeiske menneskerettighetskonvensjonen er inkorporert i norsk rett gjennom menneskerettsloven § 2 nr. 1, og bestemmelsene i konvensjonen har ved motstrid forrang foran bestemmelser i annen lovgivning, jf. mrl. § 3.[21] På straffeprosessens område har konvensjonen i tillegg vekt gjennom folkerettens sektormonistiske stilling, jf. strpl. § 4 første ledd.

Når problemstillingen om motstrid mellom EMK og bestemmelser i annen lovgivning oppstår, skal det først å fremst forsøkes å harmonisere bestemmelsene slik at motstrid faller bort. [22] Høyesterett benytter et prinsipp om selvstendig tolkning, blant annet går ut på at domstolen skal benytte de samme tolkningsprinsippene som EMD når de tolker konvensjonen.[23] Dette gjelder likevel med begrensninger. Norske domstoler skal være varsom med å foreta en like dynamisk tolkning av EMK som EMD gjør, da dette kan legge unødige bånd på norsk lovgivningsmyndighet og tilegne domstolen større rettskapende rolle enn tiltenkt.[24] Norske domstoler skal være forsiktig i å innfortolke sikkerhetsmarginer for å sikre at Norge ikke blir dømt for konvensjonsbrudd, da dette vil at bestemmelsene tolken strengere enn nødvendig.[25]

I Grunnlovens kapittel E om menneskerettigheter, har staten i § 92 forpliktet seg å «respektere og sikre menneskerettighetene» etter Grunnloven og internasjonale traktater som Norge er bundet av. Høyesterett har i HR-2016-2554-P uttalt at «Grunnloven § 92 ikke kan tolkes som en inkorporasjonsbestemmelse, men må forstås som et pålegg til domstolene og andre myndigheter om å håndheve menneskerettighetene på det nivå de er gjennomført i norsk rett.»[26] Grunnloven er altså lex superior, og inkorporerte menneskerettighetsbestemmelser vil dermed ikke gå foran grunnlovsbestemmelser ved motstrid.[27]

---

[21] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven – mrl.).
[22] Rt. 2000 s. 996 på side 1007.
[23] Rt. 2000 s. 996 på side 1007, Rt. 2001 s. 1006 på side 1016, Rt. 2002 s. 557 på side 565 og Rt. 2005 s. 833 avsnitt 45.
[24] Rt. 2000 s. 996 på side 1008. Se også Rt. 2002 s. 557 på side 565 og Rt. 2005 s. 833 avsnitt 45.
[25] Rt. 2000 s. 996 på side 1008, Rt. 2001 s. 1006 på side 1016 og Rt. 2005 s. 833 avsnitt 46.
[26] HR-2016-2554-P avsnitt 70.
[27] mrl. § 3.

Grl. § 92 er likevel sentral som en tolkningsnorm. Ettersom internasjonale menneskerettigheter skal respekteres, vil disse være sentrale ved tolkingen av Norges menneskerettsbestemmelser. Høyesterett har eksplisitt uttalt dette om forholdet mellom EMK artikkel 8 og Grl. § 102, ettersom de internasjonale menneskerettsbestemmelsene var forbildet for dannelsen av Grl. § 102.[28] På bakgrunn av dette forholdet mellom Grl. § 102 og EMK artikkel 8, vil praksis fra EMD også stå sentralt ved tolkningen av vernet etter Grunnloven.[29] EMD-praksis skal likevel ikke ha like stor prejudikatsverdi for tolkingen av Grunnloven som ved EMK.[30] I Rt. 2015 s. 93 uttalte Høyesterett at «det er etter vår forfatning Høyesterett – ikke de internasjonale håndhevingsorganene – som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettsbestemmelser».[31] Høyesterett er fremdeles det organ som i siste rekke tolker Grunnloven.

2.2 EØS-relevante rettsreglers gjennomføring i norsk rett og vekten av EU-domstolens avgjørelser

Norges tilknytting til EU-retten følger av EØS-avtalen.[32] På tilsvarende måte som EMK, er EØS-avtalens hoveddel inkorporert som norsk lov gjennom EØS-loven § 1.[33] Det følger direkte av EØS-avtalens artikkel 3 første ledd at «Avtalepartene skal treffe alle generelle eller særlige tiltak som er egnet til å oppfylle de forpliktelser som følger av denne avtale». Dette er den generelle plikten for staten til å gjennomføre EØS-regelverket.[34] Hvordan de enkelte rettsaktene «som er omhandlet i eller inntatt i vedlegg til denne avtale eller i EØS-komiteens vedtak» skal gjennomføres utover hoveddelen framgår av EØS-avtalen artikkel 7. For EØS-forordninger, skal de inkorporeres som norsk lov, jf. EØS-avtalen artikkel 7 a), mens for EØS-direktiv er det overlatt staten å velge gjennomføringsform, jf. artikkel 7 b). Norge har lagt seg på en linje hvor gjennomføringen skjer gjennom transformasjon, altså at vedtakets

[28] Rt. 2015 s. 93 avsnitt 57 og HR-2016-2554-P avsnitt 81.
[29] Rt. 2015 s. 93 avsnitt 57.
[30] Rt. 2015 s. 93 avsnitt 57.
[31] Rt. 2015 s. 93 avsnitt 57.
[32] Avtale om Det europeiske økonomiske samarbeidsområde – EØS-avtalen.
[33] Lov 27. nov 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. - (EØS-loven).
[34] Sejersted (2011) s. 195.

bestemmelser omskrives som norsk lov eller forskrift, slik at den utseendemessig ikke skilles fra annen norsk lovgivning.[35]

Spesielt relevant for avhandlingens tema er kommunikasjonsverndirektivet med de endringer som følger av cookie-direktivet. Kommunikasjonsverndirektivet ble transformert til norsk rett gjennom konstatering av rettsharmoni til tidligere markedsføringslov (nå endret til ny markedsføringslov), samt ikrafttredelse av ekomloven og ekomforskriften.[36] Ettersom oppgavens tematikk omhandler tilbydere av elektroniske kommunikasjonsmidler vil ekomloven og ekomforskriften spesielt være relevante. Cookie-direktivet er del av EUs Telekompakke.[37] På bakgrunn av uenigheter mellom EFTA-landene og EU om innlemmelse av enkelte elementer av pakke og direktivet, ble kun regelverket som gjorde endringer på ekomregelverket gjennomført nasjonalt.[38] Dette skjedde gjennom endring av ekomloven og ekomforskriften.[39]

Et annet EU-rettslig regelverk av relevant for avhandlingen, er the Charter of Fundamental Rights of the European Union (Charteret). Denne traktaten har som mål å styrke beskyttelsen av fundamentale rettigheter og er blant annet inspirert av EMK.[40] Charteret er ikke gjennomført i norsk rett, ettersom traktaten gjelder for medlemmene av EU. Det er likevel relevant for problemstillingen i avhandlingen, ettersom det framkommer av kommunikasjonsverndirektivet at direktivet skal respektere rettighetene i Charteret, spesielt artikkel 7 og 8.[41] EU-domstolen tolker også direktivet i lys av Charteret ved flere anledninger.[42] Denne spesielle stillingen til charteret tilknyttet kommunikasjonsverndirektivet, medfører at det vil være relevant som tolkningsmoment også for norsk rettsanvendelse.[43]

---

[35] Sejersted (2011) s. 197-201.
[36] Lov 16. juni 1972 nr. 47 om kontroll med markedsføring og avtalevilkår - (tidligere markedsføringslov, opphevet), Lov 9. jan 2009 nr. 2 om kontroll med markedsføring og avtalevilkår mv. - (ny markedsføringslov). Se også https://europalov.no/rettsakt/kommunikasjonsverndirektivet-2002/id-2232.
[37] https://www.europalov.no/pakke/telekompakken.
[38] https://www.europalov.no/rettsakt/cookie-direktivet-forbrukerrettigheter-ved-elektronisk-kommunikasjon/id-126.
[39] Ekomloven endret ved lov nr. 54/2013 og ekomforskriften endret ved forskrift nr. 740/2013.
[40] Charteret fortalen avsnitt 4 og 5.
[41] Kommunikasjonsverndirektivets fortale avsnitt 2.
[42] Se bl.a. *Tele2 Sverige AB* [GC], *La Quadrature du Net og andre* [GC] og *H.K. v Prokuratuur* [GC] C-746/18.
[43] Se Rui (2017) s. 151-154.

EØS-rettslige regler som er gjennomført i norsk rett skal, på like linje med EMK, «i tilfelle konflikt gå foran andre bestemmelser som regulerer samme forhold», jf. EØS-loven § 2. Dette gjelder også for mellom forskrifter, og forskrifter som tjener til å oppfylle Norges forpliktelser etter avtalen og senere lovgivning.[44] EØS-loven § 2 gir utrykk for et tolkningsprinsipp. Om Stortinget ikke eksplisitt gir utrykk for at den nye lovgivningen skal være i motstrid med EØS forpliktelsen, plikter domstolen til å tolke bestemmelsen innskrenkede og forsøke å harmonisere motstriden mellom bestemmelsene.[45] Arnesen anser EØS-loven § 2 som «et lovfestet forsterket presumsjonsprinsipp».[46] EØS-loven § 2 gjelder kun ved motstrid av korrekt gjennomførte EØS rettsakter.[47] I andre tilfeller må det tas utgangspunkt i ulovfestede tolkningsprinsipp.

EU-domstolen utviklet et prinsipp om direktivkonform tolkning med grunnlag i lojalitetsplikten innenfor EU-retten.[48] I Rt. 2000 s. 1811 på side 1830 kom Høyesterett fram til at «prinsippet om direktivkonform fortolkning slik det er utviklet i EU-retten, [ikke] går lenger enn presumsjonsprinsippet i norsk rett.» Presumsjonsprinsippet går ut på at norsk lov så vidt mulig skal tolkes i samsvar med våre folkerettslige forpliktelser.[49] Dette prinsippet står sterkt i tilfeller lovgiver selv har uttalt at det ikke skal foreligge motstrid.[50] Selv om EØS-regelen er gjennomført i norsk rett eller ikke, så vil presumsjonsprisnippet stå sentralt for tolkningen av aktuelle norske lovbestemmelser.[51]

I Rt. 2000 s. 1811 konkluderte retten med at et EØS-direktiv ikke var riktig gjennomført i norsk rett, men at motstrid ikke kunne tolkes bort uten å fullstendig gå bort fra ordlyden i den norske bestemmelsen.[52] EØS-direktivet kunne ikke gis direkte virkning i norsk rett, og den norske lovbestemmelsen måtte dermed gå foran.[53] Saksforholdet i Rt. 2000 s. 1811 gjaldt rettigheter mellom private parter. Høyesterett gir utrykk for at presumsjonsprinsippet skal ha

[44] EØS-loven § 2 annen punktum.
[45] Arnesen (2011) s. 267-270.
[46] Arnesen (2011) s. 268.
[47] Arnesen (2011) s. 269.
[48] Se Rt. 2000 s. 1811 s. 1828-1829.
[49] Rt. 2000 s. 1811 s. 1826.
[50] Rt. 2000 s. 1811 s. 1831.
[51] Arnesen (2011) s. 265.
[52] Rt. 2000 s. 1811 s. 1833.
[53] Rt. 2000 s. 1811 s. 1833.

større gjennomslagskraft når det gjelder EØS-direktiv som tilsikter å begrense statens kompetanse til å gjøre inngrep overfor borgerne.[54]

EU domstolen får sin kompetanse fra TEU artikkel 19, hvor det framkommer i første avsnitt annet punktum at domstolen skal «ensure that in the interpretation and application of the Treaties the law is observed.»[55] Norge er ikke medlem av EU, og dette medfører at Norge ikke er underlagt EU-domstolens kompetanse direkte. Selv om EU-domstolen ikke har kompetanse til å avgjøre EØS-rettslige tvister som Norge tar del i, vil EU-domstolens tolkningsresultater likevel ha stor vekt overfor norsk rettsanvendelse av EØS-retten. For EU-domstolens avgjørelser som fant sted før signeringen av EØS-avtalen i 1992 følger dette direkte fra EØS-avtalen artikkel 6. Selv om norske domstoler ikke er forpliktet til å vektlegge EU-domstolens avgjørelser etter 1992 ser man at Høyesterett likevel direkte henviser til og vektlegger EU-domstolens avgjørelser etter 1992.[56] Dette medfører at EU-domstolens avgjørelser på EU-rettslige områder som Norge har bundet seg til, skal vektlegges i norsk rettsanvendelse.

3 Det overordnede rammeverket som utgjør skranker for tolkningen

3.1 Når foreligger det et inngrep i Grl. § 102 og EMK artikkel 8?

Ettersom avhandlingens tema er pålegg om utlevering av trafikk- og lokaliseringsdata, vil vernet av privatlivet kunne innebære begrensninger. For å angi hvilke begrensninger vernet setter, må de først vurderes om utleveringspålegg av trafikk- og lokaliseringsdata innebærer et inngrep i retten.

For det første må det defineres hva som er vernet i Grl. § 102 og EMK artikkel 8. Det framkommer klart av Grl. § 102 annet ledd at staten skal verne om «den personlige integritet». Grl. § 102 første ledd og EMK artikkel 8 nr. 1 nedfeller en rett for enhver til respekt av samme materielle rettigheter til privatliv, familieliv, hjem og korrespondansen. «Privatlivet» er et omfattende begrep som naturlig omfatter de andre begrepene i bestemmelsene. Det finnes ikke en uttømmende definisjon av begrepet, hverken i norsk rett

[54] Rt. 2000 s.1811 s.1832. se også Arnesen (2011) s. 270-272.
[55] Consolidated version of the Treaty on European Union (TEU).
[56] Rt. 2000 s. 1811. se også Arnesen (2011) s. 265-267, Rt. 1997 s. 1954, Rt. 1997 s. 1965 og Rt. 2002 s. 391.

eller i EMD-praksis.[57] Høyesterett bygger i Rt. 2015 s. 93 innholdet i begrepet på sentrale elementer fra EMD praksis, hvor blant annet «menneskets fysiske og psykiske *integritet*, alle de ulike elementene i den enkeltes *identitet* i videste forstand, og den *personlige autonomi*» står sentralt.[58]

I tilknytning til behandlingen av personlige opplysninger kom Høyesterett i Rt. 2014 s. 1105, til at «systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold» er et inngrep i Grl. § 102.[59] Dette er forenelig med EMD-praksis, hvor det er lagt til grunn at lagring av data om privatlivet er et inngrep.[60] Det faktum at «privatlivet» er såpass vidt begrep medfører at det sjelden konkluderes med at det ikke foreligger et inngrep. Dette gjelder spesielt på straffeprosessens område, hvor statens inngrepshjemler kan være meget inngripende.

For det andre skal bestemmelsene hovedsakelig verne mot inngrep fra «offentlige myndigheter», jf. formuleringen i EMK artikkel 8 nr. 2. Dette medfører en forpliktelse til ikke å gjøre inngrep utover det bestemmelsen tillater, noe som er hovedformålet med bestemmelsen. På straffeprosessens område vil dette sette begrensninger for påtalemyndighetens tvangsmiddelbruk. Det følger likevel at av Grl. § 102 første ledd og EMK artikkel 8 nr. 1 at «[e]nhver har rett til respekt for sitt privatliv». Denne retten til respekt utløser en viss positiv forpliktelse for staten til å sikre enhvers rett til privatlivets fred mot inngrep fra andre private eller juridiske personer.[61] For straffeprosessens område kan dette medføre en plikt til å etterforske straffbare handlinger.[62]

Utleveringspålegg av trafikk- og lokaliseringsdata overfor tilbydere av elektroniske kommunikasjonsmidler vil være en form for innhenting og bruk av opplysningene av staten. Trafikk- og lokaliseringsdata vil kunne si mye om en persons personlige forhold, f.eks. gjennom hvem en har kontakt med via telefon eller over internett. Ettersom lagring av data vil være et inngrep i retting til privatlivet i Grl. § 102 og EMK artikkel 8, vil det fra det mer til

---

[57] Rt. 2015 s. 93 avsnitt 58.
[58] Rt. 2015 s. 93 avsnitt 58, med videre henvisninger til Rt. 2012 s. 2039 avsnitt 70 og *Üner mot Nederland* [GC] 2006, no. 46410/99 avsnitt 59. se også *S. og Marper mot Storbritania* [GC] 2008, nos. 30562/04 and 30566/04 avsnitt 66.
[59] Rt. 2014 s. 1105 avsnitt 28, med videre henvisning til Innst. 186 S (2013–2014) side 27.
[60] Se *Amann mot Sveits* [GC] 2000, no. 27798/95 avsnitt 65, *S. og Marper mot Storbritania* [GC] 2008, nos. 30562/04 and 30566/04 avsnitt 67 og Prop.167 L (2020–2021) s. 15-16.
[61] *M.G.C. mot Romania* [J] 2016, no. 61495/11 avsnitt 55.
[62] *M.G.C. mot Romania* [J] 2016, no. 61495/11 avsnitt 58.

det mindre betraktninger være riktig at innhentingen og bruk av dataen også anses som et inngrep.[63]

Retten til vern av privatlivet og korrespondanse er ikke en absolutt rettighet. I EMK artikkel 8 kommer dette til utrykk i bestemmelsens annet ledd, hvor nærmere vilkår for når offentlige myndigheter kan gjøre inngrep i rettigheten framgår. Med unntak av husransakelser, som etter Grl. § 102 første ledd bare kan finne sted i kriminelle tilfeller, framgår det ikke noen unntak for retten til vern av privatlivet i Grl. § 102. Høyesterett har i imidlertid slått klart fast at Grunnlovens vern skal forstås med de begrensninger som følger av EMK artikkel 8.[64] Ettersom rettighetene i Grl. § 102 og EMK artikkel 8 ikke er absolutte, vil det ikke være tilstrekkelig å konstatere at det foreligger et inngrep. I tilfeller hvor inngrep i privatlivet blir konstatert må det deretter vurderes om inngrepet er gjort innenfor de rettslige rammene som oppstilles. Med det for øye vil det i det følgende bli redegjort for hvilke vilkår som må være oppfylt for at inngrepet ikke medfører et brudd på bestemmelsene.

3.2 Hva må til for at et inngrep skal være «in acordance with the law»?

Det første vilkåret som skal redegjøres for er kravet om at inngrepet i privatlivet etter Grl. § 102 og EMK artikkel 8 må ha hjemmel i lov. For EMK artikkel 8 følger dette direkte av bestemmelsens andre ledd, hvor det kommer fram at inngrepet må være «in acordance with the law». For Grunnlovens vedkommende følger kravet til lovhjemmel av Grl. § 113, hvor det framkommer at «myndighetenes inngrep overfor den enkelte må ha grunnlag i lov.»

Etter en naturlig språklig forståelse av «in acordance with the law», jf. EMK artikkel 8 nr. 2, medfører det at inngrepet må være forankret i medlemsstatens rettsregler. Begrepet «law», som benyttes i bestemmelsen, sikter ikke til begrepets formelle forståelse, men dets substansielle.[65] Det innebærer at det er tilstrekkelig at inngrepet er hjemlet i rett som er anerkjent av medlemslandet; det må altså ikke være lovtekst, men også rettspraksis og sedvane. For Grl. 102 jf. Grl. § 113 har Høyesterett i Rt. 2014 s. 1105 tolket «lov» dit hen at det siktes til begrepet i sin formelle forstand, og kravet dermed vil være at inngrepet må være

[63] Se Rt. 2014 s. 1105 avsnitt 28 og 30.
[64] Rt. 2015 s. 93 avsnitt 60.
[65] *Robathin mot Østeriket* [J] 2012, no. 30457/06 avsnitt 40.

forankret i lovtekst eller forskrift med hjemmel i lov.[66] Forankring i formell lov sikrer både forutberegnelighet, motvirker vilkårlighet, usaklig forskjellsbehandling og støtter under demokratiet.[67]

Lovens kvalitet står også sentralt i vurderingen av om vilkåret «in acordance with the law» er oppfylt, jf. Rt. 2014 s. 1105.[68] Når EMD og Høyesterett sikter til lovens kvalitet, er det hovedsakelig to elementer som skal vurderes.[69] For det første må rettsregelen være «accessible» (tilgjengelig).[70] Det som ligger i dette tilgjengelighetskravet, er at lovhjemmelen må være vedtatt og kunngjort på inngrepstidspunktet.[71] For det andre må regelen være tilstrekkelig klar slik at man kan forutsi konsekvensene av inngrepshjemmelen («forseeable») – forutberegnelighetskravet eller «presisjonskrav».[72] Forutberegnelighetskravet stiller kriterier både til lovgiver og til rettsanvenderne.[73]

For lovgiver innebærer forutberegnelighetskravet at loven er presist utformet; den må være tilstrekkelig klar. For skjulte straffeprosessuelle tvangsmidler, altså tvangsmidler som mistenkte ikke er klar over at blir benyttet mot han, har EMD i *Huvig mot Frankrike* uttalt at inngrepshjemmelen må være «particularly precise».[74] Begrunnelsen for at presisjonskravet her er skjerpet er at faren for misbruk og vilkårlighet er større i slike tilfeller – i tillegg til at mistenkte ikke har mulighet til selv å angripe bruken av tvangsmidlene.[75] I Rt. 2009 s. 394, som omhandlet spørsmål om kommunikasjonskontroll, uttalte Høyesterett at klarhetskravet på dette området må stå sterkt. I HR-2016-1833-A utrykkes det imidlertid usikkerhet om det der siktes til skjulte tvangsmidler eller tvangsmidler generelt.[76] Det må uansett foreligge klare og detaljerte regler, som kan anvendes dynamisk med teknologiutviklingen i samfunnet.[77] Mer

---

[66] Rt. 2014 s. 1105 avsnitt 24. Se også All 2021 s. 108.
[67] Rt. 2014 s. 1105 avsnitt 26.
[68] Rt. 2014 s. 1105 avsnitt 30. Se også HR-2016-1833-A avsnitt 15 og *Kruslin mot Frankrike* [J] 1990, no. 11801/85 avsnitt 27.
[69] Rt. 2014 s. 1105 avsnitt 30, HR-2016-1833-A avsnitt 15 og *Kruslin mot Frankrike* [J] 1990, no. 11801/85 avsnitt 27.
[70] Rt. 2014 s. 1105 avsnitt 30, HR-2016-1833-A avsnitt 15 og *Kruslin mot Frankrike* [J] 1990, no. 11801/85 avsnitt 27. Se også *Robathin mot Østeriket* [J] 2012, no. 30457/06 avsnitt 40 og *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 30.
[71] Se Grunnloven § 97, EMK artikkel 7, Rt. 2004 s. 357 avsnitt 16-17 og All 2021 s. 108-109.
[72] Rt. 2014 s. 1105 avsnitt 30, HR-2016-1833-A avsnitt 15 og *Kruslin mot Frankrike* [J] 1990, no. 11801/85 avsnitt 27. Se også *Robathin mot Østeriket* [J] 2012, no. 30457/06 avsnitt 40 og *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 30.
[73] All 2021 s. 109.
[74] *Huvig mot Frankrike* [J] 1990, no. 11105/84 avsnitt 32 og All 2021 s. 110.
[75] Rt. 2014 s. 1105 avsnitt 30.
[76] HR-2016-1833-A avsnitt 15.
[77] *Huvig mot Frankrike* [J] 1990, no. 11105/84 avsnitt 32.

konkret innebærer dette ifølge Høyesterett at inngrepshjemmelen må inneholde både klare materielle og prosessuelle vilkår.[78] Høyesterett har i Rt. 2014 s. 1105 uttalt at slike garantier tilknyttet personopplysninger kan være blant annet «formen for lagring, bruken av materialet, muligheten for innsyn, sikkerhet og sletting».[79] Disse rettsikkerhetsgarantiene er også et relevant vurderingsmoment under forholdsmessighetsvilkåret, som vil bli behandlet under 3.4.[80]

For rettsanvenderen utgjør kravet om forutberegnelighet på sin side et analogiforbud. En analogisk tolkning medfører at loven benyttes utenfor den situasjonen den faktisk regulerer.[81] Det vil være lite forenelig med det strenge klarhetskravet, samt være lite forutberegnelig. På straffeprosessens område har Høyesterett gitt utrykk for analogiforbudet i en rekke dommer. I Rt. 2014 s. 1105 konkluderte Høyesterett med at lagring av personopplysninger som var innhentet av kommunikasjonskontroll ikke kunne hjemles analogisk i strpl. § 216g bokstav a (slik den da lød) og kommunikasjonskontrollforskriften § 9, selv om klare reelle hensyn talte for at lagring skulle finne sted.[82] I HR-2016-1833-A kom Høyesterett til et lignende resultat tilknyttet tvangsbruk overfor mistenkte for å tvinge vedkommende å åpne mobiltelefonen sin ved bruk av fingeravtrykk. Høyesterett uttalte at «[f]ormålsbetraktninger kan imidlertid ikke i seg selv gi hjemmel for det tvangsmiddel som saken gjelder» og konkluderte dermed med at strpl. § 157 (slik den da lød) ikke kunne hjemle et slikt inngrep.[83] Presisjonskravet medfører dermed at tolkingsresultatet ikke kan begrense eller utvide hjemmelen utenfor en naturlig språklig forståelse av ordlyden. [84]

3.3 Hva ligger i vilkåret «legitimt formål»?

Det neste vilkåret som må være oppfylt er at det må foreligge et legitimt formål for å gjennomføre inngrep i privatlivet. De legitime formålene som kommer fram fra EMK artikkel

[78] Rt. 2014 s. 1105 avsnitt 30 og All 2021 s. 110.
[79] Rt. 2014 s. 1105 avsnitt 30.
[80] All 2021 s. 111.
[81] Nygaard (2004) s. 181.
[82] Rt. 2014 s. 1105 avsnitt 42-46. Forskrift 31. mars 1995 nr. 281 om kommunikasjonskontroll – (kommunikasjonskontrollforskriften) (opphevet).
[83] HR-2016-1833-A avsnitt 23.
[84] Se All 2021 s. 109 og HR-2018-104-A avsnitt 24.

8 nr. 2 vil også være aktuelle for grl. § 102.[85] EMK artikkel 8 nr. 2 oppstiller følgende alternative legitime formål:

> "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Vurderingstemaet er altså om formålet med inngrepet kan tolkes inn i en av disse formålene i EMK artikkel 8 nr. 2. For straffeprosessuelle inngrep er forebygging av kriminalitet mest forenelig med straffeprosessens formål. For effektivt å kunne forebygge mot straffbare handlinger, er bruk av tvangsmidler under etterforskningen nødvendig. Dette medfører at det i EMD-praksis på straffeprosessens område sjeldent vil komme på spissen om formålet er legitimt. Pålegg om utlevering av trafikk- og lokaliseringsdata faller naturlig under dette formålet, da effektiv etterforsking av straffesaker er et nødvendig middel for å forhindre kriminalitet.

3.4 Hva må foreligge for at et inngrep er «necessary in a democratic society»?

Vilkåret «necessary in a democratic society», er det siste vilkåret som står sentralt i EMK artikkel 8 nr. 2. Høyesterett har i en rekke avgjørelser gitt utrykk for at det samme vilkåret gjelder etter Grl. § 102.[86] Høyesterett legger tre momenter i vurderingen av dett vilkåret: inngrepet må være egnet, nødvendig og proporsjonalt.[87]

Kravet til at inngrepet må være egnet er nært knyttet opp mot vilkåret om at det må foreligge et legitimt formål. Om dette sier EMD i *M.K. mot Frankrike* at «the reasons adduced by the national authorities to justify it must be "relevant and sufficient"».[88] Kravet går ut på at inngrepet må være egnet til å oppnå det legitime formålet. I tilfeller hvor det legitime formålet er forebygging av kriminalitet vil vurderingen knyttes opp mot om det enkelte etterforskingsskrittet er egnet for å oppklare det straffbare forholdet.[89] Eksempelvis vil ikke

[85] Rt. 2014 s. 1105 avsnitt 28.
[86] Rt. 2014 s.1105 avsnitt 28, HR-2018-104-A avsnitt 23, HR-2018-699-A avsnitt 32, HR-2019-1226-A avsnitt 54.
[87] HR-2018-104-A avsnitt 23, HR-2018-699-A avsnitt 32 og All 2021 s. 112.
[88] *M.K. mot Frankrike* [J] 2003, no. 19522/09 avsnitt 30.
[89] All 2021 side 112.

beslag av siktedes datamaskin være egnet i et tilfelle der vedkommende er siktet for å ha ført motorvogn påvirket av alkohol, jf. vtrl. § 31 jf. § 22.[90] Et slik beslag vil neppe bidra til å oppklare om det faktisk foreligger en overtredelse av vegtrafikkloven. Et tvangsmiddel som her vil være egnet er testing av ruspåvirkning, jf. vtfl. § 22 a.

Om utleveringspålegg av trafikk- og lokaliseringsdata kan anses som egnet, avhenger om dataen i seg selv kan bidra til å oppklare det straffbare forholdet som foreligger. Dette vil i mange tilfeller være tilfelle, f.eks. tilknyttet fremstillinger av seksuelle overgrep mot barn over internett.[91] I slike tilfeller vil IP-adresser være sentrale bevis, da det vil lettere kunne identifisere riktig gjerningsperson. Annen trafikkdata kan også være relevant, eksempelvis vil data tilknyttet hvem man har hatt kontakt med over telefon eller elektroniske meldinger kunne avgjøre om en person mistenkt for å utøve trusler mot en fornærmede har hatt kontakt med vedkommende.[92] Lokaliseringsdata vil kunne være avgjørende i vurdering av volds- og/eller vinningslovbrudd, for å undersøke om mistenkte befant seg på gjerningsstedet på handlingstidspunktet.[93] Egnetheten vil også avhengte av innholdet i dataen. Ettersom innholdet i dataen ikke kan avgjøres uten å ha innhentet dataen og undersøkt den, vil det være en vanskelig vurdering å ta før utleveringspålegget finner sted. For å kunne vurdere egnetheten av dataen tilknyttet innholdet, vil det være nødvendig med prosessuelle ordninger som tillater forhåndskontroll av dataen. Forhåndskontroll av dataen av retten eller et annet uavhengig organ vil kunne tilrettelegge for en vurdering av om innholdet i den spesifikke dataen vil være avgjørende for å oppklare det straffbare forholdet.

Nødvendighetskravet er formulert av EMD i *M.K. mot Frankrike* som et krav om at det må foreligge «a pressing social need».[94] Det faller naturlig i en nødvendighetsvurdering at det ikke må foreligger mindre inngripende tiltak som ellers kan benyttes for å oppnå formålet. Eksempelvis vil telefonavlytting være mindre inngripende enn dataavlesing, og om telefonavlytting vil være like effektiv i saken, så skal dette inngrepet benyttes framfor dataavlesing.[95]

---

[90] Strpl. § 203 og lov 18 juni 1965 nr. 4 om vegtrafikk (vegtrafikkloven – vtrl.).
[91] Lov 20. mai 2005 nr. 28 om straff – (straffeloven, strl.) §§ 310 og 311.
[92] Strl. §§ 263 og 264.
[93] Strl. Kapittel 25 og 27.
[94] *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 33. se også *Campbell mot Storbritannia* [J] 1992, no. 13590/88 avsnitt 44 og All 2021 side 112.
[95] Strpl. §§ 216 l og 216 o.

En mulighet for staten til å tilegne seg trafikk- og lokaliseringsdata tilknyttet straffesaker vil på generell basis være nødvendig. Jo større del av privatlivet vårt som foretas over elektronisk kommunikasjon, jo flere straffbare handlinger vil kunne finne sted over elektroniske kommunikasjonsmidler. Dette skaper et samfunnsmessig behov for en mulighet for staten å få tilgang til slik data der den er egnet for å oppklare slike straffbare handlinger. Uten slike muligheter vil staten i praksis stå handlingstom mot å etterforske og bekjempe slike kriminelle handlinger. Statens adgang til slik data kan organiseres på en rekke forskjellig vis. Noe av det mest inngripende man kan se for seg er et statlig system som lagrer alt av data som skapes og som fritt er tilgjengelig for påtalemyndigheten ved behov. Dataavlesing eller ransaking og beslag vil også i flere tilfeller oppleves som mer inngripende.[96] Utleveringspålegg vil på mange måter være et lite inngripende tvangsmiddel sammenlignet med de øvrige løsningene, gitt at det foreligger tilstrekkelig materielle og prosessuelle rettsikkerhetsgarantier som sikre mot misbruk. Tilknyttet mindre alvorlige kriminelle handlinger derimot, vil det sosiale behovet for utleveringspålegg av trafikk- og lokaliseringsdata være mindre. Beskyttelsesbehovet overfor f.eks. ordensforstyrrelser er mye lavere enn ved drap, og nødvendigheten for staten til i slike tilfeller å kunne tilgang seg trafikk- og lokaliseringsdata vil på mange måter være ikke-eksisterende.[97] Motsetningsvis vil det være et sterkt behov for å beskytte befolkningen mot terrorhandlinger, og det foreligger et sterkt sosialt behov for tilgang til slik data, som langt på vei vil kunne bidra til oppklaring av slike handlinger.[98]

Det siste og muligens mest sentrale kravet under vurderingen av om inngrep er «necessary in a democratic society» er proporsjonalitetsvurderingen. Høyesterett har i Rt. 2015 s. 93 uttalt at dette er en avveining der «balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre».[99] Vurderingstemaet er altså siktedes rett til privatliv, mot statens behov for å etterforske og bekjempe straffbare handlinger. Som nevnt i tilknytning til lovkravet under punkt 2.2, vil et relevant moment i vurderingen være om det foreligger tilstrekkelige rettsikkerhetsgarantier,

[96] Strpl. §§ 192, 203 og 216 o.
[97] Strl. §§ 181 og 275.
[98] Strl. §§ 131 og 132.
[99] Rt. 2015 s. 93 avsnitt 60. Se også HR-2019-1226-A avsnitt 55, Robathin mot Østeriket [J] 2012, no. 30457/06 avsnitt 43.

eller «safeguards».[100] Vurderingen av rettsikkerhetsgarantier knytter seg til hvordan de er gjennomført i den konkrete saken.[101] For hemmelige overvåkingsmetoder har EMD i *Roman zakharov mot Russland* oppstilt visse minimumsgarantier, blant annet prosessen for behandling, bruk og lagring av dataen og tilfeller hvor lagring må slettes.[102] Slike garantier vil begrense statens konkrete inngrepsadgang. Når det under lovkravet vurderes om slike garantier framkommer av lov og er tilstrekkelig for å sikre forutberegnelighet, vil det her være avgjørende at garantiene er fulgt på en forholdsmessig måte. Eksempelvis viser EMD i *Roman zakharov mot Russland* til «the nature of offences».[103] Høyesterett har i HR-2019-1229-A lagt til grunn at «karakteren av lovbruddet et moment som kan være relevant i den samlede forholdsmessighetsvurderingen».[104] Når karakteren av lovbruddet inngår som et moment i vurderingen kan dette tilsi at det må oppstilles et krav om strafferamme for inngrepet eller at inngrepet kun kan benyttes under etterforsking av spesifikke straffebud.

Et siste moment som står sentralt i forholdsmessighetsvurderingen, er statens skjønnsmargin.[105] Det er staten som hovedsakelig har ansvar for å gjennomføre forpliktelsene etter EMK, men ettersom potensielle brudd kan bringes inn for EMD, medfører dette at det vil variere fra sak til sak hvor fritt staten står i å vurdere inngrepsadgangen.[106] I *M.K. mot Frankrike*, har EMD uttalt at denne skjønnsmarginen er begrenset på områder hvor «the right at stake is crucial to the individual's effective enjoyment of intimate or key rights», samt hvor «a particularly important facet of an individual's existence or identity is at stake».[107] For retten til respekt for privatlivet vil dette medføre at jo mer inngripende tvangsmidler er overfor mennesket integritet, identitet eller personlige autonomi, jo mindre fritt står staten i vurderingen.[108]

---

[100] *Erdem mot Tyskland* [J] 2001, no. 38321/97 avsnitt 65, *Robathin mot Østeriket* [J] 2012, no. 30457/06 avsnitt 44, *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 35, Rt. 2014 s.1105 avsnitt 30, HR-2018-104 A avsnitt 24 og HR-2019-1226-A avsnitt 57.
[101] All 2021 side 111.
[102] *Roman zakharov mot Russland* [J] 2015, no. 47143/06 avsnitt 231.
[103] *Roman zakharov mot Russland* [J] 2015, no. 47143/06 avsnitt 231.
[104] HR-2019-1226-A avsnitt 70.
[105] HR-2019-1226-A avsnitt 59.
[106] *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 33.
[107] *M.K. mot Frankrike* [J] 2013, no. 19522/09 avsnitt 33.
[108] Rt. 2015 s. 93 avsnitt 58.

4 Relevante EØS-rettslige regler og EU-domstolens tolkning av disse

4.1 Kommunikasjonsverndirektivet

En rekke bestemmelser i kommunikasjonsverndirektivet er relevante i tilknytning til avhandlingens problemstilling. En nærmere behandling av de norske reglene vil bli gjennomført nedfor under punkt. 5. Både begrepet «trafikkdata» og begrepet «lokaliseringsdata» er definert i direktivet og er gjennomført i ekomforskriften § 7-1.[109] Ved gjennomføringen av begrepet «trafikkdata» i norsk rett er det data som er «nødvendig» for å overføre kommunikasjon som kan anses som trafikkdata, jf. ekomforskriften § 7-1 første ledd annet punktum. Dette er et noe innskrenkende begrep sammelignet med «any data processed for the purpose of the conveyance» som benyttes i kommunikasjonsverndirektivet.[110] Originalteksten viser til all data produsert, mens nødvendig data vil begrense seg kun til dataen som må produseres. Dette vil likevel neppe medføre en realitetsendring. Det er kun i tilfeller hvor store deler av dataen som produseres ikke er nødvendig for at kommunikasjonen skal finne sted at trafikkdata i for stor grad blir innskrenket i norsk rett. For lokaliseringsdata er det kun den geografiske plasseringen til en «publicly available electronic communications service» som er angitt i kommunikasjonsverndirektivet, mens ekomforskriften bruker begrepet «terminalutstyr».[111] Den norske ordlyden fremstår som en utvidelse, ettersom terminutstyr ikke må være «offentlig».[112] Offentlig elektronisk kommunikasjonstjeneste er beregnet for eller er tilgjengelig for allmennheten.[113] Dette vil medføre nesten alle slike tjenester, og vil i realiteten medføre den samme type data.

Det følger av kommunikasjonsverndirektivet artikkel 5 nr. 1 at staten skal sikre «the confidentiality of communications and the related traffic data» gjennom nasjonal lovgivning. Dette er forsøkt gjennomført gjennom en rekke bestemmelser i ekomlovgivningen. Spesielt ekomloven § 2-7 femte ledd som medfører en plikt for tilbydere av elektroniske kommunikasjonsnett og -tjenester å slette og anonymisere data som de produserer og lagrer, og § 2-9 om tilbydernes taushetsplikt. Det spesifiseres i kommunikasjonsverndirektivet artikkel 5 nr. 1 at det spesielt skal sikres mot «surveillance of communications» hvis det ikke

[109] Kommunikasjonsverndirektivet artikkel 2 nr. (b) og (c).
[110] Kommunikasjonsverndirektivet artikkel 2 nr. (b).
[111] Kommunikasjonsverndirektivet artikkel 2 nr. (C) og ekomforskriften § 7-1 annet ledd.
[112] Ekomloven § 1-5 nr. 12.
[113] Ekomloven § 1-5 nr. 4.

foreligger samtykke fra brukeren eller for offentlig myndigheter i henhold til kommunikasjonsverndirektivet artikkel 15 nr. 1.

Kommunikasjonsverndirektivet artikkel 5 nr. 3 omhandler lagring og tilegning av data, og at slik data ikke skal lagres uten brukerens samtykke. Lagring og bruk kan likevel uten samtykke skje med det formål å sikre at kommunikasjon kan finne sted.[114] I tillegg førfølger det av artikkel 6 nr. 1 at slik data skal slettes eller anonymiseres når det ikke lenger er nødvendig for å sikre dette forholdet. Artikkel 9 omhandler lokaliseringsdata og legger til grunn at behandling av slik data må skje i anonym form eller med brukerens samtykke. Kommunikasjonsverndirektivet artiklene 5 nr. 3, 6 nr. 1 og 9 er gjennomført i ekomloven § 2-7 femte ledd nr. 1.

Kommunikasjonsverndirektivet artikkel 15 nr. 1 er sentral for avhandlingens område. Denne bestemmelsen gir staten tilgang til å begrense rettighetene og pliktene i bl.a. artiklene 5, 6 og 9 gjennom nasjonal lovgivning. Disse begrensningen må være nødvendige, egnet og proporsjonale, og sikre et legitimt formål slik som nasjonal sikkerhet eller etterforsking av straffbare handlinger.[115] Formålene som nevnes i bestemmelsen er uttømmende.[116] Tiltakene referert til å bestemmelsen skal være i overenstemmelse med EMK og Charteret.[117] Denne bestemmelsen har ingen likelydende bestemmelse i ekomlovgivningen. Det foreligger likevel rettsharmoni mellom norsk rett og Kommunikasjonsverndirektivet artikkel 15 nr. 1 via Grl. § 102 og gjennomføringen av EMK. Ettersom bestemmelsen krever å være i overenstemmelsen med Charteret, vil en nærmere behandling av EU-domstolens tolkning av bestemmelsen finne stede under punkt 4.3, etter at de relevante bestemmelsene i Charteret er redegjort for.[118]

4.2 The Charter of Fundamental Rights of the European Union

Spesielt relevant for tolkningen av kommunikasjonsverndirektivet artikkel 15 nr. 1 tilknyttet problemstillingen i avhandlingen, er Charteret artiklene 7, 8, 11 og 52 nr. 1.[119] Disse vil bli redegjort for i korthet, ettersom kommunikasjonsverndirektivet er det sentrale og Charteret

[114] Kommunikasjonsverndirektivet artikkel 5 nr. 3.
[115] Kommunikasjonsverndirektivet artikkel 15 nr. 1.
[116] *Tele2 Sverige AB* [GC] C-203/15 avsnitt 90.
[117] Kommunikasjonsverndirektivet artikkel 15 nr. 1 siste punktum jf. TEU artikkel 6 nr. 1 og nr. 2.
[118] Se *La Quadrature du Net og andre* [GC] avsnitt 120-122.
[119] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 27.

ikke direkte er del av norsk rett. Artikkel 7 i Charteret sikrer en rett til privatlivet, og er likelydende med Grl. § 102 første ledd første punktum og EMK artikkel 8 nr. 1. Charteret artikkel 8 omhandler beskyttelse av personlig data for enhver, og foreskriver at behandling av slik bare kan finne sted etter samtykke av personen dataen omhandler eller «legitimate basis laid down by law».[120] Artikkel 11 omhandler ytringsfrihet, og er likelydende med EMK artikkel 10 nr. 1 første setning.

Den siste sentrale bestemmelsen i Charteret er artikkel 52 nr. 1. Bestemmelsen har samme funksjon som EMK artikkel 8 nr. 2, ved å hjemle under hvilke rettslige rammer inngrep i rettighetene i charteret kan forekomme lovlig. Rettighetene etter charteret er ikke absolutte.[121] Det kreves for det første etter artikkel 52 nr. 1 at begrensninger i rettighetene må framkomme «by law» og respektere essensen i de rettighetene. I tillegg må begrensningene være proporsjonale, nødvendige og forholde seg til målene til EU og beskyttelsen av rettighetene til andre.[122] Det følger av artikkel 52 nr. 3 at rettighetene i Charteret skal tolkes i lys av de likelydende rettighetene i EMK og EMD praksis, men de skal ikke være til hinder for at EU nedfeller sterkere beskyttelse av de rettighetene.[123] Jeg viser dermed her til gjennomgangen av EMK i punkt 2.1 og 3.

4.3 kommunikasjonsverndirektivets artikkel 15 nr. 1 tolket av EU-domstolen i lys av Charteret

EU-domstolen har tolket kommunikasjonsverndirektivet artikkel 15 nr. 1 slik at offentlige myndigheter bare kan skaffe seg tilgang til trafikk- og lokaliseringsdata tilknyttet etterforsking av straffesaker i de tilfeller der tilbyderne av elektroniske kommunikasjonstjenester har lagret dataen i henhold til direktivet.[124] Dette vil medføre at i tilfeller der dataen er lagret hos tilbyderne i strid med kommunikasjonsverndirektivet, så vil ikke offentlig myndigheter kunne lovlig skaffe seg tilgang til dataen. Et eksempel på slik ulovlig lagring av data vil kunne være generell og vilkårlig lagring av trafikk- og

[120] Charteret artikkel 8 nr. 1 og nr. 2.
[121] *La Quadrature du Net og andre* [GC] avsnitt 120.
[122] Charteret artikkel 52 nr. 1 siste setning.
[123] Se om dette *La Quadrature du Net og andre* [GC] avsnitt 124-128.
[124] *La Quadrature du Net og andre* [GC] avsnitt 167 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 29.

lokaliseringsdata som et forebyggende tiltak.[125] Et annet eksempel vil være der dataen er lagret utover det som er strengt nødvendig.[126] Det er likevel opp til nasjonal rettsorden å avgjøre i hvilke tilfelle ulovlig eller utilbørlig ervervede bevis kan benyttes i straffeforfølgning.[127]

EU-domstolen uttaler i *La Quadrature du Net og andre* at:

> «access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58 may, in principle, be justified only by the public interest objective for which those providers were ordered to retain that data.»[128]

En naturlig forståelse av uttalelsen, er at offentlige myndigheter bare kan gis tilgang til dataen som tilbyderne har lagret, om formålet med lagringen og formålet med tilgangen er sammenfallende. Rui mener, etter en vurdering av *Tele2 Sverige AB* [GC] C-203/15, at staten kan gis tilgang til data lagret for andre formål.[129] Denne vurderingen ble gjort før uttalelsene i *La Quadrature du Net og andre* [GC] og *H.K. v Prokuratuur* [GC] C-746/18, som her tolkes i motsatt retning.[130] Et slikt meningsinnhold vil medføre at om staten ønsker tilgang til data med det formål å etterforske straffesaker, så vil ikke lagret data for eksempelvis kommunikasjons- eller faktureringsformål kunne innhentes.[131]

Alvorlighetsgraden av inngrepet i rettighetene i kommunikasjonsverndirektivet må være vurdert og bekreftet proporsjonale til viktigheten av det legitime formålet før begrensningene kan anses som rettferdiggjort.[132] Dette medfører at kun straffeforfølgning av alvorlig kriminalitet vil være proporsjonal til et alvorlig inngrep i de grunnleggende rettighetene, slik

---

[125] *La Quadrature du Net og andre* [GC] avsnitt 168 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 29. se også *Tele2 Sverige AB* [GC] C-203/15 avsnitt 112.
[126] Kommunikasjonsverndirektivet artikkel. 5 nr. 1 og 3 og artikkel 15. nr. 1, *Tele2 Sverige AB* [GC] C-203/15 avsnitt 109, *La Quadrature du Net og andre* [GC] avsnitt 130 og 156 og Rui (2017) s. 163.
[127] La *La Quadrature du Net og andre* [GC] avsnitt 222 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 41. For en nærmere gjennomgang av bevisavskjæringsreglene innenfor EU, se La *La Quadrature du Net og andre* [GC] avsnitt 223 – 227 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 42-44.
[128] *La Quadrature du Net og andre* [GC] avsnitt 166. se også *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 31.
[129] Rui (2017) s. 161.
[130] *La Quadrature du Net og andre* [GC] avsnitt 166 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 31.
[131] Ekomloven § 2-7 femte ledd nr. 1.
[132] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 32, *La Quadrature du Net og andre* [GC] avsnitt 131, *Ministerio Fiscal* [GC] C-207/16 avsnitt 55 og *Tele2 Sverige AB* [GC] C-203/15 avsnitt 115.

som kan være tilfelle ved lagring av trafikk- og lokaliseringsdata.[133] Motsetningsvis vil et ikke alvorlig inngrep i rettighetene medføre at straffeforfølgning av generell og mindre alvorlig kriminalitet vil være tilstrekkelig.[134]

Om et inngrep i rettighetene i kommunikasjonsverndirektivet anses som alvorlig eller ikke, ser ut til å avhenge av om dataen medfører at nøyaktige konklusjoner om de berørte personenes privatliv.[135] Dette vil generelt være tilfelle med trafikk- og lokaliseringsdata. Trafikk- og lokaliseringsdata vil blant annet kunne si noe om hverdagsvaner, bosted, hvor en person beveger seg, sosiale sammenkomster og sosiale forhold til andre.[136] Slik informasjon kan bidra til å skape en profil om personen som dataen omhandler.[137] Dataen kan på mange måte være meget sensitiv for personene.

I *H.K. v Prokuratuur* [GC] C-746/18 problematiseres det om lengden av perioden som dataen omhandler vil være avgjørende for om inngrepet kan anses som alvorlig.[138] Vil data som omhandler en kort periode medføre at staten kan få tilgang til trafikk- og lokaliseringsdata selv om det er for å straffeforfølge generell og ikke alvorlig kriminalitet?[139] Ut fra proporsjonalitetsbetraktninger, der kun data som er helt nødvendig kan tilgjengeliggjøres, vil en kunne tenke seg at dette kan la seg gjøre.[140] Men EU-domstolen er klar på at selv begrenset tilgang til trafikk- og lokaliseringsdata kan gi grunnlag for å komme med nøyaktige konklusjoner om en persons privatliv, og at tilgang til slik data «is in any event serious».[141] Ettersom det ikke kan avgjøres hvor mye dataen kan si om privatlivet før den er innhentet av det offentlige, vil det avgjørende være den generelle risikoen for privatlivskonklusjoner slik data kan medføre, uavhengig av hvor sensitiv dataen faktisk er.[142]

Det er ikke tilstrekkelig etter kommunikasjonsverndirektivet artikkel 15 nr. 1 at hjemmelen krever at offentlig myndigheters tilgang til dataen følger et legitimt formål. Det må også

---

[133] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 33, *La Quadrature du Net og andre* [GC] avsnitt 140, *Ministerio Fiscal* [GC] C-207/16 avsnitt 56 og *Tele2 Sverige AB* [GC] C-203/15 avsnitt 115.
[134] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 33, *La Quadrature du Net og andre* [GC] avsnitt 140 og *Ministerio Fiscal* [GC] C-207/16 avsnitt 57.
[135] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 39 og 45.
[136] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 36, *La Quadrature du Net og andre* [GC] avsnitt 117 og *Tele2 Sverige AB* [GC] C-203/15 avsnitt 99.
[137] *La Quadrature du Net og andre* [GC] avsnitt 117 og *Tele2 Sverige AB* [GC] C-203/15 avsnitt 99.
[138] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 26 nr. 1.
[139] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 35 og 45.
[140] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 37 og 38.
[141] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 39 og 40.
[142] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 39 og 40.

foreligge «substantive and procedural conditions governing that use».[143] Det må altså foreligge et minimum sett med rettsikkerhetsgarantier som sikrer en effektiv beskyttelse mot faren for misbruk.[144] I *H.K. v Prokuratuur* konkluderer EU-domstolen med at artikkel 15 nr. 1 i kommunikasjonsverndirektivet forhindrer:

> «national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.»[145]

Bakgrunnen for at EU-domstolen konkluderer med at nasjonal påtalemyndighet ikke kan ha kompetanse til å tilegne seg trafikk- og lokaliseringsdata, er fordi retten ikke anser de som tilstrekkelig objektive og upartiske.[146] Dette er fordi påtalemyndigheten har som oppgave å etterforske og bringe inn påtale for retten og dermed ikke vil ha et nøytralt standpunkt selv om det følger av lovgivning at de skal opptre objektive.[147] Bare i tilfeller hvor det foreligger «duly justified urgency», kan kontroll ta sted etter at påtalemyndighetene har fått tilgang.[148] Eu-domstolen åpner ikke for tilfeller der kontroll av retten eller et uavhengig forvaltingsorgan ikke finner sted i det hele tatt.

5 Adgangen til å pålegge utlevering av bevis etter strpl. § 210

Det følger av strpl. § 210 første leddførste punktum at «[t]ing som antas å ha betydning som bevis, kan retten pålegge besitteren å utlevere såfremt han plikter å vitne i saken.» Dette er det primære rettsgrunnlaget som utgjør hjemmelen for å pålegge tilbydere av elektroniske kommunikasjonsmiddel å utlevere trafikk- eller lokaliseringsdata.

---

[143] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 49, *Privacy International* [GC] C-623/17 avsnitt 77, *La Quadrature du Net og andre* [GC] avsnitt 176 og *Tele2 Sverige AB* [GC] C-203/15 avsnitt 118.
[144] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 48, *Tele2 Sverige AB* [GC] C-203/15 avsnitt 117, *Privacy International* [GC] C-623/17 avsnitt 68, *La Quadrature du Net og andre* [GC] avsnitt 132.
[145] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 59.
[146] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 53.
[147] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 47, 54 og 55.
[148] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 51 og 58. se også *La Quadrature du Net og andre* [GC] avsnitt 189.

Straffeprosessen bygger på et prinsipp om fri bevisføring, noe som i praksis medfører at partene som hovedregel kan føre de bevisene de ønsker for retten.[149] En straffeprosess som bygger på et prinsipp om fri bevisførsel tilrettelegger for det første for at resultatet bygger på den materielle sannheten, ettersom fri bevisførsel sikrer at straffesaken blir godt opplyst.[150] For det andre vil prinsippet underbygge tillitten til prosessen hos partene, ettersom en hovedregel om at partene kan føre de bevisene de ønsker, vil medføre at de «får ivareta sine interesser og blir hørt».[151] Prinsippet om fri bevisføring medfører at et forsøk på å gi en fullstendig redegjørelse av de enkelte bevismidler vil være kontraproduktivt i en avhandling som omhandler et spesifikt middel. Det samme vil gjelder for en generell redegjørelse av unntakene som begrenser den frie bevisførselen, da de er mange og omfattende. Det er likevel verdt å nevne at lovbestemt taushetsplikt er et eksempel på en begrensning i den frie bevisførselen og dette vil bli behandlet nærmere under punkt 5.4.1.

Straffeprosesslovens fjerde del om tvangsmidler inneholder en generell bestemmelse som må vurderes under benyttelsen av ethvert tvangsmiddel etter loven, nemlig straffeprosessloven § 170 a. Bestemmelsen uttaler at tvangsmidler kun kan benyttes når det er «tilstrekkelig grunn til det» og ikke kan benyttes når det er «uforholdsmessig inngripende».[152] I praksis har straffeprosessloven § 170 a liten rettslig betydning utover enkelte spesielle tilfeller, og har i Høyesterettspraksis vært mest benyttet tilknyttet vurderingen av varetektsfengsling.[153] Dette er fordi det allerede i Grunnloven og EMK foreligger en grundig utviklet forholdsmessighetsnorm som vil være dekkende for de fleste tvangsmidler som benyttes i straffeprosessen. Denne forholdsmessighetsnormen vil være mer hensiktsmessig for å vurdere inngrepet utfra, da man har flere momenter å bygge argumentene på. At det må foreligge «tilstrekkelig grunn» etter strpl. § 170 a anses som en sikkerhetsventil, som ofte har lite vurderingstyngde utover forholdsmessighetsvurderingen.[154] Tilknytte avhandlingen, ses det ikke som nødvendig å gå nærmere inn på denne bestemmelsen, da det vil ha mer teoretisk betydning.

---

[149] Rt. 2008 s. 605 avsnitt 13.
[150] Øyen (2019) s. 379.
[151] Øyen (2019) s. 379.
[152] Strpl. § 170 a.
[153] Se bl.a. Rt. 2004 s. 1655 avsnitt 13 og Geir Sunde Haugland, Norsk *Lovkommentar: Straffeprosessloven*, note 1014, rettsdata.no.
[154] Øyen (2019) s. 202.

Utleveringspålegg av trafikk- og lokaliseringsdata er ikke et skjult tvangsmiddel på lik linje med kommunikasjonskontroll. Det foreligger likevel noen fellestrekk. Ettersom tvangsmidlet rettes mot tilbydere av elektroniske kommunikasjonstjenester, og ikke den som er mistenkt i straffesaken, medfører dette at den mistenkte ikke har mulighet til å motsette seg inngrepet. Dette er et område som langt på vei krever klare og detaljerte rettsikkerhetsgarantier for når og hvordan inngrepet kan benyttes. Noen av disse følger direkte av ordlyden i bestemmelsen.

5.1 Hva kan pålegges utlevert etter strpl. § 210?

Problemstillingen for avhandlingen knytter seg til «trafikk- og lokaliseringsdata», og strpl. § 210 første ledd fastslår at «ting som antas å ha betydning som bevis» kan pålegges utlevert. Det må bare «antas» å ha betydning, og dermed er det ikke et krav om at det må foreligge sikker kunnskap om innholdet i bevismidlet, eller hva som kan utledes av det i tilknytting til saken. Høyesterett har uttalt at det må foreligge en rimelig mulighet for at materialet har betydning som bevis.[155] Det må foreligge en viss sammenheng mellom det faktum som skal opplyses og bevismidlet, for at vilkåret skal være oppfylt. Dette framstår ikke som noe streng terskel.

Strpl. § 210 første ledd benytter utrykket «ting». Dette er et ganske vidt begrep, som etter en naturlig forståelse innbefatter alle fysiske gjenstander. Dette kan f.eks. være en løsøregjenstand eller dokumentbevis. Et dokumentbevis kan være enten papirbasert eller digitalt.[156] I straffeloven § 69 annet ledd om inndragning av gjenstander regnes også «rettigheter, fordringer og elektronisk lagret informasjon» som ting. Begrepet er nokså allment og må forstås på samme måte i straffeloven og straffeprosessloven.[157] Straffelovens bestemmelse utvider den naturlige forståelsen av begrepet til også å gjelde abstrakte gjenstander. Forarbeidene til straffeprosessloven og Høyesterett har lagt seg på samme linje for elektronisk informasjon, og gitt begrepet substans med å konstatere at telefonnummer,

[155] Rt. 2007 s. 1507 avsnitt 19. Høyesterett viser her til lagmannsretten uttalelse. Når Høyesterett i dommen konkluderer med at lagmannsrettens avgjørelse må oppheves, viser de på at lagmannsretten bygger på feil forståelse av strpl. § 170a, jf. avsnitt 24. Ettersom retten ikke underbygger forståelsen av strpl. § 210, legges det til grunn at Høyesterett mener dette er riktig forståelse av «antas å ha betydning». Se Geir Sunde Haugland, *Norsk Lovkommentar: Straffeprosessloven*, note 1461, Rettsdata.no.
[156] Øyen (2019) s. 367.
[157] Dette gjelder også for f.eks. slik begrepet brukes i straffeprosessloven § 203 om beslag.

telefonsamtaler og domenenavn innbefattes.[158] At elektronisk lagret informasjon også defineres som ting følger godt med den teknologiske utviklingen i samfunnet og harmonerer med en dynamisk utvikling av jussen.

5.1.1 Hva er trafikk- og lokaliseringsdata?

Trafikkdata er definert i ekomforskriften § 7-1 første ledd annet punktum som «data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring». Dette er en nokså teknisk definisjon, som kan være vanskelig for lekmenn å forstå uten spesialkunnskap om elektronisk kommunikasjon. Det er hensiktsmessig å ta utgangspunkt i begrepet kommunikasjon, som er det videste og mest grunnleggende begrepet. Dette begrepet, i sin videste forstand, inneholder all form for informasjonsdeling, hvor enhver handling et menneske gjør er en form for kommunikasjon.[159] Begrepet er ikke spesielt definert i ekomloven eller ekomforskriften, men det følger av kommunikasjonsverndirektivet at kommunikasjon er «any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.»[160] Offentlig kringkasting skal likevel ikke falle inn under definisjonen, utover data som kan benyttes for å identifisere individuelle brukere.[161]

Nasjonal kommunikasjonsmyndighet (Nkom) har på sine hjemmesider forsøkt å gi en mer allmenn beskrivelse av hva de legger i begrepet trafikkdata. Der framkommer det at trafikkdata blant annet innebærer informasjon om hvem du er i telefonsamtaler med, lengden av disse samtaler, sendte og mottatte SMSer og internettlogg.[162] For den allmenne mann i gaten vil dette være en mer forståelig innholdsdefinisjon. I praksis vil all form for kommunikasjon vi benytter oss av tilknyttet elektroniske kommunikasjonsnett medføre trafikkdata.

---

[158] Ot.prp.nr.59 (2003–2004) s. 59. Denne uttalelsen omhandler egentlig «dokumenter eller andre ting» i strpl. § 210 tredje ledd, men det uttales at dette skal forstås likt som «ting» i første ledd. Se også HR-2018-104-A avsnitt 26. Denne uttalelsen fra høyesterett knytter seg til «ting som antas å ha betydning som bevis» i strpl. § 203, men samme forståelse må legges til grunn for strpl. § 210. Se også Rt. 2009 s. 1011 avsnitt 29 og Rt. 2012 s. 1180 avsnitt 13-14, samt Geir Sunde Haugland, *Norsk Lovkommentar: Straffeprosessloven*, note 1460 (jf. 1405), Rettsdata.no.
[159] https://snl.no/kommunikasjon.
[160] Kommunikasjonsverndirektivet artikkel 2 (d).
[161] Kommunikasjonsverndirektivet artikkel 2 (d). Bruker er definert i ekomloven § 1-5 nr. 14 og 15.
[162] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt.

«Data som er nødvendig for å overføre kommunikasjon» sikter til data som skapes når kommunikasjon overføres.[163] Overflødig data utover det som er «nødvendig» for at slik overføring skal kunne finne sted vil ikke dekkes av bestemmelsen. «Fakturering», altså data som sier noe om betalingsforholdet knyttet til overføring av kommunikasjonen, faller likevel under trafikkdata. Trafikkdata begrenses til kommunikasjon overført i et «elektronisk kommunikasjonsnett». Elektronisk kommunikasjonsnett er omfattende og teknisk definert i ekomloven § 1-5 nr. 2. Hovedelementene i begrepet er at det må foreligge et system som muliggjør «overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler». Elektromagnetiske signaler vil f.eks. innebære radiosignaler, som på forskjellige frekvenser benyttes til blant annet bruk av telefon- og internettsignaler.[164]

Lokaliseringsdata, slik begrepet benyttes i avhandlingen, følger av ekomdirektivet § 7-1 annet ledd. Dette kan være trafikk- eller signaliseringsdata ved bruk av elektronisk kommunikasjonsnett eller -tjeneste som angir den geografiske plasseringen av terminalutstyr.[165] Lokaliseringsdata er dermed et videre begrep enn trafikkdata. Terminalutstyr er produkter som kan benyttes til elektronisk kommunikasjon for tilknytning til nettermineringspunkt i elektronisk kommunikasjonsnett, eksempler på terminutstyr kan være telefoner, nettbrett og PCer.[166] Lokaliseringsdata tilknyttes ikke bare elektroniske kommunikasjonsnett, men også elektroniske kommunikasjonstjenester. Dette medfører ingen reell forskjell, ettersom elektroniske kommunikasjonstjenester «omfatter formidling av signaler i elektronisk kommunikasjonsnett», jf. ekomloven § 1-5 nr. 3. Det meste av kommunikasjon fra vanlige brukere av kommunikasjonsnett skjer via elektroniske kommunikasjonstjenester.

Lokaliseringsdata kan også være signaliseringsdata. Det framkommer av ekomforskriften § 7-2 første ledd annen setning at signaliseringsdata alene «genereres mellom terminalen og tilgjengelig basestasjon og angir terminalens geografiske plassering når den er slått på, uten at trafikkdata formidles». Dette er informasjon som genereres i nettet for å kunne dirigere trafikk til og fra terminalen, selv om enheten ikke er aktivt i bruk.[167] Signaliseringsdataen bidrar til å

[163] Ekomforskriften § 7-1 første ledd annet punktum.
[164] https://snl.no/elektromagnetiske_bølger og https://snl.no/radiobølger.
[165] Ekomforskriften § 7-1 annet ledd.
[166] Ekomloven § 1-5 nr. 8 og 12.
[167] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt.

kunne angi den geografiske plasseringen av terminalen grundigere, og ligger i kjernen av hva lokaliseringsdataen innebærer.

Det følger få materielle vilkår tilknyttet utleveringspålegg etter strpl. § 210. Det er i all hovedsak tre materielle vilkår, at det som kan utleveres må være «ting som antas å ha betydning som bevis», at den pålegget rettes mot må ha «vitneplikt» (som vil bli behandlet under punkt. 5.4) og at den pålegget rettes mot på besitte beviset (som vil bli behandlet hunder punkt. 5.3).[168] Ettersom ting er et meget vidt begrep setter dette ingen grenser for hvilken trafikk- og lokaliseringsdata som kan utleveres. I realiteten vil den mest inngripende historiske trafikk- og lokaliseringsdata, som kan si mye om en persons identitet, falle inn under begrepet «ting». Det som i større grad bidrar til å begrense påleggsadgangen, er at dataen må antas å ha betydning som bevis, at det må foreligge en rimelig mulighet for at dataen har betydning. Dette er på ingen måte en høy materiell terskel. Den sikrer likevel mot tilfeller der trafikk- og lokaliseringsdata på ingen måte kan bidra til å oppklare det straffbare forholdet. Ettersom en større og større del av vårt privatliv kommer frem av slik data, vil dette medføre at en større og større andel av slik data vil være nyttig for oppklaring av straffbare forhold. Dette medfører at terskelen for når slik data har en rimelig betydning blir mindre. Og ettersom dette er en lav terskel i utgangspunktet, så medfører dette en meget svakt materiell rettsikkerhetsgaranti mot inngrep. Utfra denne definisjonen og tolkningen av begrepet ting i strpl. § 210, vil trafikk- og lokaliseringsdata falle inn under bestemmelsens virkeområde. Begrepet ting er ikke teknologibaser, og det fremkommer i forarbeidene at elektronisk informasjon er ment å innbefattes.

5.2 Når «besitter» tilbydere av elektroniske kommunikasjonsmidler bevis?

Et av vilkårene i strpl. § 210 gjelder hvem et pålegg kan rettes mot. Dette er avgjørende for å vurdere om tilbydere av elektronisk kommunikasjonsmidler kan pålegges å utlevere bevis etter bestemmelsen. Begrepet som benyttes i strpl. § 210 er «besitteren». Etter en naturlig forståelse av begrepet er besitteren den som sitter på beviset eller som har beviset tilgjengelig. Ordlyden sondrer ikke mellom fysiske og juridiske personer. Under en etterforskning vil det ofte være behov for å sikre bevis som er tilgjengelig hos juridiske personer.

[168] Strpl. § 210 første ledd første punktum.

Påtalemyndighetens adgang til å sikre bevis ville vært begrenset uten mulighet for å pålegge juridiske personer å utlevere bevis.

Tilbydere av elektronisk kommunikasjonsmidler er definert i ekomloven. § 1-5 nr. 16: «enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste.» Når avhandlingen taler om «tilbydere av elektronisk kommunikasjonsmidler», er det med utgangspunkt i at begrepet faller inn under definisjonen i ekomloven. § 1-5 nr. 16. Det kommer fram av definisjonen at tilbydere kan være både fysiske og juridiske personer. Det er hovedsakelig juridiske personer som er aktuelle. Det følger av ekomforskriften § 1-2 at tilbydere plikter å registrere seg for Nkom. Kjente eksempler på tilbydere er Telenor og Telia, som tilbyr blant annet offentlig ekomnett og telefontjenester.[169]

5.2.1 Tilbyderes adgang og plikt til å lagre trafikk- og lokaliseringsdata etter ekomlovgivningen

Adgangen for tilbydere av elektronisk kommunikasjonsnett- eller tjenester til å lagre data er begrenset slik ekomlovgivningen lyder i skrivende stund. Når det gjelder trafikk- og lokaliseringsdata, følger det av ekomloven § 2-7 femte ledd at dataen skal «slettes eller anonymiseres så snart de ikke lenger er nødvendige». Til hvilke formål lagring av data kan finne sted, følger videre av femte ledd nr. 1 til 3. Antitetisk vil dermed adgangen til å lagre slik data kun rekke fram til sletningsplikten inntreffer. Ettersom dataen skal slettes så snart den ikke lenger er nødvendig, er det hva som er nødvendig lagring av data som er avgjørende for vurderingen. Hva som kan anses som nødvendig lagring, må vurderes opp mot formålet for lagringen, ettersom noen type lagring kan være nødvendig for et formål, men ikke for et annet. Lagring utover dette kan likevel finnes sted så lenge det foreligger samtykke fra brukeren.

Etter ekomloven § 2-7 femte ledd nr. 1 kan nødvendig lagring av data finne sted til «kommunikasjons- eller faktureringsformål». Lagring til kommunikasjonsformål er lagring av data slik at elektronisk kommunikasjon kan finne sted. Denne type lagring vil være nokså begrenset. Eksempelvis for telefonsamtaler vil behovet for lagring forsvinne så snart telefonsamtalen er mottatt, og for elektroniske meldinger vil kommunikasjonen være fullført

[169] https://www.nkom.no/files/ekomstat/Tilbyderoversikt.pdf.

så fort posten er mottatt, typisk fra serveren til tilbyderen.[170] Ettersom lagring av data for kommunikasjonsformål er såpass begrenset, vil historiske dataen tilgjengelig for staten å pålegge utlevert være nokså ikke-eksisterende.

Faktureringsformål på sin side vil nok medføre en utvidet nødvendighet for lagring av data. De fleste elektroniske kommunikasjonstjenester som betales av brukere benytter seg av abonnementsløsninger, f.eks. telefonabonnementer eller brebåndstilgang til hjemmet.[171] Med en fast pris hver måned, kan det problematiserer hvor nødvendig lagringen av store mengder data er. Om det foreligger løsninger hvor man i abonnementet mottar en begrenset mengde data, og må betale ekstra for data over denne grensen, så vil det muligens være behov å lagre data for å ha oversikt over hvor mye data som er benyttet. Her vil det likevel være større nødvendighet for å lagre trafikkdata enn lokaliseringsdata, ettersom lokaliseringsdata sier noe om geografisk plassering og ikke datamengde.[172] Lagring av trafikkdata til faktureringsformål kan være nødvendig for å stoppe «fraud consisting of unpaid use».[173]

Det foreligger et vedtatt lovforslag, som vil tre i kraft 1. januar 2022, som gjør endringer på ekomloven § 2-7 femte ledd nr. 2.[174] Denne medfører at lagring av data for å oppfylle pliktene etter § 2-8 a også skal slettes når det ikke lenger er nødvendig.[175] Ekomloven § 2-8 a trer også i kraft 1. januar 2022.[176] Plikten til å lagre data etter ekomloven § 2-8 a omhandler lagring av IP-adresser. IP-adresse står for «Internet Protocol Address» og er en unik adresse som tildeles en enhet eller et terminalutstyr som er tilkoblet internett.[177] Funksjon til IP-adressen er dermed å kunne identifisere hvilken enhet som har kommunisert elektronisk over nett. I seg selv vil IP-adressen kun kunne si noe om hvilken enhet som er benyttet og ikke i seg selv noe om innholdet i kommunikasjonen. IP-adresser er nødvendig for at elektronisk kommunikasjon over internett kan finne sted, ettersom de gjør det mulig å sende og motta data over nettet, og sikrer at den kommer fram til riktig destinasjon på internett.[178] Dette faller naturlig under definisjonen av trafikkdata som er gjennomgått ovenfor under punkt 5.1.1. Nkom anser trafikkdata å innbefatte logger fra oppkobling til internett som inneholder hvilke IP-adresser

[170] Kommunikasjonsverndirektivet fortale avsnitt 27 og Rui (2017) s. 163.
[171] Rui (2017) s. 164-165.
[172] Rui (2017) s. 164-165.
[173] Kommunikasjonsverndirektivet fortale avsnitt 29 og Rui (2017) på s. 164.
[174] Lov nr. 131/2021.
[175] Lov nr. 131/2021.
[176] Lov nr. 131/2021.
[177] Prop.167 L (2020–2021) s. 13.
[178] Prop.167 L (2020–2021) s. 13.

som er tildelt, men sier ikke at IP-adressen i seg selv er trafikkdata. EU-domstolen anser IP-adresser som del av trafikkdata, men mindre sensitiv enn annen trafikkdata.[179]

Det følger av ekomloven § 2-8 a første ledd at tilbyderne «til bruk for etterforsking av alvorlig kriminalitet, [skal] lagre de opplysninger som er nødvendige for å identifisere abonnenten». Dette skal gjøres med utgangspunkt i «offentlig IP-adresse og et tidspunkt for kommunikasjon» eller «offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse er tildelt flere abonnenter samtidig».[180] Et portnummer er nummer som gjør det mulig å identifisere et abonnement entydig.[181] Destinasjonsdata (data som sier noe om hvor kommunikasjonen går) skal ikke lagres.[182] IP-adresser skal lagres i tolv måneder.[183] Ettersom tilbyderne har adgang til å lagre trafikk- og lokaliseringsdata etter ekomloven § 2-7 femte ledd og en plikt til å lagre IP-adresser etter § 2-8 a første ledd, så vil tilbyderne besitte dataen fram til de sletter den. Om de besitter dataen etter at slettingsplikten foreligger, vil dette være ulovlig lagring.

Et sentralt moment etter EU-domstolens praksis er at dataen må være lagret i henhold til artikkel 5, 6, 9 og 15 nr. 1 i kommunikasjonsverndirektivet, for at staten tilgang til dataen skal være lovlig.[184] Tilknyttet formålet for lagring etter ekomloven § 2-7 femte ledd nr. 1 følger det direkte av kommunikasjonsverndirektivet artikkel 5 nr. 1 og artikkel 6 nr. 2. Tilknyttet etterforsking av straffbare handlinger følger dette av direktivet artikkel 15 nr. 1. Et annet krav er at lagringen må være streng nødvendig.[185] Dette følger av ordlyden i ekomloven § 2-7 femte ledd. Selv om begrepet strengt ikke benyttes i ekomloven § 2-7, må dette tolkes slik etter EU-domstolens praksis.[186] Lagring av IP-adresser etter ekomloven § 2-8 a skal finne sted i tolv måneder, jf. bestemmelsens annet ledd. Departementet har likevel vurdert det slik at en lagringstid på tolv måneder er nødvendig for å sikre politiets mulighet til å bekjempe alvorlig kriminalitet.[187] Det vises blant annet til saksbehandlingstiden for enkelte straffesaker og at

---

[179] *La Quadrature du Net og andre* [GC] avsnitt 152 og Prop.167 L (2020–2021) s. 22.
[180] Ekomloven § 2-8 a nr. 1 og 2.
[181] Prop.167 L (2020–2021) s. 14.
[182] Ekomloven § 2-8 a første ledd annet punktum.
[183] Ekomloven § 2-8 a annet ledd.
[184] *La Quadrature du Net og andre* [GC] avsnitt 167 og *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 29.
[185] Kommunikasjonsverndirektivet artikkel. 5 nr 1 og 3 og artikkel 15. nr. 1, *Tele2 Sverige AB* [GC] C-203/15 avsnitt 109, La *La Quadrature du Net og andre* [GC] avsnitt 130 og 156 og Rui (2017) s. 163.
[186] Kommunikasjonsverndirektivet artikkel. 5 nr 1 og 3 og artikkel 15. nr. 1, *Tele2 Sverige AB* [GC] C-203/15 avsnitt 109, La *La Quadrature du Net og andre* [GC] avsnitt 130 og 156 og Rui (2017) på s. 163.
[187] Prop.167 L (2020–2021) s. 46-47.

saker ofte ikke kommer i politiets søkelys før lenge etter at et straffbart forhold finner sted.[188] En generell plikt til å lagre IP-adresser i tolv måneder vil i enkelte tilfeller kunne medføre at dataen lagres lengre enn strengt nødvendig. I et slikt tilfelle vil plikten til å lagre dataen i tolv måneder stå i motstrid til kravet om at dataen skal slettes når den ikke lenger er strengt nødvendig. Da må nødvendighetskravet ha forrang ettersom det følger av kommunikasjonsverndirektivet artikkel 15, og lagringen må anses som ulovlig.[189] Ut fra departementets vurdering for hva som er strengt nødvendig vil likevel veie tungt under denne vurderingen, noe som vil medføre at motstridsituasjonen vil finne sted sjeldent i realiteten.[190]

5.3 Hvem har kompetanse til å pålegge utlevering av bevis etter strpl. § 210?

Etter straffeprosessloven § 210 første ledd er det klart at det er «retten» som har kompetansen til å pålegge utlevering av bevis. Det følger av det overordnede anklageprisnippet i straffeprosessen at domstolene bare trer i kraft på begjæring fra påtalemyndigheten.[191] Dette medfører at retten ikke på eget initiativ kan pålegge noen å utlevere bevis, det kan kun gjøres i forbindelse med en etterforsking av en straffesak, og kun når påtalemyndigheten har begjært det av retten.[192] Anklageprinsippet framhever kompetansefordelingen mellom påtalemyndigheten og domstolen, og understreker påtalemyndighetens rolle som leder av etterforskingen.[193] Dette er en viktig prosessuell garanti, ettersom det medfører at påtalemyndighetene har vært nødt til å vurdere de materielle vilkårene grundig før de legger frem begjæring for retten. Om påtalemyndigheten ikke tilstrekkelig argumenterer for at de materielle vilkårene er oppfylt, vil ikke retten kunne godkjenne begjæringen om pålegg. Domstolen fremstår også som et mer objektivt og uavhengig organ enn påtalemyndigheten, noe som medfører at en kompetansefordeling til retten vil i større grad sikre mot misbruk og vilkårlighet.

---

[188] Prop.167 L (2020–2021) s. 46-47.
[189] Rt. 2000 s. 1811 s. 1826 og 1833.
[190] Rt. 2000 s. 1811 s. 1831.
[191] For hovedforhandlingsstadiet er dette forankret i straffeprosessloven § 63. se også strpl. § 38 og Rt. 2011 s. 172 avsnitt 19. For etterforskingsstedet avhenger dette av en analogisk anvendelse av strpl. § 38, se Øyen (2019) s. 454.
[192] Øyen (2019) s. 129.
[193] Øyen (2019) s. 129.

Et unntak fra hovedregelen i strpl. § 210 første ledd, følger av annet ledd første punktum: «[d]ersom det ved opphold er fare for at etterforskingen vil lide, kan ordre fra påtalemyndigheten tre istedenfor beslutning av retten.» Strpl. § 210 annet ledd første punktum åpner opp for at påtalemyndigheten unntaksvis kan gis kompetansen til å pålegge utlevering av bevis, men det følger likevel av annet ledd annet punktum at «[p]åtalemyndighetens beslutning skal snarest mulig forelegges retten for godkjennelse». Selv om påtalemyndighetens ordre må fremlegges retten for overprøving, så vil dette da finne sted etter at påtalemyndigheten har fått tilgang til bevismaterialet. En slik etterkontroll av om de materielle vilkårene er til stede er ikke en like effektiv prosessuell rettssikkerhetsgaranti mot misbruk. Dette er likevel forenelig med EU-domstolens tolkning av kommunikasjonsverndirektivet artikkel 15. nr. 1, da det er behov for i enkelte tilfeller å gjøre unntak fra hovedregelen.[194] Om retten etter stpl. § 210 annet ledd annet punktum kommer til at påtalemyndigheten har vurdert de materielle vilkårene for utleveringspålegg uriktig, vil ordren finnes ugyldig. Dette vil kunne medføre at beviset er ervervet på ulovlig grunnlag, og dermed potensielt vil kunne avskjæres.

EU-domstolens tolkning av kommunikasjonsverndirektivet artikkel 15 nr. 1 medfører at påtalemyndigheten ikke er kompetent til å tilegne seg trafikk- og lokaliseringsdata, utenom tilfeller der det foreligger «duly justified urgency».[195] Straffeprosessloven § 210 er forenelig med denne tolkningen formelt sett. Det er kun «dersom det ved opphold er fare for at etterforskingen vil lide», at påtalemyndigheten delegeres en midlertidig kompetanse til å avgjøre bevisutlevering. Dette vil som regel være på bakgrunn av tidsmessige utfordringer, der det haster å få tilgang til bevismateriale, at vilkåret gjør seg gjeldende. For utlevering av «trafikk- og lokaliseringsdata» vil behovet for fritak fra taushetsplikt jf. strpl. § 118 (som vil bli behandlet nedenfor under 5.4.2), medføre at det sjelden vil være et så sterkt tidspress på etterforskingen at det ikke er mulig for påtalemyndigheten å begjære retten om utlevering. Tilbydernes lagringsadgang for trafikk- og lokaliseringsdata etter ekomloven § 2-7 femte ledd (gjennomgått ovenfor under punkt 5.2.1) er nokså begrenset. Dette medfører at det ofte kan foreligge et tidspress å tilegne seg dataen før den slettes hos tilbyderne. Dette kan i verste fall

[194] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 58 og 59.
[195] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 58 og 59.

medføre en uheldig forskyving av kompetansen, ettersom dette tidspresset vil medføre at påtalemyndigheten oftere anser det som fare for at etterforskingen vil lide ved opphold.

5.4 Krav om vitneplikt for å pålegge utlevering av bevis

Det er kun en juridisk person som har vitneplikt i saken, som kan pålegges å utlevere bevis, jf. strpl. § 210 første ledd første punktum. Dette medfører at tilbydere av elektronisk kommunikasjonsmidler kun kan pålegges å utlevere «trafikk- og lokaliseringsdata» om de også plikter å vite i saken. For å avgjøre dette må det tas utgangspunkt i straffeprosessloven kap. 10 om vitner.

Som tidligere nevnt, bygger norsk straffeprosess på et prinsipp om fri bevisførsel. Dette medfører at alle som hovedregel har plikt å vitne i straffesaker. Dette følger også av strpl. § 108, hvor det kommer fram at «[e]nhver plikter etter innkalling å møte som vitne og forklare seg overfor retten, med mindre annet er bestemt ved lov.» Ettersom utgangspunktet er fri bevisførsel og vitneplikt, vil det som avgjør om tilbydere av elektronisk kommunikasjonsmidler har vitneplikt, være om det foreligger et unntak bestemt ved lov, jf. strpl. § 108.

For tilbydere av elektronisk kommunikasjonsmidler gjør straffeprosessloven § 118 seg gjeldende. Det følger av bestemmelsens første ledd, første og annet punktum at retten ikke kan ta imot forklaring fra «tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste» uten samtykke fra departementet, om de har lovbestemt taushetsplikt. Sagt med andre ord; hvis tilbydere av elektronisk kommunikasjonsmidler har lovbestemt taushetsplikt, kan de ikke vitne i saken om departementet ikke har samtykket i det. For problemstillingen i denne avhandlingen, vil en lovhjemmel som gir tilbydere av elektroniske kommunikasjonsmidler taushetsplikt når det kommer til å meddele brukernes trafikk- og lokaliseringsdata være avgjørende for om slik informasjon dekkes av forklaringsforbudet i strpl. § 118.

5.4.1 Lovbestemt taushetsplikt i ekomlovgivningen

En aktuell hjemmel for lovbestemt taushetsplikt tilknyttet trafikk- og lokaliseringsdata, følger av ekomloven. § 2-9. Det følger av første ledd at «tilbyder ... plikter å bevare taushet om

innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon». Det som er avgjørende for om trafikk- og lokaliseringsdata faller inn under taushetsplikten i ekomloven. § 2-9 første ledd, er om dataen faller inn under definisjonen av «elektronisk kommunikasjon» i ekomloven. § 1-5 nr. 1. Det følger av definisjonen at det med elektronisk kommunikasjon menes «kommunikasjon ved bruk av et elektronisk kommunikasjonsnett».[196] Begrepet elektronisk kommunikasjon skal være teknologinøytralt, og definisjonen ble dermed endret i 2013 for å synliggjøre den teknologiske utviklingen.[197] Det er deler av trafikk- og lokaliseringsdata som ikke direkte naturlig faller inn under begrepet kommunikasjon, da denne type data sier mer om hvor og hvilken type kommunikasjon som er benyttet. Slik generell informasjon, som sier noe om den direkte kommunikasjon, er en form for kommunikasjon i seg selv, da en bruker gir fra seg denne type informasjon når de benytter seg av elektroniske kommunikasjonsmidler. Ekomloven. § 1-5 nr. 1 benyttet tidligere begrepet «overføring», men dette begrepet ble tatt ut av loven for å synliggjøre at «annet som fører til formidling i et elektronisk kommunikasjonsnett omfattes».[198] Samlet sett framstår «trafikk- og lokaliseringsdata» å falle inn under definisjonen av «elektronisk kommunikasjon» i ekomloven. § 1-5 nr. 1. Dette medfører at «trafikk- og lokaliseringsdata» er dekket av taushetsplikten i ekomloven. § 2-9 første ledd.

5.4.2 Krav om at departementet samtykker til at tilbyderne fritas fra taushetsplikten

Ett av vilkårene i strpl. § 118 første ledd første punktum, er at «departementet» ikke har samtykket til at retten kan ta imot forklaringen som er underlagt taushetsplikt. Hvis departementet samtykker så er ikke den lovbestemte taushetsplikten til hinder for at tilbydere har vitneplikt. Det kommer fram av ekomloven. § 1-4 at «myndighet etter loven er Kongen, departementet og Post- og teletilsynet» (nå Nasjonal kommunikasjonsmyndighet). Bestemmelsen åpner for at departementet kan delegere sin myndighet til andre organer, noe som også følger av regjeringens rett til å organisere forvaltningen selv.[199] Samtykkekompetansen etter strpl. § 118 er delegert til Nkom.[200]

---

[196] Ekomloven. § 1-5 nr. 1.
[197] Prop.69 L (2012–2013) s. 94.
[198] Prop.69 L (2012–2013) s. 94.
[199] Ot.prp.nr.58 (2002–2003) s. 85.
[200] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt#fritak_fra_taushetsplikt.

Vurderingstema for når samtykke skal gis, følger av strpl. § 118 første ledd tredje punktum hvor det framkommer at «samtykke kan bare nektes om åpenbaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold». Ved bruk av begrepet «bare», legger bestemmelsen opp til at terskelen for å gi samtykke er lav. Dette medfører at det skal litt til for at de to alternative vilkårene for å nekte samtykke i strpl. § 118 er oppfylt. Det må altså foreligge grunner for å nekte samtykke i motsetning til grunner for å gi samtykke. Dette er en subtil forskjell som i realiteten nok ikke vil medføre en stor differanse. Det må «virke urimelig overfor den som har krav på hemmelighold» for at samtykke ikke skal gis.

Det første vilkåret, «åpenbaringen vil kunne utsette staten eller allmenne interesser for skade», framstår ikke som generelt relevant for trafikk- og lokaliseringsdata. Trafikk- og lokaliseringsdata er data tilknyttet de enkeltpersonene som dataen omhandler, og vil på generell basis ikke medføre at staten eller allmenne interesser kan skades. Dette avhenger av hvilken samfunnsstilling brukeren av den elektroniske kommunikasjonstjenesten har, og innholdet i dataen. Det andre vilkåret I strpl. § 118 første ledd tredje punktum, at åpenbaringen vil «virke urimelig overfor den som har krav på hemmelighold», framstår som mer aktuelt. Den som har krav på hemmelighold, er brukeren av det elektroniske kommunikasjonsmidlet. Vurderingstemaet er om det vil virke «urimelig». Hva som anses som urimelig, vil måtte vurderes fra sak til sak, alt etter hvor inngripende tiltaket er i privatlivet til brukeren, og hvor sensitiv data det er tale om.

Det materielle vilkåret om vitneplikt for den som skal utlevere beviset vil medføre en sterk rettsikkerhetsgaranti. Ettersom det som hovedregel kreves at Nkom har samtykket til at tilbyderen av elektroniske kommunikasjonsnett og -tjenester er fritatt fra taushetsplikt for at trafikk- og lokaliseringsdata kan utleveres, vil dette skape et ekstra ledd som vurderer vilkårene før utlevering finner sted. Nkom er uavhengig av både retten og påtalemyndigheten, og vil dermed, fritt fra etterforskingen, vurdere terskelen på selvstendig grunnlag.

På Nkom sine hjemmesider, framkommer det hva de vurderer som urimelig tilknyttet trafikk- og signaleringsdata.[201] Som gjennomgått under punkt 5.1.1, kan lokaliseringsdata være både trafikkdata og signaleringsdata. For trafikkdata framkommer det at det gjøres en avveining

[201] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt#fritak_fra_taushetsplikt.

mellom «hensynet til den personlige integritet og personvern mot politiets behov for bevis i straffesaker og samfunnets ønske om kriminalitetsbekjempelse.»[202] Denne vurderingen vil ligge tett opp mot forholdsmessighetsvurderingen i strpl. § 170 a, grl. § 102, EMK artikkel 8 og kommunikasjonsverndirektivet artikkel 15. nr. 1. I tillegg vurderes «hvor viktig elektroniske spor er for etterforsking av saken, og muligheter for å anvende andre etterforskingsmetoder.»[203] Dette er imidlertid lite forenelig med vilkåret at det skal virke urimelig for den som har krav på hemmelighold. Disse vurderingsmomentene knytter seg kun opp mot påtalemyndighetens behov for dataen, mens ordlyden i bestemmelsen viser til hensyn for personen dataen omhandler. Det er brukeren som skal stå i fokus for vurderingen. Disse momentene bidrar i liten grad til å finne frem til når det virker urimelig overfor brukeren. Urimelighetsvurdering vil langt på vei knytte seg opp mot hvor sensitiv dataen er, hvor mye data det er tale om og hvilken periode dataen omhandler. Det fremkommer i tillegg en form for forholdsmessighetsvurdering mellom den personlige integritet mot behovet for beviset. Dette vil være mer forenelig med en urimelighetsvurdering.

For signaleringsdata blir det litt mer komplisert. Her framkommer det at «trafikkdata bør innhentes og analyseres før det kan tas en reell vurdering av behovet for fritak fra taushetsplikten for signaleringsdata.»[204] Terskelen for å samtykke til utlevering av signaliseringsdata er dermed høyere enn ved trafikkdata. Samtidig kan dette medføre at terskelen for å utlevere trafikkdata blir lavere i tilfeller der signaleringsdata er relevant, ettersom det er behov å vurdere trafikkdataen. Det fremstår mangelfullt at dette ikke er et lovfestet krav som følger direkte av ordlyden. I tillegg burde dette også være et vurderingstema tilknyttet trafikkdata, da denne dataen også kan si mye om en persons identitet.

5.4.3 Unntak fra taushetsplikten i ekomloven § 2-9

Det materielle kravet om departementets samtykke til unntak fra vitneplikt er ikke absolutt, og det finnes enkelte unntak. Dette medfører at kravets styrke i enkelte tilfeller svekkes. For det

[202] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt#fritak_fra_taushetsplikt.
[203] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt#fritak_fra_taushetsplikt. se også Se Thomas Chr. Poulsen, *Norsk Lovkommentar: Straffeprosessloven*, note 733, Rettsdata.no.
[204] https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt#fritak_fra_taushetsplikt.

første kan retten overprøve departementets avgjørelse om samtykke, jf. strpl. § 118 andre ledd. Retten vil i det tilfelle foreta en «avveining av hensynet til taushetsplikten og hensynet til sakens opplysning».[205] Retten tar altså en avveining av privatpersonens behov for taushetsplikt opp mot hvor nødvendig beviset er for avgjørelsen av saken. Dette er i seg selv en rettsikkerhetsgaranti som sikre at vurderingen fra påtalemyndigheten og Nkom er korrekt.

Det følger av ekomloven. § 2-9 tredje ledd første punktum at «[t]aushetsplikten er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse». Om trafikk- og lokaliseringsdata kan tolkes inn i en av disse unntakene fra den lovbestemte taushetsplikten, vil informasjonen ikke være dekket av strpl. § 118. Slik data kan utleveres til påtalemyndigheten uten ytterligere materielle skranker enn at de antas å ha betydning som bevis. Dette fremstår lite forenelig med kravet om at det må foreligge klare materielle vilkår for å tilegne seg slik data. Dataen er i seg selv i mindre sensitiv enn annen trafikkdata, og gjør det på den måten i mindre grad mulig å kunne trekke konklusjoner om privatlivet.[206]

Det følger også et unntak fra taushetsplikten av § 2-8 b om utlevering av IP-adresser. Ekomloven § 2-8 b er i skrivende stund ikke tredd i kraft, men vil tre i kraft 1. januar 2022. Det følger av bestemmelsen at opplysninger lagret etter § 2-8 a (Dette gjelder IP-adresser, se punkt. 5.2.1 ovenfor), skal uten hinder av taushetsplikt etter § 2-9 utleveres til politiet eller påtalemyndigheten».[207] Etter denne bestemmelsen foreligger det ytterligere materielle vilkår. Dette medfører at mangel på samtykkekravet som gjelder generelt for trafikk- og lokaliseringsdata ikke i seg selv vil medføre et svakere materielt vern av disse opplysningene. Ekomloven § 2-8 b innfører et generelt strafferammekrav på 3 år eller med, noe som langt på vei sikrer at alvorligheten av den straffbare handlingen er et moment som må vurderes før tilgang kan gis.[208] I tillegg medfører den et krav til at dataen må være nødvendig for etterforskningen.[209] Det må foretas en konkret vurdering av behovet for beviset, men nødvendighetskravet må ikke tolkes så strengt at det krever at beviset er det eneste som kan

[205] Strpl. § 118 annet ledd.
[206] *La Quadrature du Net og andre* [GC] avsnitt 152 og Prop.167 L (2020–2021) s. 22.
[207] Lov nr. 131/2021.
§ 2-8 b første ledd første punktum.
[208] Ekomloven § 2-8 b første ledd.
[209] Ekomloven § 2-8 b første ledd.

oppklare saken.[210] Dette kravet er noe strengere enn kravet til at tingen må antas å ha betydning som bevis i strpl § 210 første ledd.

Det fremstår som usikkert hvordan ekomloven § 2-9 tredje ledd står mot utlevering av IP-adresser i ekomloven § 2-8 b, som også kan kategoriseres som abonnementsopplysninger og elektronisk kommunikasjonsadresse.[211] Den nye bestemmelsen er et forsøk fra departementets side på å stramme inn vilkårene for å få tilgang til slike opplysninger for at de skal være sammenfattende med de overordnede kravene som følger av grunnloven, EMK og EØS-retten.[212] Medfører den nye bestemmelsen i ekomloven § 2-8 b at kravet til å få utlevert IP-adresser skjerpes? Når ikke tilgangen etter ekomloven § 2-9 tredje ledd endres ved innføringen av § 2-8 b, medfører dette at det foreligger to hjemler for utlevering av IP-adresser, som har forskjellige materielle terskler. Ut fra systembetraktninger fremstår dette som noe rotete fra lovgivers side.

Ut fra av ekomloven § 2-8 b er det påtalemyndigheten som direkte er tildelt kompetansen til å tilegne seg IP-adresser. IP-adresser er i en mindre sensitiv del av trafikkdata, og er av den grunn mindre inngripende enn resten av trafikk- og lokaliseringsdata som kan pålegges utlevert etter strpl. § 210 første ledd.[213] Det følger i tillegg strengere materielle vilkår etter denne bestemmelsen enn det som følger av hjemmelen for utleveringspålegg i strpl. § 210. Dette vil bidra til å balansere rettsikkerhetsgarantiene, ved at det foreligger svakere prosessuelle garantier, men strengere materielle garantier. Tilbydere er likevel pliktet til å lagre IP-adresser i tolv måneder, som er en utvidet lagringsadgang enn den som følger for resten av trafikk- og lokaliseringsdata i ekomloven § 2-7 femte ledd.

At utleveringspåleggskompetansen er direkte fordelt påtalemyndigheten er problematisk tilknyttet EU-domstolens tolkning av kommunikasjonsverndirektivet artikkel 15 nr. 1, hvor de kom til at kompetansen ikke kunne tilfalle påtalemyndigheten med mindre det forelå duly justified urgency.[214] Tilknyttet denne vurderingen konkluderer departementet med at:

> «I lys av det skillet som oppstilles i *La Quadrature du Net*, der IP-data omtales som en kategori av data som er mindre følsomme enn andre former for trafikkdata, og i lys av

[210] Prop.167 L (2020–2021) s. 54.
[211] Prop.167 L (2020–2021) s. 13 og 48.
[212] Prop.167 L (2020–2021) s. 13 og 49.
[213] *La Quadrature du Net og andre* [GC] avsnitt 152 og Prop.167 L (2020–2021) s. 22.
[214] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 58 og 59.

> at forslaget her ikke kan sies å muliggjøre presise slutninger om folks privatliv, finner departementet ikke at det nå er nødvendig å innføre et generelt krav om forhåndskontroll for utlevering av IP-adresser på grunnlag av EU-domstolens praksis.»[215]

Denne vurderingen fremstår som problematisk. Under vurderingen av dette spørsmålet i *H.K. v Prokuratuur* [GC] C-746/18, gjøres det intet skille tilknyttet hvor presis slutning som kan trekkes om folks privatliv, men omhandler trafikkdata generelt.[216] Dette skille i alvorlighetsgrad fremkommer under vurderingen knyttet til hvilket formål som kan begrunne tilegning av data. Da dette ikke blir vurdert under det siste spørsmålet, fremstår det som klart av EU-dosmtolens konklusjon at dette prosessuelle kravet skal gjelde for alle typer trafikkdata. selv om under vurderingen av proporsjonaliteten av inngrepet må legges vekt på inngrepets størrelse og hvilke andre rettsikkerhetsgarantier som foreligger, fremstår det likevel mangelfullt at IP-adresser kan utleveres uten at retten har vært inne og vurdert forholdet overhode. Hjemmelen i ekomloven § 2-8 b er også et unntak fra taushetsplikten, slik at Nkom heller ikke på noen måte er inne og vurderer nødvendigheten av inngrepet. Selv om bestemmelsen oppstiller strenge materielt vilkår i et nødvendighetskrav og et strafferammekrav, fremstår denne manglende prosessuelle beskyttelsen å være uforenelig med EU-domstolens konklusjon i *H.K. v Prokuratuur* [GC] C-746/18.

6 Avslutning

Temaet og problemstillingen i avhandlingen omhandlet de rettslige rammene for statens adgang til å pålegge tilbydere av elektroniske kommunikasjonsmidler å utlevere trafikk- og lokaliseringsdata, jf. strpl. § 210.

Hjemmelsgrunnlaget for utleveringspålegg av trafikk- og lokaliseringsdata fremstår problematisk opp mot klarhetskravet i EMK artikkel 8 og Grl. § 113. Det gjelder spesielt kravet om klare materielle og prosessuelle vilkår. Avhengig av hvilken trafikk- og lokaliseringsdata man er ute etter, vil vilkårene variere betraktelig. For store deler av datamengden foreligger kun terskelen om at dataen må antas å ha betydning som bevis.

---

[215] Prop.167 L (2020–2021) s. 58.
[216] *H.K. v Prokuratuur* [GC] C-746/18 avsnitt 46-59.

Denne terskelen kan ikke sies å være spesielt streng. Det foreligger også en del unntak til taushetsplikten, som ved § 2-8 b medfører nye materielle vilkår, og hele hjemmelsgrunnlaget fremstår nokså rotete. Strafferammekravet og nødvendighetskravet som følger av § 2-8 b gjelder kun for IP-adresser, som er en mindre sensitiv del av trafikkdata. Det fremstår som noe mangelfullt at disse kravene ikke også gjelder for den mer inngripende typen data som kan pålegges utlevert av strpl. § 210.

I tillegg vil formålet med lagringen måtte være sammenfallende med formålet for innhentingen. Dette er problematisk overfor norsk lagrinspraksis etter ekomloven. For det første vil det meste av den lagrede trafikk- og lokaliseringsdataen være lagret for kommunikasjons- eller faktureringsformål. Det er kun lagring tilknyttet IP-adresser i ekomloven § 2-8 som er for etterforsking av alvorlig kriminalitet. Dette vil medføre at all annen trafikk- og lokaliseringsdata som bli tilegnet for etterforsking av straffbare handlinger ikke vil være forenelig med kravet om sammenfallende formål etter EU-domstolens tolkning av kommunikasjonsverndriektivet artikkel 15 nr. 1.

Alvorlighetsgraden av den straffbare handlingen vil være et avgjørende moment under proporsjonalitetsvurderingen etter EMK og EØK, og dette må holdet opp mot alvorlighetsgraden av inngrepet. EU-domstolen viser klart til at et alvorlig inngrep finner sted når du kan trekke nøyaktige konklusjoner om en persons privatliv. Dette vil nesten alltid være tilfelle tilknyttet trafikk- og lokaliseringsdata. Etter lovgivningen i dag, er det kun tilknyttet tilgang til IP-adresser at dette alvorlighetskravet kommer frem. Dette er noe paradoksalt ettersom IP-adresser i seg selv er mindre sensitiv data enn generell trafikk- og lokaliseringsdata. At det ikke fremkommer klart av hjemmelsgrunnlaget for utlevering av den øvrige trafikk- og lokaliseringsdataen at det materielt kreves at dataen skal benyttes for å bekjempe alvorlige straffbare handlinger er mangelfullt.

De prosessuelle kravene til forhåndskontroll av retten etter et uavhengig forvaltningsorgan utenom tilfeller det foreligger duly justified urgency, er i all dekket for utleveringspålegg etter strpl. § 210. Selv om den begrensede lagringsadgangen for tilbyderne medfører at det ofte vil foreligge fare for at etterforskningen vil lide ved opphold, så vil Nkom uansett i de feleste tilfeller ha vurdert påtalemyndighetens begjæring om fritak fra taushetsplikt. Retten vil uansett begå etterkontroll av pålegget fra påtalemyndigheten. Dette stiller seg spesielt annerledes til adgangen til å pålegge utlevering av IP-adresser etter ekomloven § 2-8 b, hvor det hovedsakelig kun foreligger maternelle vilkår. Her vil det ikke foreligge forholds- eller

etterkontroll av hverken retten eller Nkom, og dette fremstår som lite forenelig med EU-domstolens konklusjon i *H.K. v Prokuratuur* [GC] C-746/18.

7 Referanseliste

Lover:

- Kongeriket Norges Grunnlov 17. mai 1814
- Lov 18. juni 1965 nr. 4 om vegtrafikk
- Lov 16. juni 1972 nr. 47 om kontroll med markedsføring og avtalevilkår - (tidligere markedsføringslov, opphevet)
- Lov 9. jan 2009 nr. 2 om kontroll med markedsføring og avtalevilkår mv. - (ny markedsføringslov)
- Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker
- Lov 27. nov 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS)
- Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
- Lov 4. juni 2003 nr. 83 om elektronisk kommunikasjon
  - Endret ved lov nr. 54/2013
  - Endret ved lov nr. 131/2021
- Lov 20. mai 2005 nr. 28 om straff
- Lov av 19. juni 2020 nr. 77 om etterretningstjenesten

Lovforarbeider:

- Ot.prp.nr.58 (2002–2003) Om lov om elektronisk kommunikasjon (ekomloven)
- Ot.prp.nr.59 (2003–2004) Om endringer i straffeloven, straffeprosessloven og sjøloven mv. (fast promillegrense og avholdspliktregler for større skip, et eget straffebud mot tortur, forklaringsplikt for ansatte i finansinstitusjoner mv.)
- Prop.69 L (2012–2013) Endringer i ekomloven
- Innst.186 S (2013–2014) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Per-Kristian Foss, Martin Kolberg, Marit Nybakk, Jette F. Christensen, Anders Anundsen, Hallgeir H Langeland, Per Olaf Lundteigen, Geir Jørgen Bekkevold og Trine Skei Grande om grunnlovfesting av sivile og politiske menneskerettigheter, med unntak av romertall X og romertall XXIV

- Prop.167 L (2020–2021) Endringer i ekomloven (lagring av IP-adresser mv.)

Forskrifter:

- Forskrift 31. mars 1995 nr. 281 om kommunikasjonskontroll – kommunikasjonskontrollforskriften (opphevet).
- Forskrift 16. feb 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste
    - Endret ved forskrift nr. 740/2013

Høyesterettspraksis:

- Rt. 1997 s. 1954
- Rt. 1997 s. 1965
- Rt. 2000 s. 996
- Rt. 2000 s. 1811
- Rt. 2001 s. 1006
- Rt. 2002 s. 391
- Rt. 2002 s. 557
- Rt. 2004 s. 357
- Rt. 2004 s. 1655
- Rt. 2005 s. 833
- Rt. 2008 s. 605
- Rt. 2009 s. 394
- Rt. 2009 s. 1011
- Rt. 2011 s. 172
- Rt. 2012 s. 1180
- Rt. 2014 s. 1105
- Rt. 2015 s. 93
- HR-2016-1833-A
- HR-2016-2554-P
- HR-2018-104-A
- HR-2018-699-A
- HR-2019-1226-A

Internasjonale traktater og avtaler:

- Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950 (entered into force 3 september 1953)
- Avtale om det Europeiske økonomiske samarbeidsområde
- Consolidated version of the Treaty on European Union
- The Charter of Fundamental Rights of the European Union
- Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon
- Europaparlaments- og rådsdirektiv 2009/136/EF av 25. november 2009 om endring av direktiv 2002/22/EF om forsyningsplikt og brukerrettigheter i forbindelse med elektroniske kommunikasjonsnett og -tjenester, direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor og forordning (EF) nr. 2006/2004 om samarbeid mellom nasjonale myndigheter med ansvar for håndheving av lovverk om forbrukerbeskyttelse

Praksis fra EMD:

- *Huvig mot Frankrike* [J], no. 11105/84, [24. april 1990], ECLI:CE:ECHR:1990:0424JUD001110584
- *Kruslin mot Frankrike* [J], no. 11801/85, [24. april 1990], ECLI:CE:ECHR:1990:0424JUD001180185
- *Campbell mot Storbritannia* [J], no. 13590/88, [25. mars 1992], ECLI:CE:ECHR:1992:0325JUD001359088
- *Amann mot Sveits* [GC], no. 27798/95, [16. Februar 2000], ECLI:CE:ECHR:2000:0216JUD002779895
- *Erdem mot Tyskland* [J], no. 38321/97, [5. juli 2001], ECLI:CE:ECHR:2001:0705JUD003832197
- *Üner mot Nederland* [GC], no. 46410/99, [18. oktober 2006], ECLI:CE:ECHR:2006:1018JUD004641099
- *S. og Marper mot Storbritania* [GC], nos. 30562/04 and 30566/04, [4. desember 2008], ECLI:CE:ECHR:2008:1204JUD003056204
- *Robathin mot Østeriket* [J], no. 30457/06, [3. juli 2012], ECLI:CE:ECHR:2012:0703JUD003045706
- *M.K. mot Frankrike* [J], no. 19522/09, [18. april 2013], ECLI:CE:ECHR:2013:0418JUD001952209

- *Roman zakharov mot Russland* [GC], no. 47143/06, [4. Desember 2015], ECLI:CE:ECHR:2015:1204JUD004714306
- *M.G.C. mot Romania* [J], no. 61495/11, [15. Mars 2016], ECLI:CE:ECHR:2016:0315JUD006149511

Praksis fra EU-domstolen:

- Dom av 21. desember 2016 [GC], *Tele2 Sverige AB*, C-203/15, *Watson og andre*, C-698/15, ECLI:EU:C:2016:970
- Dom av 2. oktober 2018 [GC], *Ministerio Fiscal*, C-207/16, EU:C:2018:788
- Dom av 6. oktober 2020 [GC], *Privacy International*, C-623/17, EU:C:2020:790
- Dom av 6. oktober 2020 [GC], *La Quadrature du Net og andre*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791
- Dom av 2. mars 2021 [GC], *H.K. v Prokuratuur*, C-746/18, ECLI:EU:C:2021:152

Juridisk litteratur:

- Aall, Jørgen, *Rettsstat og Menneskerettigheter 2*, 1. utg., fagbokforlaget 2021
- Nygaard, Nils, *Rettsgrunnlag og standpunkt*, 2. utg., universitetsforlaget 2004
- Rui, Jon Petter, «Fra EU-domstolen - Grenser for myndighetenes lagring av og tilgang til trafikk- og lokaliseringsdata», Tidsskrift for strafferett 2017, s. 146-168.
- Sejersted, Fredrik mfl., *EØS-RETT*, 3. utg., Universitetsforlaget 2011
    - Fredrik Sejersted, «DEL III Lovgivningsprosessen og nasjonal gjennomføring», i Sejersted, Fredrik mfl., EØS-RETT, 3. utg., Universitetsforlaget 2011, side 177-217.
    - Finn Arnesen, «DEL IV Rettskildene», i Sejersted, Fredrik mfl., EØS-RETT, 3. utg., Universitetsforlaget 2011, side 219-274.
- Øyen, Ørnulf, *straffeprosess*, 2. utg., Fagbokforlaget 2019

Annen elektronisk litteratur:

- Haugland, Geir Sunde, *Norsk Lovkommentar: Straffeprosessloven*, note 1014, rettsdata.no – 22.12.21

- Haugland, Geir Sunde, Norsk Lovkommentar: Straffeprosessloven, note 1460 (jf. 1405), Rettsdata.no – 22.12.21

- Haugland, Geir Sunde, *Norsk Lovkommentar: Straffeprosessloven*, note 1461, Rettsdata.no – 22.12.21
- Poulsen, Thomas Chr., *Norsk Lovkommentar: Straffeprosessloven*, note 733, Rettsdata.no – 22.12.21

Linker til nettsider:

- https://www.nkom.no/sikkerhet-og-beredskap/personvern-og-tilbyders-taushetsplikt - 22.12.21.
- https://www.nkom.no/files/ekomstat/Tilbyderoversikt.pdf - 22.11.21
- https://europalov.no/rettsakt/kommunikasjonsverndirektivet-2002/id-2232 - 22.12.21
- https://www.europalov.no/pakke/telekompakken - 22.12.21
- https://www.europalov.no/rettsakt/cookie-direktivet-forbrukerrettigheter-ved-elektronisk-kommunikasjon/id-126 - 21.11.21
- https://snl.no/kommunikasjon - 22.12.21
- https://snl.no/elektromagnetiske_bølger - 22.12.21
- https://snl.no/radiobølger - 2212.22