Høring – Endringer i ekomloven (lagring av IP-adresser mv.)

1. Bakgrunn og sammendrag

I dette høringsnotatet foreslår Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet (departementene) at det skal innføres en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til IP-adressene for å bekjempe alvorlig kriminalitet. Det bes særlig om høringsinstansenes syn på hvilket strafferammekrav som bør oppstilles, og på hvor lang lagringstiden bør være. Forslaget medfører endringer i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven).

Norge er et av verdens mest digitaliserte land og ligger i verdenstoppen når det gjelder bruk av internett. Samfunnet har aldri vært mer avhengig av digital infrastruktur. Bedrifter og forvaltning over hele landet blir stadig mer digitalisert, og ny teknologi benyttes til nye funksjoner av folk i alle aldersgrupper. Også mange av regjeringens Covid-19-tiltak forutsetter velfungerende og sikre elektroniske kommunikasjonsnett. Taletrafikken har økt kraftig, og datatrafikken er økt og endret som følge av Covid-19-krisen. Den teknologiske og markedsmessige utviklingen fortsetter og forventes å akselerere ved innføring av neste generasjonsmobilnett (5G). Den digitale utviklingen fører til at stadig mer av aktiviteten til bedrifter og den enkelte foregår via elektroniske kommunikasjonsnett, og at vi i de fleste av våre gjøremål etterlater oss stadig flere elektroniske spor. Det medfører at krav til kommunikasjonsvern blir viktigere.

Den teknologiske utviklingen gjenspeiles samtidig i kriminalitetsbildet. Utviklingen har gitt kriminelle nye muligheter både til å utføre kriminalitet og til å unndra seg strafforfølgning. Det er en generell trend at kommunikasjon i økende grad blir internettbasert, for eksempel ved at nettbaserte anrops- og meldingstjenester (slik som Skype eller iMessage) tar over for telefonoppringninger og SMS. Ettersom kommunikasjon over internett skjer ved hjelp av IP-adresser, vil det ofte være av stor betydning for politi og påtalemyndighet å finne frem til hvilken abonnent som har benyttet en gitt IP-adresse. En plikt til å lagre IP-adresser vil blant annet kunne bidra til å forhindre og oppklare nettkriminalitet, og vil også være et viktig virkemiddel for å oppnå FNs bærekraftmål 16.2 om å stanse overgrep, utnytting, menneskehandel og alle former for vold mot og tortur av barn.

Departementene ser at det er utfordrende å finne en riktig balanse mellom kriminalitetsbekjempelse og behovet for kommunikasjonsvern og personvern. Det er av betydning for kommunikasjonsvernet at informasjon om hvilke IP-adresser abonnentene er tildelt, ikke i seg selv avslører noe om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har kommunisert med. Opplysninger om at en IP-adresse kan knyttes til straffbare forhold, må politi eller påtalemyndighet få fra annet hold. Dette kan for eksempel være fra digitale beslag, eller tips fra utlandet om at en norsk IP-adresse er benyttet for eksempel ved deling av overgrepsmateriale. IP-lagringen vil da bidra til å avdekke hvem som står bak aktiviteten.

En plikt til å lagre IP-adresser som gir abonnementsopplysninger/brukerdata, er langt mindre inngripende for kommunikasjonsvernet enn en lagringsplikt for alle trafikkdata, som gir langt mer informasjon. Uthenting av lagrede IP-adresser vil like fullt være et svært viktig verktøy i arbeidet mot kriminalitet.

For at tiltaket skal bli effektivt og målrettet også når en tilbyder tildeler samme IP-adresse til flere abonnenter samtidig, foreslås det at tilbyder i slike tilfeller også skal lagre informasjon om hvilke portnumre på abonnentsiden som er benyttet ved kommunikasjonen.

Departementene foreslår samtidig innstramninger i reglene for når opplysninger om IP-adresser mv. kan utleveres til politi og påtalemyndighet. Det foreslås at opplysningene skal kunne utleveres når det er nødvendig for å forebygge eller etterforske en handling som etter loven kan medføre straff av fengsel i *x år* eller mer, eventuelt i kombinasjon med unntak for spesifikke straffebud.

Høringsnotatet følger opp Stortingets anmodningsvedtak nr. 944, 15. juni 2017:

> «Stortinget ber regjeringen utrede om det rettslige handlingsrommet for generell lagring av IP-adresser og relevant trafikkdata bør utvides, som et nødvendig virkemiddel i kampen mot kriminalitet, herunder overgrep mot barn. Utredningen må inkludere hvordan hensynet til personvern og internasjonale forpliktelser kan ivaretas.»

2. Om IP-adresser mv.

En IP-adresse («Internet Protocol Address») er en unik adresse som tildeles en enhet som er tilkoblet internett. Som en unik identifikator gjør IP-adressen det mulig at datapakker som sendes og mottas over nettet, kommer frem til rett destinasjon. Noe forenklet kan en IP-adresse derfor sammenlignes med et telefonnummer eller en postadresse for brevforsendelser.

Når en internettilbyder gir en abonnent tilgang til internett, tildeler nettilbyderen abonnenten en IP-adresse. Denne kan enten være tildelt fast (statisk) eller midlertidig (dynamisk). Med fast tildelt IP-adresse vil abonnentens IP-adresse alltid være den samme. Abonnenter med dynamisk tildelt IP-adresse vil midlertidig tildeles en IP-adresse, for eksempel når man kobler seg opp til nettet hjemme, eller basert på tidsintervaller. Dynamiske tildelinger er mye brukt overfor privatpersoner.

Dynamisk tildeling av IP-adresser brukes av flere grunner, blant annet fordi det forenkler tildelingsprosessen og administrasjonen av nettverket for tilbyderen, for eksempel ved bruk av DHCP («Dynamic Host Configuration Protocol»). Det har vært vanlig praksis å benytte dynamisk tilordning av IP-adresser før IPv4-adresser var sett på som en knapp ressurs.

Informasjon om hvilken IP-adresse en abonnent er blitt tildelt, gir ikke i seg selv informasjon om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har vært i kontakt med. Informasjon om IP-adresser omtales derfor gjerne som abonnementsopplysninger eller brukerdata. Denne typen informasjon har først og fremst betydning for å kunne koble opplysninger om kommunikasjon til en bestemt abonnent. Informasjon om hvilken abonnent som er tildelt en IP-adresse i et aktuelt tidsrom, kan bidra til å identifisere hvem som kommuniserer. Dette kan sammenlignes med at informasjon om hvilken abonnent som har et gitt telefonnummer, kan bidra til å identifisere hvem som står bak en telefonoppringning.

Normalt vil det bare være internettilbyderen som har informasjon om hvilken abonnent som er tildelt en gitt IP-adresse. Historiske opplysninger om hvilken abonnent som benyttet en IP-adresse på et bestemt tidspunkt, spesielt ved bruk av dynamisk tildeling av IP-adresser, vil bare finnes dersom tilbyderen fører logg over dette.

Når det i dette høringsnotatet refereres til «lagring av IP-adresser» og lignende, siktes det til internettilbyderes lagring av opplysninger om hvilke IP-adresser abonnentene er tildelt og på hvilke tidspunkter. Det siktes ikke til lagring av IP-adresser som foretas av andre, for eksempel nettsteders logging av hvilke IP-adresser som har besøkt nettstedet.

Det har etter hvert utviklet seg en mangel på globale IP-adresser. Denne begrensede tilgangen på IP-adresser har ført til at internettleverandører har tatt i bruk NAT-teknologi («Network Address Translation») for deling av IP-adresser mellom abonnenter. Dette gjør det mulig for mange abonnenter å benytte én enkelt IP-adresse samtidig. Delt bruk muliggjøres ved at det for hver individuell kommunikasjon opprettes en midlertidig kobling mellom abonnent og benyttet IP-adresse. Abonnentenes individuelle kommunikasjon skilles fra hverandre ved at bindingen også inkluderer en port (eller flere porter som brukes fortløpende) som benyttes i kommunikasjonen. Abonnentens binding i form av benyttet IP-adresse og port utgjør en unik representasjon av kommunikasjonen for kommunikasjonens levetid. Etter endt kommunikasjon vil bindingen kunne gjenbrukes fort, og den kan da knyttes til en annen abonnents kommunikasjon. Potensielt kan svært mange abonnenter dele én IP-adresse. Dersom internettilbyderen logger både hvilke IP-adresser og portnumre som er benyttet, samt tidspunktene for dette, vil det ved deling av IP-adresser kunne være mulig å identifisere en enkeltabonnent selv om IP-adressen ble delt av flere. Dette forutsetter at man har kjennskap til både IP-adresse, portnummer og et tilstrekkelig presist angitt kommunikasjonstidspunkt. Det siste kan være særlig utfordrende, og bruken av NAT-teknologi gjør at det ikke nødvendigvis er mulig å identifisere én enkelt abonnent utelukkende på grunnlag av en IP-adresse og et tidspunkt for kommunikasjonen. IP-adressen og tidspunktet vil imidlertid kunne gi en liste over alle abonnentene som benyttet IP-adressen på det aktuelle tidspunktet.

Versjonen av internett-protokollen som er mest utbredt i dag, IPv4, blir gradvis erstattet av den nye standarden IPv6. Innenfor IPv6 finnes det et langt større antall unike IP-adresser. Det er forventet at bruken av dynamisk tildeling av IP-adresser vil fortsette etter overgangen til IPv6, men at behovet for dagens bruk av NAT på grunn av adressemangel, vil falle bort. Det må imidlertid legges til grunn at IPv4

og IPv6 vil sameksistere i lang tid fremover, og at noen av overgangsmekanismene kan kreve NAT-lignende loggbehov.

3. Gjeldende rett

3.1 Gjeldende regler om lagring av IP-adresser

Etter gjeldende rett har ikke tilbyder plikt til å lagre opplysninger om hvilke IP-adresser abonnentene har disponert. Det følger av ekomloven § 2-7 femte ledd at data som er nødvendige for å identifisere abonnenten, skal slettes eller anonymiseres så snart de ikke er nødvendige for kommunikasjons- eller faktureringsformål eller for å oppfylle krav fastsatt i medhold av lov, med mindre brukeren samtykker til videre lagring. Tilsvarende krav til sletting følger av personopplysningsloven, jf. personvernforordningen artikkel 17.

Datatilsynet la i sin praksis etter den tidligere personopplysningsloven til grunn at tilbydere kunne lagre informasjon om hvilke IP-adresser abonnentene har disponert, i inntil tre uker dersom det var nødvendig for driftsrelaterte formål. Etter det departementene kjenner til, er dette også lagt til grunn av bransjen ved tolkningen av den nye personopplysningslovens regler. Det varierer imidlertid mellom tilbyderne, og mellom tilbydernes ulike tjenester for nettilgang, om opplysningene lagres i 21 dager eller kortere, og om det lagres slike opplysninger overhodet.

3.2 Utlevering av abonnentinformasjon

Det følger av ekomloven § 2-9 første ledd første punktum at tilbydere plikter å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon. Dette omfatter også abonnentinformasjon, herunder opplysninger om abonnenters disponering av IP-adresser.

Av tredje ledd første punktum følger det samtidig at taushetsplikten ikke er til hinder for at det gis opplysninger til påtalemyndigheten eller politiet «om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse». Dette omfatter også opplysninger om hvem som er tildelt en dynamisk IP-adresse, forutsatt at begjæringen knytter seg til et bestemt oppkoblingstidspunkt, jf. Ot.prp. nr. 58 (2002–2003) *Om lov om elektronisk kommunikasjon (ekomloven)* kapittel 16 side 93. Unntaket i tredje ledd første punktum modifiseres i fjerde ledd, som fastsetter at anmodninger fra påtalemyndigheten eller politiet etter tredje ledd skal etterkommes med mindre «særlige forhold gjør det utilrådelig».

Utlevering av abonnementsopplysninger til påtalemyndigheten eller politiet etter § 2-9 tredje ledd krever ikke at Nasjonal kommunikasjonsmyndighet fritar tilbyder fra taushetsplikten eller kjennelse fra retten, slik tilfellet er for andre trafikkdata. Det kreves heller ikke at utleveringen skjer som ledd i etterforskningen av et straffbart forhold, jf. Ot.prp. nr. 58 (2002–2003) kapittel 16 side 94. Unntaket fra taushetsplikten gjelder for alle oppgavene politiet utfører, også politiets sivile gjøremål, jf. Ot.prp. nr. 31 (1997–1998) punkt 3.6 side 8 om den tilsvarende bestemmelsen i teleloven § 9-3.

Det er lagt til grunn i Ot.prp. nr. 31 (1997–1998) *Om lov om endringer i lov 23. juni 1995 nr. 39 om telekommunikasjon* at «[d]et er først og fremst den som skal gi

opplysninger som nevnt i tredje ledd som må ta stilling til om det foreligger særlige forhold som gjør det utilrådelig å etterkomme anmodning fra påtalemyndighet eller politi om opplysninger», jf. kapittel 6 side 16. Videre uttales det at anvendelse av unntaket særlig vil være aktuelt i saker som ikke gjelder etterforskning, for eksempel i tilknytning til forvaltningssaker og namssaker.

Det følger av ekomloven § 2-9 tredje ledd andre punktum at taushetsplikten heller ikke er til hinder for at det gis opplysninger som nevnt i første punktum «ved vitnemål for retten». I sivile saker begrenses dette imidlertid av bevisforbudet i tvisteloven § 22-3, slik at det kreves samtykke fra departementet eller rettens kjennelse, jf. Rt. 2010 side 774 avsnitt 40.

For utlevering til andre offentlige myndigheter enn politi og påtalemyndighet kreves det lovhjemmel som gjør unntak fra taushetsplikten, jf. § 2-9 tredje ledd tredje punktum. Et eksempel på en slik lovhjemmel er skatteforvaltningsloven § 10-6, som åpner for å pålegge utlevering av abonnementsopplysninger dersom særlige hensyn gjør det nødvendig, og det foreligger mistanke om overtredelse av bestemmelser gitt i eller i medhold av loven.

Åndsverkloven § 87 gir særregler om tilgang til opplysninger som identifiserer innehaver av abonnement brukt ved inngrep i opphavsretten eller andre rettigheter etter loven. Bestemmelsen viderefører § 56 b i åndsverkloven 1961 uten materielle endringer, jf. Prop. 104 L (2016–2017) kapittel 14 side 351–352 med henvisning til Prop. 65 L (2012–2013) kapittel 8 side 88 flg. Bestemmelsen trer på dette området i stedet for bestemmelsene i tvisteloven kapittel 28 om bevissikring utenfor rettssak, jf. § 87 fjerde ledd. Etter bestemmelsens andre ledd første punktum skal Nasjonal kommunikasjonsmyndighet anmodes om samtykke til fritak fra taushetsplikten, som bare kan nektes når det kan utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf. det tilsvarende vurderingstemaet i tvisteloven § 22-3 andre ledd. For at en begjæring skal tas til følge, må retten finne at hensynene som taler for utlevering, veier tyngre enn hensynet til taushetsplikten, jf. tredje ledd første punktum, noe som tilsvarer vurderingstemaet etter tvisteloven § 22-3 tredje ledd. I åndsverkloven § 87 tredje ledd andre punktum er det angitt enkelte vurderingsmomenter for avveiningen.

4. Rettslige rammer for regler om IP-lagring

4.1 Retten til privatliv

Retten til privatliv er vernet gjennom Grunnloven § 102. Bestemmelsen lyder:

> § 102
>
> Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.
>
> Statens myndigheter skal sikre et vern om den personlige integritet.

Bestemmelsen kom inn i Grunnloven som ledd i grunnlovsreformen i 2014. Komiteen ga i Innst. 186 S (2013–2014) punkt 2.1.9 side 27 uttrykk for at bestemmelsen gir rett til et vern av personopplysninger ved at den «skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede».

Grunnloven § 102 gir ikke anvisning på noen adgang til eller vilkår for å gjøre inngrep i retten til privatliv. Høyesterett har imidlertid lagt til grunn at det kan gjøres inngrep i retten etter Grunnloven § 102 første ledd første punktum dersom tiltaket har en tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, se Rt. 2014 side 1105 avsnitt 28 og Rt. 2015 side 93 avsnitt 60.

Grunnloven § 102 første ledd første punktum har klare likhetstrekk med EMK artikkel 8 og må tolkes i lys av denne, men likevel slik at fremtidig praksis fra internasjonale håndhevingsorganer ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene, jf. Rt. 2015 side 93 avsnitt 57.

EMK artikkel 8 lyder (i norsk oversettelse):

> 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.

Begrepet «privatliv» skal i henhold til EMDs praksis tolkes vidt, se *S. og Marper mot Storbritannia* 4.12.2008 avsnitt 66 til 67 med videre henvisninger. EMD har i sin praksis lagt til grunn at offentlige myndigheters lagring av personopplysninger som knytter seg til privatlivet i bestemmelsens forstand, utgjør et inngrep i retten etter EMK artikkel 8 nr. 1, se *Amann mot Sveits* avsnitt 65 og *S. og Marper mot Storbritannia* 4.12.2008 avsnitt 67. Behandling av personopplysninger kan også utgjøre et inngrep når det foretas av private, såfremt inngrepet kan tilskrives offentlige myndigheter, se *Vukota-Bojić mot Sveits* 18.10.2016 avsnitt 46 til 47.

EMD har i *Benedik mot Slovenia* 24.4.2018 lagt til grunn at interessen i å verne om sin identitet ved aktivitet på internett omfattes av artikkel 8, jf. avsnitt 119. Det må derfor legges til grunn at en plikt til lagring av IP-adresser vil utgjøre et inngrep i retten til privatliv etter EMK artikkel 8 nr. 1. Inngrep i retten etter EMK artikkel 8 nr. 1 må kunne rettferdiggjøres etter artikkel 8 nr. 2. Dette innebærer at inngrepet må ivareta et legitimt formål, ha tilstrekkelig hjemmel og være forholdsmessig.

Kravet om legitimt formål innebærer at inngrepet må ivareta et av formålene nevnt i artikkel 8 nr. 2. Dette omfatter blant annet offentlig trygghet, forebygging av uorden eller kriminalitet og beskyttelse av andres rettigheter og friheter.

Hjemmelskravet («i samsvar med loven») innebærer at inngrepet må ha et rettslig grunnlag i nasjonal rett, som også må være tilstrekkelig presist og sikre nødvendige garantier mot vilkårlighet, jf. *L.H. mot Latvia* 29.4.2014 avsnitt 47. Hvilke garantier som er nødvendige, må vurderes i lys av inngrepets art og omfang, se *P.G. og J.H. mot Storbritannia* 25.9.2001 avsnitt 46. Kravet om garantier henger for øvrig tett sammen med proporsjonalitetskravet, og disse kravene vurderes derfor etter omstendighetene samlet, se for eksempel *S. og Marper mot Storbritannia* avsnitt 99.

Proporsjonalitetskravet innebærer at inngrepet må være «nødvendig i et demokratisk samfunn». Det ligger i dette at det må foretas en interesseavveining

mellom inngrepet i privatlivet og de legitime formålene. EMD uttrykte kravet slik i *Olsson mot Sverige* 24.3.1988 avsnitt 67:

> «(…) the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued»

Departementene er ikke kjent med praksis fra EMD som direkte gjelder adgangen til å pålegge internettilbydere å lagre informasjon om abonnentenes IP-adresser. Det finnes imidlertid noe praksis vedrørende lagringsplikt for andre typer abonnementsdata, som kan ha en viss overføringsverdi. Saken *Breyer mot Tyskland* 30.1.2020 gjaldt ekomtilbyderes plikt etter tysk telekommunikasjonslovgivning til å registrere informasjon som identifiserer kunder med forhåndsbetalte SIM-kort (kundens telefonnummer, navn og adresse, fødselsdato og dato for kontraktsinngåelsen) uavhengig av om tilbyderen har behov for opplysningene for egne formål.

Domstolen la til grunn at lagringsplikten utgjorde et inngrep i retten til privatliv etter EMK artikkel 8 nr. 1, jf. avsnitt 81, og at lagringen hadde tilstrekkelig hjemmel og forfulgte et legitimt formål, jf. henholdsvis avsnitt 84 og 86. Vurderingen av kravene til garantier i forbindelse med utlevering av de lagrede opplysningene hang etter EMDs syn så tett sammen med proporsjonalitetsvurderingen at dette måtte vurderes samlet, jf. avsnitt 85.

Domstolen foretok deretter en proporsjonalitetsvurdering, jf. avsnitt 88 flg. Det ble lagt til grunn at kriminalitetsbekjempelse, særlig bekjempelse av organisert kriminalitet og terrorisme, samt ivaretakelse av offentlig sikkerhet og beskyttelse av borgere utgjorde tvingende samfunnsmessige behov («pressing social needs»). I den forbindelse anerkjente domstolen videre at moderne kommunikasjonsformer og forandringer i kommunikasjon krever at etterforskningsverktøyene tilpasses, jf. avsnitt 88.

Når det gjaldt nytten og effektiviteten av tiltaket, anførte klagerne at det ikke var empirisk grunnlag for at tiltaket førte til redusert kriminalitet, og at tiltaket lett kunne omgås ved bruk av falsk identitet og stjålne simkort mv. Om dette uttalte EMD i avsnitt 90:

> «90. The Court acknowledges that pre-registration of mobile-telephone subscribers strongly simplifies and accelerates investigation by law-enforcement agencies and can thereby contribute to effective law enforcement and prevention of disorder or crime. Moreover, it considers that the existence of possibilities to circumvent legal obligations cannot be a reason to call into question the overall utility and effectiveness of a legal provision. Lastly, the Court reiterates that in a national security context national authorities enjoy a certain margin of appreciation when choosing the means for achieving a legitimate aim and notes that according to the comparative law report there is no consensus between the member States as regards the retention of subscriber information of pre-paid Sim-card customers (see paragraph 58 above). Having regard to that margin of appreciation, the Court accepts that the obligation to store subscriber information under section 111 of the Telecommunications Act was, in general, a suitable response to changes in communication behaviour and in the means of telecommunications.»

Det avgjørende ble dermed hvorvidt tiltaket var «proportionate and struck a fair balance between the competing public and private interests», jf. avsnitt 91. Ved denne vurderingen tok EMD utgangspunkt i hvor inngripende tiltaket var. Det ble i denne forbindelse vist til at det bare ble lagret en begrenset mengde opplysninger, som ikke inkluderte «highly personal information» eller gjorde det mulig å bygge «personality profiles» eller spore abonnentenes bevegelser, og som ikke omfattet opplysninger om «individual communication events», jf. avsnitt 92. Det ble lagt til

grunn at «the interference was, while not trivial, of a rather limited nature», jf. avsnitt 95.

Ved vurderingen av nødvendige garantier viste EMD blant annet til at lagringstiden ikke fremsto som for lang i lys av behovet, og at omfanget av lagrede data syntes å være begrenset til det som var nødvendig for formålet, jf. avsnitt 96. Det ble samtidig lagt til grunn at proporsjonalitetsvurderingen ikke bare kunne knytte seg til de lagrede dataene, men også reglene om tilgang til og bruk av opplysningene, jf. avsnitt 97. Ved vurderingen av tilgangsreglene viste EMD blant annet til at det var tilstrekkelig klart angitt hvilke myndigheter som kan kreve å få opplysningene utlevert, jf. avsnitt 99. EMD viste også til at reglene var utformet slik at det ved siden av utleveringsreglene var nødvendig med ytterligere rettslig grunnlag for de enkelte myndighetenes innhenting, jf. avsnitt 100. Videre pekte EMD på at adgangen til innhenting var begrenset av et nødvendighetskriterium, jf. avsnitt 100:

> «Moreover, the retrieval is limited to necessary data and this necessity requirement is safeguarded by a general obligation for the respective authorities retrieving the information to erase any data they do not need without undue delay. The Federal Constitutional Court had pointed out that the requirement of "necessity" meant in the context of prosecution of offences that there had to be at least an initial suspicion (see paragraph 21 above (§ 177)). The Court accepts that there are sufficient limitations to the power to request information and that the requirement of "necessity" is not only inherent in the specific legal provisions subject of this complaint but also to German and European data-protection law.»

Endelig vurderte EMD mulighetene for tilsyn og kontroll, jf. avsnitt 102 flg. Domstolen pekte i denne forbindelse på at tidligere praksis knyttet til mer vesentlige inngrep i privatlivet hadde begrenset overføringsverdi, og uttalte, jf. avsnitt 103:

> «In sum it considers that the level of review and supervision has to be considered as an important, but not decisive element in the proportionality assessment of the collection and storage of such a limited data set.»

Det var ikke et krav etter de tyske reglene at utlevering skulle godkjennes av en domstol eller av en annen uavhengig myndighet. EMD kom likevel til at mekanismene for tilsyn og kontroll var tilstrekkelige, og viste blant annet til datatilsynsmyndighetenes tilsynskompetanse, jf. avsnitt 105–107:

> 105 (…) each retrieval and the relevant information regarding the retrieval (time, data used in the process, the data retrieved, information clearly identifying the person retrieving the data, requesting authority, its reference number, information clearly identifying the person requesting the data) are recorded for the purpose of data protection supervision. This supervision is conducted by the independent Federal and Länder data protection authorities. The latter are not only competent to monitor compliance with data protection regulation of all authorities involved but they can also be appealed to by anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies.
>
> 106. Lastly, the Court notes that the Federal Constitutional Court held that legal redress against information retrieval may be sought under general rules (paragraph 22 above (§ 186)) – in particular together with legal redress proceedings against the final decisions of the authorities.
>
> 107. The Court considers that the possibility of supervision by the competent data protection authorities ensures review by an independent authority. Moreover, since anyone, who believes his or her rights have been infringed, can lodge an appeal the lack of notification and confidentiality of the retrieval procedure does not raise an issue under the Convention.»

På denne bakgrunn kom domstolen til at inngrepet var «nødvendig i et demokratisk samfunn», og at artikkel 8 følgelig ikke var krenket, jf. avsnitt 109–110.

EMD har i flere andre saker vurdert langt mer omfattende regelverk og systemer for datalagring og avlytting, se særlig *Roman Zakharov mot Russland* 4.12.2015 (storkammer) og *Szabó og Vissy mot Ungarn* 12.1.2016. Ettersom inngrepets art og styrke er av vesentlig betydning for vurderingen etter EMK artikkel 8, har avgjørelser som gjelder langt mer inngripende lagring av trafikkdata og/eller innholdsdata begrenset overføringsverdi ved vurderingen av mindre inngripende regler om lagring av kun abonnementsopplysninger, jf. også betraktningene i *Breyer mot Tyskland* avsnitt 103 nevnt over. Det redegjøres derfor ikke nærmere for disse avgjørelsene her.

Utlevering av abonnementsinformasjon er vurdert av EMD i *Benedik mot Slovenia,* som gjaldt opplysninger om dynamisk IP-adresse. I denne saken hadde det slovenske politiet fått oppgitt den dynamiske IP-adressen til en person som kunne mistenkes for å ha befatning med overgrepsmateriale. Det slovenske politiet henvendte seg til ulike internettilbydere og fikk oppgitt navnet og bostedsadressen til klagerens far. Klageren ble etter hvert utpekt som den mistenke, og han ble senere dømt for blant annet oppbevaring og distribuering av overgrepsmateriale. Spørsmålet for EMD var særlig om utleveringen av klagerens fars navn og bostedsadresse på bakgrunn av den dynamiske IP-adressen var «i samsvar med loven», jf. EMK artikkel 8 nr. 2. EMD kom til at lovgivningen som var anvendt som grunnlag for utleveringen, ikke sikret tilstrekkelig klarhet og garantier mot vilkårlige inngrep i rettighetene etter artikkel 8, jf. avsnitt 132.

EMD uttalte at de slovenske reglene om henholdsvis kommunikasjonsvern og utlevering av opplysninger i forbindelse med etterforskning var vanskelige å forene, jf. avsnitt 127. EMD viste til at den slovenske grunnloven krever at ethvert inngrep i kommunikasjonsvernet må skje etter kjennelse fra en domstol. Den slovenske konstitusjonsdomstolen hadde imidlertid lagt til grunn at klageren hadde gitt avkall på sin berettigede forventing om personvern, og at grunnlovsbestemmelsen derfor ikke kom til anvendelse. EMD var ikke enig, og mente at klageren hadde en berettiget forventning om at hans identitet ville holdes fortrolig, og at en kjennelse fra en domstol derfor var nødvendig. EMD trakk også frem at lovgivningen ikke i tilstrekkelig grad sikret garantier mot misbruk, jf. avsnitt 129–130:

> «129. (…) Bearing in mind the Constitutional Court's finding that the 'identity of the communicating individual' fell within the scope of the protection of Article 37 of the Constitution (see paragraph 128 above) and the Court's conclusion that the applicant had a reasonable expectation that his identity with respect to his online activity would remain private (see paragraphs 115 to 118 above), a court order was necessary in the present case. Moreover, nothing in the domestic law prevented the police from obtaining it given that they, a few months after obtaining the subscriber information, during which time apparently no investigative steps had been taken in the case, requested and obtained a court order for what would seem to be, at least in part, the same information as that which had already been in their possession (…). The domestic authorities' reliance on section 149b(3) of the CPA [bestemmelsen i den slovenske straffeprosessloven om utlevering av opplysninger fra tjenestetilbydere til politiet] was therefore manifestly inappropriate and, what is more, it offered virtually no protection from arbitrary interference.
>
> 130. In this connection, the Court notes that at the relevant time there appears to have been no regulation specifying the conditions for the retention of data obtained under section 149b(3) of the CPA and no safeguards against abuse by State officials in the

> procedure for access to and transfer of such data. As regards the latter, the police, having at their disposal information on a particular online activity, could have identified an author by merely asking the ISP provider to look up that information. Furthermore no independent supervision of the use of these police powers has been shown to have existed at the relevant time, despite the fact that those powers, as interpreted by the domestic courts, compelled the ISP to retrieve the stored connection data and enabled the police to associate a great deal of information concerning online activity with a particular individual without his or her consent (see paragraphs 108 and 109 above).»

Ettersom inngrepet derfor ikke hadde tilstrekkelig hjemmel, undersøkte domstolen ikke nærmere kravene til legitimt formål og proporsjonalitet.

EMK artikkel 8 stiller ikke bare krav til myndighetenes inngrep i privatlivet, men medfører også positive forpliktelser til å sikre respekt for privatlivet, jf. *K.U mot Finland* 2.12.2008 avsnitt 42–43 med videre henvisninger. I denne saken hadde en ukjent person lagt ut en annonse på en kontaktannonseside på nettet, i klagerens navn. Klageren var på dette tidspunktet 12 år. Annonsen oppga klagerens alder, beskrev utseendet hans og lenket til klagerens hjemmeside. Videre ble det i annonsen gitt uttrykk for at han var ute etter et intimt forhold med en gutt på hans alder eller eldre. Da forholdet ble anmeldt, anmodet politiet om å få utlevert informasjon om hvem som hadde fått tildelt den dynamiske IP-adressen som var benyttet. Som følge av lovfestet taushetsplikt kunne internettilbyderen imidlertid ikke utlevere denne informasjonen, jf. dommens avsnitt 6–14. EMD la til grunn at en praktisk og effektiv beskyttelse av klageren krevde at det ble tatt effektive grep for å identifisere og rettsforfølge gjerningspersonen, jf. avsnitt 49. Videre uttalte EMD at selv om kommunikasjonsvern og ytringsfrihet er grunnleggende hensyn ved bruk av internett, kan disse rettighetene ikke være absolutte. I visse tilfeller må disse rettighetene vike for andre hensyn, som å forebygge uorden og kriminalitet og beskytte andres rettigheter og friheter. Lovgivningen måtte derfor sikre det nødvendige rammeverket for denne avveiningen, jf. avsnitt 49. EMD kom på denne bakgrunn til at artikkel 8 var krenket, jf. avsnitt 50.

Retten til privatliv er også vernet av SP artikkel 17. Det er ikke holdepunkter for at denne bestemmelsen på dette området stiller strengere krav enn Grunnloven § 102 og EMK artikkel 8.

4.2 Ytringsfrihet, herunder pressens kildevern

Ytringsfriheten er vernet av både Grunnloven § 100, EMK artikkel 10 og SP artikkel 19. Fremstillingen her konsentreres om EMK artikkel 10, som lyder (i norsk oversettelse):

> 1. Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å kreve lisensiering av kringkasting, fjernsyn eller kinoforetak.
>
> 2. Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.

Inngrep i retten etter nr. 1 må kunne rettferdiggjøres etter vilkårene i nr. 2, som krever at inngrepet har tilstrekkelig hjemmel, har et legitimt formål og er forholdsmessig.

Pressefriheten utgjør et viktig element i retten til ytringsfrihet etter artikkel 10. I saken *Goodwin mot Storbritannia* 27.3.1996, uttalte EMDs flertall (avsnitt 39):

> «The court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance [...].»

Selv om det ikke fremgår direkte av ordlyden i artikkel 10, følger det av EMDs praksis at pressens ytringsfrihet også omfatter retten til kildevern, jf. blant annet *Goodwin* avsnitt 39, der EMD uttalte:

> «[...] Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms [...].Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected.»

Statens skjønnsmargin er begrenset på dette området, og EMD foretar en inngående prøving av vilkårene etter artikkel 10 nr. 2, jf. blant annet *Goodwin* avsnitt 40.

Kildevernet etter EMK artikkel 10 medfører blant annet begrensninger for adgangen til pålegge journalister å avsløre en kildes identitet, og til å fremlegge dokumenter som indirekte medfører at kildens identitet avsløres. Det vil utgjøre et inngrep i kildevernet hvis myndighetene pålegger journalister å utlevere dokumenter eller materiale med henblikk på etterforskning av en forbrytelse, hvis dokumentene eller materialet kan føre til avsløring av kildens identitet, jf. *Sanoma Uitgevers B. V mot Nederland* 14.09 2010 avsnitt 64–72. Ransakelser hos journalister med formål om å skaffe opplysning om en kildes identitet vil typisk utgjøre en krenkelse av kildevernet, jf. eksempelvis *Roemen og Schmit mot Luxemburg* 25.02.2003 avsnitt 47–60.

Det er uklart om og eventuelt i hvilken utstrekning EMK artikkel 10 gir en rett til å ytre seg eller kommunisere anonymt på internett. I *Breyer mot Tyskland* hadde klagerne anført at lagringen av abonnementsinformasjonen også utgjorde et inngrep etter artikkel 10, men EMD tok ikke stilling til spørsmålet, se avsnitt 60–62.

4.3 EØS-retten

Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (kommunikasjonsverndirektivet) er en del av det harmoniserte regulatoriske rammeverket for elektroniske kommunikasjonstjenester og -nett i EU, og er innlemmet i EØS-avtalen. Direktivet er gjennomført i norsk rett gjennom ekomloven med forskrifter. Det følger av direktivet artikkel 5 nr. 1 at medlemsstatene gjennom nasjonal lovgivning plikter å sikre fortrolighet for kommunikasjon som foregår via offentlige kommunikasjonsnett og offentlig tilgjengelige elektroniske kommunikasjonstjenester, samt fortrolighet for trafikkopplysninger knyttet til slik kommunikasjon. Videre skal medlemsstatene særlig forby enhver annen person enn brukerne å avlytte, oppfange, lagre eller på andre måter oppfange eller overvåke kommunikasjonen og tilhørende trafikkopplysninger uten samtykke fra brukeren, unntatt dersom dette er tillatt i henhold til lov, i samsvar med artikkel 15 nr. 1.

Av direktivet artikkel 15 nr. 1 følger det at medlemsstatene ved lov kan treffe tiltak som griper inn i rettighetene etter blant annet artikkel 5, av hensyn til blant annet «forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger». Et slik tiltak må være «nødvendig, egnet og rimelig i et demokratisk samfunn». Det er videre angitt at medlemsstatene kan vedta «lovgivningstiltak om lagring av opplysninger i et begrenset tidsrom» dersom dette er berettiget ut fra en av grunnene angitt i bestemmelsen. Slik direktivet lyder i EU, er det videre angitt i artikkel 15 nr. 1 siste punktum at tiltakene skal være i samsvar med «de allmenne prinsippene i fellesskapsretten, herunder prinsippene i artikkel 6 nr. 1 og 2 i traktaten om den Europeiske union», som refererer til EUs pakt om grunnleggende rettigheter og EMK. Slik direktivet er inntatt i EØS-avtalen, er denne passusen erstattet med «de allmenne prinsippene i EØS-retten», jf. EØS-komiteens beslutning nr. 80/2003 20. juni 2003.

EU-domstolen har i flere avgjørelser vurdert hvorvidt regler om datalagring oppfyller kravene i EUs pakt om grunnleggende rettigheter, herunder retten til respekt for privatliv og kommunikasjon (artikkel 7) og retten til beskyttelse av personopplysninger (artikkel 8). Pakten er ikke gjort til en del av EØS-avtalen og er derfor ikke bindende for Norge. Den kan likevel få betydning for tolkningen av EU-regelverk som er innlemmet i EØS-avtalen, og som i tråd med homogenitetsmålsettingen skal tolkes og anvendes likt i Norge og EU. Videre kan pakten indirekte få en viss betydning ved at den påvirker tolkningen av parallelle bestemmelser i Grunnloven og EMK, slik som bestemmelsene om rett til respekt for privatliv og ytringsfriheten. Pakten har imidlertid også bestemmelser uten klare paralleller i Grunnloven og EMK, slik som retten til beskyttelse av personopplysninger.

Digital Rights Ireland (sak C–293/12 og C–594/12) gjaldt gyldigheten av EU-direktiv 2006/24/EC, det såkalte datalagringsdirektivet, sett i lys av artikkel 7, 8 og 11 i EU-pakten. Datalagringsdirektivet påla lagring av nærmere angitte opplysninger knyttet til elektronisk kommunikasjon, jf. artikkel 3 og 5. Direktivet påla ikke lagring av opplysninger som avslørte innholdet i kommunikasjonen. EU-domstolen uttalte at opplysningene som skulle lagres, likevel samlet sett kunne gjøre det mulig å trekke svært presise slutninger om privatlivet til de det ble lagret informasjon om, blant annet om vaner, bosted, bevegelser, utførte aktiviteter, sosiale forhold og sosiale miljøer de har besøkt, jf. avsnitt 26 og 27. Dette utgjorde et inngrep i retten til privatliv og retten til beskyttelse av personopplysninger. Spørsmålet for domstolen var da om inngrepet kunne rettferdiggjøres.

Det ble lagt til grunn at direktivet ivaretok et legitimt formål – å bidra til å bekjempe alvorlig kriminalitet, jf. avsnitt 44. Domstolen så deretter nærmere på om lagringen av opplysninger som direktivet krevde, utgjorde et proporsjonalt inngrep i retten til privatliv og til beskyttelse av personopplysninger. Domstolen uttalte at kravet om proporsjonalitet innebærer at direktivet måtte være egnet til å oppnå de legitime formålene det søker å oppnå, og ikke måtte overskride grensen for hva som var nødvendig for å oppnå disse formålene jf. avsnitt 46. I den konkrete vurderingen konkluderte domstolen med at datalagringen var egnet til å oppnå formålet om å bekjempe alvorlig kriminalitet jf. avsnitt 49. Det avgjørende ble da om inngrepet overskred grensene for det som var nødvendig jf. avsnitt 51 flg.

Domstolen trakk i denne forbindelse frem at lagringsforpliktelsene etter direktivet omfattet alle trafikkdata for alle typer elektronisk kommunikasjon for alle abonnenter og registrerte brukere, uten noen differensiering, begrensninger eller unntak i lys av formålet om å bekjempe alvorlig kriminalitet, jf. avsnitt 56 til 58. Direktivet krevde ikke at det var noen forbindelse, verken direkte eller indirekte, mellom personer som ble berørt av lagringsplikten, og alvorlig kriminalitet. Det gjaldt heller ikke noen unntak for lagring av informasjon om personer omfattet av taushetsplikt for særlige yrkesgrupper. Videre manglet direktivet begrensninger, herunder objektive kriterier, for å begrense offentlige myndigheters tilgang til opplysninger og deres senere bruk av dem, samt materielle og prosessuelle vilkår for slik tilgang og bruk. Direktivet oppstilte blant annet ikke objektive kriterier for å begrense hvor mange personer som kunne få tilgang, til det som var strengt nødvendig. Videre var det heller ikke vilkår om at tilgang ble begrenset til det som var strengt nødvendig basert på en forutgående avgjørelse fra en domstol eller et uavhengig forvaltningsorgan, jf. avsnitt 62. Direktivet krevde heller ikke at lagringstiden ble avgjort ut fra objektive kriterier for å sikre at lagringen ble begrenset til det strengt nødvendige, jf. avsnitt 64. Domstolen vurderte dessuten at direktivet ikke påla tilstrekkelige forpliktelser til å sørge for sikkerhet ved behandlingen, jf. avsnitt 67.

Domstolen kom på denne bakgrunn til at datalagringsdirektivet gikk lenger enn det som var proporsjonalt, jf. avsnitt 69 til 71. Direktivet ble derfor erklært ugyldig. Det var da ikke nødvendig å foreta en nærmere vurdering i lys av artikkel 11 om ytringsfrihet.

I kjølvannet av *Digital Rights Ireland*-avgjørelsen oppstod det uklarhet om hvorvidt nasjonal lovgivning som gjennomførte forpliktelsene etter datalagringsdirektivet, også var i strid med EU-pakten. I *Tele 2*-avgjørelsen (sak C–203/15 og C–698/15), som gjaldt svensk og britisk datalagringslovgivning, tok domstolen stilling til om og i hvilken grad kommunikasjonsverndirektivet artikkel 15 lest i lys av EU-pakten var til hinder for nasjonal lovgivning om lagring og utlevering av trafikk- og lokasjonsdata i den hensikt å bekjempe kriminalitet.

Domstolen presiserte at både lovgivning som pålegger tjenestetilbydere en lagringsplikt, og lovgivningen som regulerer offentlige myndigheters tilgang til opplysningene som er lagret, faller innenfor kommunikasjonsverndirektivets virkeområde, jf. avsnitt 75 og 76. Ved vurderingen av inngrepets styrke la domstolen til grunn at den svenske lovgivningen påla en «general and indiscriminate» lagring av alle trafikk- og lokasjonsdata om alle abonnenter og registrerte brukere for alle former for elektronisk kommunikasjon, og der tjenestetilbyderne må lagre disse opplysningene systematisk og kontinuerlig uten unntak, jf. avsnitt 97. Samlet sett gjorde disse opplysningene det etter domstolens vurdering mulig å trekke svært presise slutninger om privatlivet til de det ble lagret informasjon om, jf. avsnitt 99. Lovgivning som åpnet for slik lagring, innebar derfor et svært vidtrekkende og særlig alvorlig inngrep i de grunnleggende rettighetene i EU-pakten artikkel 7 og 8. Det ble lagt til grunn at dersom formålet med slik lovgivning var å bekjempe kriminalitet, ville kun et formål om å bekjempe alvorlig kriminalitet gi tilstrekkelig grunnlag for så alvorlige inngrep i de grunnleggende rettighetene, jf. avsnitt 102.

Når slik lovgivning videre ikke sørget for differensiering, begrensninger eller unntak ut fra formålet med lovgivningen, ville lagringsplikten ramme personer

uten noen forbindelse, selv ikke en indirekte eller fjern forbindelse, til alvorlig kriminalitet, jf. avsnitt 106. Lovgivningen ville også kunne ramme personer som var underlagt yrkesbestemt taushetsplikt. Slik lovgivning var ikke begrenset til det som var strengt nødvendig, og den kunne derfor ikke anses å være i tråd med kommunikasjonsverndirektivet artikkel 15, jf. EU-pakten artikkel 7, 8 og 52(1), se dommens avsnitt 107 og 125.

Domstolen ga likevel uttrykk for at en lagringsplikt ikke uten videre er i strid med kommunikasjonsverndirektivet og EU-pakten, jf. avsnitt 108:

> «Artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7,8 og 11 samt artikel 52, stk. 1, er derimod ikke til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen.»

I avsnitt 109–111 presiseres nærmere vilkårene for slik lagring. Det er imidlertid noe uklart hvorvidt lagringen må begrenses med hensyn til både opplysningskategorier, kommunikasjonsmåter, berørte personer og lagringstid, eller kun noen av disse.

Om hvilke formål som kan begrunne utlevering av de lagrede dataene, uttalte domstolen at myndighetene kun kan gis tilgang til dataene for å bekjempe alvorlig kriminalitet, jf. avsnitt 115. Domstolen la videre til grunn at det må gjelde klare og presise materielle vilkår for utlevering som begrenser adgangen til det strengt nødvendige, jf. avsnitt 116–117. Om prosessuelle vilkår for utlevering uttalte domstolen i avsnitt 120:

> «Med henblik på i praksis at sikre fuld iagttagelse af disse betingelser er det afgørende, at de kompetente nationale myndigheders adgang til de lagrede data i princippet, undtagen i behørigt begrundede hastende tilfælde, er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne domstols eller denne enheds afgørelse træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af disse myndigheder inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning (…)»

Ministerio Fiscal **(**C-207/16) gjaldt kravene til at offentlige myndigheter kunne få utlevert opplysninger om eierne av SIM-kort brukt i en stjålet mobiltelefon. Spansk politi ønsket å få utlevert opplysninger i forbindelse med etterforskning av et ran av blant annet en mobiltelefon. Spørsmålet i saken var om kommunikasjonsverndirektivet artikkel 15 lest i lys av EU-parken artikkel 7 og 8 måtte forstås slik at opplysningene bare kunne utleveres i forbindelse med kriminalitetsbekjempelse dersom formålet er bekjempe alvorlig kriminalitet, og hvilke kriterier som i så fall skal anvendes ved vurderingen av et lovbrudds alvorlighet.

Domstolen viste til at kommunikasjonsverndirektivet artikkel 15 åpner for unntak av hensyn til forebygging, etterforskning, avsløring og rettslig forfølging av *straffbare handlinger*, og ikke kun alvorlige straffbare handlinger, jf. avsnitt 53. Domstolen bygger videre på uttalelsene i *Tele2* om at lovgivningen som åpner for utlevering til offentlige myndigheter, må være proporsjonal sett i lys av alvorlighetsgraden av inngrepet i de grunnleggende rettighetene, jf. avsnitt 54 til 58. Alvorlige inngrep vil kunne rettferdiggjøres under henvisning til bekjempelse

av alvorlig kriminalitet. Når utleveringen ikke innebærer et alvorlig inngrep, vil bekjempelse av alminnelig kriminalitet kunne være proporsjonalt.

EU-domstolen viste til at den konkrete saken kun gjaldt opplysninger om hvilke SIM-kort som var brukt sammen med den stjålne mobiltelefonen i en tolvdagersperiode, og opplysninger om identiteten til eierne av SIM-kortene, for eksempel navn og eventuelt adresse, jf. avsnitt 59 og 60. Politiet skulle ikke få utlevert opplysninger om kommunikasjon foretatt med den stjålne telefonen eller hvor den befant seg. Med mindre disse opplysningene ble sammenholdt med andre opplysninger, ville de ikke gjøre det mulig å trekke presise slutninger om privatlivet til personene som opplysningene gjaldt. Utlevering av opplysningene om SIM-kort og identitet ble derfor ikke ansett å utgjøre et alvorlig inngrep i de grunnleggende rettighetene til de berørte personene, og bekjempelse av alminnelig kriminalitet, ikke kun alvorlig kriminalitet, ble ansett å kunne rettferdiggjøre inngrepet, jf. avsnitt 61 til 63.

I avgjørelsen i de forente sakene C-511/18, C-512/18 og C-520/18 (*La Quadrature du Net*) 6. oktober 2020 uttalte EU-domstolen i storkammer seg særskilt om adgangen til å pålegge lagring av IP-adresser. Saken gjaldt datalagringsregler i Frankrike og Belgia. EU-domstolen viste til at opplysninger om IP-adresser, selv om de anses som trafikkdata, genereres uavhengig av den konkrete kommunikasjonen og hovedsakelig tjener til å identifisere den fysiske personen som eier utstyret som internettkommunikasjonen skjer fra. På denne bakgrunn ble det lagt til grunn at denne kategorien av data er mindre sensitiv enn andre trafikkdata, jf. avsnitt 152. Samtidig uttalte domstolen at IP-adresser likevel kan brukes til å spore nettbruk, og at lagringen av slike data derfor utgjør et «alvorlig inngrep» i grunnleggende rettigheter, jf. avsnitt 153.

EU-domstolen uttalte videre at det ved balanseringen av de grunnleggende rettighetene og interessene må tas i betraktning at informasjon om IP-adresser kan være helt avgjørende ved etterforskning av straffbare handlinger begått på internett, blant annet i saker om overgrepsmateriale, jf. avsnitt 154. Selv om internettbrukere har en berettiget forventning om at identiteten ikke avsløres, var en generell og udifferensiert lagring av IP-adresser etter EU-domstolens vurdering derfor ikke i prinsippet i strid med kommunikasjonsverndirektivet og EU-pakten. Det er en forutsetning at de materielle og prosessuelle vilkårene som skal regulere bruken av disse dataene, overholdes strengt, jf. avsnitt 155.

EU-domstolen la samtidig til grunn at lagringen må begrunnes ut ifra formål om å bekjempe alvorlig kriminalitet, forebygge alvorlige trusler mot offentlig sikkerhet eller ivareta nasjonal sikkerhet. Videre ble det lagt til grunn at lagringstiden ikke må overstige det som er strengt nødvendig, og at det må etableres strenge vilkår og garantier vedrørende bruk av dataene, jf. avsnitt 156 og 168.

5. Lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

EU vedtok 15. mars 2006 direktiv 2006/24/EF (datalagringsdirektivet). Formålet med direktivet var å harmonisere lovgivningen om lagring av data fremkommet ved bruk av elektronisk kommunikasjon, for å gi justismyndighetene et verktøy for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet. Dataene skulle lagres av tilbydere av offentlig elektronisk kommunikasjonstjeneste eller offentlig

elektronisk kommunikasjonsnett. Direktivet la detaljerte føringer for hva som skulle lagres, og påla blant annet lagring av en mengde data som er nødvendige for å spore og identifisere kilder til en kommunikasjon, dato, tid, sted og varighet. Dette omfattet trafikkdata, lokaliseringsdata og abonnements-/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon. Data om hvilke IP-adresser abonnentene var tildelt for internettkommunikasjon, var omfattet av lagringsplikten.

Direktivet overlot til nasjonale myndigheter å ta nærmere stilling til flere viktige spørsmål. Dette gjaldt blant annet spørsmålene om tilgang til og utlevering av dataene som lagres, lagringstiden (som i henhold til direktivet skulle være mellom 6 og 24 måneder), kostnader, hvem som skal føre tilsyn med ordningen og valg av teknologi for lagringen.

Direktivet ble gjennomført i norsk rett ved lov 14. april 2011 nr. 11 om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett). Som nevnt i punkt 4.3 over kom EU-domstolen i *Digital Rights Ireland* (C–293/12 og C–594/12) i april 2014 til at direktivet var ugyldig. Lovendringene er derfor ikke satt i kraft. I det følgende redegjøres det kort for hvordan data om IP-adresser er regulert i den norske gjennomføringsloven.

Gjennomføringsloven pålegger tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, og tilbyder av slik tjeneste, å lagre blant annet «data nødvendig for å identifisere abonnenten eller brukeren» til bruk for «etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold», jf. ny § 2-7 a i ekomloven. Lagringstiden er seks måneder. Lagringsplikten er nærmere spesifisert i forskrift 15. mai 2013 nr. 484 om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften). Det følger av forskriften § 2-5 at lagringspliktige data ved internettaksess blant annet omfatter «tildelt IP-adresse for kommunikasjonen» (nr. 2), tidspunkter for av- og pålogging (nr. 4 og 5) og «data som identifiserer den digitale abonnentlinjen eller annet sluttpunkt for kommunikasjonens avsender» (nr. 7).

For størsteparten av de lagrede dataene ble det i gjennomføringsloven fastsatt at utlevering av data i etterforskingsøyemed krever rettens kjennelse, jf. nye §§ 210 b og 210 c i straffeprosessloven. Det kreves som utgangspunkt at det foreligger skjellig grunn til mistanke om en straffbar handling med strafferamme på fengsel i 4 år eller mer, jf. § 210 b første ledd bokstav a. Utlevering av data etter basestasjonssøk forutsetter at den straffbare handlingen kan medføre straff av fengsel i 5 år eller mer, jf. § 210 c første ledd bokstav a. I begge tilfeller skal utlevering av data også kunne skje dersom handlingen er utøvet som ledd i organisert kriminalitet og kan straffes med fengsel i 3 år eller mer, jf. bestemmelsenes første ledd bokstav b. Det er videre åpnet for utlevering i enkelte andre typer saker som vil være særlig vanskelig å etterforske uten tilgang til data, gjennom en uttømmende oppregning av straffebud, jf. bestemmelsenes første ledd bokstav c. I tillegg kreves det at data skal ha vesentlig betydning for etterforskningen, jf. § 210 b tredje ledd og § 210 c andre ledd.

Disse skjerpede kravene for tilgang til lagrede data ble imidlertid ikke gjort gjeldende for abonnementsopplysninger, herunder opplysninger om IP-adresse. For slike opplysninger ble gjeldende rett videreført. Dette ble begrunnet slik i

Prop. 49 L (2010–2011) *Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)* punkt 12.6 side 103:

> «Abonnementsopplysninger, herunder også elektronisk kommunikasjonsadresse, er gjennomgående å anse som mindre beskyttelsesverdige opplysninger enn trafikkdata og lokaliseringsdata. Å oppgi for eksempel hemmelig telefonnummer og IP-adresse utgjør vanligvis et mer beskjedent innhugg i personvernet enn utlevering av trafikkdata og lokaliseringsdata. Etter departementets syn kan det derfor forsvares å gi større tilgang til abonnementsopplysninger enn trafikkdata. Det foreslås således ingen endringer i gjeldende rett (ekomloven § 2-9 tredje ledd) for så vidt gjelder slike opplysninger.»

Dette innebærer at data om tildelt IP-adresse som skulle lagres etter gjennomføringsloven, skulle kunne utleveres uten rettens kjennelse, og til bruk for alle oppgaver politiet utfører, jf. punkt 3.2 over om ekomloven § 2-9 tredje ledd.

6. Utenlandsk rett

6.1 Sverige

I april 2019 fremmet den svenske regjeringen en proposisjon om endring i de svenske reglene om lagring og tilgang til opplysninger om elektronisk kommunikasjon for å bekjempe kriminalitet. Formålet med lovforslaget var å sikre at de svenske datalagringsreglene er i samsvar med EU-retten, blant annet i lys av EU-domstolens vurderinger i *Tele 2*-avgjørelsen, se punkt 4.3 over. Den svenske riksdagen vedtok lovendringene i samsvar med regjeringens forslag. Endringene trådte i kraft 1. oktober 2019.

Lagen (2003:389) om elektronisk kommunikation kapittel 6, 16 a § pålegger virksomheter som tilbyr offentlige kommunikasjonsnett som i alminnelighet tilbys mot betaling, eller allment tilgjengelige elektroniske kommunikasjonstjenester en lagringsplikt for visse typer opplysninger om elektronisk kommunikasjon. Bestemmelsens første og andre ledd lyder:

> **16 a §** Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § är skyldig att lagra sådana uppgifter som avses i 20 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.
>
> Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt samt vid internetåtkomst. Även vid en misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

Etter bestemmelsens *første ledd* omfatter lagringsplikten opplysninger om abonnement og andre opplysninger som angår en bestemt elektronisk meddelelse, som er nødvendig for å spore og identifisere kommunikasjonskilden, sluttmålet for kommunikasjonen, dato, tidspunkt og varighet for kommunikasjonen, type kommunikasjon, kommunikasjonsutstyr og lokalisering av mobilt kommunikasjonsutstyr ved kommunikasjonens begynnelse og slutt. Slike opplysninger er i utgangspunktet underlagt taushetsplikt, jf. 6 kapittel 20 § første ledd 1 og 3. I 16 a § *andre ledd* presiseres det at lagringsplikten blant annet gjelder opplysninger som genereres eller behandles ved internettilgang. I forarbeidene er det presisert at lagringsplikten også omfatter opplysninger om IP-adresse og abonnent jf. Prop. 2018/19:86 side 43. Opplysninger som genereres eller

behandles i forbindelse med internettilgang, skal lagres i ti måneder fra den dagen kommunikasjonen avsluttes, jf. 16 d § første ledd andre strekpunkt jf. andre ledd.

Utlevering av abonnentsopplysninger, herunder IP-adresser, er særskilt regulert i lagen om elektronisk kommunikasjon 6 kapittel 22 § første ledd. Tilbyderne plikter å utlevere abonnementsopplysninger, herunder opplysninger om IP-adresser, til påtalemyndigheten, politiet og andre kriminalitetsbekjempende myndigheter ved mistanke om et straffbart forhold, jf. første ledd 2. Det kreves ikke at forholdet er av en viss alvorlighet. Opplysningene skal videre utleveres til politiet blant annet dersom det er behov for dem i forbindelse med «efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns fara för deras liv eller allvarlig risk för deras hälsa», jf. første ledd 3, og ved forbindelse med etterforskning og identifisering vil ulykker og dødsfall, jf. første ledd 6. Bestemmelsen åpner også på nærmere vilkår for utlevering til andre offentlige myndigheter, blant annet Kronofogdemyndigheten, Skatteverket og Finansinspektionen.

Det stilles ikke krav om at utlevering skal besluttes av en domstol eller et annet uavhengig organ.

6.2 Danmark

I Danmark er postvirksomheter og tilbydere av telenett og teletjenester pålagt en generell plikt til å bistå politiet ved gjennomføringen av inngrep i den såkalte meddelelseshemmeligheten ved å utlevere teleopplysninger, samt en plikt til å lagre opplysninger om teletrafikk til bruk i forbindelse med kriminalitetsbekjempelse, jf. lov om rettens pleje § 786 første og fjerde ledd, som lyder:

> Det påhviler postvirksomheder og udbydere af telenet eller teletjenester at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler m.v., ved at give de i § 780, stk. 1, nr. 3 og 4, nævnte oplysninger samt ved at tilbageholde og udlevere forsendelser m.v.
>
> (…)
>
> *Stk. 4*. Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om denne registrering og opbevaring.

Lagringsplikten etter fjerde ledd er nærmere regulert i Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen). Opplysninger som skal lagres i forbindelse med internettsesjoner, følger av § 5:

> **§ 5.** En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om en internet-sessions initierende og afsluttende pakke:
>
> 1) afsendende internetprotokol-adresse,
>
> 2) modtagende internetprotokol-adresse,
>
> 3) transportprotokol,
>
> 4) afsendende portnummer,
>
> 5) modtagende portnummer og
>
> 6) tidspunktet for kommunikationens start og afslutning.

Stk. 2. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal endvidere registrere følgende oplysninger om en brugers adgang til internettet:

1) den tildelte brugeridentitet,

2) den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,

3) navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet og

4) tidspunktet for kommunikationens start og afslutning.

(…)

Opplysningene nevnt i § 5 skal oppbevares i ett år, jf. logningsbekendtgørelsen § 9.

Tilbyderne er etter den danske teleloven forpliktet til å utlevere opplysninger om sluttbrukers adgang til kommunikasjonsrett og -tjenester til politiet, herunder opplysninger om sluttbrukers adgang til internett (blant annet IP-adresser). Disse bestemmelsene omfatter imidlertid bare statiske IP-adresser. Opplysninger om dynamisk IP-adresse må utleveres etter retsplejelovens regler om *edition*, jf. § 780 flg. Det kreves som utgangspunkt forutgående kjennelse fra retten, men saken kan i særlige tilfeller forelegges for retten etter at utlevering har funnet sted. Det kreves i alle tilfeller at utleveringen er proporsjonal.

6.3 Finland

Lagringsplikt for ekomtilbydere følger av *Lag om tjänster inom elektronisk kommunikation* (917/2014) 157 §. Loven pålegger ikke lagring av data som tilbyderne ikke har behov for å lagre for egne formål, men forlenger lagringstiden for data som tilbyderne allerede behandler for egne formål. Plikten gjelder for tilbydere som pålegges lagringsplikt etter beslutning av inrikesministeriet.

Ved internettaksess omfatter lagringsplikten blant annet opplysninger som identifiserer abonnenten og opplysninger om tildelt IP-adresse, jf. 157 § tredje ledd, jf. andre ledd 3) og *Föreskrift om teleföretagens skyldighet att lagra uppgifter för myndigheternas behov* (53 B/2014 M) § 6. Lagringstiden er ni måneder regnet fra kommunikasjonstidspunktet, jf. *Lag om tjänster inom elektronisk kommunikation* 157 § fjerde ledd.

Det følger av 157 § første ledd at opplysninger som omfattes av lagringsplikten, bare kan benyttes i saker om straffbare forhold som nevnt i 10 kap. 6 § andre ledd i *tvångsmedelslagen* (806/2011). Dette omfatter:

1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,
2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,
3) olovligt brukande som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning,
4) utnyttjande av person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,
5) narkotikabrott,
6) förberedelse till brott som begås i terroristiskt syfte, deltagande i utbildning för ett terroristbrott, finansiering av terroristgrupp, resa i syfte att begå ett terroristbrott eller främjande av resa som görs i syfte att begå ett terroristbrott,
7) grovt tullredovisningsbrott,
8) grovt döljande av olagligt byte,

9) förberedelse till tagande av gisslan, eller
10) förberedelse till grovt rån.»

6.4 Island

Lög um fjarskipti (nr. 81/2003) pålegger ekomtilbydere plikt til lagring av trafikkdata, inkludert IP-adresser, jf. § 42 tredje ledd. Dataene skal lagres i seks måneder, og deretter slettes. Tilbyderne er forpliktet til å bistå politiet og utlevere informasjon som identifiserer abonnenten, jf. § 47 syvende ledd. Det kreves ikke at utlevering skal besluttes av en domstol.

7. Departementenes vurderinger

7.1 Bør det innføres plikt til IP-lagring?

7.1.1 Utgangspunkter

Retten til privatliv, herunder retten til person- og kommunikasjonsvern, er en grunnleggende forutsetning for et demokratisk samfunn. Staten har et ansvar for å sikre vern om denne integriteten. Samtidig er det hevet over tvil at informasjon om IP-adresser vil være et viktig verktøy i kriminalitetsbekjempelsen, og at slike opplysninger dermed vil bidra til å ivareta den enkeltes vern mot kriminalitet. Lagring av IP-adresser i inntil 21 dager er ikke tilstrekkelig for politi- og påtalemyndighetens behov i dagens digitaliserte samfunn. Det er derfor nødvendig å vurdere lagringsplikt for IP-adresser.

Behovet for å lagre IP-adresser som et ledd i kriminalitetsbekjempelse må veies mot hensynet til kommunikasjonsvernet. Tiltaket må være proporsjonalt, balansert og ikke gå lenger enn nødvendig. Det må også stilles krav til sikker lagring og annen behandling av personopplysninger, både fra private og offentlige aktører.

7.1.2 Behovet for opplysninger om IP-adresser i kriminalitetsbekjempelsen

Den teknologiske utviklingen har ført til endrede kommunikasjonsformer og gitt kriminelle nye muligheter både til å utføre kriminalitet og unndra seg strafforfølgning. Dette skaper en rekke utfordringer for politiets og påtalemyndighetens arbeid.

Det er en generell trend at kommunikasjon i økende grad blir internettbasert, for eksempel ved at nettbaserte anrops- og meldingstjenester (slik som Skype eller iMessage) tar over for telefonoppringninger og SMS. Opplysninger om nettbasert kommunikasjon blir dermed stadig viktigere i alle typer saker der kommunikasjonsdata er av betydning. Dette gjelder både saker der den straffbare handlingen begås over internett, og saker der internettkommunikasjon er benyttet ved for eksempel forberedelser eller koordinering av fysiske straffbare handlinger. Uten mulighet til å forfølge slike digitale spor får politiet i mange tilfeller vesentlig dårligere tilgang på informasjon i etterforskningen enn det som var situasjonen tidligere, når kommunikasjonen i større grad foregikk via taletelefon og SMS mv. Tilgang til informasjon om knytningen mellom IP-adresse og abonnent vil, uavhengig av kriminalitetsform, kunne styrke politiets generelle evne til å bekjempe kriminalitet.

Utfordringene som følge av den teknologiske utviklingen gjør seg gjeldende i en rekke ulike saker, men er særlig tydelige når det gjelder nettrelaterte seksuallovbrudd. Dette gjelder blant annet ulike former for nettovergrep og produksjon og deling av overgrepsmateriale. Det fremgår av Politidirektoratets rapport om anmeldt kriminalitet i 2018 at antallet seksuallovbruddssaker øker, spesielt saker om seksuelle overgrep mot barn. Fra 2014 til 2018 er økningen på over 75 %. Dette skyldes i første rekke at politiet har avdekket nettverk av personer som chatter og deler seksualiserte fremstillinger av barn.[1] Det er også flere som blir utsatt for seksuell utpressing på nettet, der seksualiserte bilder eller filmer brukes til å presse den som er avbildet, for penger, til å sende mer materiale eller til å utføre seksuelle handlinger via direkteoverføring (webkamera) på internett eller i det virkelige liv.[2] I slike saker er det sannsynligvis store mørketall, og det forventes en økning i antall saker fremover.[3]

Ettersom kommunikasjon over internett skjer ved hjelp av IP-adresser, vil det ofte være av stor betydning for politi og påtalemyndighet å finne frem til hvem som har benyttet en gitt IP-adresse, uavhengig av hvilke konkrete straffbare forhold det dreier seg om. Politiet får på ulike måter kjennskap til IP-adresser som kan knyttes til straffbare forhold, for eksempel gjennom undersøkelse av databeslag, utlevering av brukerinformasjon fra nettsteder og nettjenester (for eksempel sosiale medier), tips, anmeldelser eller monitorering av fildelingsnettverk. I mange tilfeller er informasjon om hvem som har benyttet en IP-adresse, helt avgjørende for å komme videre i saken. Dette gjelder for eksempel når politiet avdekker eller mottar opplysninger om at en norsk IP-adresse kan knyttes til internettrelaterte overgrep mot barn, og det ikke finnes andre opplysninger enn IP-adressen som kan bidra til å identifisere gjerningspersonen.

Kripos mottar daglig informasjon fra aktører i andre land om norske brukere som har lastet ned eller delt overgrepsmateriale. En hovedkilde er amerikanske NCMEC (National Center for Missing and Exploited Children), som blant annet mottar og behandler tips fra amerikanske tjenestetilbydere. Øvrige kilder omfatter Europol, Interpol, National Child Exploitation Coordination Center (NCECC) og politimyndigheter i andre land samt norske aktører. Det har vært stor vekst i antall tips fra NCMEC, med 50 tips i 2014 til 10445 tips i 2018. I 2019 gikk antall tips fra NCMEC uventet ned til 6816. Andelen tips som genererte oppfølging, var imidlertid større enn tidligere, noe som indikerer at kvaliteten på tipsene er gått opp.

Også for kriminalitet som forebygges og etterforskes av Politiets sikkerhetstjeneste (PST), for eksempel saker knyttet til statlige aktørers virksomhet i Norge som innebærer trusler mot norske sikkerhetsinteresser, og radikalisering på nett, vil informasjon om tilknytningen mellom abonnent og IP-adresse kunne være av stor betydning.

Informasjon om tilknytningen mellom abonnent og IP-adresse er både av betydning for å finne frem til gjerningspersoner og for arbeidet med identifisering av ofre, for eksempel i saker om nettovergrep. Videre er informasjonen ikke bare viktig ved etterforskning av lovbrudd som er begått, men også ved avverging av lovbrudd. Dette kan for eksempel være tilfellet dersom det publiseres anonyme

[1] Politidirektoratet, *STRASAK-rapporten 2018* side 17.
[2] Politidirektoratet, *STRASAK-rapporten 2018* side 17.
[3] Politidirektoratet, *Trusler og utfordringer innen IKT-kriminalitet* (2017) side 15–16.

trusler om skoleskyting eller lignende på nett. Informasjonen kan også være vesentlig for forebygging av lovbrudd, for eksempel dersom det mottas tips om ekstremistiske ytringer i nettfora.

Selv om bruksområdet for informasjonen oftest vil være å knytte en abonnent til en gitt IP-adresse, kan det også være behov for å få utlevert IP-adresser med utgangspunkt i en gitt abonnent. Dette kan for eksempel være tilfellet ved undersøkelse av datamateriale i en etterforskning rettet mot en bestemt mistenkt. I stedet for å innhente abonnementsinformasjon med utgangspunkt i hver enkelt IP-adresse som finnes i materialet, kan det innhentes en oversikt over hvilke IP-adresser den mistenkte ble tildelt i det aktuelle tidsrommet. Da vil det enklere kunne avdekkes om og i hvilken utstrekning IP-adresser i materialet kan knyttes til den mistenkte.

Det er grunn til å understreke at informasjon om koblingen mellom IP-adresse og abonnent sjelden vil muliggjøre en entydig identifikasjon av en konkret *bruker* uten nærmere etterforskning. Informasjon om koblingen mellom IP-adresse og abonnent vil imidlertid kunne være avgjørende informasjon for hvor den videre etterforskningen i saken bør rettes. På tilsvarende måte som ved bruk av en telefontjeneste kan brukeren i det enkelte tilfellet være en annen enn abonnenten. Flere brukere kan også ha nettilgang gjennom samme abonnement, for eksempel flere medlemmer av samme husstand, eller hos en abonnent med leieboere. Abonnenten kan dessuten være en arbeidsplass, en skole, et universitet eller en kafé med et trådløst nettverk som kundene kan benytte seg av. Da vil det kunne være nødvendig med omfattende videre etterforskning for å forsøke å finne frem til en konkret bruker. Det vil også kunne vise seg at det ikke vil være mulig å identifisere en konkret bruker selv om abonnenten er kjent.

Brukeren kan også forsøke å skjule sin identitet gjennom krypterings- og anonymiseringsløsninger, for eksempel VPN-teknologi (virtuelt privat nettverk) eller TOR («The Onion Router»). Sistnevnte er et informasjonssystem som gjør det mulig å sende trafikk over et verdensomspennende, frivillig nettverk av datamaskiner i den hensikt å skjule brukerens plassering eller aktivitet for andre. VPN ble blant annet utviklet for at brukere via fjernaksess skulle kunne få sikker tilgang til bedriftsinterne nett via internett, som om de var direkte tilkoblet det private nettet. VPN-teknologi oppretter en sikker virtuell forbindelse mellom bruker og lokalnettverket i den andre enden av forbindelsen, ved hjelp av særskilte kommunikasjonsprotokoller og normalt ved bruk av kryptering. VPN-teknologi vil også kunne brukes til å maskere hvilken IP-adresse som benyttes. I slike tilfeller vil det normalt ikke være mulig å identifisere en abonnent eller bruker med mindre VPN-tilbyderen har logget informasjon om bruken som gjør dette mulig, eller dersom man finner knytninger til VPN-tjenesten ved en teknisk undersøkelse av en mistenkt persons datautstyr eller telefon. At det ikke alltid vil være mulig å identifisere en abonnent eller bruker, betyr imidlertid ikke at lagring av IP-informasjon er uten verdi. Etter departementenes vurdering er det et klart behov for disse opplysningene i kriminalitetsbekjempelsen.

7.1.3 Hensynet til kommunikasjonsvernet og ytringsfriheten

Kommunikasjonsvernet

Data om kommunikasjonen forteller mye om oss og nettverket vårt, og oppfattes av de fleste som svært privat og noe vi ønsker å verne om. Kommunikasjonsvernet har vært en sentral del av tele- og ekomreguleringen siden telegraflovens tid.

Den økte bruken av digitale løsninger og internett bidrar til at den enkelte av oss legger igjen langt flere digitale spor enn tidligere, og fører til at person- og kommunikasjonsvernet blir enda viktigere enn før. Kommunikasjonsvern innenfor ekomsektoren innebærer at den enkelte så langt som mulig uforstyrret skal kunne kommunisere ved hjelp av elektroniske hjelpemidler uten å bli kikket i kortene av andre. Derfor har tele- og internettselskapene i dag en sletteplikt for all informasjon som genereres, etter at informasjonen ikke lenger trengs til kommunikasjonsformål. I vurderingen av om det bør innføres en plikt til lagring av IP-adresser, er det sentralt å se hen til i hvilken grad en slik lagringsplikt vil gripe inn i kommunikasjonsvernet, og på hvilken måte.

Lagring av trafikkdata, som IP-adresser utgjør en mindre del av, har vært diskutert flere ganger tidligere og har møtt en del motstand, blant annet i forbindelse med behandlingen av Prop. 49 L (2010–2011). Trafikkdata kan gi informasjon om hvem som har kommunisert med hvem, hvor kommunikasjonen har funnet sted, når kommunikasjonen fant sted, og hvordan. Data fra mobiltelefonen kan i tillegg si noe om hvor man til enhver tid befinner seg, også når det ikke kommuniseres. IP-adresser har tradisjonelt vært ansett som mindre beskyttelsesverdige opplysninger enn andre trafikkdata og signaleringsdata.

Lagring av IP-adresser omfatter ikke lagring av informasjon om innholdet i abonnentens internettkommunikasjon, hvem abonnenten har vært i kontakt med, eller hvor abonnenten befinner seg. I seg selv vil informasjon om IP-adresser som hovedregel kun gi opplysning om at abonnenten har hatt internettilgang på et gitt tidspunkt. Dersom abonnenten tildeles midlertidige (dynamiske) IP-adresser, vil dette i tillegg kunne gi informasjon om hvilke tidspunkter abonnenten har koblet seg på og av internett.

Vurderingen av i hvilken grad en lagringsplikt vil gripe inn i kommunikasjonsvernet, kan imidlertid ikke bare knytte seg til de lagrede opplysningene isolert. Formålet med lagringen vil nettopp være å kunne knytte opplysningene til annen informasjon, slik som hvilken nettaktivitet en IP-adresse er benyttet til. Dette kan for eksempel være informasjon om at en IP-adresse er benyttet ved besøk på et nettsted, eller ved nedlasting eller opplasting av data, bruk av nettbaserte meldingstjenester og sosiale medier osv. Dersom politiet får tilgang til opplysninger om at en bestemt IP-adresse har vært benyttet til å besøke en nettside, vil lagringen av IP-adressen gjøre det mulig å finne ut hvilken abonnent som har utført nettaktiviteten. Når dette potensialet for å koble IP-opplysninger til informasjon om nettaktivitet tas i betraktning, er det klart at en lagringsplikt for IP-adresser griper inn i den enkeltes person- og kommunikasjonsvern.

Departementene vil understreke at informasjon om innhold i nettaktivitet, og hvilke IP-adresser som har besøkt nettsteder, ikke vil være tilgjengelig for politi og påtalemyndighet uten videre. Internettilbydere har ikke anledning til å lagre informasjon om innholdet i abonnentenes internettkommunikasjon eller om hvem de har vært i kontakt med, og en plikt til lagring av IP-adresser vil ikke endre på dette. Informasjon om nettaktivitet vil politi og påtalemyndighet måtte skaffe til veie fra annet hold. Det kan for eksempel være fra beslaglagte enheter, fra

nettsteder mv. eller fra virksomheter som er blitt utsatt for datainnbrudd eller lignende. For at informasjonen skal eksistere, er man avhengig av at den lagres av nettsteder, virksomheter, programvare på enheter osv. Samtidig vil personvernregelverket begrense adgangen til å lagre opplysninger om nettaktivitet som kan knyttes til enkeltpersoner, og slik informasjon vil derfor ofte bare være lagret i den utstrekning nettsteder, virksomheter mv. har funnet det nødvendig å lagre dem for egne formål, for eksempel sikkerhetsformål. Bare i helt begrenset utstrekning har politiet mulighet til å skaffe til veie informasjon om nettaktivitet som ikke er lagret av andre for egne formål. Dette kan skje for eksempel gjennom monitorering av deling av overgrepsmateriale over såkalte «peer-to-peer»-nettverk, eller dersom aktiviteten knytter seg til politiets egne nettsteder, for eksempel når politiet mottar tips på internett.

Ofte vil det kreve omfattende etterforskning å skaffe til veie informasjon om nettaktivitet. Det vil ofte være nødvendig med bruk av tvangsmidler som ransaking, beslag og utleveringspålegg, noe som forutsetter at straffeprosesslovens vilkår for dette er oppfylt. Det vil også ofte være behov for rettsanmodninger om utlevering av informasjon fra utenlandske nettsteder mv. I andre tilfeller vil politi og påtalemyndighet være helt avhengig av å motta informasjonen gjennom tips og anmeldelser.

Ved vurderingen av kommunikasjonsvern- og personvernulempene må det også sees hen til risikoen for at informasjonen kan komme på avveie, for eksempel ved datainnbrudd hos en internettilbyder. Kommer informasjonen uvedkommende i hende, vil den kunne bidra til å knytte abonnenter eller brukere til nettaktivitet. Det må imidlertid understrekes at også eventuelle uvedkommende som får tilgang til informasjonen etter et datainnbrudd, vil være avhengig av informasjon fra annet hold for å kunne koble IP-opplysningene til nettaktivitet. Det må videre tas i betraktning at koblingen mellom en IP-adresse og abonnent i seg selv sjelden vil muliggjøre en entydig identifikasjon av konkrete brukere. Tilbyder plikter uansett etter ekomloven å sørge for integritet og sikkerhet, jf. omtale i punkt 7.3.3. Dette vil også gjelde ved lagring av IP-adresser.

Departementene understreker for øvrig at inngrepet i kommunikasjonsvernet ved en plikt til IP-lagring må sees i sammenheng med vilkårene for utlevering av de lagrede IP-adressene, jf. punkt 7.5 nedenfor. Vilkårene for utlevering må sikre at informasjonen bare kan utleveres i den utstrekning det er nødvendig og forholdsmessig.

Ytringsfriheten

Ved vurderingen av om det bør innføres en plikt til lagring av IP-adresser, må det også vurderes om en slik lagring vil kunne gripe inn i ytringsfriheten, herunder pressens kildevern.

Som redegjort for ovenfor, dreier ikke IP-lagring seg om å lagre informasjon om innholdet i abonnentens internettkommunikasjon, eller om hvem abonnenten har vært i kontakt med. Den lagrede informasjonen vil derfor ikke i seg selv kunne identifisere pressens kilder. Dersom lagring av IP-adresser skal kunne bidra til å identifisere en kilde, vil de lagrede opplysningene måtte kobles med informasjon fra annet hold. Informasjon om hvilke IP-adresser en uidentifisert kilde har benyttet, vil politi og påtalemyndighet vanskelig kunne få tak i fra annet hold enn fra den journalistiske virksomheten. Dette vil reglene om kildevern sette klare begrensninger for. Det vises til Justis- og beredskapsdepartementets høringsnotat

24. september 2018 *Forslag til endringer i kildevernreglene i straffeprosessloven og tvisteloven* for en utførlig omtale av kildevernet etter straffeprosessloven og EMK.

Det må også sees hen til om en plikt til IP-lagring vil kunne påvirke den reelle muligheten til å kunne ytre seg anonymt eller motta anonyme ytringer på internett, og med dette ha en «nedkjølende effekt» på ytringsfriheten. Dersom man har informasjon om hvilken IP-adresse som er benyttet for eksempel i forbindelse med en anonym ytring på et nettsted, vil IP-informasjonen kunne bidra til å avdekke vedkommendes identitet. Det må også her understrekes at IP-lagring ikke vil muliggjøre omfattende overvåking av enkeltpersoners nettbruk. Informasjon om hvilken IP-adresse som er benyttet i forbindelse med en anonym ytring, dersom den finnes overhodet, er ikke noe som kan skaffes til veie uten videre. Videre må det også her tas i betraktning at koblingen mellom en IP-adresse og abonnent i seg selv sjelden vil muliggjøre en entydig identifikasjon av konkrete brukere, samt at vilkårene for utlevering må sikre at informasjonen bare utleveres i den utstrekning det er nødvendig og forholdsmessig.

7.1.4 Samlet vurdering

Dagens lagringstid på inntil 21 dager er for kort dersom informasjonen skal kunne benyttes til kriminalitetsbekjempelse. Etter departementenes vurdering bør internettilbyderne derfor pålegges en lagringsplikt som går utover dette.

Departementene er oppmerksom på at noen som begår lovbrudd over internett, kan forsøke å skjule sin identitet gjennom krypterings- og anonymiseringsløsninger, for eksempel VPN-teknologi eller TOR, jf. punkt 7.1.2 over. Departementene legger imidlertid til grunn at en lagringsplikt samlet sett likevel vil ha stor verdi for kriminalitetsbekjempelsen, og anser derfor ikke at dette bør tillegges avgjørende vekt.

Lagringen skal bidra til å avdekke hvem som står bak nettaktivitet, kommunikasjon osv. som kan knyttes til straffbare forhold. For at lagringen skal nå sitt formål, kan lagringsplikten etter departementenes vurdering ikke være begrenset til nærmere bestemte abonnenter eller kategorier av abonnenter, for eksempel basert på konkret mistanke om straffbare forhold.

En plikt til å lagre IP-adresser vil som nevnt innebære et inngrep i den enkeltes person- og kommunikasjonsvern. Det må legges til grunn at en lovfestet plikt til å lagre koblingen mellom IP-adresser og abonnenter vil utgjøre et inngrep i retten til privatliv etter Grunnloven § 102 og EMK artikkel 8, jf. punkt 4.1 over. Lagringsplikt vil da bare være tillatt såfremt inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig. Det kan legges til grunn at en plikt til å lagre IP-adresser vil ivareta et legitimt formål, ettersom EMK artikkel 8 nr. 2 åpner for inngrep blant annet for å ivareta offentlig trygghet, forebygging av uorden eller kriminalitet og beskyttelse av andres rettigheter og friheter. Departementene viser videre til at EMK artikkel 8 også innebærer en positiv forpliktelse til å muliggjøre etterforskning av lovbrudd, jf. *K.U mot Finland* nevnt i punkt 4.1 over, der EMK artikkel 8 ble ansett å ha blitt krenket fordi den finske lovgivningen ikke i tilstrekkelig grad åpnet for utlevering av IP-informasjon.

Det må imidlertid foretas en konkret vurdering av om en plikt til lagring av IP-adresser vil være et proporsjonalt inngrep. Blant annet må det vurderes om

inngrepet er begrenset til det nødvendige med hensyn til lagringstid og vilkårene for utlevering, og om det i tilstrekkelig grad sikres «nødvendige garantier», blant annet hva gjelder tilsyn og kontroll, jf. *Breyer mot Tyskland* og *Benedik mot Sloveni*a. Den nærmere utformingen av reglene vil være avgjørende for at tiltaket samlet sett skal oppfylle kravene i Grunnloven § 102 og EMK artikkel 8.

På bakgrunn av EU-domstolens avgjørelse i *La Quadrature du Net*, jf. punkt 4.3 over, legger departementene til grunn at generell lagring av IP-adresser på nærmere vilkår er tillatt etter EØS-retten. Også etter kommunikasjonsverndirektivet artikkel 15 må det foretas konkrete vurderinger av nødvendighet og proporsjonalitet, knyttet til de ulike sidene ved reglene. Lagringen må ha som formål å bekjempe «alvorlig kriminalitet», og lagringstiden må ikke overstige det som er strengt nødvendig. Videre må det gjelde tilstrekkelig strenge vilkår og garantier vedrørende bruk av dataene.

Departementene understreker at en lagringsplikt for IP-adresser ikke vil kunne muliggjøre omfattende overvåking av enkeltpersoners nettbruk. Koblingen mellom en IP-adresse og abonnent vil også i seg selv sjelden muliggjøre en entydig identifikasjon av en konkret bruker, jf. punkt 7.1.2 ovenfor. Siden en IP-adresse svært ofte deles av flere brukere, kan man ikke legge til grunn uten videre at brukeren og abonnenten er den samme. Dersom abonnenten er en arbeidsplass, en skole, et universitet eller et serveringssted, vil det kunne være et svært høyt antall brukere bak én IP-adresse. Innhenting av abonnementsinformasjonen vil altså være et steg på veien mot ytterligere etterforskning.

Når det gjelder ytringsfriheten, herunder kildevernet, er det etter departementenes vurdering tvilsomt om regler om IP-lagring i seg selv utgjør et inngrep i ytringsfriheten etter EMK artikkel 10. Etter departementenes vurdering vil lagringen i alle tilfeller ikke være et uproporsjonalt inngrep, fordi opplysningene i seg selv ikke vil være kildeidentifiserende. Det er etter departementenes vurdering også lite praktisk at den lagrede informasjonen vil bidra til å muliggjøre kildeidentifikasjon. Hvis det i et konkret tilfelle likevel skulle oppstå spørsmål om å benytte IP-informasjon for å identifisere en kilde, vil det etter departementenes vurdering trolig være politiets fremgangsmåter for å skaffe til veie tilleggsinformasjon som IP-opplysningene i så fall må kobles med, som vil komme i forgrunnen ved vurderingen av skrankene i EMK artikkel 10. Det vises til punkt 4.2 over om begrensningene for adgangen til å rette tvangsmidler, for eksempel ransaking, mot en journalistisk virksomhet.

Departementenes samlede vurdering er at lagring av IP-adresser ikke innebærer et så stort inngrep i kommunikasjonsvernet at det bør hindre politiets mulighet til å nyttiggjøre seg opplysningene ved kriminalitetsbekjempelse. Det vises særlig til at informasjonen som lagres, isolert sett ikke sier noe om hva abonnentene har foretatt seg på nettet eller hvem de har vært i kontakt med. Lagringen vil derfor ikke kunne benyttes til noen form for systematisk overvåking av enkeltpersoners nettbruk. Departementene kan heller ikke se at lagringen vil gripe inn i ytringsfriheten på en slik måte at ytringsfriheten må anses som et avgjørende mothensyn. Den nærmere utformingen av reglene, jf. punkt 7.3 til 7.6 under, vil være avgjørende for at reglene samlet sett skal oppfylle kravene i Grunnloven, EMK og kommunikasjonsverndirektivet, og ivareta hensynet til kommunikasjonsvern og ytringsfrihet på en tilfredsstillende måte.

7.2 Særskilte problemstillinger knyttet til deling av IP-adresser mellom abonnenter

Som nevnt i punkt 2 har internettilbyder tatt i bruk teknologi for deling av IP-adresser mellom abonnenter, i første rekke såkalt NAT-teknologi («Network Address Translation»). Dette gjør det mulig å tildele samme IP-adresse til mange abonnenter samtidig. Potensielt kan svært mange abonnenter dele én IP-adresse. Det varierer mellom tilbyderne i hvilken utstrekning abonnentene tildeles IP-adresser som deles med andre, og hvor mange abonnenter som i så fall deler adresse. Bruken varierer også mellom de ulike nettløsningene internt hos tilbyderne. Deling av IP-adresser er særlig utbredt i mobilnettet.

Når en IP-adresse har blitt tildelt flere abonnenter på samme tid, vil det normalt ikke være mulig å identifisere én av disse abonnentene kun med utgangspunkt i en IP-adresse og et gitt tidspunkt for kommunikasjonen. Ettersom det er flere som benytter adressen samtidig, vil IP-adressen og tidspunktet bare kunne gi en liste over alle abonnentene som benyttet IP-adressen på det aktuelle tidspunktet. Ved IP-deling vil lagring av kun IP-adresser derfor kunne ha mer begrenset nytteverdi.

Helt uten verdi er informasjonen likevel ikke. For eksempel kan det etter omstendighetene være av verdi å kunne konstatere at en konkret abonnent *ikke* er på listen over abonnenter som var tildelt en gitt IP-adresse. Videre kan det være tilfellet at politiet i etterforskningen blir kjent med flere IP-adresser fra ulike tidspunkter som sannsynligvis kan knyttes til samme gjerningsperson. I så fall kan det undersøkes om det er abonnenter som kan knyttes til alle IP-adressene og tidspunktene.

En mulighet for å knytte en delt IP-adresse til en enkeltabonnent er å identifisere, lagre og innhente informasjon om såkalte *portnumre* (på abonnentssiden). Et portnummer er et nummer som ved kommunikasjonen kommer i tillegg til IP-adressen, og som gjør det mulig å kommunisere med én bestemt prosess på enheten det kommuniseres med. Det er dette nummeret som gjør det mulig at kommunikasjonen kommer frem til rett destinasjon selv om flere abonnenter deler IP-adresse, ettersom kombinasjonen av IP-adresse og portnummer på et gitt tidspunkt vil være unik for den enkelte. Dersom internettilbyderen logger både hvilke IP-adresser og portnumre som er benyttet, samt tidspunktene for dette, vil det ved deling av IP-adresser være mulig å identifisere en enkeltabonnent selv om IP-adressen ble delt av flere. Dette forutsetter at politiet har kjennskap til både IP-adresse, portnummer og et tilstrekkelig presist angitt kommunikasjonstidspunkt.

Lagring av portnumre er ikke fullt ut sammenlignbart med lagring av tildelt IP-adresse. Mens informasjonen om tildelte IP-adresser i seg selv bare avslører at en abonnent har hatt internettilgang på et gitt tidspunkt, vil portinformasjonen også kunne si noe om tidspunktet abonnenten har kommunisert på. Lagring av portinformasjon vil imidlertid etter departementenes vurdering ikke gjøre lagringsplikten vesentlig mer inngripende.

For at en plikt til lagring av IP-adresser skal imøtekomme politiets behov også ved deling av IP-adresser, bør lagringsplikten etter departementenes syn også omfatte slik informasjon som er nødvendig for å identifisere abonnenten ved deling av IP-adresser. Muligheten til å identifisere abonnenten bør ikke bero på tilbydernes

tekniske løsning. Departementene viser videre til at dette er løsningen i både Sverige og Finland.[4]

Det kan samtidig ikke helt utelukkes at det ved bruk av NAT i enkelte tekniske løsninger vil være nødvendig å lagre noe mer informasjon for å identifisere abonnenter, som også sier noen om destinasjon, for eksempel hvilken IP-adresse og porten man har kommunisert med. Mindre tilbydere med få IP-adresser kan dessuten ha behov for å legge til elementer for å åpne opp for flere kunder og samtidig kunne knytte en IP-adresse til en bruker. Departementene ber tilbyderne informere om det er mulig å unngå å bruke NAT-løsninger som innebærer at man også må lagre destinasjonsinformasjon. Alternativt dersom dette ikke kan unngås, for eksempel når standardiserte løsninger benyttes, om det i så fall kan tilpasses løsninger som hindrer lagring av eventuell destinasjonsinformasjon. Departementene ber særlig om tilbakemelding fra tilbydere om dette vil være mulig.

7.3 Utformingen av regler om lagringsplikten

7.3.1 Hvem skal lagre?

I dag dekker seks store tilbydere av internettjenester over 95 % av markedet i Norge. I tillegg finnes det ca. 300 registrerte tilbydere som leverer internettaksess som tjeneste. De fleste av disse leverer sine tjenester på basis av de store infrastruktureiernes nett. Det bør derfor vurderes om en plikt til å lagre IP-adresser bør rette seg mot samtlige tilbydere av internettaksess.

I utgangspunktet vil politiet ha behov for tilgang til IP-adresser på generelt grunnlag, uavhengig av hvilken tilbyder som benyttes. Videre finnes det et ukjent antall organisatoriske og tekniske løsninger blant internettilbydere, som gjør det komplisert å avgrense til spesifikke typer tilbydere.

Det er tekniske og merkantile forhold som vil være avgjørende for hvordan en lagringsplikt vil påvirke tilbydere av internettjenester, og ikke nødvendigvis størrelsen på virksomheten. I hovedsak er det tre faktorer som er avgjørende for kompleksiteten og merkostnaden ved en lagring av IP-adresser.

For det første har det betydning om tilbyder drifter en egen løsning for IP-allokering. Med IP-allokering menes prosessen å knytte et endepunkt i et nettverk, for eksempel en husstand, til en IP-adresse. Blant tilbydere som ikke eier egen infrastruktur, er det stor variasjon i hvor mye av dette tilbyderen selv løser, og hvor mye som er satt bort til en underleverandør. Ved en forespørsel om utlevering av abonnementsopplysninger må IP-adresser fra underleverandør knyttes opp mot abonnentinformasjon hos tilbyder (eller motsatt). Dette kan kreve endringer i eksisterende løsninger.

For det andre er det avgjørende om tilbyder har et tilstrekkelig antall IP-adresser, eller om det brukes en NAT-løsning som kan medføre at mer data må lagres, og at det dermed blir en større kostnad knyttet til utstyr som støtter loggingen. I enkelte NAT-løsninger vil også behovet for å logge hyppigere øke betraktelig, ettersom

[4] Se *Lagen (2003:389) om elektronisk kommunikation* kapittel 6, 16 a §, jf. Prop. 2018/19:86 side 44 (Sverige) og *Föreskrift om teleföretagens skyldighet att lagra uppgifter för myndigheternas behov* § 6 (Finland).

knytningen mellom adresse og bruker varer i kortere tid før adressen allokeres til noen andre.

For det tredje må det også vurderes i hvilken grad det er lagt til rette for logging i tilbyders nåværende system. Avhengig av den tekniske løsningen den enkelte tilbyder anvender, kan loggefunksjonalitet være noe som allerede eksisterer. Det kan også være tilfellet at store deler av det tekniske systemet må byttes ut, dersom det ikke er lagt til rette for logging.

Det må legges til grunn at næringen selv vil være i stand til å finne hensiktsmessige løsninger for lagring og utlevering gjennom avtaler. For eksempel kan enkelte tilbydere være registrert som tilbydere og tilby internett, mens det er en annen tilbyder som drifter tjenesten og tildeler IP-adresse. Den første tilbyderen vil da ikke ha oversikt over hvilke IP-adresser som er tildelt en abonnent. I slike tilfeller kan informasjonen være lokalisert på flere steder og må sammenstilles, for eksempel vet den ene tilbyderen hvilken IP-adresse som er tildelt, mens navn, adresse mv. er lagret i databasen til den andre tilbyderen.

Det er mulig å legge lagringsplikten til ett av disse leddene og derigjennom regulere forholdet mellom tilbyderne når det gjelder lagringsplikten. Det kan imidlertid være mer hensiktsmessig at det blir opp til tilbyderne å løse dette seg imellom i det enkelte tilfellet, for eksempel gjennom avtaler. Slik unngår man en regulering som potensielt vanskeliggjør ulike former for organisering, samtidig som regelverket gir fleksibilitet til næringen når det gjelder hvordan de ønsker å løse dette.

Etter departementenes vurdering vil det dermed være mulig å pålegge alle tilbydere en lagringsplikt. Lagringsplikten vil være avgrenset til tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett.

Departementene foreslår at pliktsubjektene angis som «tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, og tilbyder av slik tjeneste». Dette tilsvarer formuleringen i ekomloven § 2-8 første ledd om plikten til å tilrettelegge for lovbestemt tilgang til informasjon, og vil omfatte alle aktører i markedet som tilbyr internettilgang til allmennheten, jf. ekomloven § 1-5 nr. 4. Lagringsplikten vil gjelde uavhengig av teknologisk plattform.

Departementene foreslår samtidig at det gis en forskriftshjemmel som gir Nkom anledning til å fastsette unntak for tilbydere. Det vil eksempelvis være aktuelt å fastsette unntak dersom det skulle vise seg at den tekniske utviklingen går i en slik retning at det ikke lenger vil være hensiktsmessig å pålegge alle tilbydere en lagringsplikt, eller dersom det skulle vise seg å finnes tilbydere som opererer i et så spesialisert marked at lagringsplikt ikke gir mening.

7.3.2 Hva skal lagres?

Formålet med lagringen er å gjøre det mulig å koble IP-adresser til abonnenter, jf. punkt 2 og 7.1.2 over. Dette innebærer at lagringsplikten må omfatte opplysninger om hvilke IP-adresser abonnentene er tildelt, og på hvilke tidspunkter. Dersom samme IP-adresse tildeles flere abonnenter samtidig, vil det i tillegg være nødvendig med informasjon om portnumre, jf. punkt 7.2.

Lovregler om lagringsplikten kan utformes på flere måter. Reglene må sikre at lagringsplikten omfatter alle de opplysningene som er nødvendige for å nå formålet, samtidig som den ikke må omfatte flere opplysninger enn nødvendig. Videre må reglene fungere på tvers av tilbydernes ulike systemer og være teknologinøytrale.

Det er etter departementenes vurdering minst to ulike tilnærminger ved utformingen av reglene. Én tilnærming vil være å angi i lov eller forskrift hvilke typer opplysninger som skal lagres. Dette vil ha den fordel at det blir klargjort nøyaktig hvilke opplysninger som skal lagres, for eksempel tildelt IP-adresse, tidsrom for dette, portnumre osv. Ulempen med denne løsningen er imidlertid at det vil være utfordrende å utforme en uttømmende liste over opplysninger som både er dekkende og treffende på tvers av ulike systemer.

En annen tilnærming vil være at det i stedet for å angi nøyaktig hvilke opplysninger som skal lagres, fastsettes en plikt til å lagre de opplysninger som er nødvendige for formålet – nemlig å kunne identifisere abonnenter som gis internettilgang. Fordelen med denne tilnærmingen er at den er teknologinøytral, og at en slik bestemmelse vil sikre at bare de nødvendige opplysningene lagres.

Ulempen med en helt generell og teknologinøytral bestemmelse som pålegger lagring av «de opplysninger som er nødvendige for å identifisere abonnenten» eller lignende, er imidlertid at det ikke vil fremgå uttrykkelig hva abonnenten skal kunne identifiseres med utgangspunkt i. Hva som er nødvendig å lagre for å kunne identifisere en abonnent i et konkret tilfelle, kommer an på hva abonnenten skal kunne identifiseres ut ifra, med andre ord hva slags informasjon tilbyderen får fra politi eller påtalemyndighet for å foreta identifiseringen. Dette kan illustreres med et eksempel: Dersom en tilbyder bes om å identifisere en abonnent som har delt overgrepsmateriale, og politiet opplyser om både tidspunktet for dette og IP-adressen som ble benyttet, vil tilbyderen kunne foreta identifiseringen ut ifra en logg over hvilke IP-adresser abonnentene har vært tildelt og på hvilke tidspunkter, forutsatt at IP-adressen ikke har vært delt mellom flere abonnenter. Da vil ikke tilbyderen ha behov for å lagre mer enn dette. Dersom politiet derimot bare skulle ha kjennskap til IP-adressen, og ikke tidspunktet for delingen, vil tilbyder ikke kunne identifisere abonnenten uten å lagre andre typer data, for eksempel ved å logge hvilke nettsteder abonnentene har besøkt. Det er ikke meningen at lagringsplikten skal omfatte slike data. Hvis reglene bare fastsetter en generell plikt til å lagre de opplysninger som er nødvendige for å identifisere abonnenten, vil det ikke fremgå uttrykkelig av ordlyden at slike data ikke omfattes.

Tilsvarende problemstillinger vil oppstå for tilbydere som tildeler samme IP-adresser til flere abonnenter, jf. punkt 7.2 over. I slike tilfeller vil det ikke være mulig å identifisere en enkelt abonnent kun med utgangspunkt i en IP-adresse og et tidspunkt for kommunikasjonen. Det vil etter omstendighetene være mulig å identifisere en enkelt abonnent dersom politiet har kjennskap til et portnummer. Uten informasjon om portnummer, vil identifisering etter omstendighetene bare være mulig dersom tilbyderen har lagret data om hvilke nettsteder abonnentene har besøkt e.l. Lagringsplikten bør etter departementenes vurdering omfatte portnumre tildelt abonnenten, jf. punkt 7.2, men ikke mer enn dette. Denne begrensningen vil imidlertid ikke fremgå uttrykkelig av en generell bestemmelse som pålegger lagring av de opplysninger som er nødvendige for å identifisere abonnenten.

Etter departementenes vurdering fremstår det som en hensiktsmessig tilnærming å velge en mellomløsning ved utformingen av bestemmelsen, der lagringsplikten begrenses til det som er nødvendig, samtidig som det presiseres hva abonnenten skal kunne identifiseres med utgangspunkt i. Lagringsplikten kan da presiseres slik at det skal lagres de opplysninger som er nødvendige for å identifisere abonnenten ut ifra:

a) en IP-adresse og et tidspunkt for kommunikasjon, eller
b) en offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse tildeles flere abonnenter samtidig.

Departementene er ikke kjent med at det i dag brukes løsninger hvor det er behov for å lagre ytterligere informasjon for å kunne identifisere en abonnent (for eksempel portnummer på destinasjonssiden), men ber om høringsinstansenes innspill på om slike løsninger er i bruk.

7.3.3 Hvordan og hvor skal data lagres?

Ved innføring av en lagringsplikt vil tilbyderne måtte lagre en betydelig mengde data som de ellers ville vært pålagt å slette. Lagringen har et annet formål (etterforskningsformål) enn lagring som skjer i dag, dataene skal lagres lenger enn tilsvarende data lagres i dag, og de skal også brukes av andre (politi og påtalemyndighet). Det må derfor vurderes om det er behov for å stille nærmere krav til hvordan og hvor dataene skal lagres.

Departementene understreker imidlertid at det allerede i dag stilles krav til tilbyder om å gjennomføre nødvendige sikkerhetstiltak for vern av kommunikasjon og data i egne elektroniske kommunikasjonsnett og -tjenester. I tillegg skal tilbyder uten ugrunnet opphold varsle abonnenten dersom det foreligger særlig risiko for brudd på sikkerheten.

De største internettilbyderne har i dag egne politisvarfunksjoner som håndterer henvendelser fra politiet, og egne sikrede systemer for å håndtere henvendelsene og prosessering av data for utlevering. For ansatte som håndterer slike saker kan det innhentes uttømmende og utvidet politiattest. I den grad saker omfatter informasjon som er sikkerhetsgradert, må saken håndteres av personer som er sikkerhetsklarert. I tillegg bruker politiet og tilbyderne kryptering der dette er nødvendig for å sikre kommunikasjonen og datautlevering.

Ved en innføring av lagringsplikt vil det med andre ord være et godt alternativ å videreføre dagens krav til sikkerhetstiltak. Når det gjelder *hvor* data skal lagres, kan det tenkes flere mulige løsninger. Det kan stilles krav om at dataene skal lagres (på servere) i Norge, at de skal lagres i egne databaser og at lagring ikke kan settes ut til andre, men må skje i tilbyderens infrastruktur.

Da lovendringene knyttet til datalagringsdirektivet ble vedtatt, ble det ikke foreslått å stille krav til hvor dataene skulle lagres. Departementet mente at muligheten for å føre tilsyn og kontroll med overholdelse av vilkårene for lagring og bruk er avgjørende, uavhengig av hvor lagringen skjer. Det ble senere sendt på høring et forslag til lovendringer som blant annet omhandlet kostnadsfordeling, hvor det var ønskelig å legge til rette for en ordning der tilbyderne skulle stimuleres til å velge en felles lagringsløsning.

Departementene kan ikke se at det for en lagringsplikt som beskrevet i dette høringsnotatet er ønskelig å stille krav til hvor dataene lagres. For det første er det et betydelig mindre omfang av data som lagres, og dataene er å anse som mindre sensitive enn dataene som ble omfattet av datalagringsdirektivet. For det andre kan departementene ikke se at det har vært en teknologisk utvikling som skulle tilsi en annen løsning.

Det bør etter departementenes syn heller ikke settes begrensninger på at dataene skal lagres i tilbyderens egne systemer/infrastruktur. Det forutsettes at tilbyderne kan inngå avtale for eksempel med andre tilbydere for å sikre at lagringsplikten oppfylles. I tillegg er driftsutsetting relativt vanlig, og departementene kan ikke se at det er hensiktsmessig å begrense dette gjennom lovverket. Det bør fortsatt kunne inngås databehandleravtaler som i dag.

Det bør også vurderes om det er behov for å stille krav til *hvordan* dataene lagres. Ekomloven oppstiller allerede krav til tilbyderne, både når det gjelder kommunikasjonsvern og sikkerhet. Etter ekomloven § 2-7 første ledd skal tilbyder gjennomføre nødvendige sikkerhetstiltak for vern av kommunikasjon og data i egne elektroniske kommunikasjonsnett- og tjenester. Ved vurderingen av hva som er «nødvendig» skal det sees hen til hva som er den beste løsningen på markedet til enhver tid. I henhold til Ot.prp. nr. 58 (2002–2003) side 93 gjelder prinsippet om forholdsmessighet mellom kostnadene og sikkerheten som oppnås, og tilbyder skal yte en sikkerhet som er tilpasset risikoen. Ekomloven § 2-9 fastslår at tilbydere plikter å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter. Tilbydere plikter også å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder får anledning til å skaffe seg kjennskap til slike opplysninger. Til det siste fastslår ekomloven § 2-10 at tilbyder skal tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig. I Prop. 69 L (2012–2013) *Endringer i ekomloven* på side 26 defineres begrepet «sikkerhet»:

> «Sikkerhet innenfor elektronisk kommunikasjon defineres gjerne som sikring av tilgjengeligheten til ekomnett og -tjenester, sikring av nettets og kommunikasjonens integritet og sikring av kommunikasjonens konfidensialitet. Det vil si at nett og tjenester skal være sikret mot brudd og ha riktig kvalitet, og at nett, systemer og innhold skal være sikret mot manipulasjon og innsyn.»

Gjeldende regelverk inneholder altså allerede krav for å sikre at kommunikasjonsvernet, taushetsplikten og sikkerhet overholdes. På bakgrunn av dette mener departementene at det ikke er behov for ekstra regulering knyttet til lagringsplikten.

Det er uansett viktig å merke seg at dataene som lagres, vil bli hentet ut fra allerede eksisterende data som har oppstått for kommunikasjonsformål. Dette innebærer at det må tas forbehold for at dataene ikke er opprettet og sammenstilt med tanke på at de skal brukes som bevis i straffesaker, og opplysningene må leses i lys av dette.

7.4 Lagringstid

Ved vurderingen av hvor lenge IP-adresser bør lagres, må det foretas en avveining mellom politiets og påtalemyndighetens behov for opplysningene og hensynet til kommunikasjonsvernet. Ved vurderingen må det tas i betraktning at inngrepet i

kommunikasjonsvernet blir større jo lenger opplysningene lagres. En lengre lagringstid medfører at det samlet sett lagres en større mengde opplysninger, og at lagringen vil kunne bidra til å knytte abonnenter og brukere til aktivitet over nettet som er skjedd lenger tilbake i tid.

For at et inngrep i retten til privatliv skal være lovlig, må det være nødvendig i et demokratisk samfunn, jf. redegjørelsen i punkt 4.1 for EMK artikkel 8. I EU-domstolens avgjørelse *La Quadrature du Net* er det fastslått at lagringstiden ved lagring av IP-adresser må være begrenset til det strengt nødvendige. Bestemmelsene i Grunnloven, EMK og kommunikasjonsverndirektivet setter dermed rammer for hvor lenge IP-adresser kan lagres, og innebærer et krav om at lagringstiden må være nødvendig og forholdsmessig.

Departementene har vurdert hvilken lagringstid for IP-adresser som er nødvendig for å kunne ivareta formålet. Det er i denne sammenhengen flere faktorer som må tas i betraktning. Det må tas høyde for at det ofte vil gå tid fra en straffbar handling begås, til den oppdages. Etterforskningen kan altså knytte seg til et forhold som ligger langt tilbake i tid. Videre vil det kunne forekomme at informasjon om IP-adresser som avdekkes i etterforskningen, knytter seg til nettaktivitet enda lenger tilbake i tid, for eksempel ved forberedelsene til den straffbare handlingen. Dette gjelder for kriminalitet som forebygges og etterforskes både av PST og det øvrige politiet. For at lagringen skal ha tilstrekkelig nytteverdi i kriminalitetsbekjempelsen, er det derfor viktig at den ikke er for kort.

En annen vesentlig faktor er at det i etterforskningen vil kunne ta tid å avdekke IP-adressene. Selv når en straffbar handling oppdages umiddelbart, vil det derfor kunne være tidkrevende å finne frem til en IP-adresse som kan knyttes til den straffbare handlingen. Dette kan for eksempel skyldes at IP-adressene må fremskaffes gjennom undersøkelse av beslaglagte enheter som er beskyttet med passord eller kryptering, som det kan være tidkrevende å forsere. Det kan videre være tilfellet at IP-adresser må innhentes fra utenlandske nettsteder, for eksempel sosiale medier. Det tar sjelden kortere tid enn 3–4 uker å få svar på slike anmodninger. I Sverige lagres opplysningene i ti måneder, i Danmark i tolv måneder og i Finland i ni måneder. Etter departementenes vurdering bør lagringstiden være innenfor det samme spennet som i de øvrige nordiske landene, slik at denne kan være for eksempel seks, ni eller tolv måneder. En lagringstid på seks eller ni måneder vil bedre ivareta kommunikasjonsvernet og personvernet for alle brukere av internett, enn en lagringstid på tolv måneder. Samtidig vil en lagring på tolv måneder i større grad ivareta politiets behov. Det bes særlig om høringsinstansenes syn på hvor lang lagringstiden bør være.

7.5 Vilkår for utlevering av lagrede opplysninger

7.5.1 Materielle vilkår for utlevering

Det er etter gjeldende rett vid adgang til å utlevere opplysninger om tildelte IP-adresser, jf. omtalen av ekomloven § 2-9 tredje og fjerde ledd i punkt 3.2 over. Unntaket fra taushetsplikten gjelder for alle oppgavene politiet utfører. Utlevering til bruk i etterforskingsøyemed krever heller ikke at den straffbare handlingen er av en viss alvorlighet.

Etter departementenes vurdering bør vilkårene for utlevering av opplysningene som skal lagres etter forslaget her, strammes inn sammenlignet med gjeldende rett. Dette er etter departementenes syn nødvendig for å ivareta kravet om proporsjonalitet etter Grunnloven, EMK og kommunikasjonsverndirektivet, jf. punkt 4.1 og 4.3 over.

Det er grunn til å understreke at den lagrede informasjonen om IP-adresser har betydning for etterforskning av straffbare handlinger på mange andre måter enn å bidra til å identifisere ukjente gjerningspersoner. Informasjonen kan også være avgjørende for å identifisere eventuelle fornærmede og vitner. Den kan videre være vesentlig for analyse og annen bearbeiding av innhentet kommunikasjonsdata, eller for å muliggjøre innhenting av ytterligere materiale for eksempel gjennom beslag og utleveringspålegg. Etter departementenes vurdering bør reglene om utlevering derfor ikke utformes slik at det oppstilles spesifikke begrensninger for hvilke måter IP-informasjon kan benyttes i etterforskning osv. Dette bør i stedet bero på hva som er nødvendig for det formålet opplysningene innhentes for. Departementene foreslår derfor at utleveringsreglene utformes slik at informasjonen kan innhentes av politi og påtalemyndighet når det er nødvendig for enkelte nærmere angitte formål.

Ved vurderingen av hvilke formål politi og påtalemyndighet skal kunne innhente opplysningene for, må det foretas en avveining mellom behovet for informasjonen og hensynet til kommunikasjonsvernet.

Etter departementenes syn må det stilles krav om at kriminaliteten må være av en viss alvorlighetsgrad, både av hensyn til kommunikasjonsvernet og som følge av kravene etter Grunnloven, EMK og EØS-retten. Etter EU-domstolens praksis, jf. punkt 4.3 over om *La Quadrature du Net*, kan lagring av IP-adresser for kriminalitetsbekjempende formål bare rettferdiggjøres dersom formålet er å bekjempe «alvorlig kriminalitet». Departementene legger til grunn at reglene om utlevering må utformes i samsvar med dette.

Selv om EU-domstolen i flere avgjørelser om ulike former for datalagring har lagt til grunn at lagringen må begrunnes i hensynet til alvorlig kriminalitet, gir praksis liten veiledning med hensyn til hva som regnes som «alvorlig kriminalitet» («serious crime») i EØS-rettens forstand, eller hvilke kriterier som skal tas i betraktning ved vurderingen av et lovbrudds alvorlighet. Etter departementenes vurdering er det også noe usikkert om det finnes én enhetlig terskel på dette punktet som må legges til grunn uavhengig av hva slags lagring det er tale om. EU-domstolen har understreket i blant annet *Tele 2*, *Ministerio Fiscal* og *La Quadrature du Net* at kravet om at «alvorlige inngrep» i grunnleggende rettigheter bare kan rettferdiggjøres dersom formålet er å bekjempe «alvorlig kriminalitet», er et utslag av det generelle kravet om proporsjonalitet.

Adgangen til utlevering kan begrenses enten ved å sette et krav til strafferamme, eller å begrense utleveringen til forebygging og etterforskning av bestemte straffebud. Man kan også tenke seg en kombinasjon der det settes krav til strafferamme, samtidig som det åpnes for utlevering også for å forebygge eller etterforske bestemte straffebud med lavere strafferamme.

Som det fremgår av punkt 7.1.2 er det ikke slik at behovet for IP-informasjon knytter seg til bekjempelse av spesifikke former for kriminalitet. Det er heller ikke slik at informasjonen bare har betydning for straffbare handlinger som begås over

internett, selv om behovet er særlig tydelig i slike saker, der det ofte ikke finnes andre opplysninger enn IP-adressen som kan bidra til å identifisere gjerningspersonen. Det har lenge vært en klar trend at kommunikasjonen i samfunnet i økende grad blir internettbasert. Opplysninger om nettbasert kommunikasjon blir dermed stadig viktigere i alle typer saker der kommunikasjonsdata er av betydning. Etter departementenes vurdering vil det derfor være mest formålstjenlig at reglene om utlevering som utgangspunkt knyttes opp mot et generelt strafferammekrav, eventuelt i kombinasjon med nærmere bestemte straffebud.

Informasjon om IP-adresser kan være av stor betydning for etterforskningen av en rekke former for kriminalitet som isolert sett ikke nødvendigvis kan medføre lange fengselsstraffer. Handlingene kan like fullt oppleves svært alvorlig for de som rammes av dem. Dette kan for eksempel gjelde handlinger som rammes av straffeloven § 201 om uberettiget befatning med tilgangsdata, § 351 andre ledd om skadeverk i form av endring og sletting mv. av data, § 263 om trusler og § 267 om krenkelse av privatlivets fred, samt § 298 om seksuelt krenkende atferd uten samtykke, § 305 om seksuelt krenkende atferd mv. overfor barn under 16 år og § 306 om avtale om møte for å begå seksuelt overgrep. Disse bestemmelsene har alle en strafferamme på bot eller fengsel inntil 1 år. Videre har straffeloven § 202 om identitetstyveri, § 204 datainnbrudd, § 266 om hensynsløs atferd, § 371 om bedrageri og § 332 om heleri, som blant annet kan ramme spredning av private bilder alle en strafferamme på bot eller fengsel inntil 2 år. Blant straffebudene med en strafferamme på bot eller fengsel i inntil 3 år finner man blant annet straffeloven § 183 om oppfordring til en straffbar handling, § 185 om hatefulle ytringer, § 264 om grove trusler og § 311 om fremstilling av seksuelle overgrep mot barn.

Dette tilsier at strafferammekravet bør settes til minimum ett eller to års fengsel, eventuelt i kombinasjon med unntak for spesifikke straffebud der IP-informasjon er av særlig stor betydning. Departementene har ikke tatt endelig stilling til hvilket strafferammekrav som bør settes, og ber særlig om høringsinstansenes syn på dette.

Når det åpnes for å utlevere opplysninger til etterforskning, bør det etter departementenes vurdering også åpnes for at opplysningene kan utleveres når det er nødvendig for å forebygge en handling av tilsvarende alvorlighet. Opplysninger om hvem en IP-adresse tilhører antas å ha størst betydning i etterforskningen av et lovbrudd som er begått eller pågår. Men dersom en handling kan forebygges før den inntreffer ved hjelp av informasjon om hvem en IP-adresse tilhører, bør politiet etter departementenes syn kunne innhente denne informasjonen i samme omfang som opplysningene kan innhentes til etterforskning. I en rekke bestemmelser som åpner for utlevering av opplysninger til politiet til forebygging og etterforskning er strafferammen sammenfallende for disse formålene, jf. blant annet passloven § 8 a, vegtrafikkloven § 43 b og utlendingsloven ny § 84 a, jf. lov 12. juni 2020 nr. 65 om endringer i utlendingsloven mv. (utlevering av opplysninger til politiet mv.). Departementene legger til grunn at det samme bør gjelde her, men ber om høringsinstansenes syn på spørsmålet.

Kravet til at det skal være *nødvendig* å utlevere opplysningene til politiet for å oppnå de nevnte formålene, kan ikke tolkes så strengt at utleveringen må være den eneste mulige løsningen. Det er på den annen side ikke tilstrekkelig at innhenting

av slike opplysninger kun vil lette arbeidet. Kravet om nødvendighet innebærer også at det ikke kan innhentes flere opplysninger enn det som i det enkelte tilfellet trengs for formålet.

7.5.2 Utlevering av informasjon med utgangspunkt i både IP-adresse og abonnent?

Som nevnt i punkt 7.1.2 vil bruksområdet for informasjon om tildelte IP-adresser oftest være å knytte en abonnent til en gitt IP-adresse. Det kan imidlertid også være behov for informasjon om IP-adresser med utgangspunkt i en gitt abonnent, med andre ord informasjon om hvilke IP-adresser og eventuelt portnumre en konkret abonnent er blitt tildelt på et gitt tidspunkt eller i et gitt tidsrom. Dette gjelder særlig ved undersøkelse av datamateriale i en etterforskning rettet mot en bestemt mistenkt. I stedet for å innhente abonnementsinformasjon med utgangspunkt i hver enkelt IP-adresse som finnes i materialet, kan det da innhentes en oversikt over hvilke IP-adresser den mistenkte ble tildelt i det aktuelle tidsrommet, slik at det langt enklere kan avdekkes om og i hvilken utstrekning den mistenktes IP-adresser forekommer i materialet. Dette vil kunne være langt mer effektivt og ressursbesparende, og det vil også kunne være viktig for å avkrefte mistanke som det viser seg å ikke være grunnlag for.

Innhenting med utgangspunkt i en konkret abonnent vil videre bidra til å begrense mengden av opplysninger som innhentes. Alternativet til å innhente informasjon med utgangspunkt i abonnent, vil kunne bli at det innhentes informasjon om alle IP-adressene som forekommer i et datamateriale, noe som kan medføre at det må innhentes en betydelig mengde informasjon som viser seg å være irrelevant.

Etter departementenes vurdering bør det på denne bakgrunn også åpnes for utlevering av IP-informasjon med utgangspunkt i en gitt abonnent. Dette bør etter departementenes syn bero på de samme vilkårene som for utlevering med utgangspunkt i en IP-adresse.

7.5.3 Prosessuelle garantier ved utlevering

Utlevering av abonnementsopplysninger til påtalemyndigheten eller politiet krever etter gjeldende rett ikke rettens kjennelse eller at Nasjonal kommunikasjonsmyndighet fritar tilbyder fra taushetsplikten. Etter departementenes vurdering bør gjeldende rett videreføres på dette punktet.

Om kravene etter EMK på dette punktet vises det til punkt 4.1 over. Som EMD la til grunn i *Breyer mot Tyskland*, må det ved vurderingen av behovet for prosessuelle garantier sees hen til i hvilken grad det gripes inn i personvernet. Dersom datalagringen er mindre inngripende, kan mer generelle regler om politiets og påtalemyndighets innhenting og behandling av personopplysninger mv. utgjøre tilstrekkelige garantier, uten at det er behov for forutgående vurdering av en domstol eller et annet uavhengig organ i hvert enkelt tilfelle, jf. dommens avsnitt 105–107. Selv om lagring av IP-adresser (og eventuelt portnummer) nok må anses som noe mer inngripende enn lagringen det var tale om i denne saken, kan det etter departementenes syn ikke legges til grunn at dette vil være så inngripende at det er påkrevd etter EMK med en uavhengig forhåndsgodkjenning av hver enkelt utlevering.

Departementene kan heller ikke se at dette er påkrevd etter kommunikasjonsverndirektivet. Departementene legger til grunn at de forholdsvis detaljerte kravene EU-domstolen oppstilte i *Tele 2*-avgjørelsen med hensyn til prosessuelle vilkår for utlevering, ikke uten videre kan overføres til lovgivning om lagring av IP-adresser. Sentralt i *Tele 2*-avgjørelsen var at lagringen gjorde det mulig å trekke svært presise slutninger om privatlivet til de det ble lagret informasjon om, jf. punkt 4.3 over. Som EU-domstolen la til grunn i *Ministerio Fiscal* vedrørende utlevering av abonnementsopplysninger, blir proporsjonalitetsvurderingen en annen når dette ikke er tilfelle. Informasjonen som lagres ved lagring av IP-adresser, kan etter departementenes syn ikke betraktes som informasjon som vil gjøre det mulig å trekke presise slutninger om privatlivet til de det lagres informasjon om. I *La Quadrature du Net* uttalte EU-domstolen at det må gjelde strenge vilkår og garantier vedrørende bruk av IP-adresser, jf. avsnitt 156, men det ble ikke slått fast at det er påkrevd med uavhengig forhåndsgodkjenning av den enkelte utlevering.

Politiets og påtalemyndighetens behandling av opplysninger til politimessige formål reguleres av politiregisterloven med tilhørende forskrift. Regelverket gjennomfører direktiv (EU) 2016/680 om fysiske personers vern i forbindelse med kompetente myndigheters behandling av personopplysninger med sikte på å forebygge, etterforske, avsløre eller rettsforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner og om fri utveksling av slike opplysninger […]. Direktivet bygger på de samme grunnleggende prinsipper som personvernforordningen, men med nødvendige tilpasninger som følge av den kriminalitetsbekjempende virksomhetens særpreg. Regelverket stiller blant annet krav om at behandling av opplysninger skal være formålsbestemt, nødvendig og relevant, at opplysninger ikke skal lagres lenger enn det som er nødvendig for formålet med behandlingen, samt krav til informasjonssikkerhet og internkontroll.

Regelverket etablerer på samme måte som personvernforordningen flere mekanismer som ivaretar den registrertes rettigheter.

For det første vil den registrerte kunne be om innsyn i opplysninger om seg selv, jf. politiregisterloven § 49 andre ledd, der det fremgår at den registrerte har rett til å få opplyst hvilke opplysninger som er registrert om seg selv. Innsynsretten gjelder imidlertid ikke ubegrenset, jf. bestemmelsens fjerde ledd. I den enkelte straffesak har den registrerte rett til dokumentinnsyn i samsvar med straffeprosesslovens regler.

Den registrerte har videre klageadgang, og kan etter lovens § 54 klage blant annet på avgjørelser om innsyn, retting, sperring og sletting.

Videre er politiets behandling av opplysninger underlagt Datatilsynets tilsynskompetanse, jf. lovens § 58. Tilsynskompetansen omfatter all behandling av opplysninger i politiet og påtalemyndigheten, herunder for behandling av opplysninger i den enkelte straffesak, med unntak av opplysninger som behandles av Politiets sikkerhetstjeneste eller opplysninger som er underlagt kompetansen til kontrollutvalget for kommunikasjonskontroll. For PST er det EOS-utvalget som er tilsynsmyndighet. Etter § 59 skal Datatilsynet etter begjæring fra den registrerte, eller den som antar å være registrert, kontrollere at opplysninger om vedkommende er behandlet i samsvar med loven og at reglene om innsyn er fulgt. Slik begjæring skal besvares snarest mulig og senest innen 30 dager, jf. politiregisterforskriften § 42-4.

Datatilsynets virkemidler er nærmere regulert i § 60. Tilsynets virkemidler ble ytterligere styrket ved lov 21. juni 2017 nr. 94, da det ble tilføyd et nytt fjerde ledd som gir Datatilsynet adgang til å fastsette tvangsmulkt for å sikre oppfølging av ilagte pålegg.

Etter departementenes vurdering er det ikke behov for særskilte regler om behandling av innhentede opplysninger etter den nye bestemmelsen, eller etablering av ytterligere mekanismer for å ivareta den registrertes rettigheter hva gjelder behandlingen. De alminnelige reglene i politiregisterloven og forskriften anses dekkende. Opplysninger skal etter politiregisterloven § 50 ikke lagres lenger enn det som er nødvendig for formålet med behandlingen. Opplysninger som er innhentet utenfor straffesak vil derfor ofte kunne slettes etter relativt kort tid. Opplysninger som innhentes som ledd i en straffesak, og som for eksempel er brukt som bevis i saken, vil inngå som en del av straffesakens dokumenter og følge de alminnelige reglene for behandling av disse.

7.6 Bruk av opplysninger om IP-adresser i sivile saker

Det følger av tvisteloven § 21-5 at enhver plikter å gi forklaring om faktiske forhold og gi tilgang til gjenstander mv. som kan utgjøre bevis i en rettssak, med de begrensninger som følger av reglene om bevisforbud og bevisfritak i kapittel 22 og andre bevisregler i loven. Denne forklarings- og bevisføringsplikten gjelder også for ekomtilbydere. For taushetsbelagte opplysninger gjelder imidlertid bevisforbudet i tvisteloven § 22-3. Etter § 22-3 første ledd kan det som hovedregel ikke føres bevis når dette vil krenke lovbestemt taushetsplikt for den som har opplysningene som følge av tjeneste eller arbeid for blant annet tilbyder eller installatør av elektronisk kommunikasjonsnett eller -tjeneste. Opplysningene som skal lagres etter forslaget her, vil være taushetsbelagte etter ekomloven § 2-9.

Det følger av ekomloven § 2-9 tredje ledd andre punktum at taushetsplikten ikke er til hinder for at det gis opplysninger om abonnement «ved vitnemål for retten». Bevisforbudet for taushetsbelagte opplysninger i tvisteloven § 22-3 gjelder likevel i sivile saker, jf. Rt. 2010 side 774 avsnitt 40. Opplysningene som skal lagres etter forslaget her, er dermed underlagt bevisforbud etter tvisteloven. Det innebærer at opplysningene som utgangspunkt ikke kan føres som bevis i sivile saker, og at tilbyder ikke vil ha adgang eller plikt til å utlevere opplysninger for dette formålet.

Tvisteloven § 22-3 andre og tredje ledd oppstiller samtidig unntak fra bevisforbudet. Etter § 22-3 andre ledd kan departementet samtykke i at beviset føres. Departementets kompetanse er delegert til Nkom. Nkoms samtykke skal bare nektes «når bevisføring kan utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold». Etter tredje ledd kan retten etter «en avveining av hensynet til taushetsplikten og hensynet til sakens opplysning» ved kjennelse bestemme at beviset skal føres selv om samtykke er nektet, eller at beviset ikke skal mottas selv om Nkom har samtykket.

En innføring av en plikt til å lagre IP-adresser vil innebære at opplysninger om IP-adresser lagres betydelig lenger enn i dag. Dette kan medføre at det i økt grad oppstår spørsmål om IP-informasjon skal kunne føres som bevis etter unntakene i tvisteloven § 22-3. Utlevering av IP-adresser til bruk i sivile saker, vil utgjøre et ytterligere inngrep i kommunikasjonsvernet. Ettersom det er politiets og påtalemyndighetens behov for opplysningene i kriminalitetsbekjempelsen som begrunner forslaget om lagring av IP-adresser mv., kan det spørres om det bør

oppstilles flere begrensninger i adgangen til å benytte opplysningene som bevis i sivile saker, utover de begrensningene som allerede følger av utgangspunktet om bevisforbud i tvisteloven § 22-3.

Ved vurderingen av dette spørsmålet må det tas i betraktning at adgangen til å gjøre unntak fra bevisforbudet blant annet skal ivareta den enkeltes behov for å få håndhevet sine rettigheter, jf. tvisteloven § 1-1 første ledd. Særlig når det gjelder straffbare rettskrenkelser av en slik alvorlighet at det kan begrunne utlevering av opplysninger om IP-adresser til politi eller påtalemyndighet etter forslaget her, kan det også være aktuelt med forfølging av krenkelsen i sivilprosessens former, for eksempel i en sak om erstatning. Det vil kunne føre for langt dersom den som er utsatt for krenkelsen, blir avskåret fra å kunne benytte opplysninger om IP-adresser for å kunne forfølge slike sivilrettslige krav.

I de aller fleste tilfeller der det oppstår spørsmål om å føre taushetsbelagte opplysninger som bevis i en sivil sak, vil det være slik at opplysningene ikke er samlet inn for dette formålet. Dette er et av hensynene som ivaretas ved at tvisteloven som hovedregel forbyr at opplysningene føres som bevis. Tvisteloven § 22-3 favner også om opplysninger som er vesentlig mer inngripende enn det som foreslås lagret i høringsnotatet her, uten at det av den grunn er oppstilt særskilte begrensninger i adgangen til å benytte opplysningene som bevis. Dette kan for eksempel være opplysninger av svært sensitiv karakter som er innsamlet som ledd i forvaltningens saksbehandling. Tvisteloven § 22-3 gjelder for øvrig for trafikkdata som lagres for driftsformål hos ekomtilbydere, og som derfor finnes tilgjengelig i en kortere periode.

Åndsverkloven § 87 gir som nevnt særregler om at det etter omstendighetene kan gis tilgang til opplysninger som identifiserer innehaver av abonnement brukt ved inngrep i opphavsrett eller andre rettigheter etter loven, jf. pkt. 3.2. En plikt til å lagre IP-adresser vil innebære at åndsverkloven § 87 kan bli aktuell å benytte i flere tilfeller enn i dag. Departementene viser til at vurderingstemaet etter åndsverkloven § 87 tilsvarer vurderingstemaet etter tvisteloven § 22-3 tredje ledd. Det vises for øvrig til vurderingene i Prop. 65 L (2012-2013) *Endringer i åndsverkloven (tiltak mot krenkelser av opphavsrett på Internett)* vedrørende de kryssende hensynene som gjør seg gjeldende.

Tvisteloven § 22-3 og åndsverkloven § 87 ivaretar de motstridende hensynene som gjør seg gjeldende, og er sentrale bestemmelser for muligheten til sivilrettslig håndheving ved inngrep i rettigheter på Internett og i andre sivile saker. Departementene mener at det er viktig at det fortsatt skal være adgang til sikring av bevis og bevisføring i sivile saker, og ser derfor ikke behov for å begrense den faktiske adgangen rettighetshaverne har i dag. En innføring av en plikt til å lagre IP-adresser vil imidlertid innebære at opplysningene om IP-adresser lagres betydelig lenger enn i dag. Det er usikkert hva en slik utvidet lagringstid for IP-adresser i praksis vil innebære i sivile saker og hvilken betydning dette vil ha for blant annet kommunikasjonsvernet. Departementene ber derfor særskilt om høringsinstansenes syn på dette. Vi ber også om synspunkter på om det kan være behov for begrensninger på bruken av opplysninger som omfattes av utvidet lagring i sivile saker.

8. Forslag til lovbestemmelser

Forslag til endringer i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon:

§ 2-8 a *Plikt til lagring av IP-adresser*

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre de opplysninger som er nødvendige for å identifisere abonnenten med utgangspunkt i

a) offentlig IP-adresse og et tidspunkt for kommunikasjon eller

b) offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse er tildelt flere abonnenter samtidig.

Opplysningene skal lagres i seks/ni/tolv måneder fra den dagen kommunikasjonen avsluttes.

Tredje ledd skal regulere kostnadsfordelingsmodell og kan se slik ut om modell D eller E blir besluttet:

Alternativ 1 (Modell D):

Tilbyders merkostnader for investeringer som påløper for å oppfylle lagringsplikten dekkes av tilbyder med 20 prosent. Staten dekker resten av merkostnadene for investeringer, merkostnadene for drift og kostnadene for utlevering av informasjon etter første ledd.

Alternativ 2 (Modell E):

Tilbyders merkostnader for investeringer og drift som påløper for å oppfylle lagringsplikten dekkes av tilbyder med 20 prosent. Staten dekker resten av merkostnadene for tilbyders investeringer og drift, og kostnadene for utlevering av informasjon etter første ledd.

Skulle modell A, B eller C velges, vil tredje ledd tilpasses disse modellene.

Myndigheten kan pålegge tilbyder et system for kostnadsdeling. Tilbyder skal fremvise revisorbekreftede beregninger for påløpte kostnader.

Myndigheten kan gi forskrift om lagringsplikten etter første ledd, herunder om kostnader. Myndigheten kan gi unntak fra lagringsplikten.

§ 2-8 b *Utlevering av opplysninger lagret etter § 2-8 a*

Opplysninger lagret etter § 2-8 a skal uten hinder av taushetsplikt etter § 2-9 utleveres til politiet eller påtalemyndigheten når det er nødvendig

Alternativ 1: for å forebygge eller etterforske en handling som etter loven kan medføre straff av fengsel i x år eller mer

Alternativ 2: for å forebygge eller etterforske en handling som etter loven kan medføre straff av fengsel i x år eller mer, eller som rammes av straffeloven §§ xxx

Kongen kan gi forskrift om utlevering av data etter første ledd.

9. Merknader til de enkelte bestemmelsene

Til § 2-8 a

Første ledd pålegger tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, og tilbyder av slik tjeneste å lagre opplysninger som er nødvendige for å identifisere abonnenter som er gitt tilgang til internett.

Plikten påhviler tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, og tilbyder av slik tjeneste. Dette omfatter store og små bedrifter som tilbyr andre tilgang til offentlig elektronisk kommunikasjonsnett eller tjenester som helt eller i det vesentlige består av fremføring eller dirigering av signaler i et elektronisk kommunikasjonsnett og som normalt tilbys mot vederlag.

Rekkevidden av lagringsplikten er presisert ved at det er angitt i bestemmelsen hvilke opplysninger abonnenten skal kunne identifiseres ut ifra. Med dette siktes det til opplysninger som fremlegges for tilbyder ved en forespørsel om identifisering av en abonnent. Dersom en IP-adresse ikke deles mellom flere, skal tilbyder lagre de opplysninger som nødvendige for å identifisere abonnenten ut ifra i offentlig IP-adresse og et tidspunkt for kommunikasjon, jf. *bokstav a*. Dette vil som minimum omfatte opplysninger om hvilke IP-adresser abonnentene har disponert, og i hvilket tidsrom. Dersom samme IP-adresse tildeles flere abonnenter samtidig, skal tilbyder i tillegg lagre de opplysninger som er nødvendige for å identifisere en enkelt abonnent med utgangspunkt i portnummer, jf. *bokstav b*.

Kravet om nødvendighet innebærer at det ikke skal lagres flere opplysninger enn det formålet krever. Det skal ikke lagres opplysninger om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har vært i kontakt med.

Det følger av *andre ledd* at opplysningene skal lagres i seks/ni/tolv måneder fra den dagen kommunikasjonen avsluttes. Opplysningene må lagres uavhengig av om abonnentens kundeforhold avsluttes før utløpet av lagringstiden.

Tredje ledd skal regulere kostnadsfordelingsmodellen. Dette høringsnotatet beskriver kostnadsmodellene A til E, og departementene vil komme tilbake med lovtekst og særmerknader i lovproposisjonen når kostnadsmodell er avklart. Inntil videre vises til informasjonen som fremgår av punkt 10.

Femte ledd gir hjemmel for ytterligere regulering i forskrift. Dersom det viser seg å bli behov for det, kan det blant annet gis bestemmelser som presiseres nærmere hvilke opplysninger som er omfattet av lagringsplikten. Det kan videre fastsettes bestemmelser om unntak fra lagringsplikten og om dekning av kostnader.

Til § 2-8 b

Bestemmelsen gir regler om utlevering av opplysninger lagret etter § 2-8 a. Når vilkårene for utlevering er oppfylt, plikter tilbyder å utlevere opplysningene uten hensyn til taushetsplikt etter § 2-9. Bestemmelsen åpner kun for utlevering til politi og påtalemyndighet. Det ligger til politiet eller påtalemyndigheten å ta stilling til om vilkårene for utlevering er oppfylt i det enkelte tilfellet. Tilbyder skal derfor ikke foreta noen selvstendig vurdering av vilkårene i bestemmelsen.

Bestemmelsen åpner for utlevering av opplysninger både med utgangspunkt i IP-adresser mv. og abonnenter. Det vil si at det både kan innhentes opplysninger om hvilken abonnent som var tildelt en gitt IP-adresse på et gitt tidspunkt, og om hvilke IP-adresser en gitt abonnent var tildelt i en tidsperiode og eventuelt om benyttede portnumre i perioden.

Første ledd oppstiller et generelt nødvendighetskrav, og angir i bokstav a til c ulike formål som opplysningene kan utleveres for. Kravet om nødvendighet innebærer at det ikke kan innhentes flere opplysninger enn det som i det enkelte tilfellet trengs for formålet. Det må foretas en konkret vurdering av behovet for opplysningene, som må veies mot hensynet til kommunikasjonsvernet.

Etter første ledd *første alternativ* kan opplysningene utleveres når det er nødvendig for å forebygge eller etterforske en handling som etter loven kan medføre straff av fengsel i x antall år eller mer. Strafferammekravet innebærer at saken må inkludere minst én handling som alene kan straffes med fengsel i x år eller mer Bestemmelsen vil omfatte straffebud som åpner for fengsel «inntil» den fastsatte terskelen. Forhøyelse av strafferammen som følge av gjentakelse, jf. straffeloven § 79 første ledd bokstav b, kommer ikke i betraktning. Forhøyelse av strafferammen som følge av at samme handling bryter flere straffebud (idealkonkurrens), vil derimot komme i betraktning, jf. straffeloven § 79 første ledd bokstav a. Det samme gjelder dersom handlingen er utøvet som ledd i aktivitetene til en organisert kriminell gruppe, jf. bokstav c.

Etter *annet alternativ* åpnes det for at opplysninger i tillegg kan utleveres for å forebygge eller etterforske enkelte straffebud med lavere strafferamme enn den generelle. Hvilke straffebud dette skal omfatte, vil måtte vurderes i lys av hva den generelle strafferammen settes til. Selv om departementet ikke har konkludert på hvilke straffebud som skal omfattes, er det en forutsetning at det dreier seg om straffebud der IP-informasjon er av særlig stor betydning for å forebygge eller etterforske handlingen.

Det understrekes at abonnementsinformasjon kan være nødvendig i en etterforskning for andre formål enn å identifisere ukjente gjerningspersoner. Informasjonen kan også være nødvendig blant annet for å identifisere eventuelle fornærmede og vitner, analyse og annen bearbeiding av innhentet kommunikasjonsdata, eller for å muliggjøre innhenting av ytterligere materiale for eksempel gjennom beslag og utleveringspålegg.

Det følger av *andre ledd* at Kongen kan gi forskrift om utlevering av data etter første ledd. Forskriftshjemmelen kan blant annet benyttes for å presisere rekkevidden av utleveringsplikten eller til å fastsette nærmere bestemmelser om hvordan utlevering skal skje.

10. Kostnadsfordelingsmodell

10.1 Tidligere arbeid med kostnadsfordelingsmodell

I forbindelse med at EUs datalagringsdirektiv (direktiv 2006/24/EF) ble besluttet gjennomført i norsk rett, jf. Prop. 49 L (2010–2011), etablerte

Samferdselsdepartementet og Justis- og beredskapsdepartementet et utvalg som fikk i oppdrag å utarbeide et forslag til ny modell for hvordan kostnader skal beregnes og fordeles mellom ekomtilbyderne og myndighetene. Kostnadsdelingsutvalget leverte 1. februar 2012 sin rapport «Forslag til kostnadsfordelingsmodell i forbindelse med innføring av datalagringsdirektivet i norsk rett». Datalagringsdirektivet ble senere opphevet av EU-domstolen, og lovendringene trådte ikke i kraft i Norge. Selv om lagringsmodellen den gang var annerledes og mye mer omfattende enn det departementene foreslår i dette høringsnotatet, bygger enkelte av modellene som foreslås nedenfor, delvis på Kostnadsutvalgets utredning og begrunnelser for fordelingen mellom tilbydere og staten.

Departementet hørte forslag til kostnadsfordeling i mars 2012 basert på blant annet Kostnadsutvalgets utredning. Høringsnotatet ligger her og viser videre til utredningen: https://www.regjeringen.no/no/dokumenter/horingsbrev/id675976/

Departementene vil med dette høringsnotatet be om innspill til de fem ulike kostnadsfordelingsmodellene som presenteres nedenfor.

10.2 Dagens ordning

Det følger av ekomloven § 2-8 at tilbyder skal tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres. Etter dagens ordning bekostes investeringskostnadene for slik tilrettelegging av tilbyder ut ifra en tanke om at tilbyder selv har behov for dataene til kommunikasjons- og faktureringsformål, og derfor uansett måtte ha dataene tilgjengelig i perioden politiet kan få tilgang. Det følger også av § 2-8 at «[t]ilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten for de merkostnader som følger av disse tjenestene». Politiet betaler med andre ord for tilbyders driftskostnader ved tilretteleggingen, forutsatt at dette er merkostnader, i tillegg til tilbyders uthentingskostnader ved utlevering av IP-informasjon til politiet. Dette er avtaleregulert mellom politiet og de forskjellige tilbyderne i en rekke enkeltavtaler mellom partene.

10.3 Vurderingskriterier

I departementenes vurdering av hvilken kostnadsfordelingsmodell som er mest hensiktsmessig, er det enkelte hensyn som særlig vektlegges. Det første hensynet er kriminalitetsbekjempelse, som er hovedformålet med lovforslaget. I dette ligger det at politiet skal kunne innhente IP-informasjon i de sakene de faglig sett har behov for det i kampen mot alvorlig kriminalitet. Videre vektlegger departementene at modellen skal ivareta kommunikasjonsvernet og konkurransen i ekommarkedet slik at modellen understøtter samfunnsøkonomisk kostnadseffektivitet. Siden formålet med forslaget er kriminalitetsbekjempelse, kan ikke tilbyderne forventes å dekke alle kostnadene.

10.4 Kategorisering av kostnader

Kostnadene i forslaget kategoriseres som investeringskostnader, faste driftskostnader og uthentingskostnader. Investeringskostnader forklares som kostnader til anskaffelse og oppgradering av maskinvare og programvare. Faste driftskostnader omfatter drift, vedlikehold, testing, avskriving av investeringer,

lisens- og supportkostnader, leiekostnader og tilhørende personellkostnader. Uthentingskostnader omfatter kostnader knyttet til selve uthentingen av data, og inkluderer blant annet personell- og administrasjonskostnaden for behandling av utleveringsbegjæringer. Denne fordelingen legges til grunn i omtalen av de ulike fordelingsmodellene under. Departementene ber om høringsinstansenes innspill på forslag til kostnadskategorisering.

10.5 Alternative fordelingsmodeller

Det er tre ulike utgangspunkter for valg av kostnadsfordelingsmodell. Det ene er at tilbyderne skal dekke kostnadene forbundet med å etterkomme offentligrettslige pålegg. Det andre er at staten må dekke kostnadene knyttet til pålegg som skal ivareta samfunnsmessige hensyn. Det tredje er at kostnadene fordeles mellom tilbyderne og staten. Fordelingen kan gjøres på ulike måter.

En modell der tilbyderne dekker egne kostnader til klargjøring for lagring uten kompensasjon, er i overensstemmelse med utgangspunktet for andre næringer som er pålagt kriminalitetsbekjempende tiltak, for eksempel finansnæringen som blant annet dekker kostnadene for hvitvaskingsregisteret. Dette er også dagens ordning i ekomsektoren for tilrettelegging for lovbestemt tilgang til informasjon, jf. ovenfor. Det kan imidlertid argumenteres for at kostnadene som følger av lovendringen, forventes å bli større enn dagens kostnader og vil medføre uheldige virkninger i markedet dersom tilbyderne skal dekke disse. På den annen side vil en modell hvor staten fullt ut dekker kostnadene, ikke gi tilbyderne insentiv for å velge kostnadseffektive løsninger, og dermed medføre en økt totalkostnad for samfunnet samlet sett. Det er derfor departementenes vurdering at en modell hvor kostnadene fordeles mellom staten og tilbyder, vil være mest hensiktsmessig, både av hensyn til virkninger i markedet og av hensyn til insentiv for valg av kostnadseffektive løsninger. På bakgrunn av dette og i tråd med tidligere utredninger har departementene vurdert følgende modeller:

A. Staten godtgjør tilbyder for uthentingskostnader. Dette innebærer at tilbyder selv må dekke investeringskostnader og faste driftskostnader.
B. Staten godtgjør tilbyders investeringskostnader og uthentingskostnader. Dette innebærer at tilbyder selv dekker faste driftskostnader.
C. Staten godtgjør tilbyders faste driftskostnader og uthentingskostnader. Dette innebærer at tilbyder selv dekker egne investeringskostnader.
D. Investeringskostnader deles mellom staten og tilbyderne i henhold til en fordelingsnøkkel. Staten dekker faste driftskostnader og uthentingskostnader.
E. Investeringskostnader og faste driftskostnader deles mellom staten og tilbyderne i henhold til en fordelingsnøkkel. Staten dekker uthentingskostnader.

Tabellen under viser en oversikt over hvem som dekker de ulike kostnadskategoriene i de ulike modellene.

Tabell 1 - Oversikt over alternative kostnadsfordelingsmodeller

	Investerings-kostnader	**Faste driftskostnader**	**Uthentings-kostnader**
Modell A	Tilbyder	Tilbyder	Staten

Modell B	Staten	Tilbyder	Staten
Modell C	Tilbyder	Staten	Staten
Modell D	Tilbyder/Staten	Staten	Staten
Modell E	Tilbyder/Staten	Tilbyder/Staten	Staten

Modellene A, B og C er modeller som innebærer kostnadsdeling mellom staten og tilbyderne fordelt etter kategoriene investerings-, drifts- og uthentingskostnader. I modell A dekker staten uthentingskostnadene. I modellene B og C dekker staten i tillegg henholdsvis investeringskostnadene eller de faste driftskostnadene. Modell C ligger nær opptil dagens praktisering av kostnadsfordelingen mellom tilbyderne og politiet.

Modellene D og E skiller seg fra A, B og C ved at én eller flere av kostnadskategoriene deles mellom tilbyder og staten etter en på forhånd fastsatt fordelingsnøkkel. Fordelingsnøkkelen kan enten være fast for alle tilbyderne, eller fastsettes etter vurdering av utvalgte kriterier for den enkelte tilbyder. Det er fordeler og ulemper ved begge varianter, for eksempel knyttet til variasjon i størrelse på tilbyderne, variasjon i eksisterende system hos tilbyderne, administrasjonskostnader ved individuelle tilpasninger osv. Departementene ber om innspill til fordeler og ulemper ved fast eller individuelt tilpasset fordelingsnøkkel, samt forslag til vurderingskriterier som eventuelt bør inngå i en modell hvor man benytter individuelt tilpasset fordelingsnøkkel.

10.5.1 Insentiv og kostnadseffektivitet

I et konkurranseutsatt marked vil tilbyderne søke å minimere enhver kostnad for å opprettholde god lønnsomhet. Tilbyderne vil derfor ha insentiver til å finne kostnadseffektive løsninger når de selv må dekke en kostnad eller en andel av en kostnad.

I modell A må det forventes at tilbyderne vil søke å finne de totalt sett mest kostnadseffektive løsningene for drift og investering. For modellene B og C vil tilbyderne i hovedsak søke løsninger som minimerer henholdsvis de faste driftskostnadene og investeringskostnadene. Modellene gir imidlertid insentiver for tilbyderne til å vri kostnader over på kostnadskategoriene som staten skal dekke.

Insentivene som følge av kostnadsdeling etter kostnadskategori mellom staten og tilbyderne kan føre til høyere kostnader for tilbyderne og staten samlet sett. Dersom en av modellene A, B eller C skal benyttes, må det for å motvirke slike effekter utformes avtaler som sikrer kostnadseffektivitet samlet sett. Erfaringene fra dagens kostnadsfordelingsmodell tilsier at det er uklarheter knyttet til hvilke kostnader som faller innenfor den enkelte kostnadskategori. Dette kan bidra til den relativt store variasjonen i prisen politiet betaler de ulike tilbyderne for å få utlevert etterspurte IP-informasjon. I tillegg kan noe av prisvariasjonen skyldes at tilbyderne benytter forskjellig utstyr og løsninger. Ulik størrelse på tilbyderne og ulikt antall forespørsler medfører trolig variasjoner i prosesser og rutiner for uthenting av IP-informasjon, noe som igjen resulterer i varierende uthentingskostnader mellom tilbydere.

Dersom en av modellene B, C eller D skal benyttes, vil det derfor vurderes om det bør utdypes hvilke kostnader som inngår i de ulike kategoriene på et

detaljeringsnivå som gjør det lettere å forholde seg til både for tilbyderne og for staten. I den grad det skulle være hensiktsmessig, kan dette vurderes for en senere forskriftsbestemmelse. Det vil være viktig å finne måter å gjøre dette på som ikke er til hinder for at nye tekniske løsninger tas i bruk.

I modell D og E deles én eller flere av kostnadskategoriene i henhold til en fordelingsnøkkel. Som det kommer frem av Kostnadsutvalgets utredning, vil selv en liten andel av kostnadene tillagt tilbyderne gi dem insentiv for å velge en kostnadseffektiv løsning.

På bakgrunn av at dette lovforslaget i liten grad gir egenverdi for tilbyderne, kan bruk av fordelingsnøkkel for én eller flere kostnadskategorier fremstå som mer rettferdig overfor tilbyderne sammenlignet med modell A, B og C, samtidig som man ivaretar insentiver for valg av kostnadseffektive løsninger.

Modell D gjenspeiler i størst grad at lagringsordningen først og fremst kommer i stand til bruk for politiet og derfor i hovedsak dekkes av staten, med de uheldige virkninger knyttet til insentiv for å vri kostnader over på staten som er beskrevet over. Modell E vil i størst grad gi insentiv for valg av kostnadseffektive løsninger, men samtidig pålegge tilbyderne kostnader som i liten grad har egenverdi for dem selv.

For samtlige kostnader som staten skal dekke, må det etableres en kontrollordning for eksempel i form av en kompetent enhet i staten eller en tredjepart (revisor), som gjennomgår og godkjenner tilbydernes tekniske løsningsforslag og andre kostnader som dekkes. Der hvor kostnadene fordeles etter en fordelingsnøkkel mellom stat og tilbyder, vil det imidlertid være et mindre behov for å kontrollere valgt løsning, ettersom tilbyderne selv har insentiver for å velge den mest kostnadseffektive løsningen. Denne fordelen er størst i modell A og E.

10.5.2 **Fordelingsvirkninger**

Graden av negative virkninger for tilbyderne vil først og fremst avhenge av størrelsen på kostnaden som tilbyderne skal bære. I modell A og C, og i noen grad modell D og E, vil tilbyderne måtte dekke investeringskostnadene. Det vil kunne medføre at nyetablerte tilbydere, samt tilbydere uten tilfredsstillende lagringsløsninger, må foreta investeringer for å innfri kravene ved innføring av lovforslaget. Dette vil kunne være til hinder for etablering og kan i verste fall drive små aktører ut av markedet. I modell A og B, og i noen grad modell E, må tilbyderne dekke faste driftskostnader. Det vil også kunne føre til at kapitalsvake tilbydere må avvikle virksomheten som følge av økte driftskostnader knyttet til lagringsplikten i lovforslaget. Alle modellene vil kunne medføre en viss form for konkurransevridning i ekommarkedet. Dette er ikke ønskelig, men må veies opp mot gevinstene knyttet til kostnadseffektivitet for samfunnet samlet sett.

Det er lagt til grunn at staten må betale for uthenting av IP-informasjon i alle modellene. Dette begrunnes av argumenter om at staten bør betale for politiets innhenting av IP-adresser til bruk i politiets arbeid uten at omfanget av dette belastes tilbyderne. Dersom man legger hele eller deler av uthentingskostnadene på tilbyderne, vil det kunne gi uheldige konkurransevridende effekter ved at enkelte tilbydere må bære større kostnader enn andre tilbydere avhengig av hvor ofte politiet ber om utlevering av IP-informasjon.

Det antas at større tilbydere som kan fordele sine ekstrakostnader over mange kunder, lettere kan bære en lagringsplikt enn små tilbydere med langt færre kunder. På den annen side vil virkningene avhenge av om tilbydere med færre kunder kan kjøpe tjenesten som en integrert løsning i tilgangstjenesten.

10.6 Nærmere om uthentingskostnader

En sentral del av formålet med lovforslaget er å legge til rette for at politiet skal kunne innhente IP-informasjon i de sakene de faglig sett har behov for det i kampen mot alvorlig kriminalitet. Politiet har opplyst at de forventer at antall anmodninger om uthenting av IP-informasjon vil øke betydelig ved innføring av lovforslaget, og det vil derfor være en forutsetning for oppfyllelse av formålet med lovforslaget at politiet kan innhente IP-informasjon i flere saker enn i dag. Departementene forutsetter at politiet begrenser uthentingen av IP-informasjon til det som er nødvendig for politiets arbeid, slik at hensynet til kommunikasjonsvernet ivaretas i enkeltsaker.

Som det fremkommer i neste kapittel om økonomiske og administrative konsekvenser, er det relativt stor variasjon i prisingen hos tilbyderne ved utlevering av IP-informasjon til politiet. Dette kan blant annet indikere at det er betydelig variasjon i hvor kostnadseffektive systemer og prosesser de ulike tilbyderne har. Det er derfor en målsetting for departementene at det blir implementert forenklinger i systemene slik at uthentingskostnadene kan gå ned til et rimelig nivå, særlig gjelder dette hos de største tilbyderne som mottar flest uthentingshenvendelser. Automatisering og forenkling kan være aktuelt på to nivåer – for det første på tilbyders hånd for å finne frem den aktuelle informasjonen, og for det andre ved selve utleveringen/overleveringen til politiet (for eksempel en API-lignende ordning). Departementene har gjennom uformelle henvendelser til markedsaktører fått forståelse av at det til en viss grad kan være mulig å forenkle fremskaffelsen av den aktuelle informasjonen i tilbydernes systemer uten at det vil gå på bekostning av sikkerheten og kvaliteten. Departementene vurderer om dette skal utredes i samarbeid med tilbyderne og politiet, og ber særlig om synspunkter til mulighetene for automatiseringer/forenklinger.

10.7 Departementenes foreløpige vurdering

Departementene mener at det er viktig å gi insentiv til etablering av kostnadseffektive løsninger og minimere uheldige konkurransevridende effekter i ekommarkedet når kostnadene fordeles mellom stat og tilbyder etter en fordelingsnøkkel.

I alle modeller er det lagt til grunn at staten dekker uthentingskostnadene. For å sikre at valg av systemløsninger også ivaretar kostnadseffektivitet knyttet til uthenting av IP-informasjonen, kan man tenke seg at tilbyder dekker de nye investeringene som må til for å oppfylle lagringsplikten basert på det utstyret tilbyder allerede har, og som de nye investeringene skal passe sammen med, mens staten dekker eventuelle investeringer som vil føre til automatisering av drift og lavere uthentingskostnader. Det medfører en forutgående dialog mellom tilbyder og politi, eventuelt med hjelp av Nkom, og en enighet om investeringene som foretas.

Modell E er den modellen som ligger tettest opp mot modellen som Kostnadsutvalget anbefalte i høringen om datalagringsdirektivet, hvor kostnadene fordeles mellom stat og tilbyder etter en fordelingsnøkkel. Den gang ble det imidlertid vurdert ekstern lagring som tilbyder ikke skulle ha tilgang til selv. Kostnadsutvalget kom ikke med et konkret forslag til fordeling for ordningen som den gang var aktuell, men mente at selv en liten andel av kostnadene tillagt tilbyder ville sikre kostnadseffektivitet. Kostnadseffektiviteten vil også sikres et stykke på vei i modell D. Modell D tar i tillegg større hensyn til at lagringsplikten ikke gir fordeler for tilbyder.

Dersom man velger en modell med en fordelingsnøkkel mellom stat og tilbyder (modell D eller E), kan det argumenteres for at fordelingsnøkkelen bør gjenspeile at lagringsplikten først og fremst er til nytte for politiet, og at kostnadene derfor i størst grad bør dekkes av staten. På bakgrunn av dette kunne man for eksempel se for seg en fast fordelingsnøkkel hvor staten og det private dekker henholdsvis 80 og 20 pst. av investeringskostnadene eller investerings- og driftskostnadene som påløper som følge av lagringsplikten i lovforslaget. Departementene ber om høringsinstansenes innspill til fordeler og ulemper ved en slik fordelingsnøkkel.

Departementene viser for øvrig til at dersom man viderefører en ordning som i dag hvor politiet innenfor gjeldende budsjettrammer må dekke uthentingskostnader og driftskostnader gjennom stykkprisfinansiering, vil ikke politiet kunne hente ut IP-informasjon i de sakene de faglig sett ville gjort dette uten å måtte nedprioritere ressurser til andre oppgaver. Som det fremkommer i punkt 11.2.2, så ville politiets kostnader til uthenting av IP-adresser etter dagens betalingssystem trolig vært minst 40 mill. kroner høyere dersom lagringsplikten var innført i dag. Dette synliggjør at det vil påløpe betydelige kostnader knyttet til uthenting av IP-informasjon. Uavhengig av hvilken modell som velges, vil finansiering av statens andel av kostnadene behandles i den ordinære budsjettprosessen. Ikraftsetting av loven vil skje etter at finansieringen er avklart, og tidligst fra starten av 2022.

11. Økonomiske og administrative konsekvenser

Departementene har innhentet informasjon fra Politidirektoratet og Kripos om antall anmodninger politiet sender tele- og internettilbydere om IP-adresser, utleveringskostnader for anmodningene, forventet økning i anmodninger i lys av lovforslaget beskrevet i dette høringsnotatet samt hvilke kostnader et slikt lovforslag vil medføre for politiet. Det er også innhentet estimat fra et utvalg av tilbydere over forventede investerings-, drifts- og utleveringskostnader som følge av endringene lovforslaget medfører.

11.1 Dagens situasjon

Tilbyder har som nevnt ovenfor en plikt etter ekomloven § 2-7 til å slette eller anonymisere trafikkdata, lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren så snart de ikke lenger er nødvendig av kommunikasjons- eller faktureringsformål.

Politiet kan imidlertid få tilgang til slike data så lenge de er lagret etter nærmere regler i straffeprosessloven og ekomloven § 2-9. Det følger av ekomloven § 2-8 at tilbyder skal tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres. Det følger også av denne

bestemmelsen at «[t]ilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten for de merkostnader som følger av disse tjenestene».

11.1.1 Omfang

Kripos opplyser at det ikke foreligger en nasjonal oversikt over antall anmodninger om IP-adresser fra politiet til tele- og internettilbydere. For å gi et estimat på antall anmodninger politiet sender tilbyderne i dag, samt antallet politiet ikke etterspør fordi de er kjent med at informasjonen ikke er tilgjengelig hos tilbyderne, har Kripos laget en forenklet modell som skal gi en indikasjon på omfanget. Modellen gir et estimat på at politiet årlig sender om lag 35 000 anmodninger, og at de ville sendt ytterligere om lag 75 000 anmodninger dersom informasjonen hadde vært tilgjengelig hos tilbyder. Kripos understreker at det er stor usikkerhet knyttet til estimatet, og at det må forstås som en indikasjon på antall anmodninger.

11.1.2 Utleveringskostnader

Dagens praksis er at kompensasjon for utlevering av IP-informasjon avtales mellom politiet og den enkelte tilbyder. Kripos opplyser at det er stor variasjon i stykkprisen den enkelte tilbyder krever for å levere etterspurt informasjon, samt at enkelte tilbydere utfører tjenesten gratis. Tilbakemeldingene fra Kripos og enkelte av de største tilbyderne indikerer et stykkprisintervall på mellom 250 og 1 250 kroner for de som tar betalt for utleveringen, og at driftskostnader relatert til tilretteleggingen er inkludert i disse uthentingskostnadene. Tilbakemeldingen fra enkelte av tilbyderne indikerer samtidig at de rene uthentingskostnadene ligger noe lavere enn stykkprisintervallet skulle tilsi.

Dette viser at det er relativt stor variasjon i prisingen hos tilbyderne ved utlevering av IP-informasjon til politiet, og indikerer at det er betydelig variasjon i hva tilbyderne inkluderer i utleveringskostnader og at det er betydelig variasjon i hvor kostnadseffektive systemer og prosesser de ulike tilbyderne har.

11.2 Ved innføring av den skisserte lovendringen

11.2.1 Omfang

Det er vanskelig å anslå hvor ofte politiet og påtalemyndigheten vil be om utlevering av IP-adresse og eventuelt portnumre i fremtiden, gitt forslaget til lovendring. Politiet forventer imidlertid en betydelig økning ved innføring av en lagringsplikt.

11.2.2 Kostnader

Det er innhentet anslag på hva en lagringsplikt for IP-adresse og portnumre i en tidsperiode på tre, seks eller tolv måneder vil medføre av utgifter for de største tilbyderne. De av tilbyderne som har kommet med estimater, understreker at det er betydelig usikkerhet knyttet til estimatene for investerings-, drifts- og utleveringskostnader, som følge av pågående endringer i systemer og løsninger. Med utgangspunkt i disse estimatene har departementene skissert kostnadsintervaller for hva det vil koste for tilbyder av en viss størrelse å lagre IP-

adresser og portnumre i henholdsvis tre, seks eller tolv måneder, fordelt på investerings-, drifts- og utleveringskostnader (se tabell under).

Tabell X - Kostnadsintervall ved lagring av IP-adresse og portnumre per tjenestetilbyder (i tusen kroner)

	3 mnd	***6 mnd***	***12 mnd***
Investeringskostnader (engangskostnad)	*1 000 – 4 500*	*1 000 – 4 500*	*1 000 – 4 500*
Driftskostnader (årlig)	*100 – 1 500*	*100 – 2 000*	*100 – 3 000*
Totalt	*1 100 – 6 000*	*1 100 – 6 500*	*1 100 – 7 500*

Estimatene viser at engangskostnader per tilbyder knyttet til investeringer vil være på mellom 1 og 4,5 mill. kroner. Årlige driftskostnader vil være på mellom 100.000 kroner og 3 mill. kroner avhengig av lagringstiden.

Nkom har i tillegg hentet inn kostnadsestimater for noen få tilbydere med færre kunder. Kostnadene som oppgis for lagring, sikring av opplysningene og drift hos tilbydere med relativt få kunder, er fra 40 000 og oppover.

Basert på tallene som er innhentet fra tilbydere med ulik størrelse, ser det ut til at kostnadene til en viss grad er skalerbare, og avhengig av antall kunder. Kostnadene vil imidlertid også avhenge av andre faktorer som for eksempel bruken av NAT og hvilke tekniske løsninger som velges hos den enkelte tilbyder. NAT krever at man lagrer mer data, noe som gir høyere kostnader. Kostnadene ved NAT kan ikke angis presist og vil variere med omfanget av bruken, og hvilke tekniske løsninger som er valgt.

Departementene understreker igjen at kostnadsestimatene er usikre og at kostnadene vil variere fra tilbyder til tilbyder, særlig fordi en rekke tilbydere ikke har systemer som gir NAT-informasjon i dag, og må anskaffe disse.

Tilbyder som kjøper tilgang til infrastruktur, vil til dels kunne kjøpe løsninger fra infrastruktureier, jf. beskrivelsen i punkt 7.3.1. Prisene for dette er ikke kjent i dagens marked. Departementene antar at løsninger som oppfyller lagringsplikten, kan gjøres til en integrert del av tilgangsavtalene, og ber særlig om høringsinstansenes innspill.

Videre er det viktig at politiet har gode systemer for å motta, dekode, presentere og lagre data fra tilbydere. Tilpasninger i politiets system for å motta, dekode, presentere og lagre data er del av politiets løpende utviklingskostnader på området, og håndteres innen gjeldende budsjettrammer. Ikraftsettelse av lovforslaget vil ikke i stor grad påvirke politiets behov for å gjøre justeringer i sine IKT-systemer.

Som vist over er det stor variasjon i kostnadene knyttet til lagring og utlevering av IP-informasjon hos de ulike leverandørene. Forslaget til lovendring er forventet å berøre alle tjenesteleverandører. Det er på det nåværende tidspunkt ikke mulig å angi nøyaktig hva den samlete investeringskostnaden vil utgjøre, og heller ikke den samlete årlige driftskostnaden eller utleveringskostnadene.

Tar man utgangspunkt i Kripos' estimater for antall anmodninger som ville vært sendt i dag dersom lagringsplikten var innført, og benytter en gjennomsnittssats på

500 kroner per anmodning, vil merkostnadene bare knyttet til uthenting bli i underkant av 40 mill. kroner. I og med at politiet forventer at behovet vil vokse fremover, vil altså uthentingskostnadene som staten må dekke, bli betydelig høyere enn 40 mill. kroner, gitt at politiet anmoder om IP-informasjon når de faglig sett har behov for det. Det er usikkerhet knyttet til hvor store disse kostnadene vil bli i tiden fremover, men estimatene over indikerer at kostnadene vil bli betydelige.

11.2.3 **Gevinster**

Innføring av lagring av IP-adresser og portnumre i en tidsperiode på seks/ni/tolv måneder vil bidra i politiets arbeid med kriminalitetsbekjempelse, og dermed komme samfunnet som helhet til gode. Tilgang til informasjon om IP-adresser og portnumre er blant annet forventet å føre til raskere avklaring i etterforskningssaker, noe som gjør at politiet og påtalemyndigheten vil kunne behandle flere saker med samme ressursinnsats. Formålet er altså å gi politiet et effektivt verktøy i kampen mot alvorlig kriminalitet, jf. omtale under punkt 7.1.

Forslaget om å innføre en lagringsplikt vil i liten grad komme tilbyderne til gode.