DET KONGELIGE KOMMUNAL-
OG MODERNISERINGSDEPARTEMENT

Prop. 167 L

(2020–2021)

Proposisjon til Stortinget (forslag til lovvedtak)

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

DET KONGELIGE KOMMUNAL-
OG MODERNISERINGSDEPARTEMENT

Prop. 167 L

(2020–2021)

Proposisjon til Stortinget (forslag til lovvedtak)

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

Innhold

1	**Proposisjonens hovedinnhold**	5
2	**Bakgrunnen for proposisjonen**	7
2.1	Politiets behov	7
2.2	Hensynet til kommunikasjonsvern og ytringsfrihet	8
3	**Høringen**	9
3.1	Høringsinstanser	9
3.2	Høringssvar	12
4	**Nærmere om IP-adresser, portnumre, NAT-løsninger mv.**	13
4.1	Hva er en IP-adresse?	13
4.2	Mangel på IP-adresser og bruk av NAT-teknologi	13
4.3	Nærmere om lagring av portnummer	14
4.4	Krypteringsløsninger (VPN mv.)	14
5	**Rettslige rammer**	15
5.1	Innledning	15
5.2	Retten til privatliv og vern av kommunikasjon etter Grunnloven og EMK	15
5.3	Ytringsfrihet, herunder pressens kildevern	19
5.4	Kommunikasjonsvern etter EØS-retten	20
6	**Nordisk rett**	24
6.1	Sverige	24
6.2	Danmark	25
6.3	Finland	25
6.4	Island	26
7	**Overordnet om forslaget**	27
7.1	Gjeldende rett	27
7.2	Forslaget i høringsnotatet	28
7.3	Høringsinstansenes syn	28
7.3.1	Oppsummering	28
7.3.2	Nærmere om innspillene	28
7.4	Departementets vurdering	33
7.4.1	Vurdering av de rettslige rammene for å kunne innføre en plikt til å lagre IP-adresser	33
7.4.2	Vurdering av behovet for å innføre en lagringsplikt for IP-adresser mv.	34
8	**Nærmere om lagringsplikten**	35
8.1	Hvem lagringsplikten skal gjelde for	35
8.1.1	Gjeldende rett	35
8.1.2	Forslaget i høringsnotatet	35
8.1.3	Høringsinstansenes syn	36
8.1.4	Departementets vurdering	36
8.2	Hvilke opplysninger skal lagres?	37
8.2.1	Gjeldende rett	37
8.2.2	Forslaget i høringsnotatet	37
8.2.3	Høringsinstansenes syn	38
8.2.4	Departementets vurdering	39
8.3	Hvor og hvordan skal IP-opplysninger lagres?	41
8.3.1	Gjeldende rett	41
8.3.2	Forslaget i høringsnotatet	41
8.3.3	Høringsinstansenes syn	42
8.3.4	Departementets vurdering	43
8.4	Lagringstid	44
8.4.1	Gjeldende rett	44
8.4.2	Forslaget i høringsnotatet	44
8.4.3	Høringsinstansenes syn	44
8.4.4	Departementets vurdering	46
8.5	Materielle vilkår for utlevering av opplysninger	47
8.5.1	Gjeldende rett	47
8.5.2	Forslaget i høringsnotatet	48
8.5.3	Høringsinstansenes syn	49
8.5.4	Departementets vurdering	51
8.6	Prosessuelle krav og kontroll med utlevering av opplysninger	54
8.6.1	Gjeldende rett	54
8.6.2	Forslaget i høringsnotatet	55
8.6.3	Høringsinstansenes syn	55
8.6.4	Departementets vurdering	57
8.7	Særlig om pressens kildevern	60
8.7.1	Gjeldende rett	60
8.7.2	Forslaget i høringsnotatet	60
8.7.3	Høringsinstansenes syn	60
8.7.4	Departementets vurdering	61
9	**Utlevering av IP-adresser i sivile saker og etter ekomloven § 2-9**	64
9.1	Gjeldende rett	64
9.2	Forslaget i høringsnotatet	65
9.3	Høringsinstansenes syn	65
9.4	Departementets vurdering	67
9.4.1	Utlevering av IP-adresser i medhold av tvisteloven § 22-3 og åndsverkloven § 87	67

9.4.2 Utlevering av IP-adresser til politi og påtalemyndighet, samt annen myndighet etter ekomloven § 2-9 .. 68

10 Kostnadsfordeling 69
10.1 Gjeldende rett 69
10.2 Forslaget i høringsnotatet 69
10.2.1 Alternative fordelingsmodeller 69
10.2.2 Insentiv og kostnadseffektivitet 70
10.2.3 Fordelingsvirkninger 71
10.2.4 Nærmere om uthentings-kostnader 71
10.3 Høringsinstansenes syn 72
10.4 Departementets vurdering 73

11 Økonomiske og administrative konsekvenser 76
11.1 Dagens situasjon 76
11.1.1 Omfang 76
11.1.2 Utleveringskostnader 76
11.2 Ved innføring av lovendringen 76
11.2.1 Omfang 76
11.2.2 Kostnader 76
11.2.3 Gevinster 77

12 Merknader til lovforslaget..... 79

Forslag til lov om endringer i lov om elektronisk kommunikasjon (lagring av IP-adresser mv.) 82

DET KONGELIGE KOMMUNAL-
OG MODERNISERINGSDEPARTEMENT

Prop. 167 L

(2020–2021)

Proposisjon til Stortinget (forslag til lovvedtak)

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

Tilråding fra Kommunal- og moderniseringsdepartementet 9. april 2021, godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

Regjeringen foreslår at det skal innføres en plikt for tilbydere av elektroniske kommunikasjonstjenester (ekomtjenester) til å lagre IP-adresser (unik adresse som tildeles en enhet som er tilkoblet internett) mv., slik at politiet kan få tilgang til IP-adressene for å bekjempe alvorlig kriminalitet.

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 digital teknologi benyttes til nye funksjoner av folk i alle aldersgrupper. Den teknologiske og markedsmessige utviklingen fortsetter og forventes å akselerere ved innføring av neste generasjons mobilnett (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. Retten til privatliv og vern av kommunikasjon er grunnleggende forutsetninger for et demokratisk samfunn, som staten har et ansvar for å sikre. Den digitale utviklingen i samfunnet medfører at tiltak som ivaretar personvern og 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 straffeforfølging. 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 oppklare nettkriminalitet. Det vil også være et viktig virkemiddel for å oppnå FNs bærekraftsmål 16.2 om å stanse overgrep, utnytting, menneskehandel og alle former for vold og tortur mot barn.

Departementet ser at det kan være utfordrende å finne en riktig balanse mellom kriminalitetsbekjempelse og behovet for kommunikasjonsvern og personvern. Det er av betydning for vurderingen av inngrepet i 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 abonnementsopplysninger knyttet til en IP-adresse vil like fullt være et svært viktig verktøy i arbeidet mot kriminalitet, ettersom det ofte vil være en forutsetning for at IP-adresser som innhentes på bakgrunn av andre hjemler, har verdi for etterforskingen.

Når det i denne proposisjonen refereres til «lagring av IP-adresser» mv., 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.

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.

Departementet foreslår at lagringstiden for IP-dataene skal være tolv måneder. Etter departementets vurdering vil dette være nødvendig for at politiet og påtalemyndigheten skal kunne nyttiggjøre seg opplysningene på en tilstrekkelig effektiv måte i kriminalitetsbekjempelsen. Samtidig vil lagringstiden ikke være lenger enn strengt nødvendig, slik at kommunikasjonsvernet ivaretas på en god måte.

Departementet foreslår at opplysningene bare skal kunne utleveres til politiet for å bekjempe alvorlig kriminalitet. Nærmere bestemt foreslår departementet at opplysningene som lagres etter lovforslaget, bare skal kunne utleveres til politiet eller påtalemyndigheten når det er nødvendig for å etterforske en handling som etter loven kan medføre straff av fengsel i tre år eller mer, eller som rammes av nærmere bestemte straffebud, herunder seksuallovbrudd mot barn eller saker hvor tilgang til IP-adresser vil være av særlig betydning for oppklaring av saken.

Det foreslås å ta inn en egen bestemmelse i ekomloven som avskjærer utlevering av IP-adresser lagret etter den nye bestemmelsen til andre formål enn etterforsking av alvorlig kriminalitet. For IP-data som ekomtilbyderne har lagret for eget formål i henhold til ekomloven § 2-7 femte ledd nummer 1, gjøres det ingen endringer i gjeldende rett.

For å sikre person- og kommunikasjonsvernet foreslår departementet også at det fastsettes nærmere krav som legger til rette for tilsyn og kontroll med utlevering av IP-adresser.

Departementet foreslår at kostnadene ved ordningen deles mellom tilbyderne av ekomtjenester og staten ved at staten dekker uthentingskostnadene og at tilbyderne dekker investeringskostnader og faste driftskostnader.

Proposisjonen 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 Bakgrunnen for proposisjonen

2.1 Politiets behov

Den teknologiske utviklingen har ført til endrede kommunikasjonsformer og gitt kriminelle nye muligheter både til å utføre kriminalitet og unndra seg straffeforfølging. 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 telefontjenesten 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 til informasjon i etterforskingen enn det som var situasjonen tidligere, da kommunikasjonen i større grad foregikk via telefontjenesten og SMS mv.

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 prosent. Dette skyldes i første rekke at politiet har avdekket nettverk av personer som chatter og deler seksualiserte fremstillinger av barn. Det er også flere som blir utsatt for 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. I slike saker er det sannsynligvis store mørketall, og det forventes en økning i antall saker fremover.

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. 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. En IP-adresse kan enten være tildelt fast eller midlertidig. Tilgang til informasjon om tilknytningen mellom IP-adresse og abonnent vil, uavhengig av kriminalitetsform, kunne styrke politiets generelle evne til å bekjempe kriminalitet.

Politiet får på ulike måter kjennskap til IP-adresser som kan knyttes til straffbare forhold, for eksempel gjennom undersøkelser 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 hvilken abonnent 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.

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

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.

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 etterforsking 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.

2.2 Hensynet til kommunikasjonsvern og ytringsfrihet

Data om kommunikasjonen forteller mye om den som kommuniserer. Dette oppfattes som svært privat og er noe vi ønsker å verne om. Vern av kommunikasjon er en grunnleggende forutsetning for en fri og åpen debatt i ethvert demokratisk samfunn, fordi det vil kunne ha negativ innvirkning på den frie meningsdannelsen dersom kommunikasjonen ikke er vernet.

Kommunikasjonsvernet er en sentral del av ekomreguleringen, og det skal sikre konfidensialitet, autentisitet og integritet til innholdet i elektronisk kommunikasjon og informasjon om overføringen av kommunikasjonen (metadata). Brukerne må ha tillit til at de trygt kan kommunisere gjennom elektroniske kommunikasjonsnett uten at de må avgi mer informasjon enn det som er nødvendig, og uten at uvedkommende kan få tilgang til kommunikasjonen. Det må derfor 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.

Prinsippet om vern av kommunikasjon står sterkt både i norsk rett og i internasjonale menneskerettighetskonvensjoner. Tilbydere av elektroniske kommunikasjonsnett og -tjenester plikter å sikre kommunikasjonsvernet. Kommunikasjonsvernet vil ha betydning for tilliten til og bruken av digitale tjenester, og det er et viktig premiss for digitaliseringen. Kommunikasjonsvernet anses ofte som en del av personvernet, fordi det er vanskelig å tenke seg et effektivt personvern uten at også kommunikasjonen mellom to eller flere parter kan være fortrolig. Men kommunikasjonsvernet omfatter også informasjon som kommer fra juridiske personer og som ikke faller inn under kategorien personopplysninger, slik som for eksempel forretningssensitiv informasjon.

Den økte bruken av digitale løsninger og internett bidrar til at alle legger igjen langt flere digitale spor enn tidligere. Dette fører til at person- og kommunikasjonsvernet blir enda viktigere. 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 det skjer, og fastsette rammer som gjør at inngrepet blir så lite som mulig. IP-adresser utgjør en del av trafikkdata som genereres når det kommuniseres elektronisk. Tradisjonelt har IP-adresser vært ansett som mindre beskyttelsesverdige opplysninger enn andre trafikkdata, jf. nærmere omtale av IP-adresser i kapittel 4.

Det må likevel legges til grunn at en lovfestet plikt til å lagre koblingen mellom IP-adresser og abonnenter vil utgjøre et inngrep i den enkeltes person- og kommunikasjonsvern og i retten til privatliv og respekt for kommunikasjon etter Grunnloven § 102 og EMK artikkel 8, jf. kapittel 5. Det er derfor svært viktig å finne en rimelig balanse mellom formålet med lagringen på den ene siden, og hensynet til person- og kommunikasjonsvernet på den andre.

Selv om en lagringsplikt vil være tillatt når inngrepet ivaretar et legitimt formål og har tilstrekkelig hjemmel, må det foretas en konkret vurdering av om en plikt til lagring av IP-adresser vil være et forholdsmessig og proporsjonalt inngrep. Inngrepet må derfor begrenses til det nødvendige med hensyn til lagringstid.

Det er dessuten viktig at vilkårene for utlevering sikrer at informasjonen bare blir utlevert i den utstrekning det er nødvendig og forholdsmessig. I tillegg må det i tilstrekkelig grad sikres «nødvendige garantier», blant annet når det gjelder tilsyn og kontroll.

Den nærmere utformingen av reglene vil derfor være avgjørende for at tiltaket samlet sett skal oppfylle kravene i blant annet Grunnloven § 102 og EMK artikkel 8.

3 Høringen

Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet sendte forslag om lagring av IP-adresser mv. på høring 9. oktober 2020 med frist til å avgi uttalelse innen 11. januar 2021. 35 høringsinstanser hadde merknader. Høringsinnspillene vil bli omtalt i tilknytning til de enkelte forslagene. De finnes i sin helhet på regjeringen.no.[1]

3.1 Høringsinstanser

Forslaget ble sendt på høring til disse instansene:

Departementene

Barne-, ungdoms- og familiedirektoratet
Barneombudet
Datatilsynet
Digitaliseringsdirektoratet
Direktoratet for e-helse
Direktoratet for forvaltning og økonomistyring
Direktoratet for samfunnssikkerhet og beredskap
Domstoladministrasjonen
Finanstilsynet
Forbrukerrådet
Forbrukertilsynet
Forsvaret
Fylkesmannen i Agder
Fylkesmannen i Innlandet
Fylkesmannen i Møre og Romsdal
Fylkesmannen i Nordland
Fylkesmannen i Oslo og Viken
Fylkesmannen i Rogaland
Fylkesmannen i Troms og Finnmark
Fylkesmannen i Trøndelag
Fylkesmannen i Vestfold og Telemark
Fylkesmannen i Vestland
Fylkesmennenes fellesadministrasjon
Generaladvokaten
Kommisjonen for gjenopptakelse av straffesaker
Konkurransetilsynet
Kontrollutvalget for kommunikasjonskontroll
Kripos
Likestillings- og diskrimineringsombudet
Medietilsynet
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet
Norges vassdrags- og energidirektorat
Patentstyret
Politidirektoratet
Politiets sikkerhetstjeneste
Politihøgskolen
Regelrådet
Regjeringsadvokaten
Riksadvokaten
Riksarkivet
Sivil klareringsmyndighet
Sivilombudsmannen
Skattedirektoratet
Spesialenheten for politisaker
Statens sivilrettsforvaltning
Statens vegvesen Vegdirektoratet
Statsadvokatembetet
Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)
Sysselmannen på Svalbard
Teknologirådet
Tolldirektoratet
Utlendingsdirektoratet
Utlendingsnemnda
ØKOKRIM

Sametinget

Det juridiske fakultet ved Universitetet i Oslo
Det juridiske fakultet ved Universitetet i Bergen
Det juridiske fakultetet ved Universitetet i Tromsø
Forsvarets forskningsinstitutt
Forsvarets høgskole
Senter for rettsinformatikk ved Universitetet i Oslo

3NET AS
Abelia
Advokatforeningen
Afiber AS
Akademikerne
Alta Kraftlag SA

[1] https://www.regjeringen.no/no/dokumenter/horing---endringer-i-ekomloven/id2766348/

Altibox AS
Altifiber AS
Amnesty International Norge
Andøy Energi AS
Antirasistisk senter
Arbeidsgiverforeningen Spekter
AT&AT Global Network Services Norge
Austevoll Kraftlag SA
Avur AS
Bankenes ID-tjeneste AS
Bardufoss Kabel TV AS
Bergen Fiber AS
Bildende Kunstneres Hjelpefond
BONO – Billedkunst Opphavsrett i Norge
Breiband.no AS
Brukerklagenemnda
Buypass AS
Ceragon Netwoks AS – Norway
Chili Mobil AS
Com4 AS
Commfides Norge AS
Creative Commons Norge
CREO – forbundet for kunst og kultur (MFO)
Danske Bank
Den internasjonale juristkommisjonen, avdeling Norge
Den Norske Advokatforening
Den Norske Ballettskole AS
Den Norske Dataforening
Den Norske Dommerforening
Den Norske Fagpresses Forening
Den norske Forfatterforening
Den norske Forleggerforening
Den norske UNESCO-kommisjonen
Det norske komponistfond
Discovery Networks Norway AS (Discovery)
DIXI Ressurssenter for voldtatte i Oslo og Stavanger
DNB Bank ASA
Easy Connect AS
eforum
Eidsiva Bredbånd AS
Eika Gruppen AS
EL & IT Forbundet
Elektronikkbransjen
Elektronisk Forpost Norge (EFN)
Enivest AS
eRate Norway AS
EVRY Norge AS
Facebook
Fagpressen
Fellesorganisasjonen Foto-Norge
Fellesskap mot seksuelle overgrep
Fiber1 AS
Finans Norge
Finansnæringens Hovedorganisasjon
FolkOrg
Fond for utøvende kunstnere (FFUK)
FONO
Forbundet Frie Fotografer (FFF)
Forskerforbundet
Forsvarergruppen
FriBit
Funksjonshemmedes Fellesorganisasjon
GlobalConnect AS
Google Norge
Grafill – Norske grafiske designere og illustratører
GramArt
Gramo
Hammerfest Energi Bredbånd AS
Haugaland Kraft AS
Hovedorganisasjonen Virke
Hørselshemmedes Landsforbund
Hålogaland Kraft Bredbånd AS
Ice
IFPI Norge
IKT-Norge
Innovasjon Norge
Institusjonsfotografene
Intelcom Group AS
Intelligent Telecom Services
IP Only Networks
Istad Fiber AS
Juridisk rådgivning for kvinner (JURK)
Jussbuss
Jussformidlingen
Jusshjelpa
Kabel Norge
Klepp Energi AS
Kopinor
Kragerø Bredbånd AS
KROM – Norsk forening for kriminalreform
KS
Kunstnernettverket
Landsforeningen Norske Malere
Landslaget for lokalaviser
Landsorganisasjonen i Norge
Last Mile Communications
Lofotkraft AS
Lycamobile Norway Ltd.
Lynet Internett AS
Lyse Fiber AS
Mediebedriftenes Landsforening
Mediehuset Tek AS
Motion Picture Association (MPA) v/adv. Simonsen Vogt Wiig
Motion Picture Licensing Corporation Norge (MPLC)
Musikkfondene
Musikkforleggerne

Nasjonalbiblioteket
Nasjonalmuseet for kunst, arkitektur og design
NextGenTel AS
NextNet AS
NONA – The Norwegian Online News Association
NOPA – Norsk forening for komponister og tekstforfattere
Nordea Bank ABP
Nordic Content Protection (Stop Nordic)
Nordic Entertainment Group
Nordic Screens AS
Nordmøre Energiverk AS
Nordvest Fiber AS
Norges Blindeforbund
Norges Fotografforbund
Norges Handikapforbund
Norges Juristforbund
Norges museumsforbund
Norges Politilederlag
Norges Røde Kors
Norsk Artistforbund (NA)
Norsk audiovisuell oversetterforening (NAViO)
Norsk Bibliotekforening
Norsk Billedhoggerforening
Norsk faglitterær forfatter- og oversetterforening (NFF)
Norsk filmforbund
Norsk filminstitutt
Norsk filmklubbforbund
Norsk forening for jus og EDB
Norsk Journalistlag
Norsk Komponistforening (NKF)
Norsk kritikerlag
Norsk kulturråd
Norsk Lokalradioforbund
Norsk lyd- og blindeskriftsbibliotek
Norsk Oversetterforening (NO)
Norsk PEN
Norsk Presseforbund
Norsk Redaktørforening
Norsk rikskringkasting AS (NRK)
Norsk Sceneinstruktørforening
Norsk senter for informasjonssikring (NorSIS)
Norsk Skuespillerforbund (NSF)
Norsk teater- og orkesterforening
Norsk Tidsskriftforening
Norsk Videogramforening (NVF)
Norske arkitekters landsforbund
Norske Barne- og Ungdomsbokforfattere
Norske Billedkunstnere (NBK)
Norske Dansekunstnere
Norske Dramatikeres Forbund
Norske Filmregissører
Norske Grafikere
Norske Konsertarrangører
Norske Kunsthåndverkere (NK)
Norske Reklamefotografer
Norske Scenografer
Norske tekstilkunstnere
NORTIB – Norsk Tele- og Informasjonsbrukerforening
Norwaco
Notodden Energi AS
NTE Marked AS
Næringslivets Hovedorganisasjon – NHO
OMOD-Organisasjonen Mot Offentlig Diskriminering
Orange Business Norway AS
Organisasjonen mot politisk overvåking
P4 Radio Hele Norge AS
Phonero AS
Platearbeiderforeningen
Politiets Fellesforbund
Powertech Information Systems
Redd Barnas Rettighetssenter
Rettighetsalliansen
Rettspolitisk forening
RiksTV AS
Saga Mobil AS
Samarbeidsrådet for tros- og livssynssamfunn
Sandefjord Bredbånd AS
Schibsted ASA
Signal Bredbånd AS
Signicat AS
Sparebank 1 Banksamarbeidet DA
Stiftelsen Elektronikkbransjen
Stiftelsen for en Kritisk og Undersøkende Presse (SKUP)
Stiftelsen Fritt Ord
Stine Sofies Stiftelse
Strålfors AS
Tafjord Marked AS
Talkmore
Tampnet AS
TDC AS
Tekna – Teknisk-naturvitenskapelig forening
Telenor Norge AS
Teleplan Consulting AS
Telia Norge AS
TONO
Tussa IKT AS
TV 2 AS
Unge Kunstneres Samfund
Unio
Universitets- og høgskolerådet (UHR)
Vesterålskraft Bredbånd ASD
Viken Fiber AS
Vipps AS
Virke kunnskap teknologi og utdanning (Virke KTU)

Virke produsentforeningen
Yrkesorganisasjonenes Sentralforbund

3.2 Høringssvar

Følgende instanser hadde merknader til høringsnotatet:

Forsvarsdepartementet

Datatilsynet
Det nasjonale statsadvokatembetet
Norges institusjon for menneskerettigheter (NIM)
Oslo statsadvokatembeter
Politidirektoratet (vedlagt innspill fra Kripos, Politihøgskolen, Politiets utlendingsenhet, Økokrim og politidistriktene Sør-Øst, Innlandet, Sør-Vest, Nordland, Øst, Oslo, og Trøndelag)
Politiets sikkerhetstjeneste
Riksadvokaten
Statens sivilrettsforvaltning
ØKOKRIM

Abelia
Advokatforeningen
Altibox AS
Bredbåndsfylket AS
Den internasjonale juristkommisjon (ICJ)
Den Norske Dommerforening
EL og IT Forbundet
Elektronisk Forpost Norge
Enivest AS
Forleggerforeningen
GlobalConnect AS
IKT-Norge
KS
Norsk Journalistlag
Norsk Presseforbund, Norsk Redaktørforening
Norsk rikskringkasting
Norwaco
«Person som ikke har oppgitt navn»
Politiets Fellesforbund
Redd Barna
Rettighetsalliansen
Stine Sofies Stiftelse
Tekna – Teknisk-naturvitenskapelig forening
Telenor
Telia

Følgende instanser har meldt at de ikke har merknader:

Helse- og omsorgsdepartementet
Samferdselsdepartementet
Utenriksdepartementet

Domstoladministrasjonen
Norges vassdrags- og energidirektorat
Skattedirektoratet

Forsvarets høgskole

BONO
Kopinor

4 Nærmere om IP-adresser, portnumre, NAT-løsninger mv.

4.1 Hva er en IP-adresse?

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. Når en internettilbyder gir en abonnent tilgang til internett, tildeler tilbyderen 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»).

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.

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 det følgende refereres til «lagring av IP-adresser mv.», 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.

4.2 Mangel på IP-adresser og bruk av NAT-teknologi

Det har etter hvert utviklet seg en mangel på globale IP-adresser. Den begrensede tilgangen på IP-adresser har ført til at internettilbydere 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.

Det varierer mellom ekomtilbyderne 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 deling av IP-adresser vil lagring av IP-adresser alene derfor kunne ha mer begrenset nytteverdi. Det vil likevel kunne være av verdi å konstatere at en konkret abonnent ikke er på listen over abonnenter som var tildelt en gitt IP-adresse. Videre vil politiet i etterforskingen kunne bli 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.

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-teknologi på grunn av adressemangel, kan 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.

4.3 Nærmere om lagring av portnummer

En mulighet for å knytte en delt IP-adresse til en enkeltabonnent, er å identifisere, lagre og innhente informasjon om såkalte portnummer på abonnentsiden, heretter omtalt som portnummer. Et portnummer er et nummer som ved kommunikasjonen kommer i tillegg til IP-adressen, og som gjør det mulig å identifisere abonnenten entydig. Et portnummer er en slags logisk adresse i kommunikasjonsprotokollen. 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 én enkeltabonnent. Dette forutsetter at politiet har kjennskap til både IP-adresse, portnummer og et tilstrekkelig presist angitt kommunikasjonstidspunkt. Lagring av portnummer 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 i et gitt tidsrom, vil portinformasjonen også kunne si noe om at kommunikasjon har funnet sted og presisere nærmere tidspunktet for kommunikasjonen. Lagringsplikten er begrenset til portnummer som tildeles den aktuelle abonnent. Eventuelt portnummer hos avsender i den andre enden av abonnentens internettforbindelse (destinasjonssiden), skal ikke lagres.

4.4 Krypteringsløsninger (VPN mv.)

Brukere av internett vil kunne skjule IP-adresser 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 for eksempel finner knytninger til VPN-tjenesten ved en teknisk undersøkelse av en mistenkt persons datautstyr eller telefon.

5 Rettslige rammer

5.1 Innledning

Både nasjonale og internasjonale regler har betydning for utformingen av regler om lagring av IP-adresser. For det første har Grunnloven § 102 regler som verner privatlivet, herunder kommunikasjon. I tillegg finnes det forskjellige internasjonale regelsett som danner rammer for norsk lovgivning. Av særlig betydning i denne sammenheng er Den europeiske menneskerettskonvensjonen av 4. november 1950 (EMK), som gjennom menneskerettsloven av 21. mai 1999 nr. 30 er gjort til norsk lov, og som etter § 3 ved motstrid går foran annen norsk lovgivning. Videre er Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (kommunikasjonsverndirektivet) av særskilt betydning ved fastsettelsen av rammer for kommunikasjonsvernet og vurderinger av i hvilken grad det kan gjøres inngrep i dette. Direktivet er gjennomført i norsk rett gjennom ekomloven med forskrifter. I det følgende redegjøres det for de rettslige rammene for lovforslaget, slik det ovennevnte regelverket er tolket i praksis.

5.2 Retten til privatliv og vern av kommunikasjon etter Grunnloven og EMK

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

> «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 Den europeiske menneskerettsdomstolens (EMD) 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* 16.2.2000 avsnitt

65 og *S. og Marper mot Storbritannia* avsnitt 67. Behandling av personopplysninger kan også utgjøre et inngrep når det foretas av private, såfremt inngrepet kan tilskrives offentlige myndigheter, se *Vukota-Bojic 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 dermed 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»

Departementet 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 SIM-kort 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 til 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 mistenkte, 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 etterforsking, 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 forventning 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 FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17. Det er ikke holdepunkter for at denne bestemmelsen på dette området stiller strengere krav enn Grunnloven § 102 og EMK artikkel 8.

5.3 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 mot Storbritannia* 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 mot Storbritannia* avsnitt 40.

Kildevernet etter EMK artikkel 10 medfører blant annet begrensninger i adgangen til å 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 mate-

riale med henblikk på etterforsking 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. Ransaking hos journalister med formål om å skaffe opplysninger 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.

5.4 Kommunikasjonsvern etter 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 kommunikasjonsnett og -tjenester 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 trafikkdata knyttet til slik kommunikasjon. Videre følger det av artikkel 5 nr. 1 at medlemsstatene særlig skal forby enhver annen person enn brukerne å avlytte, registrere, lagre eller på andre måter oppfange eller overvåke kommunikasjonen og tilhørende trafikkdata uten samtykke fra brukeren, unntatt dersom dette er tillatt i henhold til lov i samsvar med artikkel 15 nummer 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 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.

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 dem 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 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 ifra 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, var proporsjonale, og de foreslåtte norske reglene er aldri blitt satt i kraft.

I *Tele2-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 lovgivning som regulerer offentlige myndigheters tilgang til opplysninger 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. Lovgivningen 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 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 nr. 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 enkelte 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, samt at det må foreligge en tilstrekkelig betryggende kontrollmekanisme for tilgang til de aktuelle dataene, enten ved en domstol eller en uavhengig administrativ enhet, jf. avsnitt 120.

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 etterforsking av et ran av blant annet en mobiltelefon. Spørsmålet i saken var om kommunikasjonsverndirektivet artikkel 15 lest i lys av EU-pakten artikkel 7 og 8 måtte forstås slik at opplysningene bare kunne utleveres i forbindelse med kriminalitetsbekjempelse dersom formålet er å 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*-avgjørelsen 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 om 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. Når det gjaldt IP-adresser viste domstolen til at opplysninger om IP-adresser, selv om de inngår blant de ulike formene for 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 en internettbrukers søkemønster og derigjennom lage profiler av nettbrukeren, jf. avsnitt 153. Domstolen mente at dette kan utgjøre et alvorlig inngrep:

> «Den lagring og analyse af de nævnte IP-adresser, som en sådan sporing kræver, udgør således alvorlige indgreb i internetbrugerens grundlæggende rettigheder...».

EU-domstolen uttalte videre at det ved avveiningen av de rettighetene og interesser som gjør seg gjeldende, må tas i betraktning at i etterforsking av lovovertredelser begått på nettet, kan IP-adresser utgjøre det eneste etterforskingsmiddelet som kan gjøre det mulig å identifisere personen IP-adressen var tildelt på tidspunktet for lovbruddet, jf. avsnitt 154. Dette kan blant annet gjelde i saker om overgrepsmateriale. Domstolen uttalte videre at selv om internettbrukere har en berettiget forventning om at identiteten deres ikke avsløres, vil en generell og udifferensiert lagring av IP-adresser som er tildelt kilden til en forbindelse, i prinsippet ikke være i strid med kommunikasjonsverndirektivet artikkel 15 sammenholdt med EU-pakten. Domstolen viste til at 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 for å oppnå formålet, og at det må etableres strenge vilkår og garantier vedrørende bruk av dataene, jf. avsnitt 156 og 168.

EU-domstolen i storkammer avsa 2. mars 2021 avgjørelse i sak C-746/*18 H.K. v Prokuratuur,* som gjaldt tilgang til trafikk- og lokasjonsdata til bruk for kriminalitetsbekjempende formål.

H.K. var straffeforfulgt i Estland for tyveri, bruk av en annens bankkort og vold mot en person som deltok i en rettssak. Den øverste domstolen i Estland forela i forbindelse med behandlingen av saken, tre spørsmål for EU-domstolen.

De to første gjaldt bruk av trafikk- og lokasjonsdata i saker som ikke dreier seg om alvorlig kriminalitet, og ble av domstolen behandlet samlet. Domstolen konkluderte her med at kommunikasjonsverndirektivet artikkel 15 sammenholdt med EU-pakten artikkel 7, 8 og 11 samt artikkel 52 første ledd, skal tolkes slik at den er til hinder for nasjonal lovgivning som gir offentlige myndigheter adgang til trafikk- eller lokasjonsdata som kan gi opplysninger om den kommunikasjonen som en bruker har foretatt ved hjelp av et elektronisk kommunikasjonsmiddel, eller om plasseringen av det terminalutstyr som vedkommende har brukt, og som kan gjøre det mulig å dra presise slutninger om vedkommendes privatliv, så fremt dette ikke er begrunnet i bekjempelse av alvorlig kriminalitet eller forebygging av alvorlige trusler mot den offentlige sikkerhet. Bekjempelse av kriminalitet generelt er ikke tilstrekkelig. Dette gjelder uavhengig av «*varigheden af den periode, for hvilken der er anmodet om adgang til de nævnte data, og mængden eller arten af de data, der er tilgængelige i en sådan periode»,* jf. dommen avsnitt 60.

Det tredje spørsmålet som ble forelagt domstolen, var om påtalemyndigheten, som har til oppgave å lede den strafferettslige etterforskingen og eventuelt utøve den offentlige påtalekompetansen i en senere rettssak, kan gis hjemmel til å gi en offentlig myndighet adgang til trafikk- og lokasjonsdata i forbindelse med en strafferettslig etterforsking. Domstolen kom her til at artikkel 15 sammenholdt med artikkel 7, 8 og 11 samt artikkel 52 i EU-pakten, skal tolkes slik at den er til hinder for en slik ordning, jf. dommen avsnitt 60.

I denne forbindelse gjennomgikk domstolen også de betingelser som må oppstilles for at offentlige myndigheter skal få tilgang til trafikk- og lokasjonsdata, se avsnitt 48 følgende. Domstolen fastslo at det er opp til nasjonal rett å fastsette de regler som gjelder for krav om utlevering av trafikk- og lokasjonsdata. For å oppfylle kravet om proporsjonalitet, må slike bestemmelser imidlertid oppfylle en rekke vilkår, se dommens avsnitt 48. Det må fastsettes materielle og prosessuelle betingelser for bruk av informasjonen, jf. avsnitt 49 og 50. Videre uttalte domstolen at med henblikk på å sikre etterlevelse av disse betingelsene i praksis, er det avgjørende at de kompetente nasjonale myndigheters adgang til de lagrede data er undergitt en forutgående kontroll, som foretas enten av en domstol eller av en uavhengig administrativ enhet, jf. avsnitt 51. Departementet vil komme tilbake til rekkevidden av et slikt krav om forhåndskontroll i punkt 8.6 om prosessuelle betingelser.

6 Nordisk 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 *Tele2*-avgjørelsen. Den svenske riksdagen vedtok lovendringene i samsvar med regjeringens forslag. Endringene trådte i kraft 1. oktober 2019. Lagen (2003:389) om elektronisk kommunikation 6 kapittel, 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 abonnementsopplysninger, herunder IP-adresser, er særskilt regulert i 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 i forbindelse med etterforsking og identifisering av 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, blant annet fordi denne typen opplysninger ikke anses som like inngripende som eksempelvis lokaliseringsdata.

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 internetprotokoladresse, 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 kommunikasjonsnett 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 følgende. 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.

Departementet er kjent med at de danske reglene er planlagt revidert i løpet av 2021 på grunn av *La Quadrature du Net*-dommen.

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 Overordnet om forslaget

7.1 Gjeldende rett

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. Liknende 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 departementet 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.

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 abonnementsopplysninger, 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 etterforskingen 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) kapittel 3.6 side 8 om den tilsvarende bestemmelsen i teleloven § 9-3. Dette ble i sin tid begrunnet med at det aktuelle unntaket som det er snakk om å gjøre fra taushetsplikten, er begrenset: «*Det er bare en abonnents navn, adresse og telefonnummer/datakommunikasjonsadresse det skal kunne gis opplysninger om.*»

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 etterforsking, 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.

7.2 Forslaget i høringsnotatet

I høringsnotatet foreslo departementene å innføre en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til informasjon som er nødvendig for å kunne identifisere abonnenten, for å bekjempe alvorlig kriminalitet. Forslaget innebærer at ekomtilbyderne får en plikt til å lagre IP-adresser i en bestemt tidsperiode, i stedet for å ha en plikt til å slette opplysningene, så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål, slik reglene er i dag. Sletting gjøres normalt innen tre uker.

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

Departementene foreslo videre innstramninger i reglene for når de lagrede opplysningene skulle kunne utleveres til politi og påtalemyndighet. Departementene foreslo ikke en eksakt strafferamme, men det ble antydet at strafferammekravet burde 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 foreslo at lagringstiden for IP-data skulle være enten seks, ni eller tolv måneder fra den dagen kommunikasjonen avsluttes, og det ble bedt om høringsinstansenes syn på dette. Det ble videre foreslått at lagringen skulle gjelde for samtlige tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett, og at det skulle være opp til tilbyderne hvor og hvordan opplysningene skulle lagres.

7.3 Høringsinstansenes syn

7.3.1 Oppsummering

Følgende høringsinstanser støtter forslaget om innføring av en plikt til å lagre IP-adresser mv.: *KS, Norwaco, Rettighetsalliansen, Riksadvokaten, Det nasjonale statsadvokatembetet, Oslo statsadvokatembeter, Politiets Sikkerhetstjeneste (PST), Politiets Fellesforbund, Statens sivilrettsforvaltning, Redd Barna, Stine Sofies Stiftelse* samt *Politidirektoratet* som har innhentet innspill fra *Kripos*, *ØKOKRIM*, *Politiets utlendingsenhet*, *Politihøgskolen* samt *politidistriktene Sør-Øst*, *Innlandet*, *Sør-Vest*, *Nordland*, *Øst*, *Oslo* og *Trøndelag*.

Følgende høringsinstanser er imot forslaget om innføring av en plikt til å lagre IP-adresser mv.: *Datatilsynet, EL og IT Forbundet, Elektronisk Forpost Norge, Tekna, NRK, Norsk Journalistlag, Norsk Presseforbund* og *Norsk Redaktørforening*.

Flere andre høringsinstanser tar ikke eksplisitt stilling til hvorvidt de støtter eller er imot å innføre en plikt til å lagre IP-adresser mv., men mener at forslaget slik det foreligger, ikke er i tråd med EMK eller EØS-retten, og/eller at det har andre mangler. Flere viser til at det bør foretas nærmere utredninger før forslaget kan fremmes, og at forslaget bør ses i sammenheng med andre forslag om lagring av data samt Personvernkommisjonens arbeid. Enkelte viser samtidig til at de ser behovet for å innføre en plikt til å lagre IP-adresser. Noen høringsinstanser viser til at lagring og sporing av IP-adresser enkelt kan omgås ved hjelp av VPN, Dark Web eller TOR, og de stiller spørsmål om effektiviteten av forslaget. Noen mener også at nytten av lagringsplikten ikke er tilstrekkelig dokumentert. Det redegjøres nærmere for de enkelte innspillene under kapittel 7.3.2.

7.3.2 Nærmere om innspillene

Riksadvokaten peker på at tilgang til opplysninger om IP-adresser er et viktig virkemiddel ved oppklaring av kriminalitet som begås, planlegges, muliggjøres eller formidles via internett. Riksadvokaten mener departementenes forslag ivaretar behovet for kriminalitetsbekjempelse og er svært positiv til forslaget.

Det nasjonale statsadvokatembetet støtter forslaget om at det innføres en plikt til å lagre IP-adresser, herunder en plikt til å lagre portnumre på abonnentssiden. Det bemerkes at Norge er det siste landet i Europa som eventuelt innfører en slik plikt. Sletting av data etter 21 dager har hatt direkte innvirkning på de muligheter norsk politi har hatt til å avdekke gjerningspersoner som står bak til dels svært grov kriminalitet. Det vises også til at utvidet lagringsplikt vil få positiv betydning for norsk politis mulighet til å bistå andre land gjennom internasjonalt rettslig samarbeid; med dagens regler er det i praksis ofte for sent å innhente denne informasjonen når forespørsel om bistand kommer fra andre land.

Det nasjonale statsadvokatembetet peker på at opplysningene det er snakk om, er lagret kryptert og på et meget høyt sikkerhetsnivå hos teleselskapene. Opplysningene må bearbeides i dataprogram hos politiet og ses i sammenheng med øvrig etterforskningsmateriale for å kunne nyttiggjøres. Forespørselen til teleselskapene vil normalt være

målrettet, og risikoen for misbruk er minimal. På denne bakgrunn støttes høringsnotatets overordnede vurdering om at IP-lagring ikke er et så stort inngrep i kommunikasjonsvernet at det bør hindre politiets tilgang til informasjonen i forbindelse med kriminalitetsbekjempelse.

Oslo statsadvokatembeter peker på at den tekniske utviklingen har vært betydelig siden høringen om implementeringen av datalagringsdirektivet i 2010. Det er ingen grunn til å betvile at politiet eller påtalemyndigheten i større grad enn i dag vil etterspørre opplysninger knyttet til IP-adresser når lagringstiden økes.

Politidirektoratet – som har innhentet innspill fra *Kripos, ØKOKRIM, Politiets utlendingsenhet, Politihøgskolen* samt *politidistriktene Sør-Øst, Innlandet, Sør-Vest, Nordland, Øst, Oslo* og *Trøndelag* – slutter seg til de vurderinger og forslag som fremmes i høringsnotatet. Det er bred støtte til de foreslåtte endringer i de mottatte høringsinnspillene fra etaten. Det påpekes at lengre lagringstid av abonnementsinformasjon for IP-adresser har vært et savn hos politiet lenge, og en lovfesting i samsvar med forslaget vil medføre en tilpasning til regelverkene i de fleste europeiske land. Endringene vil bidra til en mer effektiv etterforsking av straffbare forhold, der sentrale bevis i stadig større grad er å finne på nettet. Lagring av IP-adresser i inntil 21 dager er ikke tilstrekkelig for å kunne benytte slik informasjon til kriminalitetsbekjempelse i dagens digitaliserte samfunn.

Politidirektoratet har særskilt trukket frem høringsinnspillet fra *Kripos,* der det innledningsvis vises til at det i dag knapt finnes straffesakstyper hvor IP-adresser ikke kan ha betydning. I stadig flere etterforskinger får politiet kjennskap til IP-adresser som kunne ha løst saken dersom disse dataene kunne berikes med abonnementsinformasjon. Svært ofte er dette imidlertid ikke mulig, da dataene som kunne identifisert brukerne, er slettet eller ikke lagret i det hele tatt.

ØKOKRIM peker på at sikring av digitale spor er stadig viktigere for en effektiv kriminalitetsbekjempelse, og de slutter seg til departementenes argumentasjon om behovet for å lovregulere lagringsplikt for IP-adresser og portnumre. Det bemerkes at digitalisering av kriminaliteten er tiltagende, herunder vises det til bruk av digitale betalingstjenester etc. som verktøy for å begå kriminalitet. Det er også vist til konkrete straffesaker der manglende lagring av IP-adresser har vanskeliggjort etterforskingen.

Politiets Sikkerhetstjeneste (PST) er svært positive til forslaget. Informasjon om tilknytning mellom abonnent og IP-adresse vil være av stor betydning for å bekjempe alvorlig kriminalitet, både med sikte på etterforsking, avverging og forebygging av lovbrudd. Behovet gjør seg gjeldende for hele PSTs portefølje, som omfatter de mest alvorlige truslene mot riket.

Politiets Fellesforbund mener at forslaget om å styrke politiets mulighet til å forfølge digital kriminalitet, er en positiv utvikling, som forbundet ønsker å støtte opp om. Forslaget er særskilt viktig for de av forbundets medlemmer som arbeider med overgrep mot barn, og som opplever at barn som er utsatt for overgrep kunne vært reddet om tilbyderne var pålagt å lagre informasjon om brukerne. Det er vist til at selv om det er viktig å ta i betraktning personvern er også rettssikkerhet og muligheten til å avdekke grov seksualisering av blant annet barn, noe som må prioriteres. Den foreslåtte lovendringen vil bidra til dette viktige arbeidet.

Statens sivilrettsforvaltning (SRF) stiller seg positive til departementenes forslag. Påbud om lagring av IP-adresser vil styrke etterforskingen i straffesaker hvor det er begått alvorlige overgrep og/eller trusler/tvang over internett. I tillegg kan forslaget ha positive konsekvenser for statens adgang til å fremme regresskrav mot skadevolder etter utbetalt voldsoffererstatning.

Redd Barna støtter forslaget om å åpne for plikt til lagring av IP-adresser, slik at disse kan brukes for å etterforske seksuell utnyttelse og overgrep mot barn over internett, og liknende kriminalitet rettet mot barn. For at barns rettsvern skal være reelt, må politiet ha etterforskingsmidler som står i forhold til den økende tilgangen til internett og risikoene dette utgjør for barn. Det er i den sammenheng vist til Kripos' rapport «*Seksuell utnyttelse av barn og unge over internett*» der det ble fremhevet at manglende krav til lagring av abonnementsinformasjon for IP-adresser er en utfordring for politi og påtalemyndighet ved etterforsking og iretteføring av seksuallovbrudd begått ved bruk av internett. At politiet og påtalemyndigheten selv mener manglende lagringsplikt utgjør et hinder for etterforsking og iretteføring, er etter Redd Barnas syn et vektig argument i favør av å innføre en lagringsplikt. Redd Barna skriver også at de materielle vilkårene for utlevering av lagrede opplysninger må være strenge nok til å være i tråd med menneskerettslige krav.

Stine Sofies Stiftelse stiller seg bak forslaget om å innføre en plikt til lagring av IP-adresser, da dette er viktig både for å kunne identifisere gjerningspersoner, fornærmede og vitner.

Datatilsynet mener det ikke bør innføres en plikt til å lagre IP-adresser. Dersom det innføres

en slik plikt, må denne begrenses til de sakene hvor det har størst betydning, som nettovergrep og deling av overgrepsbilder. I tillegg må reglene om bevisinnhenting i straffeprosessloven følges, og det må foretas en uavhengig forhåndskontroll av om vilkårene for innhenting er oppfylt. Forslaget om lagring av IP-adresser innebærer at alle tilbyderne må etablere en ny database over tildelte IP-adresser for politiets bruk. Den registrerte i databasen har dermed en rekke rettigheter som retten til innsyn, sletting, korrigering, dataminimering etc., i henhold til kravene i personopplysningsloven og personvernforordningen. Datatilsynet viser videre til at forslaget vil gjøre det mulig å tegne et bilde av hvor den enkelte befinner seg rent fysisk, nærmest til enhver tid. Slik sett vil forslaget utfordre retten til anonym ferdsel. Forslaget drøfter i liten grad forholdsmessigheten og nødvendigheten av at nesten alle norske borgere skal registreres. Datatilsynet viser også til at det aller meste av det som skal lagres vil være å anse som overskuddsinformasjon, og at det er forbudt å behandle andre eller flere personopplysninger enn det som er nødvendig for å nå formålet med behandlingen. Datatilsynet mener oppsummert at forslaget ikke er godt nok utredet i og med at sentrale menneskerettslige spørsmål og personvernkonsekvensene av lovforslaget ikke er tilstrekkelig vurdert i notatet. Et tiltak av dette omfanget kan ikke oversendes Stortinget uten at dette har blitt utredet grundigere og sendt på ny høring. Datatilsynet vil også bemerke at Stortinget i anmodningsvedtak nr. 944, 15. juni 2017 spesielt ba om at hensynet til personvern skulle ivaretas.

Norges institusjon for menneskerettigheter (NIM) er i utgangspunktet positiv til forslaget om lagring av IP-adresser, men mener forslaget er mer inngripende enn hva departementene legger til grunn. Etter NIMs vurdering vil strafferammekravet på 1–2 år for å kunne utlevere IP-adresser til politiet samt manglende rettssikkerhetsgarantier utgjøre et uforholdsmessig inngrep i retten til privatliv. De viser til at rettsikkerhetsmekanismene i forslaget må styrkes betydelig for å ivareta prosessuelle krav etter EMK artikkel 8. Forslaget om utlevering av IP-adresser vil også kunne gripe inn i kildevernet, og denne problemstillingen bør utredes nærmere.

Advokatforeningen viser til at generell og udifferensiert lagring av IP-adresser, etter EU-domstolens storkammerdom av 6. oktober i 2020 i saken *La Quadrature du Net*, kun kan aksepteres når formålet er (i dansk oversettelse) «*beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed*». Etter Advokatforeningens syn vil det neppe være forenlig med EU-domstolens dom å utlevere de nevnte dataene til andre formål enn dem EU-domstolen har forutsatt.

Den internasjonale juristkommisjon – norsk avdeling (ICJ) viser til at en lovbestemmelse som foreslått, forutsetter en utredning av personvernkonsekvenser i henhold til personvernforordningen artikkel 6 tredje ledd og utredningsinstruksen. Lagringsplikt vil bare være tillatt såfremt inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig. ICJ stiller også spørsmål om departementet har utredet problemstillingen vedrørende lovligheten av en plikt til å lagre IP-adresser grundig nok, og ICJ etterlyser særlig en utredning av forholdet mellom *La Quadrature du Net*-dommen og *Tele2*-dommen, herunder hvorvidt *Tele2*-dommens krav om at en lovlig datalagring må være begrenset med hensyn til personer, kommunikasjonsmidler, kategorier av data som lagres og lagringstid, innebærer *kumulative* vilkår som alle må være oppfylt for at slik lagring kan være lovlig. ICJ viser til at det er argumentert for en slik forståelse i litteraturen.

ICJ stiller også spørsmål om lagring av IP-adresser for å bekjempe kriminalitet er et effektivt virkemiddel, ettersom det er enkelt å skjule seg bak kryptering, for eksempel VPN. For at det skal kunne rettferdiggjøres å gjøre et så stort inngrep i personvernet som en generell og udifferensiert lagring av alle IP-adresser er, må det være forholdsmessig og nødvendig i et demokratisk samfunn. Effektiviteten av virkemidlet vil stå sentralt i vurderingen. Et ineffektivt virkemiddel vil fort kunne bli ansett som uforholdsmessig inngripende.

Elektronisk Forpost Norge (EFN) er en digital rettighetsorganisasjon, og en del av European Digital Rights. EFN mener departementenes forslag i realiteten representerer kartlegging av en stor del av nett- og mobilbrukers nettaktiviteter. Samlingen av trafikkdata som foreslås, vil i realiteten gi oversikt over hvem som snakker med hvem eller hvem som gjør hva, hvor og når. Det må derfor anses som et svært strengt inngrep i privatlivet. EFN kan ikke se at fordelene ved slik bevissikring er større enn ulempene de gir. Lovforslaget er diffust siden konkrete bestemmelser om hva som skal lagres, skal gis ved forskrift. EFN viser også til at formålet med lagringen omfatter alt fra kriminalitetsforebygging til sivile rettssaker, og den foreslåtte strafferammen som skal brukes for å avgrense denne typen bevissikring, er svært lav, ett til to år. Det spesifiseres heller ingen krav til lagringen eller hvordan dataene om

brukerne kan benyttes, da det ikke er krav om domstolskontroll eller andre krav, utover at politiet selv er ansvarlig for hva de mener de trenger.

Abelia tar ikke stilling til hvorvidt forslaget til lagringsplikt for IP-adresser bør innføres, men mener forslaget må ses i sammenheng med andre krav til lagring og utlevering av informasjon til myndighetene. Leverandører av digital infrastruktur og tjenester er avhengige av forutsigbare og stabile rammevilkår for å kunne planlegge og gjøre investeringer for fremtiden. Forslaget bør blant annet vurderes i lys av Personvernkommisjonens arbeid, og eventuelle lovendringer bør vurderes utsatt frem til disse vurderingene foreligger, for å unngå potensielle nye endringer i etterkant av dette.

EL og IT Forbundet er prinsipielt imot lagring av IP-adresser som foreslått, og de mener at hensynet til alles rett til privatliv skal vektes tyngre enn potensiell nytte i kriminalitetsbekjempelse og etterretningsarbeid. De viser til at det vil kunne skje en formålsglidning, og at aksepten for overvåkning forskyves med små skritt av gangen. EL og IT Forbundet påpeker at det er et viktig prinsipp at det ikke er kontrolltiltaket alene som bør vurderes i spørsmål om inngripen i personvern, men derimot totaliteten av alle kontrolltiltak. EL og IT Forbundet mener det er et paradoks at det mangler dokumentasjon på at tiltak som lagring av IP-adresser har en direkte og reduserende effekt på alvorlig kriminalitet. De viser også til at lagring av mer informasjon også betyr at mer informasjon kan lekkes og misbrukes. EL og IT Forbundet viser for øvrig til at lagring og sporing av IP-adresser enkelt kan omgås for de som er ute etter å skjule sine spor. En relativt enkel måte å omgå dette på vil være å bruke Dark Web eller TOR-tjenester til å skjule datatrafikken.

Altibox viser til at de forstår viktigheten av at politiet må kunne manøvrere i den digitale verden, og de har en positiv holdning til dette. Det er likevel viktig for tilbydere av ekomtjenester at kostnadsdekning og ansvar håndteres på en korrekt og utfyllende måte. Det må være klart hvilke opplysninger som skal lagres for å oppnå formålet, og hvem som skal lagre dataene. Det minst inngripende alternativet må velges for lagringstid. I tillegg må vilkårene for utlevering være klare og enkle å overholde, og kostnadsdekning må i hovedsak bæres av staten. Lovgiver bør også tenke helhetlig i spørsmålene om utlevering av denne type informasjon til forskjellige samfunnsaktører slik som politiet, E-tjenesten osv.

GlobalConnect viser til at en vidtrekkende plikt til å lagre IP-adresser om alle, uavhengig av konkret mistanke, er et stort inngrep i befolkningens personvern. Omfattende lagring av denne typen data vil både kunne føre til en «nedkjølingseffekt» og åpne for en formålsutglidning. Departementenes beskrivelse av sivile søksmål er et godt eksempel på det. GlobalConnect forventer dessuten at politiet og påtalemyndigheten i fremtiden vil skaffe seg ny programvare og funksjonalitet som gjør det mulig å bruke IP-adresser på en langt mer inngripende måte enn i dag, for eksempel gjennom stordataanalyser i kombinasjon med andre data. GlobalConnect er bekymret for om Norge har det nødvendige rettslige handlingsrommet til å gjennomføre lovendringen, og de viser til at det ikke legges opp til noen form for uavhengig domstolsprøving av pålegg om utlevering. Videre vil informasjon om IP-adresser kombinert med tidspunkt kunne avsløre mer enn kun identiteten på abonnent eller bruker. GlobalConnect har samtidig forståelse for påtalemyndighetenes legitime behov for å etablere mekanismer som gjør det mulig å avdekke identiteten til gjerningspersoner. GlobalConnect oppfordrer for øvrig departementene til gjennomgående å velge de løsningene som skaper minst mulig rom for fortolkning, og som avklarer innholdet i forslaget, ansvarsforholdene og kostnadsfordeling når hjemmelsloven vedtas.

IKT-Norge, Bredbåndsfylket (Troms) AS og *Enivest AS* viser til at det er avgjørende at de grunnlovsmessige og menneskerettslige rammene for inngrep i borgernes rettigheter respekteres, og at man innenfor rammene har en restriktiv tilnærming for å unngå utilsiktede og uheldige virkninger på befolkningens tillit til og bruk av kommunikasjonsteknologi. Bransjen ønsker å bidra for å finne gode løsninger som balanserer hensynet til kommunikasjonsvern med hensynet til å bekjempe alvorlig kriminalitet. Målet må være at politi og påtalemyndighet skal få bedre verktøy til kriminalitetsbekjempelse, mens inngrepene i brukernes rettigheter minimeres. Det er viktig å unngå at det lagres og utleveres flere opplysninger enn hva som er nødvendig for å oppfylle formålet, og minimere risiko for at opplysninger misbrukes eller havner på avveie. For å opprettholde tilliten til elektroniske kommunikasjonstjenester, er det videre av stor betydning at ansvaret for ordninger med innsyn i abonnementsopplysninger er tydelig plassert hos myndighetene. Disse høringsinstansene mener også at det er viktig å ha klart for seg hvilke begrensninger som ligger i en lagringsplikt som foreslått, for eksempel ved at bruk av VPN vil kunne vanskeliggjøre identifiseringen. Det vises også til problemet med å kunne identifisere hvem som har vært faktisk bruker av en for-

bindelse i tilfeller der flere brukere er knyttet til det samme abonnementet på offentlige WiFi-nettverk.

Telenor viser til at det gjennom ulike krypterings- og anonymiseringsløsninger er mulig å skjule sin identitet på nettet. En lagringsplikt som foreslått, vil dermed kunne omgås og ha begrenset verdi for formålet. Telenor viser videre til at summen av ekominformasjon som lagres, og som kan spores til den enkelte borger, etter hvert er betydelig. Det er avgjørende at departementene i det videre arbeidet med saken ser dette i sammenheng, også i lys av arbeidet til personvernkommisjonen. Telenor ønsker ikke å lagre mer informasjon om kundenes data- og telefonbruk enn hva de trenger for eget formål. Det vil være skadelig for Telenors virksomhet dersom deres tjenester oppfattes å utfordre person- og kommunikasjonsvernet, og det er heller ikke ønskelig i et samfunnsperspektiv. Samtidig erkjenner Telenor politiets behov for oppdaterte verktøy i en digital hverdag. Telenor understreker at et eventuelt forslag om IP-lagring må rammes tydelig inn, blant annet med hensyn til person- og kommunikasjonsvern, utlevering av opplysninger samt en kostnadsfordelingsmodell som ikke legger en urimelig byrde på den enkelte Internet Service Provider (ISP). Det må ikke lagres og utleveres flere opplysninger enn hva som er nødvendig for å oppfylle formålet. Telenor bemerker også at det alltid er en viss risiko for at data som ekomtilbydere utleverer til politiet, kan være beheftet med feil eller mangler, både fordi data ikke er samlet inn for dette formålet og fordi ulike typer av feil kan oppstå.

Telia viser til at kommunikasjons- og personvernhensyn må vektlegges, og at det må tas høyde for at blant annet journalisters og advokaters kommunikasjon kan være underlagt et særskilt vern. Telia erkjenner imidlertid at disse hensynene må veies opp mot at digitale spor kan være av essensiell betydning for at politiet skal kunne beskytte samfunnet og borgerne. Telia bemerker at forslaget om lagring av IP-adresser med fordel burde vurderes i sammenheng med den foreslåtte tilretteleggingsplikten i ny lov om etterretningstjenesten, så vel som arbeidet som nå utføres av personvernkommisjonen. Telia viser til at det må unngås at det lagres og utleveres flere opplysninger enn nødvendig, eller at opplysningene benyttes til andre formål enn å bekjempe alvorlig kriminalitet. Kravene til hvilke opplysninger som skal lagres og gjøres tilgjengelig, må være eksakte og entydige, og reglene må utformes slik at tilbyderne ikke risikerer å bryte konfidensialitetskrav i ekomloven og personopplysningsloven når de responderer på utleveringsbegjæringer fra politiet.

Tekna – Teknisk-naturvitenskapelig forening er skeptisk til forslaget om at IP-adresser og person-ID skal kunne lagres lenger enn dagens rammer på tre uker. Forslaget gir vide rammer til politiet, og det innebærer blant annet muligheter til å samle inn tidsserier med IP-adresser fra alle nettbaserte enheter til en gitt person. Det betyr at de foreslåtte IP-adresseregistrene kan gi omfattende oversikt over hvor vi er og hva vi gjør. Tekna bemerker også at forslaget mangler krav til domstolsbehandling for uthenting av informasjon, og at et strafferammekrav for uthenting av informasjon ikke er tilstrekkelig. Tekna viser videre til at digitaliseringen av stadig nye tjenester i samfunnet fører til at personvernutfordringene ved å kunne identifisere personer bak IP-adresser, blir større. Departementenes sammenligning av IP-adresser med et telefonnummer halter, og det leder inn i en blindsone hvor reelle personvernutfordringer og faren for formålsutglidning underkommuniseres.

KS viser til at en plikt til å lagre IP-adresser som gir abonnementsopplysninger/brukerdata, er langt mindre inngripende for kommunikasjonsvernet enn en lagringsplikt for alle trafikkdata. KS deler også departementenes oppfatning av at uthenting av lagrede IP-adresser like fullt vil være et svært viktig verktøy i arbeidet mot kriminalitet. Slik KS vurderer det, har departementene i lovforslaget balansert hensynene til kriminalitetsbekjempelse og person- og kommunikasjonsvern på en god måte.

Norsk Journalistlag (NJ) mener de foreslåtte endringene i ekomloven innebærer en omgåelse av de reglene som i dag oppstiller et vern om anonyme kilders identitet. Hvilke konsekvenser forslaget vil kunne få for journalisters vern av anonyme kilder, er svært tynt utredet. NJ mener departementene ikke har funnet riktig balanse mellom kriminalitetsbekjempelse og behovet for kommunikasjonsvern, og at forslaget går ut over kildevernet. Politiet vil ved forslaget kunne gjennomføre etterforsking før gjeldende vilkår for å ta i bruk ordinære metoder er oppfylt. Skal lovforslaget i det hele tatt vurderes, må en korrekt forståelse av hva dette vil kunne innebære for journalisters vern av anonyme kilder, legges til grunn. Dette er ikke gjort fra departementenes side, og følgelig må konsekvensen av dette etter NJs syn være at det foreliggende forslaget forkastes.

Norsk Presseforbund og *Norsk Redaktørforening* viser til at de har overordnet forståelse for bakgrunnen for forslaget, men mener forslaget tar for

lett på konsekvensene for kildevernet, da disse verken er kartlagt eller ordentlig drøftet. Forslaget vil åpenbart kunne ha en nedkjølende effekt på kildevernet og ytringsfriheten. Norsk Presseforbund og Norsk Redaktørforening viser videre til at det er fare for at for mye og for detaljerte data lagres, og at det inkluderer lagring av data som gjør at det ligger utenfor føringene fra EU-domstolen om hva som vil være forholdsmessig. De mener at forslaget slik det nå foreligger, ikke kan innføres, da det har for store mangler, og konsekvensene for kildevernet og ytringsfriheten vil være for store.

NRK er bekymret for lovforslagets konsekvenser for kildevernet. Hensynet til ytrings- og informasjonsfriheten – og kildevernet spesielt – er etter NRKs mening ikke tilstrekkelig ivaretatt. Slik forslaget nå er utformet, er det også i strid med de skranker som er trukket opp i rettspraksis for denne type masselagring og utlevering av opplysninger. NRK påpeker for øvrig faren for at IP-data kommer på avveie, og bemerker at det ikke er lagt opp til noen særskilte sikkerhetsmekanismer når det gjelder lagring av disse dataene. NRK stiller også spørsmål ved hvor stor nytte lovforslaget reelt vil få for kriminalitetsbekjempelse, siden de som driver kriminell virksomhet antakelig allerede benytter krypterte løsninger i stor grad. På denne bakgrunn mener NRK at lovforslaget bør skrinlegges. Alternativt må det foretas en ny gjennomgang av lovforslaget hvor et minimumskrav må være at forslaget ikke åpner for lagring eller utlevering av metadata, og at det begrenses til å omfatte bekjempelse av alvorlig kriminalitet på nivå med beskyttelse av nasjonal sikkerhet og avverging av alvorlige trusler mot befolkningens sikkerhet.

Norwaco er en kollektiv forvaltningsorganisasjon for rettigheter etter åndsverkloven. Norwaco viser til at ulovlig bruk av verk på internett utgjør en stor trussel mot vederlaget til opphavere, utøvende kunstnere og produsenter, og at det er viktig for rettighetshaverne å kunne håndheve sine rettigheter også på internett. Norwaco støtter derfor forslaget om innføring av en plikt for tilbydere av ekomtjenester til å lagre IP-adresser.

7.4 Departementets vurdering

7.4.1 Vurdering av de rettslige rammene for å kunne innføre en plikt til å lagre IP-adresser

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. Lagringsplikt vil derfor 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 for å bekjempe alvorlig kriminalitet, 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. Departementet viser til at EMK artikkel 8 også innebærer en positiv forpliktelse til å muliggjøre etterforsking av lovbrudd, jf. *K.U. mot Finland*, der EMK artikkel 8 ble ansett for 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 vilkår 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 Slovenia*. Den nærmere utformingen av reglene vil være avgjørende for at tiltaket samlet sett skal oppfylle kravene i Grunnloven § 102 og EMK artikkel 8.

EØS-retten setter også viktige rammer for hvordan forslag om plikt til å lagre IP-adresser kan innrettes.

EU-domstolens avgjørelse i *La Quadrature du Net* omhandler blant annet lagring av IP-adresser. En rekke høringsinstanser har i sine innspill særlig tatt opp betydningen av denne dommen, og de har stilt spørsmål ved om forslaget om lagring av IP-adresser og portnummer er i tråd med dommen.

La Quadrature du Net fastslår at en generell og udifferensiert lagring av IP-adresser i prinsippet ikke er i strid med kommunikasjonsverndirektivet og EU-pakten. Det er imidlertid en forutsetning at de materielle og prosessuelle vilkårene som skal regulere bruken av disse dataene, overholdes strengt. Dommen legger samtidig til grunn at lagring må begrunnes ut ifra formål om å bekjempe alvorlig kriminalitet, forebygge alvorlige trusler mot offentlig sikkerhet eller ivareta nasjonal sikkerhet. Videre legges det til grunn at lagringstiden ikke må overstige det som er strengt nødvendig for å oppnå formålet, og at det må etableres strenge vilkår og garantier vedrørende bruk av dataene.

Departementet legger i lys av dommen til grunn at generell og udifferensiert lagring av IP-adresser på nærmere vilkår vil være tillatt etter EØS-retten så lenge forutsetningene oppstilt i dommen ivaretas. Det redegjøres nærmere for vurderingen av vilkårene i kapittel 8.

7.4.2 Vurdering av behovet for å innføre en lagringsplikt for IP-adresser mv.

Etter departementets syn er dagens lagringstid for IP-adresser, som er begrenset til den lagringstiden som er nødvendig for kommunikasjons- eller faktureringsformål, for kort til å kunne være et effektivt virkemiddel for kriminalitetsbekjempelse. Av hensyn til å kunne bekjempe kriminalitet på en effektiv måte, mener departementet at internettilbydere bør pålegges en lagringsplikt som går utover dagens regulering.

Departementet viser til at informasjon om hvilken IP-adresse en abonnent er blitt tildelt, ikke i seg selv gir informasjon om innholdet i abonnentens internettkommunikasjon, om hvem abonnenten har vært i kontakt med eller geografisk posisjon. Eventuelle opplysninger om at en IP-adresse kan knyttes til straffbare forhold, må derfor politiet eller påtalemyndigheten få fra annet hold, for eksempel ved digitale beslag, eller tips om at en bestemt IP-adresse er benyttet i forbindelse med kriminell virksomhet. En lagringsplikt for IP-adresser vil ikke i seg selv kunne muliggjøre omfattende overvåking av enkeltpersoners nettbruk.

Som redegjort for i kapittel 4, har mangelen på globale IP-adresser ført til at IP-adresser deles mellom abonnenter ved hjelp av NAT-teknologi. Abonnentenes individuelle kommunikasjon skilles da fra hverandre ved hjelp av portnumre, som gjør det mulig at kommunikasjonen kommer frem til rett destinasjon. En kombinasjon av IP-adresse og portnummer på et gitt tidspunkt vil være unik for den enkelte abonnent. 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 én enkeltabonnent. For at en plikt til lagring av IP-adresser skal imøtekomme politiets behov, bør derfor lagringsplikten etter departementets syn også omfatte en plikt til å lagre portnumre på abonnentsiden. En lagringsplikt for portinformasjon vil imidlertid gi noe mer informasjon, jf. nærmere redegjørelse under kapittel 8.2.

Departementet gjør oppmerksom på at selv om lagring av portinformasjon på abonnentsiden vil gjøre det mulig å identifisere den konkrete *abonnenten*, vil det i mange tilfeller likevel ikke være mulig å identifisere en konkret *bruker* gjennom å koble en IP-adresse og portnummer til en abonnent. IP-adresser deles ofte av et stort antall brukere, for eksempel dersom abonnenten er en arbeidsplass, en skole, et universitet eller et serveringssted. Man kan dermed ikke uten videre legge til grunn at brukeren og abonnenten er den samme. Innhenting av abonnementsinformasjonen vil da være et steg på veien mot ytterligere etterforsking, og det vil kunne være avgjørende informasjon for hvor den videre etterforskingen i saken bør rettes.

Departementet viser for øvrig til at flere av høringsinstansene har stilt spørsmål ved effekten av å innføre en lagringsplikt for IP-adresser, siden mange som begår lovbrudd over internett vil kunne forsøke å skjule sin identitet gjennom krypterings- og anonymiseringsløsninger, slik som VPN-teknologi eller TOR. Departementet er oppmerksom på problemstillingen, men legger til grunn at en lagringsplikt likevel samlet sett vil ha stor verdi for kriminalitetsbekjempelse. Det vises her til politiets egne vurderinger av behovet. At det finnes krypterings- og anonymiseringsløsninger bør derfor ikke tillegges avgjørende vekt.

Departementet foreslår etter dette at det innføres en lagringsplikt for IP-adresser. For at lagringen skal nå sitt formål, bør lagringsplikten gjelde for alle abonnenter, og den bør ikke begrenses ut fra for eksempel konkret mistanke om straffbare forhold. Den enkeltes person- og kommunikasjonsvern vil ivaretas gjennom krav til at lagringstiden ikke skal være lengre enn nødvendig, samt strenge vilkår for når opplysninger om IP-adresser skal kunne utleveres til politi- og påtalemyndighet. Departementet foreslår også at det fastsettes nærmere krav som legger til rette for tilsyn og kontroll.

8 Nærmere om lagringsplikten

8.1 Hvem lagringsplikten skal gjelde for

8.1.1 Gjeldende rett

Etter gjeldende rett har ikke tilbyder plikt til å lagre opplysninger om hvilke IP-adresser abonnentene har disponert. Tilbydere av ekomtjenester kan imidlertid lagre opplysninger om IP-adresser for eget formål etter ekomloven § 2-7 femte ledd, vanligvis i inntil tre uker. Det vises til redegjørelsen under kapittel 7.1.

8.1.2 Forslaget i høringsnotatet

I dag dekker seks store tilbydere av internetttjenester over 95 prosent av markedet i Norge. I tillegg finnes det ca. 300 tilbydere som er registrerte som tilbydere av internettaksess som tjeneste. De fleste av disse leverer sine tjenester over de store infrastruktureiernes nett. 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.

I høringsnotatet ble det redegjort for at 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 lagring av IP-adresser. For det første har det betydning om tilbyder drifter en egen løsning for IP-allokering. Med IP-allokering menes prosessen med 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 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 tilgang til 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 den må sammenstilles, for eksempel ved at den ene tilbyderen har oversikt over 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 for næringen når det gjelder hvordan de ønsker å løse dette.

I lys av dette mente departementene at det ikke var hensiktsmessig å skille mellom tilbydere ut fra størrelse og markedsandel, og foreslo at

plikten til å lagre IP-adresser bør rette seg mot samtlige tilbydere av internettaksess. En lagringsplikt for alle ville også hindre faren for at noen små tilbydere uten lagringsplikt, av den grunn ville være attraktive for kriminelle. Lagringsplikten ble foreslått å være avgrenset til tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett. Departementene foreslo at pliktsubjektene ble angitt 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 den vil omfatte alle aktører i markedet som tilbyr internettilgang til allmennheten, jf. ekomloven § 1-5 nr. 4. Lagringsplikten ble foreslått å gjelde alle tilbydere uavhengig av teknologisk plattform. Departementene foreslo samtidig at det gis en forskriftshjemmel som gir Nasjonal kommunikasjonsmyndighet anledning til å fastsette unntak for tilbydere. Det vil eksempelvis kunne 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.

8.1.3 Høringsinstansenes syn

Ingen høringsinstanser har gitt uttrykk for at de er uenige i forslaget om at lagringsplikten skal gjelde for alle tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett.

Telenor støtter forslaget om at lagringsplikten skal gjelde for alle internettilbydere, fordi den enkelte har en relasjon til egne abonnenter. Prinsippet må gjelde uavhengig av driftsløsninger og modeller i grossistmarkedet. Politiet bør først innhente informasjon fra internettilbyderen som «eier» relevant IP-adresse, og deretter få opplyst hvilken tjenestetilbyder som innehar abonnenten. Politiet bør så fremme en anmodning til riktig tjenestetilbyder for å få utlevert abonnementsopplysninger.

Altibox viser til store variasjoner i teknisk innretning hos aktørene. Noen har selv informasjonen, andre har utkontraktert tjenesten med å tildele IP-adresser. Lovforslaget må ikke legge begrensinger på forretningsmodellene til aktørene. Lagring og utlevering må kunne håndteres i samarbeidskonstellasjoner, partnerskap eller overlates til en samarbeidspartner, så lenge dataene er tilgjengelige for politiet, og håndteres forsvarlig og sikkert.

IKT-Norge mener at lovforslaget forutsetter at de enkelte tilbyderne har all informasjon om abonnent, IP-adresse (eventuelt portnummer) og tidspunkt for kommunikasjon for bruk ved utleveringsbegjæringer, og mener det er uavklart hvordan lagringsplikten kan oppfylles av tilbydere som ikke har all denne informasjonen. Tilbydere som kjøper tilgang til infrastruktur fra en annen som konfigurerer og administrerer nettverket, konkurrerer om de samme sluttbrukerne, noe som også gjør det problematisk å dele all informasjon. Det er for eksempel av forretningsmessig betydning å hemmeligholde abonnentlister. IKT-Norge mener videre at forholdet til plattformtjenester (OTT) fremstår som lite utredet, og viser til at regelverksutvikling i EU går i retning av større grad av teknologinøytrale forpliktelser.

Politidirektoratet viser til at *Kripos* i sitt innspill mener at en lagringsplikt også bør gjelde for tilbydere av private nett som skoler, kommuner, hoteller, flyplasser og lignende, for at hensynet til kriminalitetsbekjempelsen og formålet med lagringsplikten skal oppfylles. Politidirektoratet tiltrer innspillet fra Kripos.

8.1.4 Departementets vurdering

Departementet viser til at forslaget i høringsnotatet om at lagringsplikten skal omfatte alle tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett, har fått støtte i høringsrunden. Departementet opprettholder derfor forslaget.

Forslaget om lagringsplikt for IP-adresser vil ikke omfatte eksempelvis Facebook, Messenger og Skype. Slike tjenester er ikke omfattet av tilbyderbegrepet i gjeldende ekomlov.

Bestemmelsene i EUs ekomdirektiv (Europaparlaments- og rådsdirektiv (EU) 2018/1972 av 11. desember 2018) fastsetter reviderte rammer for ekomlovgivningen, herunder endres tilbyderbegrepet til også å omfatte nummeruavhengige person-til-person-kommunikasjonstjenester i enkelte sammenhenger. Direktivet er EØS-relevant, men ennå ikke innlemmet i EØS-avtalen. Departementet vurderer om en eventuell gjennomføring av ekomdirektivet skal foreslås i en ny ekomlov, og vil i den forbindelse også vurdere spørsmål som gjelder regulering av nummeruavhengige person-til-person-kommunikasjonstjenester.

Departementet ser det heller ikke som aktuelt å pålegge eiere av private nett en plikt til å lagre

IP-adresser, slik *Politidirektoratet* og *Kripos* foreslår. Eiere av private nett vil normalt ikke være tilbydere av internettjenester. Det vil være andre tilbydere som leverer ekomtjenester/internett, også i private nett, og det vil da eventuelt være disse tilbyderne IP-adressene vil måtte hentes fra.

8.2 Hvilke opplysninger skal lagres?

8.2.1 Gjeldende rett

Etter gjeldende rett har ikke tilbyder plikt til å lagre opplysninger om hvilke IP-adresser abonnentene har disponert. Det er tvert imot en sletteplikt etter ekomloven § 2-7 femte ledd, som sier at trafikkdata, lokaliseringsdata eller andre data som er nødvendige for å identifisere abonnenten, skal slettes eller anonymiseres så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål eller for å oppfylle krav fastsatt i medhold av lov, med mindre brukeren har samtykket til videre lagring. Lignende krav til dataminimering og rett til sletting følger av personopplysningsloven, jf. personvernforordningen artikkel 5 og 17. Det vises også til redegjørelsen i kapittel 7.1.

8.2.2 Forslaget i høringsnotatet

I høringsnotatet vurderte departementene flere forslag til måter en lagringsplikt kan utformes på.

Formålet med lagringen er å gjøre det mulig å koble IP-adresser til abonnenter. 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.

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, slik at personvernet ivaretas. Videre må reglene fungere på tvers av tilbydernes ulike systemer og være teknologinøytrale.

Departementene la frem to ulike tilnærminger ved utformingen av reglene. Én tilnærming var 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 – å kunne identifisere abonnenter. Fordelen med denne tilnærmingen er at den er teknologinøytral, og at en slik bestemmelse vil sikre at bare de nødvendige opplysningene lagres.

Departementene viste til at en ulempe med en helt generell og teknologinøytral bestemmelse som pålegger lagring av «*de opplysninger som er nødvendige for å identifisere abonnenten*» eller lignende, er 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-adressene 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 på samme tidspunkt. 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 eller lignende. Etter departementenes vurdering burde lagringsplikten omfatte portnumre tildelt abonnenten, men ikke mer enn dette. Denne begrens-

ningen vil imidlertid ikke fremgå uttrykkelig av en generell bestemmelse, som pålegger lagring av de opplysninger som er nødvendige for å identifisere abonnenten.

Departementene foreslo derfor 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 etterspurte særskilt høringsinstansenes innspill på om 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).

8.2.3 Høringsinstansenes syn

Telenor mener det er viktig at ISP-ene (internettilgangstilbyderne) selv gis rom til å definere hva som er nødvendige dataelementer å lagre for å identifisere en abonnent, og at det ikke er behov for å regulere dette ytterligere fra myndighetenes side. Avhengig av systemkonfigurasjon og nettverksmodell vil det også være ulikt behov for informasjon om en abonnents trafikk for å kunne identifisere vedkommende. Til spørsmålet i høringsnotatet om det i dag brukes løsninger hvor det er behov for å lagre ytterligere informasjon for å kunne identifisere en abonnent, er det opplyst at selskapet ikke har nettverksmodeller i bruk som krever lagring av data om destinasjonssiden for dette formålet. Telenor understreker på generelt grunnlag at hvis en ISP må lagre offentlig IP-adresse/offentlig port/starttidspunkt/sluttidspunkt, så vil en forespørsel fra politiet på offentlig IP-adresse/offentlig port/tidspunkt alltid gi et unikt svar. Hvor mange abonnenter som deler på offentlige IP-adresser til enhver tid, kommer an på hvor mange offentlige adresser ISP-en eier og bruker på CGNAT-løsningen. Dette er konfigurerbart hos den enkelte ISP.

Telia mener at høringsnotatet sier lite om hvilke krav som stilles til tilbyderne hva angår tjenestekvalitet. Dette er faktorer som har stor betydning for hvordan loggløsningen skal etableres. Det fremgår ikke om det vil bli stilt krav om tiltak for å sikre oppetid, redundans på syslogservere, backup og gjenoppretting. Slike krav vil få stor betydning for hvor kostnadskrevende det vil være å etablere løsningen. Det understrekes at kravet til logging ikke må få som konsekvens at ved eventuell nedetid for løsningen som benyttes til logging, må tjenestene de leverer til sine kunder stenges ned.

IKT-Norge understreker at det eksisterer et mangfold av nettverkskonfigurasjoner, og at disse endres over tid med teknologisk og markedsmessig utvikling. En lagringsplikt må ikke legge begrensninger på konfigurasjon og drift av nettverk. Tilbyderne må selv få vurdere hvordan de skal oppfylle plikten etter forslaget. Det er samtidig viktig å unngå at regelverket fører til at det må produseres/lagres flere opplysninger enn nødvendig for å oppfylle formålet med plikten.

GlobalConnect støtter at departementene i lovforslaget begrenser lagringsplikten til det som er nødvendig for å kunne identifisere abonnenten, og samtidig presiserer hva abonnenten skal kunne identifiseres med utgangspunkt i. GlobalConnect mener at dette gjør det mulig for tilbyderne å fastslå hvilke konkrete opplysninger de som minimum skal lagre.

Altibox mener at plikten til å lagre ikke må innebære at det skal lagres mer enn det som er strengt nødvendig for å tilfredsstille lovens formål. Det er viktig at en lagringsplikt er knyttet til å identifisere abonnenten på internettilknytningen, og ikke den reelle bruker. Dette må også reflekteres i påtalemyndighetens tilnærming til de lagrede dataene. De peker også på at det er avgjørende å trekke opp grensegangen mellom personvern og politiets interesse.

Det nasjonale statsadvokatembetet støtter at lagringsplikten bør omfatte informasjon som er nødvendig for å identifisere abonnenten ved deling av IP-adresser og at lagringsplikten må omfatte alle opplysninger som er nødvendige for å nå formålet.

Politidirektoratet viser til at det vesentlige er at de opplysningene som lagres muliggjør identifisering av sluttbruker. Videre støttes tilnærmingen om at det fastsettes en plikt til å lagre de opplysninger som er nødvendig for formålet, som er å identifisere abonnenter som gis internettilgang. Direktoratet tiltrer for øvrig innspillet fra *Kripos* om at lagringsplikten bør knyttes opp mot et teknologinøytralt begrep og at en nærmere presisering av hvilke typer data som til enhver tid skal lagres, kan bestemmes i forskrift. Tildelingstidspunktet for IP-adressen må omfattes av lagringsplikten.

Kripos er enig i at lagringsplikten må omfatte data som gjør at identifisering er mulig også hvor NAT-teknologi benyttes. Kripos er ikke kjent med om det i dag benyttes teknologi hvor det ville være nødvendig å lagre eksempelvis IP-adresse og portnummer på destinasjonssiden for å kunne identifisere en bruker. Den teknologiske utviklingen går imidlertid nå så fort at behovet for lagring av destinasjonsdata kan bli aktuelt i nær fremtid. I denne omgang bør det således ikke utelukkes at lagringsplikten i fremtiden skal kunne utvides til å omfatte data på destinasjonssiden.

ØKOKRIM mener at en lovbestemmelse må sørge for å sikre at lagringsplikten blir tilstrekkelig teknologinøytral, slik at formålet om en identifisering av abonnenten blir ivaretatt til tross for fremtidige teknologiske endringer og nye løsninger, som strekker seg utover IP-adresser og portnummer.

Elektronisk Forpost Norge mener høringsnotatet er diffust når det gjelder hva som foreslås lagret. Elektronisk Forpost Norge mener videre at det ikke er riktig at koblingen mellom en IP-adresse og abonnent i seg selv sjelden vil muliggjøre en entydig identifikasjon av en konkret bruker. For et mobilabonnement er det høyst sannsynlig at abonnementets enhet kan knyttes til en konkret bruker. Elektronisk forpost viser også til at departementene skriver at «IP-adresser har tradisjonelt vært ansett som mindre beskyttelsesverdige» og viser til at dette kommer i konflikt med blant annet personverndirektivet 95/46/EC, GDPR og Data Protecting Working Party hvor IP-adresse er ansett som «personal data».

KS skriver at det er av betydning for kommunikasjonsvernet at informasjon om hvilke IP-adresser ulike abonnenter er tildelt, ikke i seg selv avslører noe om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har kommunisert med. KS mener at det i lovforslaget er lagt opp til en plikt om lagring av IP-adresser som synes å balansere hensynene til kriminalitetsbekjempelse og person- og kommunikasjonsvern på en god måte.

Norsk Journalistlag skriver at et system som inkluderer destinasjonsinformasjon vil kunne fange opp anonyme kilder direkte. Det vil dermed være klart i strid med EMK artikkel 10. Dette vil utvilsomt kunne gi journalister vanskeligere arbeidsvilkår og være et brudd på våre internasjonale forpliktelser om kildevern.

Norsk Presseforbund og *Norsk Redaktørforening* viser til departementets forslag om en «mellomløsning» ved utformingen av bestemmelsen, og peker på at et krav om å lagre det som er «nødvendig» og angivelsen om hva som skal være utgangspunktet, er for generell. En risikerer at tilbydere heller lagrer litt for mye enn litt for lite. En eventuell bestemmelse bør derfor formuleres mer spesifikt og uttømmende. Presseforbundet og Norsk Redaktørforening viser også til EU-domstolen i *La Quadrature du Net*-avgjørelsen og mener at departementenes forslag innebærer noe annet enn det EU-domstolen har forutsatt, som er tradisjonell lagring av IP-adresser. De er derfor ikke enige i departementenes vurdering av at forslaget som foreligger, er i tråd med EU-domstolens føringer. Presseforbundet og Norsk Redaktørforening mener at forslaget går lengre, ved at det pålegges lagring som helt presist vil kunne fastslå tidspunktet hvor identifiserte enkeltpersoner kommuniserer med andre. Nøyaktige tidspunkter, samt portnummerinformasjonen, vil gjøre det vesentlig lettere for eksempel å avsløre kommunikasjon mellom en journalist og en kilde.

Også *NRK* er bekymret for forslagets konsekvenser for kildevernet. De viser til at lovforslaget ikke kan åpne for lagring/utlevering av metadata som mottaker og kommunikasjonstidspunkter, da dette vil være klart lovstridig.

8.2.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet der det velges en mellomløsning som angir at tilbyder skal lagre de opplysninger som er nødvendige for å identifisere abonnenten, og som også angir et utgangspunkt for hva som skal lagres. Dette ivaretar nødvendig smidighet for teknisk løsning hos tilbyderne, samtidig som det setter tydelige rammer for lagringen og derved ivaretar kommunikasjonsvernet. Departementet foreslår også at formålet med lagringen settes inn i bestemmelsen. Da synliggjøres formålet med lagringen bedre, som en ramme rundt hva som kan og skal lagres. Departementet foreslår også at det klargjøres at destinasjonsdata ikke skal lagres.

Forslaget innebærer at tilbyder skal lagre IP-adresser og tidspunkt for kommunikasjon og eventuelt portnummer der det er nødvendig for å kunne identifisere abonnenten.

I høringsinnspillene kom det frem bekymring blant annet for om lagring av disse opplysningene innebærer at personers bevegelser kan følges fysisk, og om lagrede data kan benyttes til å lage en form for profil av enkeltpersoner. Til dette vil departementet bemerke at forslaget ikke i seg selv innebærer lagring av informasjon om innholdet i abonnentens internettkommunikasjon, hvem

abonnenten har vært i kontakt med eller hvor abonnenten befinner seg.

Når det gjelder hvilken *mulighet for geografisk posisjonering* som følger av forslaget til lagringsplikt, viser departementet til Telenors kommentar i høringen, der det er uttalt: «*Vi vil i denne forbindelse gjøre oppmerksom på at dersom IP-adressen er tilknyttet et fastnett-abonnement (dvs. en fysisk linje – for eksempel kobber eller fiber), vil informasjonen vedrørende IP-adresse og bruker i tillegg også (i de fleste tilfeller) kunne gi informasjon direkte/indirekte om fysisk lokasjon/plassering for terminerende ende av den fysiske linjen (dvs. installasjonsadresse for kundens abonnement) via kundedata. Det vil med andre ord avsløre hvor abonnenten har befunnet seg når vedkommende benyttet den etterspurte IP-adresse.*» Informasjonen som lagres angående et fastnett-abonnement vil med andre ord kunne kobles med annen informasjon og derigjennom kunne gi kunnskap om brukerens geografiske plassering, forutsatt at brukeren er identisk med abonnenten. Dette vil være en personvernulempe, men departementet vurderer personvernulempen ved dette til å være liten.

Departementet oppfatter imidlertid at Datatilsynet og andre høringsinstanser primært problematiserer muligheten for geografisk «sporing» av enkeltindividers forflytning med fokus på «sporing» av en bruker som kommuniserer via mobilnettene eller WiFi-løsninger, ikke via en fastnettaksess.

En IP-adresse tilordnes abonnenten og ikke brukeren. Dette medfører at alle brukere som kobler seg til åpne WiFi-løsninger på eksempelvis serveringsteder, flytoget mv. vil ha samme felles IP-adresse i nettet. Dette er IP-adressen knyttet til abonnenten, som i eksemplene her vil være henholdsvis serveringsstedet eller Flytoget AS. Tilbyderne som leverer internett til serveringsstedet og i togsettene til Flytoget AS vil altså kun ha mulighet til å vite hvilke IP-adresser som er anvendt av serveringsstedet og Flytoget AS, men ikke hvilken bruker som har kommunisert via denne adressen. Det er her viktig å skille mellom abonnent og bruker. Abonnenten Flytoget AS er ikke den samme som alle brukerne som har anvendt togets WiFi-nett.

Ved kommunikasjon i mobilnettene vil knytningen mellom abonnent og bruker være sterkere. Knytningen mellom IP-adresse og geografisk posisjon vil derimot være upresis. I utgangspunktet er det ingen knytning mellom geografisk lokasjon og en IP-adresse, da IP-adressen kun angir lokasjon i en nettverkstopologi. Det er imidlertid mulig å utlede en knytning mellom nettverkstopologi og geografiske områder gjennom sammenstilling av offentlig tilgjengelig informasjon som for eksempel adresserom tildelt en tilbyder, hvilket geografisk område denne tilbyderen opererer i og hvilke tjenestetyper som tilbys av tilbyderen. Graden av nøyaktighet og sannsynlighet i en slik eventuell utledet knytning mellom IP-adresse og geografi vil være så lav at det ikke kan hevdes å si noe kvalifisert om konkret geografisk posisjon for abonnenten.

Det vil også være mulig å utlede en knytning mellom nettverkstopologi og geografiske områder basert på beskyttet informasjon hos mobiltilbyderen om teknisk implementering i nettet og geografisk bruksområde for en IP-adresse på et gitt tidspunkt. En mobiltilbyder vil eksempelvis kunne avgrense/allokere en rekke med IP-adresser for anvendelse innenfor et nærmere geografisk område innenfor et gitt tidsrom. Detaljert informasjon om tilbyderens tekniske implementering og konfigurasjon av nettet er imidlertid ikke omfattet av lagringsplikten i lovforslaget. For øvrig vil eventuell kunnskap om slik beskyttet informasjon sammenholdt med IP-adresse, kun avgrense den geografiske posisjonen for en IP-tilordning til større geografiske områder, som for eksempel bydel, by, fylke eller landsdel.

Departementet understreker for øvrig at mulighet for geografisk lokalisering vil være lik med IPv6 som for IPv4. Når det gjelder mulighet til å se en abonnents bruksmønster vil den med IPv6 bli mindre, da problemstillingen med NAT-teknologi, behov for portnummer på abonnentssiden og derigjennom informasjon om en abonnents bruksmønster, vil kunne falle bort/bli mindre. Departementet kjenner heller ikke til andre potensielt negative personvernkonsekvenser ved overgang til IPv6.

Etter departementets mening innebærer derfor den foreslåtte lagringsplikten i seg selv ikke lagring om en gitt brukers geografiske posisjon til enhver tid. Lagring av IP-adresse knyttet til et fastnettabonnement vil, sammenholdt med installasjonsadresse for kundens abonnement, gi opplysninger om geografisk lokasjon av abonnent. Det vil innebære en personvernulempe, men departementet mener at ulempen ikke er større enn ved å få kjennskap til en abonnents adresse via et fasttelefonnummer, og ulempen anses dermed for å være liten. Geografisk lokalisering på grunnlag av IP-adresse i mobilnettene kan til en viss grad utledes med bakgrunn i beskyttet og ikke lagringspliktig informasjon om teknisk implementering og konfigurasjon av tilbyderens nett. En eventuell sammenstilling av konfigurasjonsinformasjon og

IP-adresse vil imidlertid bare gi en svært upresis informasjon om geografisk posisjon, og uansett aldri på basestasjonsnivå som er hevdet i enkelte høringsuttalelser. Departementets vurdering er derfor at den foreslåtte lagringen ikke vil synliggjøre geografisk plassering, selv ved kobling av dataene mot annen informasjon, på en måte som vil ha store personvernmessige ulemper sett i forhold til det formålet lagringen har.

Det er videre et spørsmål om hva som kan utledes av en abonnents bruk av ekomtjenester. En statisk eller dynamisk IP-adresse samt tidspunkt, sier i utgangspunktet ikke noe om en abonnents bruk, men kun hvilke IP-adresser som har vært tilordnet abonnenten (og ikke nødvendigvis brukt) på et gitt tidspunkt. Problemstillingen om informasjon om bruk er knyttet til NAT-teknologi og deling av IP-adresser. 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.

Portnummeret logges altså først ved faktisk bruk, og den lagrede informasjonen kan derfor si noe om bruksmønster, herunder oppkoblingshyppighet og vaner knyttet til tid for aktivitet og avvik fra dette. En hyppig oppkoblingsfrekvens kan blant annet gi indikasjoner indirekte på innholdet i kommunikasjonen, eksempelvis bruk av fildeling/BitTorrent-teknologi.

Det kan heller ikke utelukkes at mønster i hvilke porter som benyttes kan avdekke hvilket operativsystem som er benyttet. Dette kan da også muligens si noe om antall unike enheter som er knyttet til et abonnement. Det er imidlertid usikkert i hvilken grad dette er mulig for moderne operativsystem. Det er krevende med sikkerhet å si alt som potensielt kan leses ut av en analyse av bruksmønster. Det er pågående og kontinuerlig forskning og utvikling på området, og dermed ikke mulig å si hva fremtidige analysemetoder potensielt kan avdekke.

Lagring av portinformasjon vil etter departementets 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 departementets syn også omfatte informasjon som er nødvendig for å identifisere abonnenten ved deling av IP-adresser. Muligheten til å identifisere abonnenten bør ikke bero på tilbydernes tekniske løsninger. Departementet vurderer at lagring av portinformasjon er nødvendig for å oppnå formålet med lagringen, og vurderer at de personvernmessige ulempene ved at noe informasjon kan ledes ut av lagring av portinformasjon, er små sett i forhold til de fordeler lagringen gir for kriminalitetsbekjempelse.

8.3 Hvor og hvordan skal IP-opplysninger lagres?

8.3.1 Gjeldende rett

Etter gjeldende rett har ikke tilbyder plikt til å lagre opplysninger om hvilke IP-adresser abonnentene har disponert, og det finnes derfor ingen regler som direkte gjelder slik lagring. Ekomtilbyderne håndterer imidlertid store mengder sensitiv informasjon, og ekomloven setter derfor strenge krav til taushetsplikt og vern av kommunikasjon og data i tilbydernes ekomnett og -tjenester, jf. §§ 2-7 og 2-9. Dette inkluderer også sikker lagring så lenge dataene lagres til tilbyders nødvendige bruk, og vil også omfatte lagring som gjøres på bakgrunn av en eventuell lagringsplikt. Videre vil regler om informasjonssikkerhet i personvernforordningen sette rammer for lagringen, særlig artikkel 32 om sikkerhet ved behandlingen, men også andre regler i forordningen vil komme til anvendelse.

8.3.2 Forslaget i høringsnotatet

I høringsnotatet foreslo departementene ikke nye krav til hvor og hvordan opplysninger lagres. Departementene viste til at gjeldende regelverk allerede inneholder krav for å sikre kommunikasjonsvernet. Det er derfor ikke behov for ekstra regulering av hvordan lagringsplikten gjennomføres.

Når det gjelder *hvor* data skal lagres, viste departementene til at det kan 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.

Departementene viste også til at da lovendringene knyttet til datalagringsdirektivet ble vedtatt, ble det ikke foreslått å stille krav til hvor dataene skulle lagres. Departementene mente at muligheten for å føre tilsyn og kontroll med overholdelse av vilkårene for lagring og bruk er avgjørende, uavhengig av hvor lagringen skjer. I forbindelse med gjennomføringen av datalagringsdirektivet ble det 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.

På bakgrunn av dette vurderte departementene i høringsnotatet om lagring av IP-adresser at det ikke var ønskelig å stille krav til hvor dataene lagres. For det første er det et mindre omfang av data som lagres, og dataene er å anse som mindre sensitive enn dataene som var foreslått omfattet av datalagringsdirektivet. For det andre kunne departementene ikke se at det har vært en teknologisk utvikling som skulle tilsi en annen løsning.

Videre mente departementene at det heller ikke burde settes begrensninger på at dataene skulle 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 kunne ikke se at det er hensiktsmessig å begrense dette gjennom lovverket. Det bør fortsatt kunne inngås databehandleravtaler som i dag.

Departementene vurderte også behovet 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. Ekomloven § 2-9 fastslår at tilbydere plikter å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon.

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

8.3.3 Høringsinstansenes syn

Telenor er enig i at videreføring av dagens krav til sikkerhet er et godt alternativ ved innføring av lagringsplikt. Telenor er i dag underlagt krav som følger av ekomloven, sikkerhetsloven og GDPR. Det er den enkelte ISP som vil måtte være ansvarlig for denne sikkerheten, uavhengig av om dette gjøres internt i bedriften eller ved hjelp av underleverandører. Det bør ikke komme noen myndighetspålegg ut over dette, inkludert eventuelle pålegg om felles lagringsløsning.

GlobalConnect støtter departementenes forslag om at det ikke er nødvendig å stille krav om særskilte, kostnadsdrivende sikkerhetstiltak utover de kravene som allerede følger av ekomloven. Selskapet ser det også som positivt at lovforslaget ikke stiller krav om lagring på norsk jord, og at det også åpner for at tilbyderne kan samarbeide med hverandre og andre tredjeparter om å finne gode og kostnadseffektive løsninger.

Altibox fremhever at det bør være et premiss for et slikt lovforslag at det ikke legger begrensinger for forretningsmodellen til de enkelte aktørene. Det som er avgjørende er at dataene skal være tilgjengelige for politiet og at det gjøres på en forsvarlig og sikker måte, og ikke hvordan modellen til en aktør er, og hvordan lagringen skjer. Lagring og utlevering må kunne håndteres i samarbeidskonstellasjoner, partnerskap og lignende. Dette må videre kunne avtalemessig overlates til en samarbeidspartner i et partnerskap.

Advokatforeningen mener at det er særdeles sentralt at hjemmelen som pålegger tilbydere å lagre disse opplysningene samtidig, som et minimum, gir føringer på hvor det ikke er tillatt å lagre disse opplysningene. Foreningen peker i den forbindelse på kravene i personvernforordningen samt *Schrems 2*-dommen, og mener at det er sentralt å klargjøre at det ikke er akseptabelt å lagre denne informasjonen i for eksempel en skytjeneste i et ikke-godkjent tredjeland.

Det nasjonale statsadvokatembetet er enig i at det ikke skal stilles krav til hvor og hvordan dataene skal lagres og viser til at ekomloven allerede stiller krav til tilbyderne.

ØKOKRIM skriver at det ved innføring av lagringsplikt må stilles krav til sikker lagring og øvrig behandling av personopplysningene på lik linje med de krav og den praksis som fremgår i for eksempel ekomloven og datalagringsforskriften.

Elektronisk Forpost Norge viser til at det ikke stilles spesielle krav til lagring eller geografisk sted for lagring av datamengden ut over hva som antas ivaretatt allerede fra nett- og tjenestetilbyder. De mener det er gjennomgående i forslaget at departementene ikke vurderer vernet om personlig kommunikasjon høyt, og de stiller seg skeptisk til alle sider av departementenes vurdering på dette punktet.

Norges institusjon for menneskerettigheter bemerker at gode og tydelige regler for lagring, herunder sikkerhet i systemene og mulighetene for innsyn og sletting, vil være sentrale i vurderingen av hvorvidt prosessuelle krav etter EMK artikkel 8 anses oppfylt.

NRK påpeker faren for at IP-data kommer på avveie, og viser til at det ikke er lagt opp til noen særskilte sikkerhetsmekanismer når det gjelder lagring av disse dataene. NRK viser til at man stadig ser nye eksempler på at data kommer på

avveie. Dette gjelder også sensitive data som krever særlig beskyttelse, eksempelvis data fra Stortinget.

8.3.4 Departementets vurdering

Departementet opprettholder vurderingen av at det ikke er behov for særlige regler for hvordan og hvor de lagringspliktige dataene skal lagres.

Det stilles allerede i dag 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 de største tilbyderne kryptering der dette er nødvendig for å sikre kommunikasjonen og datautlevering.

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. Tilsvarende vil gjelde for lagringspliktige etter de foreslåtte bestemmelsene. 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* kapittel 4.2 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.»

Videre vil de lagringspliktige dataene omfattes av reglene i personvernforordningen. Her kan særlig nevnes reglene i kapittel IV avsnitt 2 om personopplysningssikkerhet. I artikkel 32 fastsettes at den behandlingsansvarlige og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Videre oppstilles i artikkel 33 og 34 plikt til å melde til henholdsvis tilsynsmyndigheten og den registrerte ved brudd på personopplysningssikkerheten.

Også de andre reglene i personvernforordningen kan få særlig betydning. *Advokatforeningen* viser i sin høringsuttalelse til reglene om lagring i tredjeland, som får betydning ved skylagring. Personvernforordningen gir i kapittel V særlige regler om overføring av personopplysninger til tredjeland. Reglene innebærer at data ikke kan overføres (og av dette følger at de heller ikke kan lagres) til tredjeland, dvs. land utenfor EØS, uten at det sikres at opplysningene gis en tilsvarende personvernbeskyttelse som de har i EØS-landene. Bestemmelsene skal sikre at det ikke er mulig å omgå den beskyttelse som ligger i personvernforordningen ved å overføre data til land utenfor EØS. Som Advokatforeningen peker på, innebærer regelen i praksis en bestemmelse om hvor det ikke er tillatt å lagre data. Dette vil også gjelde for de lagringspliktige tilbyderne. Departementet mener at dette er dekket av reglene i personvernforordningen, og at det ikke er behov for ytterligere regulering.

Det bør etter departementets 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. Dette kan også være viktig for å redusere kostnadene ved lagringen. I tillegg er driftsutsetting relativt vanlig, og departementet kan ikke se at det er hensiktsmessig å begrense dette gjennom lovverket. Det bør fortsatt kunne inngås databehandleravtaler som i dag. Avgjørende er at sikkerheten ikke reduseres ved slike avtaler, men

opprettholdes på et tilfredsstillende nivå, sett i forhold til de lagrede dataenes sensitivitet.

På bakgrunn av dette anser departementet at de regler som allerede finnes til sikring av kommunikasjonsdata, er tilstrekkelige og egnede til å ivareta kommunikasjonsvernet ved den foreslåtte lagringsplikten. Departementet mener derfor at det ikke er behov for ytterligere regulering av hvordan og hvor dataene skal lagres.

8.4 Lagringstid

8.4.1 Gjeldende rett

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, da lagringen krevde konsesjon av Datatilsynet, 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*. Da konsesjonsplikten ble opphevet i nåværende personopplysningslov, ble vurderingen av hva som er nødvendig lagringstid, lagt til ekomtilbyderne selv. Etter det departementet kjenner til, har bransjen ved tolkningen av den nye personopplysningslovens regler fortsatt å benytte samme lagringstid som tidligere var satt av Datatilsynet. Det varierer imidlertid mellom tilbyderne, og mellom tilbydernes ulike tjenester for nettilgang, om opplysningene lagres i tre uker eller kortere, og om det lagres slike opplysninger overhodet.

8.4.2 Forslaget i høringsnotatet

I høringsnotatet ble det lagt til grunn at det ved vurderingen av hvor lenge IP-adresser skal lagres, vil måtte foretas en avveining mellom politiets og påtalemyndighetens behov for opplysningene og hensynet til kommunikasjonsvernet. Det ble særskilt vist til EU-domstolens avgjørelse *La Quadrature du Net*, der det blant annet er fastslått at lagringstiden må begrenses til det strengt nødvendige.

Når det gjaldt vurderingen av hvor lang lagringstid for IP-adresser som er nødvendig for å kunne ivareta formålet, pekte departementene på at det må tas høyde for at det ofte vil gå tid fra en straffbar handling begås, til den oppdages. Etterforskingen kan altså knytte seg til et straffbart forhold som ligger langt tilbake i tid, samt til nettaktivitet som ligger enda lengre tilbake i tid. 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 således 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. IP-adresser kan videre måtte innhentes fra utenlandske nettsteder, for eksempel sosiale medier. For at lagringen skal ha tilstrekkelig nytteverdi i kriminalitetsbekjempelsen, er det derfor viktig at lagringstiden ikke er for kort. Det ble også vist til praksis fra andre nordisk land der lagringstiden er henholdsvis seks, ni, ti og tolv måneder. Departementene mente lagringstiden burde ligge innenfor dette spennet og foreslo en lagringstid på seks, ni eller tolv måneder. Høringsinstansene ble særskilt bedt om å uttale seg om hvor lang lagringstiden burde være.

8.4.3 Høringsinstansenes syn

Høringsinnspill fra tilbydersiden, herunder *Altibox*, *GlobalConnect* og *Telenor*, samt *IKT-Norge* og *Tekna*, mener at lagringstiden bør være kortest mulig for å minimere risikoen for negative konsekvenser. Det er også vist til at jo lengre lagringstiden er, jo mer inngripende er tiltaket. Enkelte av høringsinstansene peker på at det ikke er dokumentert at det er nødvendig med en lengre lagringstid enn seks måneder. Dette støttes av *Advokatforeningen*, som også peker på at myndigheten må begrunne at lagringstiden er strengt nødvendig.

Altibox mener i utgangspunktet at det minst inngripende alternativet for lagringstid for dataene bør velges.

GlobalConnect viser til at jo lengre dataene lagres, jo mer inngripende vil tiltaket være. Det foreligger ikke konkret erfaringsmateriale som tilsier at etterforsking av alvorlig kriminalitet vil ta skade dersom lagringstiden settes til seks måneder. Hensynet til forholdsmessighet taler derfor med styrke for at lovgiver velger det korteste alternativet.

IKT-Norge viser også til at for å begrense de negative konsekvensene av ordningen, bør lagringstiden begrenses til seks måneder.

Telia mener som utgangspunkt at lagringsplikten bør settes til seks måneder, men at det må lyttes til politiet, som har det nødvendige erfaringsgrunnlaget for å vurdere hvor lenge IP-adresser bør lagres for at de skal kunne dra nytte av dem. Det vil være et lite personvernvennlig utfall å innføre en lagringsplikt som likevel ikke vil være egnet til å bekjempe kriminalitet fordi lagringstiden er for kort. På den andre siden vil personvernkonsekvensene bli mer inngripende jo lenger opplysningene lagres.

Tekna ønsker en kort lagringstid, maksimum seks måneder. Slik lagring innebærer alltid en fare for misbruk av personopplysninger, og for å begrense risikoen, ønsker Tekna en konservativ tilnærming til hvor lenge slike opplysninger kan lagres.

Telenor mener at det er tungtveiende grunner for at man bør velge det minst inngripende alternativet med hensyn til person- og kommunikasjonsvern, dersom forslaget fremmes. Ut fra høringsnotatets drøftinger vil dette innebære seks måneders lagringstid.

Advokatforeningen viser til at alminnelige personvernsprinsipper tilsier at lagringsplikten ikke går lengre enn hva som er strengt nødvendig for formålet. Det er myndighetene som må begrunne nødvendigheten. Advokatforeningen kan ikke se at departementene i høringsnotatet har begrunnet at det er strengt nødvendig å pålegge lagring lenger enn seks måneder.

Høringsinstansene som primært har fokus på kriminalitetsbekjempelse, er på den andre siden relativt samstemte i at for kort lagringstid vil innebære at formålet med lovendringen ikke oppnås. Disse mener derfor at lagringstiden bør settes til minst tolv måneder. Det er i denne sammenheng vist til at opplysningene i seg selv ikke er særskilt sensitive, noe som kan tale for at man kan akseptere en lengre lagringstid.

Riksadvokaten ønsker at opplysningene lagres i tolv måneder. Da er potensialet størst for at opplysningene kan bidra til effektiv bekjempelse av kriminalitet. Ved vurderingen av lagringstid må det også ses hen til at inngrepet gjelder opplysninger som i seg selv ikke er særskilt sensitive.

Det nasjonale statsadvokatembetet mener også at en lagringstid på ett år fra avslutningen av kommunikasjonen må være et absolutt minimum. Dette harmonerer best med de fleste land i Europa og ivaretar hensyn til internasjonalt samarbeid.

Oslo statsadvokatembeter anfører at opplysningene ideelt sett ikke burde slettes før foreldelsesfristen for aktuelle straffebud er utløpt. Oppklarings- og etterforskingshensyn tilsier at lagringsperioden er lengst mulig.

Politidirektoratet viser til at en lagringstid på tolv måneder i størst grad ivaretar politiets behov. En lagringstid på tolv måneder er også det gjennomgående forslaget i høringsinnspillene fra politietaten. Politidirektoratet viser særskilt til *Kripos* som underbygger behovet for en lagringstid på tolv måneder. Dette begrunnes blant annet med at det ofte vil kreve omfattende etterforsking å skaffe til veie informasjon om nettaktivitet, og avanserte tilgangsløsninger og kryptering gjør at det kan ta lang tid før politiet kan gjennomgå datamateriale. Som regel vil det også være behov for rettsanmodninger om utlevering av informasjon fra utenlandske nettsteder. En rettsanmodning til USA om innhenting av data fra en tilbyder av innholdstjenester, vil kunne ta opptil tolv måneder.

ØKOKRIM peker også på behovet for bistand over landegrensene når det anføres at det vil være strengt nødvendig at lagringstiden settes til tolv måneder. Saksbehandlingen fra saksinntak til påtalevedtak i ØKOKRIMs saker har de siste seks årene variert fra 216 til 560 dager, i tillegg til eventuell saksbehandlingstid i ulike kontrollinstanser før sakene anmeldes.

PST peker på at sannsynligheten for å oppklare, avverge og forebygge straffbare handlinger er større jo lengre lagringstiden er, og mener lagringstiden bør være ett år. De sakene PST etterforsker har ofte internasjonale forgreininger. Internasjonalt samarbeid er tidkrevende, og PST har i flere saker mistet tilgang til verdifull informasjon på grunn av for kort lagringstid.

Forsvarsdepartementet (FD) peker på at lagringstiden vil ha betydning for om lagringen har tilstrekkelig nytteverdi i kriminalitetsbekjempelsen. I alvorlige straffesaker, eksempelvis i saker som innebærer trusler mot norske sikkerhetsinteresser, vil ofte etterforskingen være langvarig og krevende. Hensynet til muligheten for å forhindre skadevirkninger mot nasjonale sikkerhetsinteresser må her veie tyngre enn hensynet til kommunikasjonsvernet. FD anser derfor en lagringstid på tolv måneder som en hensiktsmessig avveining mellom de hensynene som gjør seg gjeldende.

Politiets Fellesforbund peker også på at det i mange tilfeller tar lang tid før man er i stand til å innhente en aktuell IP-adresse fra nettsted, sosialt medium eller lignende. Lagringstiden må mini-

mum være seks måneder, og det er ønskelig med lagring på inntil tolv måneder.

Statens sivilrettsforvaltning peker på at lagringstiden – for å oppnå formålet om styrket kriminalitetsbekjempelse – bør være så lang som mulig, og mener lagringstiden bør settes til tolv måneder. Når det særskilt gjelder nettovergrepssaker, vises det til at det er svært få av de fornærmede som anmelder slike forhold. Det kan derfor være noe tilfeldig når en straffesak rulles opp, og det kan medgå en del tid før slike forhold blir oppdaget.

Stine Sofies Stiftelse peker på at nettovergrepssaker krever omfattende ressurser og er tidkrevende. Lagringstiden bør derfor settes til tolv måneder.

Rettighetsalliansen mener at oppbevaringsperioden for abonnementsopplysninger bør settes til tolv måneder. De viser til at åndsverkloven § 87 inneholder omfattende prosedyrekrav som nødvendigvis vil ta en del tid.

8.4.4 Departementets vurdering

Departementet foreslår en lagringstid på tolv måneder.

En plikt til å lagre IP-adresser vil innebære et inngrep i den enkeltes person- og kommunikasjonsvern, jf. EMK artikkel 8 og kommunikasjonsverndirektivet artikkel 5. Lagring vil dermed bare være lovlig så fremt inngrepet er «i samsvar med loven og er nødvendig i et demokratisk samfunn» av hensyn til ivaretakelse av nærmere angitte formål, jf. EMK artikkel 8 nr. 2. Tilsvarende følger av kommunikasjonsverndirektivet artikkel 15 første ledd, der det fremgår at en innskrenkning i vernet må være «nødvendig, egnet og rimelig i et demokratisk samfunn» sett hen til de formål som begrunner innskrenkningen.

For vurderingen av om lagring skal anses som et proporsjonalt inngrep etter EMK artikkel 8, vises det blant annet til EMDs avgjørelse i saken *Breyer mot Tyskland*, avsnitt 91 følgende, der det ble lagt til grunn at proporsjonalitetsvurderingen må ta utgangspunkt i hvor inngripende tiltaket er. EMD legger videre til grunn at proporsjonalitetsvurderingen ikke bare kan knytte seg til en vurdering av de lagrede dataene, men også må ses i forhold til reglene om tilgang til og bruk av disse, jf. avsnitt 97. At det er relevant å se hen til inngrepets alvor også når det gjelder tolkningen av kommunikasjonsverndirektivet, følger av *La Quadrature du Net* avsnitt 131.

Ved vurderingen av lagringstidens lengde, har departementet videre lagt til grunn rammene trukket opp i *La Quadrature du Net* avsnitt 156, der det klart fremgår at lagringstiden for IP-adresser ikke kan overstige hva som er «strengt nødvendig» for å oppnå det angitte formålet; i dette tilfellet bekjempelse av alvorlig kriminalitet. Det må derfor legges til grunn en streng nødvendighetsvurdering når man avgjør hvor lang lagringstiden skal være.

Departementet har merket seg at flere av høringsinstansene argumenterer for at lagringstiden, av hensyn til kommunikasjonsvernet, bør være kortest mulig. De begrunner dette med at lagringen er et stort inngrep i kommunikasjonsvernet og at risikoen for misbruk av informasjonen, blir mindre jo kortere lagringstiden er. Videre er det fra enkelte av høringsinstansene pekt på at det ikke er dokumentert eller begrunnet godt nok hvorfor det er behov for en lagringstid utover seks måneder.

Til dette vil departementet for det første peke på omtalen i kapittel 8.2.4 ovenfor av hvilke opplysninger som skal lagres, og hvor sensitive disse opplysningene isolert sett er. 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. Tiltaket er således langt mindre inngripende enn lagring av andre typer data, herunder lokasjonsdata. Dersom informasjonen mot formodning skulle komme på avveie, vil den med andre ord ikke uten videre avsløre abonnentens nettaktivitet. Det er dessuten forutsatt at tilbyderne skal ivareta sikkerheten rundt informasjonen på en betryggende måte, se ovenfor under kapittel 8.3.

For det andre fremgår det etter departementets vurdering klart av høringsinnspillene fra politi og påtalemyndighet at det er behov for en lagringstid ut over seks måneder for å oppnå formålet med forslaget; å styrke politiets mulighet til å bekjempe alvorlig kriminalitet. Departementet har lagt betydelig vekt på disse innspillene.

Det er flere grunner til at en kortere lagringstid ikke vil ivareta behovet. Etterforsking av saker med forgreininger til utlandet vil ofte innebære at det kan ta inntil ett år før politiet kommer i posisjon til å etterspørre informasjon knyttet til en IP-adresse, eksempelvis når det er nødvendig å sende en rettsanmodning til USA for å få utlevert IP-adressen fra en tilbyder av innholdstjenester, slik blant annet *Kripos* har påpekt i sin høringsuttalelse. Etterforsking av datamateriell kan også av andre grunner være tidkrevende. Særskilt gjelder dette de store og komplekse sakene som behandles av ØKOKRIM og PST, der bevisbildet ofte er

svært omfattende. *ØKOKRIM* har i sin høringsuttalelse vist til at gjennomsnittlig saksbehandlingstid ligger på 216 til 560 dager, samtidig som det gjerne også har gått noe tid fra forholdet ble begått til saken ble oversendt politiet. Når det gjelder overgrepssaker på nett, er det ytterligere et moment at sakene ofte ikke anmeldes av ofrene, men kommer til politiets kunnskap på andre måter, lenge etter at forholdet er begått. En for kort lagringstid vil i slike tilfeller kunne innebære at informasjonen er slettet når politiet etterspør den, med den konsekvens at saken ikke kan oppklares.

Departementet er også enige i innspillene i høringsuttalelsen fra *Telia* om at det vil være et lite personvernvennlig utfall å innføre en lagringsplikt som likevel ikke vil være egnet til å bekjempe kriminalitet fordi lagringstiden er for kort.

I avveiningen av de rettigheter og interesser som gjør seg gjeldende ved spørsmål om hvilken lagringstid som kan tillates innenfor kommunikasjonsverndirektivet, må det også ses hen til at informasjon om IP-adresser i enkelte saker kan utgjøre det eneste tilgjengelige beviset som kan gjøre det mulig å avsløre et lovbrudd, jf. *La Quadrature du Net* avsnitt 154. Etter departementets syn bør dette også spille inn ved fastsettelse av hvor lang lagringstid som skal anses nødvendig for å oppnå formålet med inngrepet, jf. avsnitt 156. For at tiltaket skal ha tilstrekkelig effekt for slike tilfeller, kan lagringstiden ikke settes så kort at IP-adressen ikke vil være tilgjengelig i for mange saker der dette vil utgjøre det eneste beviset som kan avsløre lovbruddet.

Videre mener departementet at det ved vurderingen av lagringstidens lengde også må ses hen til statenes positive plikt til å beskytte personvernet etter EMK artikkel 8, slik dette er forstått i EMDs avgjørelse i saken *K.U. mot Finland* avsnitt 42–43. EMD la i avgjørelsen til grunn at en tilfredsstillende beskyttelse av klageren innebar at det ble tatt effektive grep for å identifisere og rettsforfølge gjerningspersonen. Manglende tilgang til IP-adresser på grunn av taushetsplikt hos internettilbyderen, ble i dommen ansett som en krenkelse av EMK artikkel 8. Konsekvensen kan bli den samme dersom lagringstiden settes for kort til å utgjøre et tilstrekkelig effektivt middel til bekjempelse av alvorlig kriminalitet. At statens positive forpliktelse til å beskytte privatlivet skal vektlegges ved tolkingen av kommunikasjonsverndirektivet artikkel 15, følger også av *La Quadrature du Net* avsnitt 126. Det vises i denne sammenheng også til forpliktelser under Barnekonvensjonen artikkel 19, som er nærmere omtalt nedenfor under kapittel 8.5.4.

Departementet vil etter dette gå inn for en lagringstid på tolv måneder. Dette er i samsvar med det behov politi og påtalemyndighet nærmest samstemt har gitt uttrykk for at foreligger, og det vil være strengt nødvendig for å oppnå formålet med lagringsplikten, herunder å ivareta hensynet til tilstrekkelig effektive virkemidler for etterforsking av overgrep mot barn.

Departementet har hensyntatt at lagringstiden settes til tolv måneder i den videre vurderingen av materielle og prosessuelle vilkår for utlevering i kapitlene 8.5 og 8.6 nedenfor.

8.5 Materielle vilkår for utlevering av opplysninger

8.5.1 Gjeldende rett

Kommunikasjonsverndirektivet er gjennomført i norsk rett gjennom ekomloven med forskrifter. 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 i utgangspunktet også abonnentinformasjon, herunder opplysninger om abonnenters disponering av IP-adresser.

Ekomloven § 2-9 tredje ledd oppstiller et unntak fra dette utgangspunktet for utlevering av opplysninger til blant annet politi og påtalemyndighet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Bestemmelsen 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) kapittel 16 side 93. Unntaket fra taushetsplikten i ekomloven § 2-9 tredje ledd gjelder for alle oppgavene politiet utfører, og er ikke begrenset til å gjelde i forbindelse med etterforsking av en straffesak. Utlevering til bruk i etterforskingsøyemed krever heller ikke at den straffbare handlingen er av en viss alvorlighet.

Etter fjerde ledd skal anmodning fra påtalemyndigheten eller politiet om opplysninger som omhandlet i tredje ledd, etterkommes med mindre særlige forhold gjør det utilrådelig. «Særlige forhold» kan tenkes å foreligge ved politiets behandling av saker som ikke gjelder etterforsking, for eksempel i tilknytning til forvaltningssaker og namssaker jf. Ot.prp. nr. 31 (1997–1998) *Om lov om endringer i lov 23. juni 1995 nr 39 om*

telekommunikasjon, kapittel 6 side 16, om den tilsvarende bestemmelsen i teleloven § 9-3 som videreføres i ekomloven § 2-9 fjerde ledd. Etter gjeldende rett er det med andre ord vid adgang til å utlevere opplysninger om tildelte IP-adresser til politi og påtalemyndighet.

8.5.2 Forslaget i høringsnotatet

I høringsnotatet la departementene til grunn at vilkårene for utlevering av opplysningene som skal lagres etter forslaget, burde strammes inn sammenlignet med bestemmelsene i ekomloven § 2-9 tredje og fjerde ledd. Dette vil være nødvendig for å ivareta kravet om proporsjonalitet etter Grunnloven, EMK og kommunikasjonsverndirektivet.

Departementene understreket at den lagrede informasjonen om IP-adresser kunne ha betydning for etterforsking av straffbare handlinger på mange andre måter enn gjennom å identifisere ukjente gjerningspersoner. Som eksempler ble det vist til identifisering av eventuelle fornærmede og vitner, analyse og annen bearbeiding av innhentede kommunikasjonsdata, eller for å muliggjøre innhenting av ytterligere bevis gjennom beslag og utleveringspålegg. Departementene mente derfor at reglene om utlevering ikke burde utformes slik at det ble oppstilt spesifikke begrensninger for hvilke måter IP-informasjon kunne benyttes, men slik at informasjonen ville kunne innhentes når det var nødvendig for enkelte nærmere angitte formål.

Ved vurderingen av hvilke formål politi og påtalemyndighet skulle kunne innhente opplysningene til, pekte man i høringsnotatet på at det måtte foretas en avveining mellom behovet for informasjonen og hensynet til kommunikasjonsvernet. Det ble lagt til grunn at kriminaliteten som kunne begrunne innhenting av informasjon måtte være av en viss alvorlighet, særlig på bakgrunn av EU-dommen *La Quadrature du Net*. Departementene la i høringsnotatet til grunn at reglene om utlevering måtte utformes i samsvar med disse føringene.

Det ble videre pekt på at praksis fra EU-domstolen ga 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. Departementene viste til at EU-domstolen i blant annet *Tele 2*, *Ministerio Fiscal* og *La Quadrature du Net*, hadde understreket 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. Det er dermed usikkert om det finnes en enhetlig terskel for hva som skal utgjøre alvorlig kriminalitet, uavhengig av hva slags lagring det er tale om.

Departementene la til grunn at adgangen til utlevering ville kunne begrenses enten ved å sette et krav til strafferamme, eller ved å begrense utleveringen til forebygging og etterforsking av bestemte straffebud, eventuelt gjennom en kombinasjon av disse. Det ble vist til at behovet for IP-informasjon ikke 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 som kan bidra til å identifisere gjerningspersonen.

Departementene vurderte det som mest formålstjenlig at reglene om utlevering som utgangspunkt ble knyttet opp mot et generelt strafferammekrav, eventuelt i kombinasjon med nærmere bestemte straffebud. Det ble vist til en rekke straffebud med strafferammer på henholdsvis ett, to og tre år, der informasjon om IP-adresser ville kunne være av betydning. Et strafferammekrav burde således etter departementenes vurdering, settes til minimum ett eller to års fengsel, eventuelt i kombinasjon med unntak for spesifikke straffebud der IP-informasjon er av særlig stor betydning. Høringsinstansenes ble særskilt bedt om å uttale seg om dette.

Departementene pekte videre på at dersom en handling kan *forebygges* før den inntreffer ved hjelp av informasjon om hvem en IP-adresse tilhører, burde politiet kunne innhente denne informasjonen i samme omfang som den kan innhentes til etterforsking. Høringsinstansene ble også bedt om å uttale seg om dette spørsmålet.

Departementene foreslo også at det ble presisert i bestemmelsen at opplysninger bare skulle kunne utleveres når dette var *nødvendig* for etterforsking og forebygging av de angitte straffbare forholdene. Det ble presisert at dette kravet ikke skulle tolkes så strengt at utleveringen måtte være den eneste mulige løsningen. På den andre siden ville det heller ikke være tilstrekkelig at innhenting av slike opplysninger bare ville lette arbeidet. Kravet om nødvendighet ville også innebære en presisering av at det ikke skulle kunne innhentes flere opplysninger enn det i det enkelte tilfellet er behov for til formålet.

8.5.3 Høringsinstansenes syn

Flere av høringsinstansene støtter forslaget om at kravet til utlevering bør strammes inn ved at det settes et krav til strafferamme for utleveringen. Det er ulike syn på hvor strengt kravet bør settes.

Høringsuttalelsene på tilbydersiden peker først og fremst på behovet for klare rammer for hva som kan utleveres. Det vises videre til at det er viktig at tilbyderne ikke pålegges ansvar for å vurdere hva som skal kunne utleveres og ikke. Enkelte av disse høringsinstansene viser også til at kravet om alvorlig kriminalitet tilsier at strafferammen settes høyt.

Abelia støtter vurderingen om at adgangen til utlevering bør begrenses, enten ved å sette et krav til strafferamme, eller å begrense utleveringen til forebygging og etterforsking av bestemte straffebud. De tar imidlertid ikke stilling til konkrete endringer i disse kravene.

Telia viser til at tiltaket bare vil kunne sies å være nødvendig i et demokratisk samfunn dersom det benyttes for å bekjempe kriminalitet av en viss alvorlighet og som også utgjør en stor trussel mot den enkelte eller samfunnet. Telia vil ikke foreslå hvor grensen bør settes. Når det gjelder forebygging, understreker Telia at politiet vil måtte ha klare holdepunkter for å tro at opplysningene er nødvendige for å forebygge handlingen, før IP-opplysningene kan begjæres utlevert.

Telenor mener mye taler for at adgangen til utlevering av opplysninger bør begrenses enten ved en minimumsterskel for strafferamme og/eller ved å begrense utleveringen til forebygging og etterforsking av bestemte straffebud. Telenor understreker samtidig at de ikke tar stilling til hva som bør være det materielle innholdet i disse kravene. Telenor er enig med departementene i at vilkårene for utlevering av opplysningene som skal lagres etter forslaget, bør strammes inn, sammenlignet med gjeldende rett, for å ivareta kravet om proporsjonalitet etter Grunnloven, EMK, kommunikasjonsverndirektivet og EØS-retten.

Tekna er skeptiske til at det ikke legges opp til høyere strafferammekrav for at politiet skal kunne få ut opplysninger om IP-adresser og person-ID fra tilbydere av ekomtjenester, men har ikke bestemte meninger om hva slags type kriminalitet som skal ligge til grunn for utleveringen.

Enkelte andre høringsinstanser så som *Datatilsynet, Advokatforeningen, NIM* m.fl., legger stor vekt på henvisningen til kravet om alvorlig kriminalitet i *La Quadrature du Net*-dommen. Disse peker på at strafferammen må speile dette kravet bedre enn det departementene har lagt opp til i høringsnotatet.

Advokatforeningen viser til at en strafferamme på fengsel i ett eller to år er forholdsvis beskjedent, og ikke gir inntrykk av et reelt ønske om å begrense innsyn til mer alvorlige forhold. Advokatforeningen er også kritisk til å åpne for utlevering i forebyggingsøyemed, fordi det i slike tilfeller er vanskelig å kontrollere det reelle behovet. Nødvendighetskravet bør også klargjøres.

Datatilsynet mener at der IP-adressen er knyttet til både et navn og tidspunkt, vil alle rettsikkerhetsmekanismer som er knyttet til praksis fra EU-domstolen, måtte gjøres gjeldende. Datatilsynet viser i den sammenheng til *Tele2/Watson*-dommen, der det stilles krav om at det må fastlegges objektive kriterier for når myndighetene kan få adgang til opplysningene, og at tilgang prinsipielt kun kan gis hvor en person er mistenkt for å planlegge, ville begå eller har begått en alvorlig kriminell handling. Dette innebærer at høringsnotatets forslag om krav om «nødvendighet» i liten grad gir tilstrekkelig veiledning for hva som skal utleveres, og at «forebygging» blir et for vidt begrep for når det er legitimt å innhente opplysningene. I den sammenheng peker Datatilsynet på at forslaget åpner for at politi eller PST i saker hvor det er «nødvendig» vil kunne innhente alle IP-adresser knyttet til en person i et gitt tidsrom. Dette åpner for en kontinuerlig overvåkning unntatt kontroll, ved at politiet kan be om ukentlige eller daglige oppdatering av benyttede IP-adresser, og dermed lage seg et bilde av personens bevegelser.

Den internasjonale juristkommisjon (ICJ) stiller spørsmål om hvorfor den samme EU-rettslige terskel om alvorlig kriminalitet skal vurderes annerledes nå enn ved Stortingets vedtak om innføring av datalagringsdirektivet. Dette bør kommenteres nærmere. Personopplysninger som for eksempel IP-adresser, skal ikke lagres uten et spesifikt formål. Det er derfor viktig at det er klart definert hva som menes med «alvorlig kriminalitet».

Norges institusjon for menneskerettigheter (NIM) viser til at det ikke er helt god sammenheng mellom det foreslåtte strafferammekravet og hva departementene ellers skriver i høringsnotatet om politiets behov, som oppgis å være å bekjempe alvorlig kriminalitet. Departementenes forslag vil gå vesentlig lenger enn føringene som kan utledes av EU-domstolens storkammerdom i *La Quadrature du Net*-saken. NIM bemerker videre at i EMDs dom i *K.U. v. Finland* ble finske myndigheter dømt for å ikke ha på plass effektive etterforskningsmidler når det gjaldt å beskytte

barns privatliv på internett i en sak hvor en person hadde stjålet et barns identitet og laget en kontaktannonse i barnets navn, dvs. i et alvorlig tilfelle. En lav strafferamme vil kunne utgjøre et uforholdsmessig inngrep sett hen til formålet om å bekjempe «alvorlig kriminalitet».

Elektronisk Forpost Norge peker på at med den lave strafferammen som er foreslått i høringsnotatet, vil uthenting av IP-adresser bli aktuell for en stor andel lovbrudd.

Norsk Presseforbund og *Norsk Redaktørforening* peker på at selv om alvorlig kriminalitet ikke er definert i loven, ble det i NOU 2009: 15 (s. 75) lagt til grunn at begrepet omfatter de formene for kriminalitet som politiet i dag vil kunne bruke skjulte tvangsmidler i etterforskingen av, det vil si handlinger som kan medføre straff i henholdsvis minst ti år eller fem år. Når forslaget legger opp til å inkludere handlinger med en strafferamme på ett til to år, vil det inkludere langt mer enn det som objektivt sett må kunne regnes som «serious crime».

NRK viser til at i praksis vil en strafferamme på enten ett eller to år innebære at de fleste straffbare forhold vil falle inn under bestemmelsene. Det framgår av *La Quadrature du Net* at en generell og ikke-målrettet lagring av IP-informasjon kun vil være tillatt for å beskytte nasjonal sikkerhet, forhindre alvorlige trusler mot befolkningens sikkerhet eller for å bekjempe alvorlig kriminalitet. Straffebud med en strafferamme opp mot ett eller to år vil ikke oppfylle dette kravet. NRK mener forslaget går svært langt, og det er etter deres vurdering ikke forenlig med rettspraksis på området.

Rettighetsalliansen mener at strafferammekravet for utlevering av abonnentopplysninger etter straffeprosessuelle regler bør settes til ett års fengsel.

Høringsinstansene fra politi og påtalemyndighet er relativt samstemt i at de materielle vilkårene for utlevering ikke må være for strenge. Dersom strafferammen settes for høyt, vil en rekke straffebestemmelser der informasjon knyttet til IP-adresser er særskilt viktig for å oppklare forholdet, i tilfelle måtte inkluderes særskilt i bestemmelsen. Det er særskilt vist til bestemmelser som gjelder overgrep mot barn over nett.

Riksadvokaten støtter forslaget om at utleveringsplikten bør knyttes til strafferamme, men mener strafferammen ikke bør settes høyere enn ett år. Dersom kravet skal settes høyere, må en rekke bestemmelser med lavere strafferamme inkluderes særskilt.

Det nasjonale statsadvokatembetet mener den svenske lovgivningen, der det er plikt til å utlevere opplysninger til politi og påtalemyndighet ved mistanke om et straffbart forhold, kan være retningsgivende. I lys av kravet om at lagring bare kan rettferdiggjøres dersom formålet er å bekjempe alvorlig kriminalitet, vil et strafferammekrav på ett år, i kombinasjon med unntak for spesifikke straffebud der lagring av IP-adresser er av særskilt betydning, kunne tilrådes.

Oslo statsadvokatembeter viser til vilkårene for kontroll av kommunikasjonsanlegg i straffeprosessloven § 216 b og anfører at hensynet til konsekvens i lovverket tilsier at adgangen til å innhente informasjon om IP-adresser under åpen etterforsking minst bør tilsvare hva politiet vil kunne få gjennom bruk av denne bestemmelsen. Strafferammen er der fem år, men det er åpnet for unntak for straffbare forhold der slik etterforsking vil være særskilt egnet. Det kan imidlertid være gode grunner til også å vurdere en lavere strafferamme. Erfaring fra store nettovergrepsaker tilsier at de fornærmede i stor grad underrapporterer hva de har blitt utsatt for, slik at omfang og overgrepets alvor først har blitt klart på et senere tidspunkt i etterforskingen.

Politidirektoratet påpeker at terskelen departementet har foreslått synes høy i forhold til graden av inngrep og mener strafferammekravet bør ligge lavere enn det som er foreslått. Dersom man skulle komme fram til at det er behov for et strafferammekrav, mener direktoratet at kravet bør settes likt med kravet til å foreta en pågripelse, dvs. at siktede mistenkes for en handling som kan medføre fengsel i minst seks måneder. Dette støttes av *Politihøgskolen* og *Kripos*. Videre vises det til Kripos' innspill om at utlevering ved behov innenfor redningsarbeid eller søk etter savnede personer også bør omfattes.

Politidirektoratet støtter at opplysninger bør kunne utleveres når det er nødvendig for å forebygge en handling av tilsvarende alvorlighet.

ØKOKRIM viser til at de sakene de behandler oftest vil ha en strafferamme på tre år og oppover, men er likevel av den oppfatning at strafferammekravet bør ligge på mistanke om lovbrudd som kan medføre frihetsstraff. ØKOKRIM peker videre på at Norge har internasjonale forpliktelser knyttet til forebygging av hvitvasking og terrorfinansiering, noe som tilsier at det bør åpnes for utlevering til forebygging av saker med samme alvorlighetsgrad som angitt for etterforsking.

PST peker også på at deres oppgaveportefølje stort sett omfatter saker med en strafferamme som ligger over fengsel i 1 år. PST tiltrer forslaget

om utlevering også til forebygging av handlinger av tilsvarende alvorlighet og viser til at PST også har metodetilgang i sin forebyggende virksomhet.

Politiets Fellesforbund mener vilkåret for utlevering bør være at forholdet kan føre til fengselsstraff. Dersom man skal sette en strafferamme, kan man eventuelt se hen til kravet om en strafferamme på to år som Nasjonal kommunikasjonsmyndighet har satt for å gi fritak fra taushetsplikten for å innhente trafikkdata på en mistenkt/siktet.

Statens sivilrettsforvaltning har ikke sterke formeninger om strafferammekravet bør settes til fengsel i inntil ett eller to år, men anser i alle tilfeller at det ikke bør kreves en strengere strafferamme enn to år.

Redd Barna er enige med departementene i at kriminaliteten må være av en viss alvorlighet, men at strafferammen i seg selv ikke nødvendigvis er noe godt mål på om kriminaliteten skal ansees alvorlig nok til å begrunne utlevering. Redd Barna slutter seg derfor til departementenes forslag om å kombinere et krav til strafferamme med henvisninger til spesifikke straffebud, eventuelt at strafferammen settes lavt nok til å omfatte blant annet straffebud som omhandler utnyttelse av barn.

Stine Sofies Stiftelse mener at et strafferammekrav på ett års fengsel er tilstrekkelig. Det vises til at flere bestemmelser som gjelder vold og seksuelle overgrep mot barn har en strafferamme på ett års fengsel.

8.5.4 Departementets vurdering

8.5.4.1 Krav om alvorlig kriminalitet

Det følger av kommunikasjonsverndirektivet artikkel 15 at medlemsstatene kan gjøre inngrep i kommunikasjonsvernet når dette er «nødvendig, egnet og rimelig i et demokratisk samfunn av hensyn til nasjonal sikkerhet (…), forsvar, offentlig sikkerhet og *forebygging, etterforsking, avsløring og rettslig forfølging av straffbare handlinger (…)*».

Rekkevidden av unntaket i artikkel 15 er tolket i flere avgjørelser fra EU-domstolen, se ovenfor under kapittel 5. I *La Quadrature du Net* ble det presisert at generell og udifferensiert lagring av IP-adresser, kun vil være tillatt når dette er begrunnet i bekjempelse av *alvorlig kriminalitet*, i tillegg til beskyttelse av nasjonal sikkerhet og alvorlige trusler mot den offentlige sikkerhet. Departementet legger til grunn at ekomlovens regler om lagring og utlevering skal utformes i samsvar med dette, slik at lagring og utlevering av informasjon om IP-adresser til politiet og påtalemyndigheten i forbindelse med kriminalitetsbekjempelse bare kan rettferdiggjøres dersom formålet er å bekjempe alvorlig kriminalitet.

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 domstolens praksis liten veiledning med hensyn til hva som regnes som «alvorlig kriminalitet» i EØS-rettens forstand eller hvilke kriterier som skal tas i betraktning ved vurderingen av et lovbrudds alvorlighet. EU-domstolen har imidlertid flere ganger uttalt at kravet om at alvorlig inngrep i grunnleggende rettigheter bare kan rettferdiggjøres dersom formålet er å bekjempe «alvorlig kriminalitet», er et utslag av det generelle kravet om proporsjonalitet, se bl.a. *La Quadrature du Net* avsnitt 131 med videre henvisninger til *Ministerio Fiscal* avsnitt 55 følgende. Etter departementets vurdering er det derfor noe usikkert om det finnes én enhetlig terskel for alvorlig kriminalitet som må legges til grunn uavhengig av hva slags inngrep det er snakk om.

Det finnes heller ingen entydig definisjon av hva som skal betegnes som «alvorlig kriminalitet» i norsk rett eller i annen internasjonal sammenheng. Spørsmålet ble imidlertid vurdert i Prop. 49 L (2010–2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) kapittel 12.6 side 103 følgende. Vurderingen av hva som skulle defineres som alvorlig kriminalitet ble i proposisjonen ikke ansett relevant for abonnementsopplysninger, herunder elektronisk kommunikasjonsadresse, ettersom slike opplysninger gjennomgående ville være å anse som mindre beskyttelsesverdige opplysninger enn andre trafikkdata og lokaliseringsdata. For abonnementsopplysninger ble det heller ikke foreslått materielle vilkår for utlevering. For utlevering av historiske, personspesifikke trafikkdata ble det imidlertid foreslått at kun straffebestemmelser med en strafferamme på fengsel i fire år eller mer, kunne begrunne utlevering av data. Det ble foreslått nærmere bestemte unntak fra strafferammekravet for sakstyper det ville være særlig vanskelig å etterforske uten tilgang til disse dataene.

Lagringsplikten som nå er foreslått er mindre inngripende enn forslaget om gjennomføring av datalagringsdirektivet i norsk rett, noe som kan tale for at lagring kan tillates også for straffbare forhold med en lavere strafferamme.

I høringsnotatet ble det foreslått en strafferamme på ett eller to års fengsel, eventuelt i kombinasjon med unntak for spesifikke straffebud. På bakgrunn av innspill i høringsrunden og av hen-

syn til kommunikasjonsvernet har departementet kommet til at bestemmelsen bør ta utgangspunkt i en høyere strafferamme enn foreslått i høringsnotatet. Denne vurderingen er også basert på at departementet nå går inn for en lagringstid på 12 måneder, som var det lengste av de alternativene som var foreslått i høringsnotatet.

Ved ikrafttredelsen av den nye straffeloven ble antallet strafferammer redusert sammenlignet med straffeloven 1902. Straffeloven 2005 inneholder ikke straffebud med strafferamme på fire år, slik at terskelen for utlevering for alvorlig kriminalitet bør settes til enten fengsel i inntil tre år eller fengsel i inntil seks år. Dersom det stilles krav om at lovbruddet kan straffes med fengsel i inntil seks år for at opplysningene kan utleveres, vil svært mange straffebud der utlevering av IP-adresser er av betydning, falle utenfor, og det ville være behov for en rekke unntak for å sikre at tiltaket oppnår hensikten. Et krav om seks års strafferamme ville etter departementets vurdering også være for høyt i lys av at inngrepets alvor, jf. kapittel 8.2.4.

Departementet har derfor falt ned på at vilkåret for utlevering bør ta utgangspunkt i handlinger som etter loven kan medføre straff av fengsel i tre år eller mer. Strafferammekravet innebærer at saken må inkludere minst én handling som alene kan straffes med fengsel i tre år eller mer, og at bestemmelsen også omfatter straffebud som åpner for fengsel i «inntil» tre år. En slik strafferamme vil etter departementets mening tydeligere markere at lagring og utlevering av IP-adresser skal begrenses til bekjempelse av alvorlig kriminalitet.

Med en strafferamme på tre år vil det i noe større utstrekning enn foreslått i høringsnotatet, være nødvendig at det også åpnes for utlevering av IP-adresser i saker som gjelder straffebud med lavere strafferamme. Selv om strafferammen gir et godt utgangspunkt for vurderingen av hvor alvorlig myndighetene anser et lovbrudd for å være, kan enkelte handlinger som ikke medfører lange fengselsstraffer, like fullt være svært alvorlige for de som rammes av dem. Særskilt gjelder dette seksuelle overgrep mot barn, der flere straffebud har en lavere strafferamme enn fengsel i inntil tre år. Det vises her til at formålet med forslaget var å gi politiet tilstrekkelige virkemidler i kriminalitetsbekjempelsen, særskilt når det gjelder overgrep mot barn.

Videre viser departementet til den positive forpliktelsen til å sikre respekt for privatlivet, jf. EMK artikkel 8, slik denne er forstått av EMD i dommen *K.U. mot Finland,* der finske myndigheter ble dømt for ikke å ha effektive etterforskingsmidler når det gjaldt å beskytte barns privatliv på internett i en sak hvor en person hadde stjålet et barns identitet og laget en kontaktannonse i barnets navn. Da saken ble anmeldt, anmodet politiet om å få utlevert den dynamiske IP-adressen som var benyttet, noe som ikke lot seg gjøre på grunn av lovbestemt taushetsplikt. Forpliktelsen skjerpes når det er barn involvert. Tilsvarende forpliktelse til effektiv bekjempelse av straffbare handlinger kan utledes av *La Quadrature du Net* avsnitt 126, som særskilt viser til bekjempelse av straffbare handlinger som gjelder mindreårige og andre sårbare personer. Endelig vises det til Barnekonvensjonen artikkel 19, der det heter at myndighetene skal treffe «alle egnede lovgivningsmessige, administrative, sosiale og opplæringsmessige tiltak for å beskytte barnet mot alle former for (…) vold (…) herunder seksuelt misbruk (…)».

At det er rom for å legge vekt på at IP-adressen kan være det eneste bevismiddel som kan gjøre det mulig å identifisere gjerningspersonen, støttes av *La Quadrature du Net*-dommen avsnitt 154, der det fremgår at det i avveiningen av de rettigheter og interesser som gjør seg gjeldende, også skal tas hensyn til slike omstendigheter. Saker om overgrep mot barn på nettet er her særskilt nevnt.

Etter departementets syn er det grunn til å inkludere andre straffebud med strafferamme under tre år, når tilgang til IP-adresser kan være av avgjørende betydning for etterforskingen av kriminalitet som gjelder seksuelt misbruk av barn. Departementet mener også at det bør kunne gjøres unntak for straffebud der IP-adressen er av helt avgjørende betydning for muligheten til å oppklare lovbruddet. Når det gjelder andre forhold med en lavere strafferamme enn tre år, viser departementet til at bestemmelser om grov kriminalitet i straffeloven gjennomgående har en strafferamme på over tre år. Grovt heleri, grovt bedrageri og grov hvitvasking straffes for eksempel med fengsel i inntil seks år, slik at denne typen lovbrudd vil omfattes dersom de kvalifiserer til å anses som grove overtredelser.

Departementet foreslår etter dette at følgende bestemmelser i føyes til i angivelsen av hvilke straffbare forhold som anses som alvorlig kriminalitet, og som skal omfattes av utleveringsplikten:

Straffeloven § 125 (Uaktsom avsløring av statshemmeligheter), § 168 (Brudd på oppholds- og kontaktforbud eller beslutning om båndlegging), § 184 (Krenkelse av representasjonen til en fremmed stat eller mellomstatlig organisasjon), § 201

(Uberettiget befatning med tilgangsdata, dataprogram mv.), § 202 (Identitetskrenkelse), § 204 (Innbrudd i datasystem), § 205 (Krenkelse av retten til privat kommunikasjon), § 251 (Tvang), § 263 (Trusler), § 266 (Hensynsløs atferd), § 297 (Seksuell handling uten samtykke), § 298 (Seksuelt krenkende atferd offentlig eller uten samtykke), § 305 (Seksuelt krenkende atferd mv. overfor barn under 16 år), § 306 (Avtale om møte for å begå seksuelt overgrep) og § 309 (Kjøp av seksuelle tjenester fra mindreårige), samt åndsverkloven § 104, jf. § 79 (Retten til eget bilde).

8.5.4.2 Forebygging og andre deler av politiets virksomhet

Som nevnt ovenfor legger kommunikasjonsverndirektivet artikkel 15 til grunn at inngrep i kommunikasjonsvernet begrunnet i kriminalitetsbekjempelse også kan omfatte forebygging av kriminalitet. I høringsnotatet ble det vist til at dersom en handling kan forebygges før den inntreffer ved hjelp av informasjon om hvem en IP-adresse tilhører, bør politiet kunne innhente denne informasjonen i samme omfang som opplysningene kan innhentes til etterforsking. Det ble vist til andre bestemmelser som åpner for utlevering av opplysninger til politiet, der forebygging og etterforsking er sidestilt. Departementene ba om høringsinstansenes syn på om det burde åpnes for utlevering til forebygging. Høringsinnspillene fra politiet, herunder særskilt fra PST og ØKOKRIM, peker på at det er et behov for opplysninger som lagres etter den nye bestemmelsen også i forebyggingsøyemed. ØKOKRIM har vist til internasjonale forpliktelser om forebygging av hvitvasking og terrorfinansiering, mens PST blant annet har vist til at de har metodetilgang i sin forebyggende virksomhet og at tilgang til IP-data i forebyggende øyemed derfor vil gi best sammenheng i regelverket.

Enkelte av høringsinstansene, særlig Advokatforeningen og Datatilsynet, er kritiske til å åpne for utlevering i forebyggingsøyemed, blant annet fordi det i slike tilfeller vil være vanskeligere å kontrollere det reelle behovet. Det anføres at det må oppstilles et krav om at politiet må ha klare holdepunkter for å tro at opplysningene er nødvendige for å forbygge handlingen, før de kan begjæres utlevert. Endelig er det pekt på at det er vanskelig å definere hva som ligger i begrepet forebygging, og at dette derfor er lite egnet som et vilkår for utlevering.

Departementet har vurdert de ulike hensynene som gjør seg gjeldende.

Når det gjelder forebygging, er det mer uklart om det bør være adgang til utlevering av IP-data enn ved etterforsking, blant annet fordi forebygging er et vidt begrep som omfatter en rekke ulike situasjoner og virkemidler. Utlevering av IP-data til forebygging kan medføre særlige utfordringer for person- og kommunikasjonsvernet, fordi det ved utlevering til forebyggingsformål vil være mer uklart hva som skal til for at politiet kan anmode om utlevering av opplysninger. Skadepotensialet kan likevel være så stort at det i noen tilfeller, av hensyn til samfunnet, må anses som proporsjonalt å gi tilgang til slike data for å forebygge alvorlige hendelser. Departementet understreker viktigheten av å kunne forebygge kriminalitet der det er mulig, med de fordeler det har både for fornærmede og samfunnet for øvrig.

Departementet mener likevel, i lys av høringsinnspillene, at tilgang til IP-data i forebyggingsøyemed bør utredes nærmere før det eventuelt åpnes for dette, og eventuelt vurderes tilgang for enkelte typer saker, f.eks. for PST. Åpning for tilgang i forebyggingsøyemed forutsetter også at det utredes tydelige og gode rammer, sett hen til det inngrepet tiltaket har for person- og kommunikasjonsvernet, slik at person- og kommunikasjonsvernet ivaretas. Departementet vil derfor komme tilbake til spørsmålet på et senere tidspunkt.

Det foreslås etter dette ikke å åpne for utlevering av opplysninger lagret i medhold av § 2-8 a til forebyggingsøyemed på det nåværende tidspunkt. Det understrekes imidlertid at lovforslaget ikke begrenser mulighetene til å innhente informasjon i forebyggende øyemed på annet grunnlag. Dette inkluderer utlevering av opplysninger som tilbyderne har lagret til egne formål, jf. ekomloven § 2-9.

Departementet har videre merket seg innspillene om at opplysningene også bør kunne utleveres ved behov innenfor redningsarbeid eller søk etter savnede personer, men foreslår ikke å ta dette inn i bestemmelsen. Det vises imidlertid til at opplysningene etter omstendighetene vil kunne utleveres til politiet med hjemmel i nødrett, eller etter § 2-9.

8.5.4.3 Nødvendighetskravet

Inngrep i kommunikasjonsvernet må være nødvendig for at inngrepet skal være lovlig. Dette kan utledes direkte av kommunikasjonsverndirektivet artikkel 15, samt av proporsjonalitetskravet som må være oppfylt for at et inngrep i privatlivet skal være lovlig etter EMK artikkel 8 nr. 2. Departementet foreslår at bestemmelsene om utlevering utformes slik at det er et krav at utlevering av

informasjon må være nødvendig for etterforsking av nærmere angitte former for kriminalitet, jf. forslaget til endringer i § 2-8 b.

Enkelte av høringsinstansene har pekt på at nødvendighetskravet gir liten veiledning for hva som skal kunne utleveres.

Departementet viser til at det i høringsnotatet ble presisert at nødvendighetskravet innebærer at det må foretas en konkret vurdering av behovet for opplysningene, som må veies mot hensynet til kommunikasjonsvernet. Kravet innebærer at det ikke skal innhentes flere opplysninger enn det som er nødvendig for formålet. Vilkåret skal ikke tolkes så strengt at utlevering av opplysningene må være den eneste løsningen. På den andre siden vil det ikke være tilstrekkelig at opplysningene bare vil kunne lette arbeidet. Av proporsjonalitetskravet følger også at inngrepet i kommunikasjonsvernet må tas med i vurderingen. Dette kan innebære at vurderingen kan falle forskjellig ut avhengig av inngrepet i kommunikasjonsvernet i den enkelte sak.

Vurderingen av om nødvendighetsvilkåret er oppfylt gjøres av politiet og påtalemyndigheten, slik at ekomtilbyderne ikke må ta stilling til om vilkårene er oppfylt.

Departementet finner ikke grunn til å presisere nødvendighetskravet ytterligere i bestemmelsen, men viser til forslag til krav til utforming av anmodninger om utlevering nedenfor under kapittel 8.6.4.

8.5.4.4 Utlevering med bakgrunn i opplysninger om abonnent

I høringsnotatet ble det lagt til grunn at de foreslåtte bestemmelsene i første omgang vil være praktiske i situasjoner der politiet, med utgangspunkt i en gitt IP-adresse, ønsker å finne frem til en abonnent. Det kan imidlertid tenkes tilfeller der politiet med utgangspunkt i en gitt abonnent, har behov for informasjon om hvilke IP-adresser vedkommende er tildelt på et gitt tidspunkt eller i et gitt tidsrom.

Dette gjelder særlig der politiet har fått informasjon om en IP-adresse ved undersøkelse av datamateriale i en etterforsking rettet mot en bestemt mistenkt. Ved å innhente en oversikt over hvilke IP-adresser den mistenkte er tildelt i et aktuelt tidsrom, vil det kunne avdekkes om og i hvilken utstrekning de tildelte IP-adressene kan gjenfinnes i det materialet politiet allerede har tilgang til. Dette vil kunne være mer effektivt og ressursbesparende, samtidig som det også kan være viktig for å avkrefte mistanke som det viser seg ikke å være grunnlag for. Det understrekes at også slik innhenting må være nødvendig, og at det må foretas en konkret vurdering av behovet for opplysningene, jf. punktet ovenfor.

Enkelte høringsinstanser er skeptiske til innhenting av informasjon med utgangspunkt i abonnenten, da de mener forslaget åpner for at politiet ved å innhente alle IP-adresser knyttet til en person i et gitt tidsrom, kan få full oversikt over benyttede IP-adresser og dermed lage seg et bilde av personens bevegelser.

Til dette vil departementet påpeke at innhenting av informasjon med utgangspunkt i en abonnent ikke i seg selv vil gi politiet informasjon om hvem vedkommende har kommunisert med eller vedkommendes bevegelsesmønster i den gitte tidsperioden. Det vises her til redegjørelsen ovenfor i kapittel 8.2 om hva man kan utlede om enkeltpersoners bevegelsesmønster basert på informasjon om tildelte IP-adresser.

Uten ytterligere informasjon om nettaktivitet, som politiet må skaffe på annet vis, eksempelvis gjennom databeslag eller andre tvangsmidler, vil utlevering bare kunne gi informasjon om hvilke IP-adresser vedkommende er tildelt i perioden, og tidspunkt for bruken når det gis ut port-informasjon, jf. kapittel 8.2.

Sett hen til dette, samt at innhenting med utgangspunkt i en konkret abonnent vil kunne begrense mengden av opplysninger politiet har behov for å innhente for å bekrefte eller avkrefte en konkret mistanke i en sak, fastholder departementet at bestemmelsen også bør åpne for utlevering av IP-adresser med utgangspunkt i en gitt abonnent, på samme vilkår som for utlevering med utgangspunkt i en IP-adresse.

8.6 Prosessuelle krav og kontroll med utlevering av opplysninger

8.6.1 Gjeldende rett

Utlevering av informasjon om IP-adresser til politiet eller påtalemyndigheten er i dag regulert i ekomloven § 2-9 tredje og fjerde ledd, som det er redegjort for ovenfor i kapittel 8.5.1.

Utlevering av abonnementsopplysninger til påtalemyndigheten eller politiet etter denne bestemmelsen krever ikke at Nasjonal kommunikasjonsmyndighet fritar tilbyder fra taushetsplikten eller kjennelse fra retten, slik tilfellet er for andre trafikkdata.

8.6.2 Forslaget i høringsnotatet

I høringsnotatet foreslo departementene at gjeldende rett burde videreføres hva gjaldt krav til forhåndskontroll ved utlevering.

Departementene viste til at EMD i saken *Breyer mot Tyskland* la til grunn at det ved vurderingen av behovet for prosessuelle garantier, må sees hen til i hvilken grad lagringen av opplysninger griper inn i personvernet. Dersom lagringen er mindre inngripende, kan mer generelle regler om politiets og påtalemyndighetens 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. Departementene mente den foreslåtte lagringsplikten var av en slik art at det ikke ville være påkrevd med en uavhengig forhåndskontroll av hver enkelt utlevering. Departementene kunne heller ikke se at dette er et krav etter kommunikasjonsverndirektivet. Når det gjaldt de forholdsvis detaljerte kravene med hensyn til prosessuelle vilkår for utlevering som EU-domstolen oppstilte i *Tele 2*-avgjørelsen, pekte departementene på at disse ikke uten videre kunne 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. Informasjonen som blir tilgjengelig ved lagring av IP-adresser, kunne etter departementenes syn ikke betraktes som informasjon som ville gjøre det mulig å trekke presise slutninger om privatlivet til de det lagres informasjon om.

Høringsnotatet la til grunn at heller ikke *La Quadrature du Net*-avgjørelsen kunne forstås slik at det gjelder et krav om forhåndskontroll for utlevering av IP-adresser. Selv om domstolen uttalte at det må gjelde strenge vilkår og garantier vedrørende bruk av IP-adresser, jf. avsnitt 156, ble det ikke slått fast at det var påkrevd med uavhengig forhåndsgodkjenning av den enkelte utlevering.

Departementene pekte i høringsnotatet videre på at politiets og påtalemyndighetens behandling av opplysninger til politimessige formål er regulert 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 at det oppstilles krav til informasjonssikkerhet og internkontroll. Regelverket etablerer på samme måte som personvernforordningen, flere mekanismer som ivaretar den registrertes rettigheter, herunder mulighet til å be om innsyn, klageadgang og uavhengig tilsyn fra EOS-utvalget og Datatilsynet for henholdsvis PST og politiet og påtalemyndigheten for øvrig.

Etter departementenes vurdering var 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 ble ansett dekkende. Det ble vist til at opplysninger etter politiregisterloven § 50 ikke skal lagres lenger enn det som er nødvendig for formålet med behandlingen. Opplysninger som er innhentet utenfor straffesak, vil 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.

8.6.3 Høringsinstansenes syn

Også når det gjelder behovet for prosessuelle garantier og kontrollmekanismer, er høringsinstansene delt i hvordan de ulike hensyn som gjør seg gjeldende, bør vektlegges.

For ekombransjens del fremgår det samlet sett av høringsuttalelsene at det er et sentralt poeng at vurderinger av om vilkårene for utlevering er oppfylt i minst mulig grad overlates til dem. I den forbindelse er det fremhevet at prosedyren for å fremsette anmodninger i større grad bør være standardisert, slik at det bl.a. fremgår hva som er hjemmelsgrunnlaget for anmodningen.

Altibox viser til at bransjen ønsker å hjelpe politiet, men at det er viktig å sikre at sentrale elementer, som sørger for at kundenes personvern og interesser ivaretas på en sikker måte, er på plass. Det bør fastsettes materielle og prosessuelle vilkår som rammer inn vilkårene for utlevering. For å gjøre det enkelt for tilbyderne å etterleve plikten til å utlevere opplysninger, bør det foreligge klare,

systematiske krav til utleverings-begjæringene. Tilbyderne bør ikke pålegges å ta nærmere stilling til det materielle grunnlaget for en utleveringsbegjæring, men må ha trygghet for at vurderingene som politi og påtalemyndighet gjør, er grundige og har tilstrekkelig hjemmel.

GlobalConnect er positive til at departementene presiserer at ansvaret for å vurdere om vilkårene for utlevering er oppfylt ligger hos myndighetene, slik at tilbyderne ikke skal foreta noen selvstendig vurdering av dette. I dag krever politi og påtalemyndighet tilgang til data på ulike måter og i ulike format, noe som både er ressurskrevende og skaper unødvendig usikkerhet. GlobalConnect oppfordrer derfor departementene til å stille krav om at politi og påtalemyndighet etablerer en standard prosess, eksempelvis ved at det utvikles et standardisert anmodningsskjema for forespørsler om utlevering av IP-adresser. Dette antas også å ville styrke rettssikkerheten og redusere antall uberettigete anmodninger.

Telenor mener påtalemyndigheten må påvise en klar hjemmel for uthenting, eksempelvis gjennom en anmodningsverifikasjon fra påtalemyndigheten som også gir informasjon om hjemmelen for anmodningen. Generelt vil Telenor minne om at lovmessige utvidelser som gir myndighetene økte muligheter for innsyn, bør følges opp med transparens omkring faktisk bruk av disse.

Telia mener det må etableres entydige krav til form og innhold i et pålegg om å utlevere opplysninger. Det er politiet som må bære det fulle ansvaret for ikke å fremme begjæringer om utlevering når vilkårene ikke er oppfylt, slik at tilbyderne ikke skal måtte ta nærmere stilling til det materielle grunnlaget for en begjæring. For tilbyderne er det viktig å kunne stole på at vurderingene som politi og påtalemyndighet gjør, herunder av nødvendigheten, er grundige, og at det ikke begjæres utlevering uten tilstrekkelig hjemmel.

Tekna er skeptiske til at departementene ikke legger opp til domstolsbehandling.

IKT-Norge viser til at det, på grunn av det sterke inngrepet i kommunikasjonsvernet som forslaget representerer, er viktig at det fastsettes materielle og prosessuelle vilkår for utlevering som tydelig rammer inn ordningen og forhindrer formålsutglidning og misbruk. Det innebærer at utleveringsbegjæringer må være berettigede og kun må finne sted i saker som dreier seg om alvorlig kriminalitet.

Det er også av betydning å klargjøre forholdet mellom opplysninger som eventuelt vil omfattes av dagens terskel i ekomloven § 2-9, og hvilke opplysninger som vil omfattes av forslagets § 2-8 b, som setter nye skranker for utlevering. I praksis fremstår rammene for når det kan være aktuelt å begjære utlevering som vide. Dersom forslaget vedtas vil det være viktig at det føres effektivt tilsyn for å sikre at nødvendighetsvurderingen er reell, og at hensynet til kommunikasjonsvernet er tilstrekkelig hensyntatt for den enkelte begjæring. Det er også viktig at tilbyderne ikke settes i en situasjon hvor de må ta nærmere stilling til det materielle grunnlaget for en utleveringsbegjæring.

Enkelte av høringsinstansene, herunder *Datatilsynet og NIM*, mener at kommunikasjonsverndirektivet og EMK stiller krav om strengere kontrollmekanismer enn det det som er foreslått i høringsnotatet.

Datatilsynet viser til at IP-opplysninger er personopplysninger, og at det vil være tilbyders ansvar å påse at det ikke utleveres opplysninger i strid med personvernforordningen. Datatilsynet mener forslaget til § 2-8 a er i strid med kommunikasjonsvernet og de siste EU-dommene, spesielt *La Quadrature du Net*, og viser til at det går et tydelig skille mellom der hvor IP-adressen er knyttet til et navn og tidspunkt, og der hvor IP-adressen kun knyttes til et navn og ikke sier noe om når kommunikasjonen har foregått. Det er anført at når en IP-adresse knyttes til både et navn og et tidspunkt, vil de lagrede dataene kunne inneholde opplysninger som kan knytte en person både til nettaktivitet, og til hvor en person befinner seg. EU-domstolen krever da forhåndskontroll for utlevering, i motsetning til der hvor bare navn og IP-adresse registreres.

Norges institusjon for menneskerettigheter (NIM) viser til at i saker hvor myndighetene tillates å innhente opplysninger som angår borgernes privatliv uten at borgerne får kjennskap til innsamlingen, har EMD i sin praksis innfortolket et krav til effektiv og uavhengig kontroll for å hindre myndighetsmisbruk, og at denne kontrollen bør ligge til den dømmende virksomhet i saker om skjult overvåking. Tilsvarende doktriner er utviklet for saker om bulkinnsamling av data. Hvilke krav til rettsikkerhetsmekanismer som vil måtte oppstilles for masselagring av IP-adresser vil til en viss grad bero på hvor inngripende et slikt tiltak anses å være. Etter NIMs syn er lagring og utlevering av IP-adresser til politiet et betydelig inngrep i retten til privatliv (personvernet) som tilsier mer omfattende og effektive garantier mot misbruk og vilkårlighet, enn det som foreslås i høringsnotatet. Det er pekt på at dersom lagringen gir politiet mulighet til å få informasjon om

den enkeltes bevegelser eller informasjon om hvem den enkelte har samhandlet med over internett, bør utlevering antakelig forhåndsgodkjennes av en uavhengig myndighet for å oppfylle kravet etter EMK artikkel 8. Under enhver omstendighet må rettsikkerhetsmekanismene i forslaget styrkes betydelig for å ivareta prosessuelle krav etter denne bestemmelsen.

Elektronisk Forpost stiller seg svært skeptisk til at det ikke er stilt krav om domstolkontroll med utlevering av abonnementsopplysninger til påtalemyndigheten og politiet, eller plikt til at Nkom fritar tilbyder fra taushetsplikten.

Advokatforeningen viser til at forslaget ikke inneholder noen konkrete angivelser av hva som kreves med tanke på nødvendighetsvurderingen, og at det legges til grunn at politi- og påtalemyndighet kan be om utlevering uten at utleveringskravet skal kunne overprøves.

NRK viser til at forslaget ikke oppfyller de prosessuelle skrankene som stilles i *La Quadrature du Net*, og at det ikke foreligger tilstrekkelige sikkerhetsmekanismer for å hindre misbruk når det ikke er lagt opp til domstolskontroll eller lignende uavhengig forhåndskontroll. Lovforslaget har ingen sikkerhetsmekanismer for å ivareta kildevernet.

Høringsinstansene fra politiet og påtalemyndigheten mener på den andre siden at forhåndskontroll ikke er nødvendig, sett hen til opplysningenes lite sensitive karakter. Disse peker også på at politiregisterlovens regler og eksisterende tilsynsmekanismer er tilstrekkelige for å ivareta kravet til kontroll med behandlingen av opplysningene etter at de er innhentet.

Det nasjonale statsadvokatembetet mener ikke det er nødvendig med domstolskontroll eller godkjennelse fra annet offentlig organ. Dette er også ordningen i de øvrige nordiske land, med unntak av Danmark.

Politidirektoratet mener gjeldende rett, der det ikke kreves rettens kjennelse eller fritak fra taushetsplikten fra Nkom for utlevering av abonnementsopplysninger til politi og påtalemyndighet, bør videreføres. Reglene i politiregisterloven med forskrift, må videre anses dekkende hva gjelder behandlingen av innhentede opplysninger.

PST mener heller ikke at utlevering bør forutsette rettens kjennelse eller uavhengige forhåndsgodkjennelse. Politiet og påtalemyndighetens behandling av opplysningene er underlagt politiregisterloven, som oppstiller tilstrekkelige mekanismer for å ivareta den registrertes rettigheter. PST er i tillegg underlagt jevnlig kontroll av EOS-utvalget.

Stine Sofies Stiftelse støtter departementenes vurdering av at det ikke bør være nødvendig med domstolskontroll eller forhåndsgodkjenning, da dette vil kunne trenere etterforskningen.

8.6.4 Departementets vurdering

Departementet vil innledningsvis peke på at abonnementsopplysninger og opplysninger om IP-adresser, som dette lovforslaget gjelder, normalt er å anse som mindre sensitive opplysninger enn andre former for trafikkdata, og lokaliseringsdata. Lagring og utlevering av slike opplysninger vil således utgjøre et mer beskjedent inngrep i personvernet enn utlevering av andre typer data. Dette er nærmere omtalt ovenfor.

At opplysningenes karakter og graden av inngrep i personvernet er sentralt også ved vurderingen av hvilke krav som må stilles til kontroll etter EMK, kan blant annet utledes av *Breyer mot Tyskland*, avsnitt 103 følgende. Saken 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 hadde behov for opplysningene for egne formål. Det ble i dommen vist til at tilgangen til mekanismer for kontroll og tilsyn ville inngå i proporsjonalitetsvurderingen. Dersom datalagringen er mindre inngripende, vil kravet til prosessuelle garantier være lavere. Selv om det i det aktuelle tilfellet ikke var et krav om forhåndskontroll for utlevering, ble det, blant annet under henvisning til datatilsynsmyndighetens kontroll med opplysningen i etterkant, lagt til grunn at mekanismene for tilsyn og kontroll var tilstrekkelige. Lagring av IP-adresser og tilhørende portnummer, slik departementet foreslår, er imidlertid noe mer inngripende enn registrering av informasjon som kun identifiserer abonnenten. Det er likevel verdt å merke seg at tilsvarende differensiering på bakgrunn av opplysningenes karakter og inngrep i personvernet ble lagt til grunn i Prop. 49 L (2010–2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett). Under henvisning til opplysningenes karakter, ble det der ikke ansett nødvendig med endringer i ekomloven § 2-9 tredje ledd for så vidt gjaldt prosessuelle krav for utlevering av IP-adresser og abonnementsopplysninger. For de øvrige opplysningene som var omfattet av direktivet, ble dette vurdert annerledes, slik at utlevering av data i etterforskingsøyemed ville kreve rettens kjennelse. Mengden av IP- informasjon som leg-

ges igjen i 2021 er imidlertid større for den enkelte abonnent enn i 2010, noe som også vil spille inn i proporsjonalitetsvurderingene.

I enkelte av høringsuttalelsene til nærværende lovforslag er det, under henvisning til *Tele2*-dommen fra 2016 og *La Quadrature du Net*-dommen fra 2020 – anført at det gjelder et krav om forhåndskontroll også for utlevering av opplysninger om IP-adresser og abonnementsopplysninger. Disse høringsinstansene mener imidlertid at opplysningene griper inn i personvernet i større grad enn hva departementene la til grunn i høringsnotatet. Det er anført at en IP-adresse, når denne knyttes til både et navn og et tidspunkt, vil inneholde opplysninger som også kan gi politiet mulighet til å få informasjon om den enkeltes bevegelser. For en nærmere beskrivelse av hvilken informasjon som blir tilgjengelig ved slik lagring som omfattes av forslaget, viser departementet til redegjørelsen ovenfor i kapittel 8.2. Forslaget er derfor etter departementets syn mindre inngripende enn hva disse høringsinstansene har lagt til grunn.

Departementet har likevel vurdert i hvilken grad det i EU-domstolens praksis oppstilles krav som nødvendiggjør innstramminger og skjerpet kontroll med utlevering av IP-adresser, etter forslaget her. I *Tele2* la domstolen til grunn forholdsvis detaljerte krav til forhåndskontroll med utlevering av trafikk- og lokasjonsdata. Departementet mener at disse kravene ikke uten videre kan overføres til utlevering av IP-adresser. Selv om abonnementsdata inngår i begrepet trafikk-data, var det sentralt i *Tele 2*-avgjørelsen at lagringen gjorde det mulig å trekke presise slutninger om privatlivet til de det ble lagret informasjon om. Informasjonen som tilgjengeliggjøres gjennom utlevering av IP-adresser etter forslaget her, kan etter departementets syn ikke betraktes som informasjon som gjør slike presise slutninger mulig i særlig grad. I *La Quadrature du Net* uttalte EU-domstolen at IP-adresser er en kategori av data som er mindre sensitiv enn andre former for trafikkdata, jf. avsnitt 152. Det må likevel gjelde strenge vilkår og garantier også 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. Dette er for øvrig i samsvar med den differensiering som gjøres i proporsjonalitetsvurderingen etter EMK basert på hvor inngripende tiltaket er, slik utledet blant annet av *Breyer mot Tyskland*.

EU-domstolen i storkammer avsa 2. mars 2021 avgjørelse i sak C-746/*18 H.K. v Prokuratuur,* som gjaldt tilgang til trafikk- og lokasjonsdata til bruk for kriminalitetsbekjempende formål. Det er redegjort for dommen i kapittel 5.3. Domstolen gjennomgikk her de betingelser som må oppstilles for at offentlige myndigheter skal få tilgang til trafikk- og lokasjonsdata, se avsnitt 48 følgende. Videre uttaler domstolen at med henblikk på å sikre etterlevelse av disse betingelsene i praksis, er det avgjørende at de kompetente nasjonale myndigheters adgang til de lagrede data er undergitt en forutgående kontroll, som foretas enten av en domstol eller av en uavhengig administrativ enhet, jf. avsnitt 51. Disse uttalelsene er knyttet til lokasjons- og trafikkdata generelt, og således til informasjon som gjør det mulig å trekke presise slutninger om privatlivet til de det ble lagret informasjon om. IP-data nevnes ikke særskilt i dommen, selv om dommens henvisning i punkt 4 til definisjonene i 2002/58-direktivet, klargjør at abonnentsdata indirekte er omfattet.

I lys av det skillet som oppstilles i *La Quadrature du Net*, der IP-data omtales som en kategori av data som er mindre følsomme enn andre former for trafikkdata, og i lys av at forslaget her ikke kan sies å muliggjøre presise slutninger om folks privatliv, finner departementet ikke at det nå er nødvendig å innføre et generelt krav om forhåndskontroll for utlevering av IP-adresser på grunnlag av EU-domstolens praksis. Departementet vil komme tilbake til spørsmålet dersom fremtidig utvikling skulle tilsi noe annet.

Ved vurderingen av prosessuelle krav, har departementet også vurdert hvorvidt det bør stilles strengere krav til utforming av anmodninger om utlevering av IP-adresser, eksempelvis ved formelle krav som sikrer at det foretas en konkret nødvendighetsvurdering og som dermed ivaretar at hensynet til kommunikasjonsvernet blir vurdert i forkant av den enkelte begjæring. Flere av høringsinstansene har påpekt at det er behov for et mer ensartet system for fremsettelse av anmodningene.

Departementet er enig i at det er hensiktsmessig både for politiet og tilbyderne at anmodninger fremmes på en mer ensartet måte. Departementet har videre kommet til at det kan være grunn til å stille noe strengere krav til utforming av anmodningene, blant annet for å sikre at vilkårene for utlevering blir tilstrekkelig vurdert. Når terskelen for å kunne be om opplysninger heves, vil behovet for klarere regler og notoritet for hjemmelsgrunnlag dessuten være større sammenlignet med tidligere regler. Slike formalkrav vil også kunne understøtte mekanismene for tilsyn og kontroll med behandlingen av opplysningene i etterkant.

I endelig utforming av ny § 2-8 b er dette hensyntatt ved at det er presisert at anmodning om

utlevering av opplysninger om hvilken abonnent som er tildelt en gitt IP-adresse skal fremsettes skriftlig. Det skal så vidt mulig opplyses om hva saken gjelder, hva som er formålet med utleveringen og hva anmodningen omfatter. Videre skal det også fremgå at nødvendigheten av anmodningen er vurdert.

Begrensningen «så vidt mulig» tar høyde for at det i enkelte tilfeller ikke vil kunne gis fullstendige opplysninger, for eksempel av etterforskingshensyn eller fordi opplysningene er graderte. For PST, som behandler informasjon som i all hovedsak er gradert etter sikkerhetsloven, vil formålet med anmodningen ofte måtte gis på et overordnet nivå, for eksempel hvilken av PSTs oppgaver etter politiloven anmodningen knytter seg til.

Det presiseres at formalkravene ikke innebærer at tilbyderne i større grad skal foreta egne materielle vurderinger av anmodningene. De vil imidlertid kunne foreta en kontroll av formalia, slik at det vil kunne bes om supplerende informasjon dersom en anmodning er vanskelig å etterkomme på grunn av mangelfulle opplysninger. Hensikten med å introdusere slike formalkrav er blant annet også å unngå at det fremsettes anmodninger som er unødvendige. Etter departementets syn må det for øvrig ved vurderingen av krav til vilkår og garantier for bruk, som det er henvist til *La Quadrature du Net*-dommen avsnitt 156, også ses hen til kravene til behandlingen av opplysningene etter at de er utlevert, herunder mekanismene for tilsyn og kontroll.

Som det ble omtalt i høringsnotatet, er politiet og påtalemyndighetens behandling av opplysninger regulert i politiregisterloven med tilhørende forskrift. Dette regelverket inneholder en rekke krav til politiets og påtalemyndighetens behandling av opplysninger for å hindre misbruk og ivareta den registrertes rettigheter.

Et viktig prinsipp er at opplysninger ikke skal lagres lenger enn det som er nødvendig for formålet med behandlingen, jf. politiregisterloven § 50. 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 vil følge de alminnelige reglene for behandling av disse. I tillegg stiller lovens § 17 krav om at bruk av opplysninger skal kunne spores. Sporbarhet er et viktig kontrollerende tiltak for å sikre at reglene i loven overholdes.

Politiets behandling av opplysninger er underlagt Datatilsynets tilsynskompetanse, jf. lovens § 58. Tilsynskompetansen omfatter all behandling av opplysninger i politiet og påtalemyndigheten, herunder behandling av opplysninger i den enkelte straffesak. For PST er det EOS-utvalget som er tilsynsmyndighet. Datatilsynet kan føre tilsyn av eget tiltak, og skal også 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. Tilsynet kan uten hinder av taushetsplikt kreve utlevert de opplysninger som er nødvendige for å gjennomføre kontrollen. Datatilsynets virkemidler dersom det avdekkes behandling i strid med regelverket er nærmere regulert i § 60. Tilsynet kan blant annet gi pålegg om at behandling i strid med reglene om informasjonssikkerhet og internkontroll skal opphøre. Datatilsynet kan også fastsette tvangsmulkt for å sikre oppfølging av ilagte pålegg.

I tillegg til den sentrale kontrollmekanismen uavhengig kontroll fra tilsynsorganet utgjør, vil den registrerte også kunne be om innsyn i opplysninger om seg selv, jf. politiregisterloven § 49 andre 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.

Departementet opprettholder på denne bakgrunn vurderingen fra høringsnotatet om at det ikke er behov for særskilte regler om behandling av innhentede opplysninger etter den nye bestemmelsen. Det legges til grunn at de alminnelige reglene i politiregisterlovgivningen er tilstrekkelige for å sikre kontrollen med behandlingen av opplysningene etter at de er utlevert til politiet.

I forslaget til ny § 2-8 b i ekomloven er det for øvrig lagt til grunn at det skal kunne gis forskrift om utlevering av data etter første ledd. Tilbyderens håndtering av anmodninger, vil ved behov kunne reguleres i denne forskriften.

Departementet vil også vurdere om det kan være hensiktsmessig å benytte felles digitale løsninger for fremsendelse og mottak av anmodninger, samt om det bør utarbeides et fast skjema som nærmere angir vilkårene for utleveringen. Et slikt system vil kunne gi grunnlag for å ta ut en systematisk oversikt over bruken, som vil kunne sendes Nasjonal kommunikasjonsmyndighet som tilsynsmyndighet etter ekomloven. En systematisk oversikt over anmodninger vil også være nyttig for kunne vurdere om det på et senere tidspunkt, eksempelvis på bakgrunn av rettsutviklingen eller den teknologiske utviklingen, kan være nødvendig å etablere strengere rammer for tilsyn og kontroll.

8.7 Særlig om pressens kildevern

8.7.1 Gjeldende rett

Det gjelder ingen særregler om kildevern ved anmodning om opplysninger fra politiet eller påtalemyndigheten i dagens ekomlov. Straffeprosessloven og tvisteloven har imidlertid flere relevante bestemmelser om forklaringsfritak og beslagsforbud. I Justis- og beredskapsdepartementets høringsnotat 24. september 2018 *Forslag til endringer i kildevernreglene i straffeprosessloven og tvisteloven* er det redegjort slik for disse reglene:

> «Etter straffeprosessloven § 108 er hovedregelen at enhver som blir innkalt som vitne plikter å møte og forklare seg for retten, med mindre noe annet er bestemt ved lov. Tilsvarende plikt har enhver som kan ha noe å forklare i en sivil sak, jf. tvisteloven § 24-1 første ledd. For medarbeidere i massemedier gir likevel loven rett til å nekte å svare på spørsmål om «hvem som er forfatter til en artikkel eller melding i skriftet eller kilde for opplysninger i det», jf. straffeprosessloven § 125 første ledd første punktum og tvisteloven § 22-11 første ledd første punktum. Det samme gjelder spørsmål om «hvem som er kilde for andre opplysninger som er betrodd redaktøren til bruk i hans virksomhet», jf. § 125 første ledd annet punktum. Tvisteloven § 22-11 første ledd annet punktum inneholder en tilsvarende bestemmelse.
>
> Formålet med straffeprosessloven § 125 og tvisteloven § 22-11 er å legge til rette for at pressen kan ivareta det samfunnsmessige og demokratiske behovet for fri debatt og meningsdannelse, jf. Ot.prp. nr. 55 (1997–98) punkt 3.2.3 side 17.
>
> […]
>
> Kildevernet er ikke bare en rett til å nekte å svare på spørsmål, men innebærer også at det i utgangspunktet ikke er adgang til å ta beslag i eller pålegge utlevering av dokumenter eller annet, som har et innhold som pressen kan nekte å forklare seg om etter straffeprosessloven § 125, jf. straffeprosessloven § 204 første ledd første punktum og § 210 første ledd første punktum. Tilsvarende gjelder for bevistilgang i sivile saker, jf. tvisteloven § 26-7 annet ledd.
>
> Forklaringsfritaket og beslagsforbudet gjelder likevel ikke ubetinget. Retten kan på strenge vilkår gjøre unntak fra kildevernet og pålegge forklaringsplikt om hvem som er kilde. En pressemedarbeider kan dessuten ha plikt til å oppgi kilder på eget initiativ, særlig etter straffeloven § 196 (avvergingsplikt), § 226 (uriktig tiltale eller domfellelse) og § 287 (hjelpeplikt).»

Det vises også til kapittel 5.3 ovenfor om ytringsfriheten, herunder pressens kildevern.

8.7.2 Forslaget i høringsnotatet

I høringsnotatet ble det lagt til grunn at det ved vurderingen av om det bør innføres en plikt til lagring av IP-adresser, også må vurderes om en slik lagring ville kunne gripe inn i ytringsfriheten, herunder pressens kildevern. Det ble i denne sammenheng presisert at IP-lagring ikke dreier 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. En forutsetning for at lagrede IP-adresser skal kunne bidra til å identifisere en kilde, vil derfor være at de lagrede opplysningene kan 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 på andre måter enn fra den journalistiske virksomheten. Dette vil reglene om kildevern sette klare begrensninger for. Det ble videre vist til Justis- og beredskapsdepartementets høringsnotat omtalt ovenfor. Notatet gir en utførlig omtale av kildevernet etter straffeprosessloven og EMK.

Departementene pekte også på at en plikt til IP-lagring ville 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, eksempelvis i tilfeller der man har informasjon om hvilken IP-adresse som er benyttet i forbindelse med en anonym ytring på et nettsted. I den forbindelse ble det pekt på at informasjon om hvilken IP-adresse som er benyttet, dersom den finnes overhodet, ikke vil være noe som kan skaffes til veie uten videre, samt til at koblingen mellom en IP-adresse og abonnent, som lovforslaget åpner for, i seg selv sjelden vil muliggjøre en entydig identifikasjon av konkrete brukere. Avslutningsvis ble det vist til at forslaget uansett oppstiller vilkår som skal sikre at utlevering skal være nødvendig og forholdsmessig.

8.7.3 Høringsinstansenes syn

Advokatforeningen mener det er avklart gjennom Rt. 2010 s. 1381 *Runestein* at kildevernet kan være

til hinder for utlevering av IP-adresser. Det er ikke arten av informasjon, en IP-adresse, som er avgjørende, men om virkningen av utlevering er slik at vernet etter EMK artikkel 10 og Grunnloven § 100 trer inn. Det er viktig at det oppstilles slike prosessuelle krav at de som utsettes for dette, har anledning til overprøving.

Den internasjonale juristkommisjon – norsk avdeling (ICJ) mener at spørsmålet om lagring av IP-adresser kan ha en nedkjølende effekt på ytringsfriheten, ikke er vurdert i tilstrekkelig grad. Departementene peker på at individet ikke automatisk kan identifiseres, men det er nettopp det man ønsker ved en slik lagringsplikt; å identifisere personen bak IP-adressen.

Norges institusjon for menneskerettigheter (NIM) viser til at ytringsfriheten er beskyttet av Grunnloven § 100, EMK artikkel 10 og FNs konvensjon om sivile og politiske rettigheter artikkel 19, og at ethvert inngrep i ytringsfriheten må oppfylle de tre vilkårene for inngrep om lovhjemmel, formåls- og forholdsmessighet. Pressefriheten, herunder kildevernet, er en sentral del av ytringsfriheten, og nyter et særlig sterkt vern. EMD har slått fast at hvor det foreligger risiko for at en kilde kan bli identifisert, må myndighetene sørge for å ha på plass klare og presise regler for å sikre at identiteten til kilden ikke blir kompromittert.

NIM forstår forslaget slik at det etter omstendighetene vil kunne oppstå situasjoner hvor politiet kan anmode om å få utlevert informasjon om hvem en IP-adresse har kommunisert med. Et inngrep i kildevernet må vurderes helhetlig ut fra den negative virkningen et slikt inngrep vil ha i en bredere samfunnsmessig kontekst. Dersom potensielle kilder ikke har tilstrekkelig tillit til at deres anonymitet vil bli ivaretatt, vil det kunne svekke pressens kildetilfang generelt og gi en «nedkjølende effekt».

Norsk Journalistlag (NJ) viser til at anonyme kilders mulighet til å kommunisere fritt med pressen er en menneskerettighet etter EMK artikkel 10 om ytringsfrihet. Kildevernet er nødvendig for å få frem informasjon som ellers ville forblitt ukjent, og er derfor begrunnet i demokratihensynet. Begrunnelsen for kildevernet gjør seg også gjeldende ved bruk av tvangsmidler. Når departementene legger til grunn at det er «*lite praktisk at den lagrede informasjonen vil bidra til å muliggjøre kildeidentifikasjon»,* er det derfor en uholdbar påstand. NJ mener foreliggende forslag er problematisk for journalisters kildevern. Det må også settes fokus på hvilke konsekvenser det vil ha dersom den lagrede informasjonen kommer uvedkommende i hende. Når det gjelder informasjon som kan avsløre en anonym kilde, er det i henhold til EMK artikkel 10 påkrevd med en uavhengig kontrollinstans som skal vurdere dette. Kontrollen bør ifølge NJ gjennomføres av en domstol, jf. de krav som er oppstilt i *La Quadrature du Net*-dommen.

Norsk Presseforbund og *Norsk Redaktørforening* viser til at EU-domstolen i *La Quadrature du Net*-dommen påpeker at IP-adresser kan brukes til å «*track an Internet user's complete clickstream and, therefore, his or her entire online activity»,* og brukes til å gjenskape «*a detailed profile of the user*». Den foreslåtte lagringsplikten vil kunne inkludere all nettbruken til enkeltpersoner, og den vil i mange tilfeller gjøre at politiet enkelt vil kunne identifisere hvem vedkommende har kommunisert med. Sannsynligheten er dermed stor for at kilder kan identifiseres, i strid med kildevernet, slik dette er beskrevet i en rekke avgjørelser fra EMD gjennom deres tolkning av EMK artikkel 10. Det må også ses hen til nedkjølingseffekten tiltak som dette vil kunne få for kildevernet.

NRK mener det er viktig å merke seg at kildevernet ikke bare omfatter opplysninger som direkte kan føre til at kilden identifiseres, men også opplysninger som mer indirekte kan lede til slik identifisering. Usikkerhet om kildevernet vil i seg selv ha en nedkjølende effekt. Forslaget vil medføre at kildevernet, som allerede er under sterkt press, svekkes ytterligere. Dette er ikke betryggende eller tilstrekkelig utredet i høringsnotatet.

NRK bemerker at man ved vurderingen av i hvilken grad lagrings- og utleveringsplikten er i strid med kildevernet, må se hen til koblingen av den lagrede informasjonen mot annen informasjon, som myndighetene vil kunne få fra mange hold – ikke bare fra den journalistiske virksomheten. Eksempelvis lagrer nettbaserte meldingstjenester og sosiale medier i stor grad informasjon om IP-adresser. Det er også vist til at forslaget omfatter mer enn plikten til å lagre og utlevere abonnementsopplysninger knyttet til IP-adressene. Det er blant annet varslet at det kan bli nødvendig å lagre/utlevere informasjon om mottaker.

NRK viser til at slik lovforslaget nå foreligger, er det ingen sikkerhetsforanstaltninger for å ivareta kildevernet. Lovforslaget vil etter NRKs syn være i strid med EMK artikkel 10.

8.7.4 Departementets vurdering

Ved innføringen av en plikt til å lage IP-adresser må det, som påpekt i høringsnotatet, vurderes

hvordan en slik lagring vil kunne gripe inn i ytringsfriheten, herunder pressens kildevern.

Det følger blant annet av *La Quadrature du Net* avsnitt 114 at det ved tolkningen av hvilke inngrep som lovlig kan gjøres i kommunikasjonsvernet i medhold av direktivets artikkel 15, også må tas hensyn til retten til ytringsfrihet. Pressefriheten, herunder kildevernet, er et viktig element i ytringsfriheten og nyter et særskilt vern under EMK artikkel 10. Det vises her til *Goodwin*-avgjørelsen mot Storbritannia avsnitt 39 som er referert ovenfor. For at et inngrep i ytringsfriheten etter EMK artikkel 10 skal være lovlig, må det ha tilstrekkelig hjemmel, et legitimt formål samt være forholdsmessig. Statens skjønnsmargin er begrenset på dette området, og EMD foretar en inngående prøving av vilkårene etter artikkel 10 nr. 2, jf. dommen avsnitt 40.

Etter departementets syn er det tvilsomt om regler om IP-lagring i seg selv vil utgjøre et inngrep i ytringsfriheten etter EMK artikkel 10. Uansett vil de foreslåtte reglene om lagring vanskelig kunne anses å utgjøre et uproporsjonalt inngrep, først og fremst fordi opplysningene i seg selv ikke vil være kildeidentifiserende. Informasjon om hvilken IP-adresse en abonnent er tildelt, vil som nevnt ovenfor i kapittel 4, ikke i seg selv gi informasjon om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har vært i kontakt med. Et viktig poeng i denne sammenheng er at destinasjonsinformasjon ikke skal lagres, jf. kapittel 8.2 ovenfor. Konsekvensen av at den lagrede informasjonen eventuelt skulle komme på avveie, noe enkelte høringsinstanser har uttrykt bekymring for, vil således også ha begrenset betydning for kildevernet.

Dersom lagring av IP-adresser skal kunne bidra til å identifisere en kilde, vil de lagrede opplysningene måtte kobles med informasjon fra annet hold. Spørsmålet om kildevern vil således først kunne komme på spissen når informasjonen om hvilken abonnent som er tildelt en gitt IP-adresse, kombineres med informasjon om en IP-adresse som politiet har fått tilgang til gjennom andre etterforskingsmetoder, eksempelvis gjennom ransaking eller beslag av data. Hvis det i et konkret tilfelle skulle oppstå spørsmål om å benytte IP-informasjon for å identifisere en kilde, vil det etter departementets vurdering trolig være politiets fremgangsmåter for å skaffe til veie tilleggsinformasjon som IP-opplysningene i så fall skal kobles med, som vil komme i forgrunnen ved vurderingen av skrankene i EMK artikkel 10.

Departementet understreker at det gjelder en rekke skranker i straffeprosessloven som begrenser adgangen til å etterforske medienes kilder, se nærmere redegjørelse i høringsnotat 24. september 2018 om endringer i reglene om kildevern i straffeprosessloven og tvisteloven, især kapittel 2 og 10. Blant annet oppstiller straffeprosessloven § 125 et forklaringsfritak om kilders identitet og §§ 204 og 210 oppstiller begrensninger i adgangen til henholdsvis beslag og utleveringspålegg. I tillegg vil bruk av skjulte tvangsmidler rettet mot pressen normalt være avskåret som følge av ulike skranker i straffeprosessloven. Adgangen til å rette etterforskingsmetoder mot en siktet som også er en pressekilde, vil dessuten måtte vurderes konkret etter straffeprosessloven § 170 a og EMK artikkel 10.

At utlevering av IP-adresser fra en redaksjon er underlagt disse begrensningene følger blant annet av Rt. 2010 s. 1381 *Runestein*. Saken gjaldt pålegg om utlevering av en IP-adresse og brukeropplysninger fra Aller Internett i forbindelse med ulovlig besittelse av et kulturminne. Høyesterett kom til at informasjonen var beskyttet av kildevernet, selv om det var tale om et innlegg fra en leser i et debattforum.

Unntak fra kildevernet i disse tilfellene er regulert av straffeprosessloven § 125 tredje ledd. Etter denne bestemmelsen kan et vitne pålegges å oppgi en kilde når «*vektige samfunnsinteresser tilsier at opplysningen gis og den er av vesentlig betydning for sakens oppklaring*». Også når disse vilkårene er til stede skal det foretas en konkret avveining, der det blant annet skal tas hensyn til om kilden har avdekket forhold som det var av samfunnsmessig betydning å gjøre kjent. Rekkevidden av denne bestemmelsen ble drøftet i Rt. 2015 s. 1286 *Rolfsen*. Ved vurderingen av om det forelå slike vektige samfunnsinteresser som skulle tilsi at politiet kunne få tilgang til materialet, viste Høyesterett blant annet til at kildevernet kunne måtte vike når saken gjaldt alvorlig kriminalitet. Selv om det var tilfellet i den aktuelle saken, fikk politiet likevel etter en konkret avveining, ikke tilgang til materialet som kunne avsløre kilden.

Etter dette er det klart at det gjelder svært strenge rammer for politiets tilgang til informasjon om en kilde, herunder en IP-adresse, hos en journalist i forbindelse med etterforsking. Politiet vil følgelig, etter departementets skjønn, bare rent unntaksvis være i en posisjon der det vil være mulig å avdekke en journalists kilde gjennom en etterfølgende anmodning om informasjon fra en ekomtilbyder.

Politiet kan også komme over kildeavslørende materiale i forbindelse med etterforsking av lov-

brudd der etterforskingen ikke er rettet mot journalistisk virksomhet. Det kan i denne sammenheng vises til vurderingen av om det burde innføres et absolutt etterforskingsforbud overfor kilder, slik drøftet i Justis- og beredskapsdepartementets høringsnotatnotat om kildevern fra 2018 kapittel 11 side 104 følgende. Departementet viste der til flere uheldige konsekvenser av et slikt forbud. Etter departementets syn må det sentrale være at de begrensningene loven oppstiller for etterforsking rettet mot pressen, innebærer at «*potensielle kilder som hovedregel kan ha tillit til at pressen ikke pålegges å oppgi vedkommendes navn, og til at dette ikke røpes gjennom ransaking, beslag eller utleveringspålegg hos og mot pressen*» (Prop. 147 L (2012–2013) kapittel 8.5.3 side 154). Det samme gjelder at tvangsmidler ikke brukes for å omgå pressens fritak fra forklaringsplikt om en kildes identitet (samme sted side 153).

For øvrig viser departementet til de materielle og prosessuelle vilkår som er gitt for innhenting av informasjon etter forslaget til ny ekomlov § 2-8 b, herunder nødvendighetskriteriet. Slik lagringsplikten for IP-adresser nå er rammet inn, kan departementet på det nåværende tidspunkt vanskelig se at lagringsplikten kan utgjøre et uforholdsmessig inngrep i pressens rett til kildevern etter EMK artikkel 10.

9 Utlevering av IP-adresser i sivile saker og etter ekomloven § 2-9

9.1 Gjeldende rett

Det følger av ekomloven § 2-9 første ledd at tilbyder og installatør har plikt til å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter. I henhold til ekomloven § 2-9 tredje ledd, er taushetsplikten likevel ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Taushetsplikten er heller ikke til hinder for at slike opplysninger gis til annen myndighet i medhold av lov. Abonnementsopplysninger som nevnt, vil omfatte opplysninger om IP-data. Tilbyderne lagrer blant annet opplysninger om IP-data til kommunikasjons- eller faktureringsformål i henhold til bestemmelsene i ekomloven § 2-7 femte ledd.

Unntaket fra taushetsplikten i ekomloven § 2-9 tredje ledd gjelder for alle oppgavene politiet utfører, også politiets sivile gjøremål. Unntaket i fjerde ledd for «*særlige forhold som gjør det utilrådelig å etterkomme anmodning fra påtalemyndighet eller politi om opplysninger*» vil ifølge forarbeidene særlig være aktuelt i saker som ikke gjelder etterforsking, for eksempel i tilknytning til forvaltningssaker og namssaker.

For utlevering til andre offentlige myndigheter enn politi og påtalemyndighet, kreves det egen lovhjemmel som gjør unntak fra taushetsplikten, jf. § 2-9 tredje ledd tredje punktum. § 2-9 tredje ledd gir altså ikke i seg selv hjemmel for fritak fra taushetsplikt overfor andre myndigheter. 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.

Videre følger det 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 henhold til tvisteloven § 21-5 plikter enhver 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. 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 Nasjonal kommunikasjonsmyndighet. Nasjonal kommunikasjonsmyndighets 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 Nasjonal kommunikasjonsmyndighet har samtykket.

Åndsverkloven § 87 gir dessuten særregler om tilgang til opplysninger som identifiserer innehaver av abonnement brukt ved inngrep i opphavsretten eller andre rettigheter etter loven. Retten kan i slike tilfeller, etter begjæring fra rettighetshaveren, pålegge en tilbyder av elektroniske kommunikasjonstjenester å utlevere slike opplysninger. Etter bestemmelsens andre ledd første punktum, skal Nasjonal kommunikasjonsmyndighet anmodes om samtykke til fritak fra taushetsplikten før retten treffer avgjørelse i saken. Samtykke til fritak kan bare 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. Dette tilsvarer vurderingstemaet etter tvisteloven § 22-3 tredje ledd. I åndsverkloven § 87 tredje ledd andre punktum er det angitt enkelte vurderingsmomenter for avveiningen.

9.2 Forslaget i høringsnotatet

I høringsnotatet ble det vist til at 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 vil kunne oppstå spørsmål om IP-data 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, reiste departementene spørsmål om det burde 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. Departementene påpekte at det må 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 gjaldt straffbare rettskrenkelser av en slik alvorlighet at det i henhold til høringsforslaget kunne begrunne utlevering av opplysninger om IP-adresser til politi eller påtalemyndighet, ville forfølging av krenkelsen i sivilprosessens former, kunne være viktig. Dette vil for eksempel kunne være aktuelt i en sak om erstatning.

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, 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.

En plikt til å lagre IP-adresser vil også innebære at åndsverkloven § 87 kan bli aktuell å benytte i flere tilfeller enn i dag.

Departementene viste i høringsnotatet til at 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 pekte også på at det var viktig at det fortsatt var adgang til sikring av bevis og bevisføring i sivile saker, og så ikke behov for å begrense den faktiske adgangen rettighetshaverne har i dag. Innføring av en plikt til å lagre IP-adresser vil imidlertid innebære at opplysningene om IP-adresser blir lagret betydelig lenger enn i dag, og departementene viste til at det er usikkert hva en slik utvidet lagringstid for IP-adresser i praksis ville innebære i sivile saker og hvilken betydning dette vil ha for blant annet kommunikasjonsvernet. I høringsnotatet ba departementene derfor særskilt om høringsinstansenes syn på dette, herunder om synspunkter på behovet for begrensninger på bruken av opplysningene som omfattes av utvidet lagring i sivile saker.

Høringsnotatet drøftet ikke særskilt spørsmålet om andre myndigheters tilgang til opplysninger om IP-adresser.

9.3 Høringsinstansenes syn

De fleste av høringsinstansene mener at bruk av opplysninger om IP-adresser som er undergitt utvidet lagringstid ikke bør utgis i sivile saker.

Abelia mener det er usikkert hva en utvidet lagringstid for IP-adresser i praksis vil innebære i sivile saker og hvilken betydning dette vil ha for kommunikasjonsvernet. Det er for eksempel mulig at parter i sivile saker kan få tilgang til informasjon som politiet ikke vil få tilgang til i en straffesak knyttet til samme hendelse. Dette er ikke drøftet i høringsnotatet, og det er uklart om slike eventuelle effekter er intensjonelle. Abelia henviser til høringssvaret fra Den Internasjonale Juristkommisjon for utdypning, og mener at dette er spørsmål som personvernkommisjonen bør utrede.

Altibox mener at det i lovendringen eksplisitt bør fremkomme at IP-data kun skal være tilgjen-

gelig i straffesaker. Formålet med lovforslaget er å bekjempe alvorlig kriminalitet, og det bør derfor være alvorlig kriminalitet som hjemler utlevering av IP-adresser.

Telenor viser til at en utvidet lagring for kriminalitetsbekjempelse ikke må få betydning i sivile saker. Telenor ser faren for formålsutglidning, og henviser til det som anføres som departementenes uttalte formål med forslaget – «å bekjempe alvorlig kriminalitet». Forslaget bør rammes inn ut fra dette. Telenor støtter at vilkårene for utlevering av opplysningene som skal lagres etter forslaget, strammes inn sammenlignet med gjeldende rett for å ivareta kravet om proporsjonalitet etter Grunnloven, EMK, kommunikasjonsverndirektivet og EØS-retten, og er enig i at en innstramming er nødvendig.

Telia viser til at det erfaringsmessig vil oppstå et press i retning av å benytte opplysninger som allerede ligger lagret, til andre formål enn det opprinnelige, som i denne sammenheng er å bekjempe og avdekke alvorlig kriminalitet. Telia mener at lovgiver må oppstille rettslige hindre mot at lagrede opplysninger benyttes i sivile saker, og er særlig bekymret for en formålsutglidning for å forfølge rettskrav på bakgrunn av påståtte krenkelser av opphavsrettigheter. Telia oppfordrer til at det lovfestes en avskjæring av muligheten for å føre opplysninger som stammer fra IP-lagring som bevis for retten i sivile saker.

IKT-Norge legger til grunn at det vil skje en økning i antall utleveringsbegjæringer fra politi og påtalemyndighet dersom forslaget vedtas, og at en tilsvarende økning i antall utleveringer i sivile saker ikke kan utelukkes dersom det også gis tilgang i slike saker. IKT-Norge er bekymret for formålsutglidning hvis tvistelovens bevisregler skal gjelde som i dag. Formålet med lovforslaget er bekjempelse av alvorlig kriminalitet, og dette har betydning for hvilke inngrep i kommunikasjonsvernet som kan forsvares. IKT-Norge oppfordrer sterkt til å lovfeste en avskjæring eller begrensning, slik at IP-data ikke kan utgis i sivile saker. Disse synspunktene støttes av *Bredbåndsfylket (Troms) AS* og *Enivest AS*.

Advokatforeningen mener det i utgangspunktet vil være i strid med *La Quadrature du Net*-dommen om IP-adresser som er lagret etter den foreslåtte lagringsplikten, skulle tillates utlevert til andre formål enn «*beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed*». Dommen innebærer at utlevering av IP-adresser som er lagret i henhold til den foreslåtte lagringsplikten, i utgangspunktet ikke kan utleveres i alminnelige sivile saker. Unntak kan eventuelt tenkes i sivile saker der kravet begrunnes i straffbare forhold. Dette bør i så fall utredes nærmere før et endelig lovforslag fremmes.

Datatilsynet er helt imot at eventuelle opplysninger skal gjøres tilgjengelig i sivile saker, og mener at problemstillingen viser at det er en risiko for formålsutglidning. Tungtveiende kriminalitetsbekjempende hensyn kan ikke begrunne en så omfattende overvåkning i åndsverkssaker. Datatilsynet forstår *La Quadrature du Net*-dommen slik at det kun er kriminalitetsbekjempelse som eventuelt kan rettferdiggjøre en lagringsplikt. Tilgang i sivile saker, særlig på et så upresist rettsgrunnlag som i dag, kan medføre at hele lagringsregimet underkjennes på EU/EØS-rettslig grunnlag.

Den internasjonale juristkommisjon – norsk avdeling (ICJ) viser til at selv om tilgang til opplysninger om IP-adresser i sivile saker krever samtykke fra Nkom eller rettens kjennelse, kan parter i sivile saker få tilgang til taushetsbelagt informasjon, som for politiet er begrenset til bekjempelse av alvorlig kriminalitet. Dette er særlig aktuelt ved bevissikring utenfor rettsak, jf. Rt. 2010 s. 774. ICJ frykter at en generell lagring over mye lengre tid enn i dag vil gjøre at sivile kan få tilgang til IP-adresser i mye større grad enn tidligere. For å hindre at informasjon om IP-adresser blir «allemannseie» er det derfor særlig viktig med en streng regulering av hvem som får tilgang til lagrede IP-adresser. Slik ICJ forstår *La Quadrature du Net*, er det kun kriminalitetsbekjempelse som formål som eventuelt kan rettferdiggjøre en lagringsplikt. Tilgang i sivile saker, særlig på et så upresist rettsgrunnlag som i dag, kan medføre at hele lagringsregimet underkjennes på EU/EØS-rettslig grunnlag.

Norsk Journalistlag mener at det ikke er noen holdepunkter for å anta at de relevante hensynene slår ulikt ut i straffesaker og i sivile saker: Kildevernets rekkevidde vil være den samme. Det er heller ikke usikkert hva som gjelder overfor andre offentlige myndigheter, slik departementene gir inntrykk av. Vernet om anonyme kilder gjelder også overfor offentlige myndigheter som Konkurransetilsynet, ligningsmyndighetene og Kredittilsynet.

Enkelte andre høringsinstanser mener at det er viktig at man fortsatt skal ha tilgang til opplysningene også i sivile saker, særskilt i saker som gjelder krenkelse av opphavsrettigheter på nett.

Rettighetsalliansen viser til at rettighetskrenkelser på internett er et alvorlig problem for medlemmene. Prosedyrekravene i åndsverkloven § 87

innebærer at utlevering av opplysninger som identifiserer innehaveren av abonnementet, kun kan skje etter beslutning fra en domstol, etter forutgående uttalelse fra Nkom, der både Nkom og domstolen vil foreta brede interesseavveininger basert på vurderingstemaene i loven. Dette innebærer at utlevering kun vil være mulig der hensynene som taler for utlevering veier tyngre enn hensynet til abonnenten. Utlevering vil derfor neppe innebære en krenkelse av EMK artikkel 8. Rettighetsalliansen viser også til at immaterielle rettigheter er beskyttet av EMK Protokoll 1 artikkel 1 om vern om eiendom, og at staten har en plikt til å legge forholdene til rette for at rettighetshaverne skal kunne håndheve sine immaterielle rettigheter. Rettighetsalliansen viser videre til at prosedyren for behandling av krav om utlevering av abonnentopplysninger i sivile saker ofte er mer tidkrevende enn i straffesaker, og at rettighetshaver etter åndsverkloven § 87 må kunne kreve opplysningene utlevert fra tilbyderne i hele perioden opplysningene faktisk er tilgjengelige hos tilbyder. *Norwaco* stiller seg bak høringssvaret fra Rettighetsalliansen.

Forleggerforeningen viser til at norsk er et lite språkområde med et begrenset marked, og at norsk litteraturproduksjon er særlig sårbart for inntektsbortfall som skyldes ulovlig distribusjon. Forleggerforeningen er medlem av Rettighetsalliansen og viser for øvrig til deres høringssvar for så vidt gjelder rettighetskrenkelser på internett.

Høringsuttalelser fra politi og påtalemyndighet peker på viktigheten av at bruk i sivile saker ikke går på bekostning av hensynet til kriminalitetsbekjempelse.

Kripos legger til grunn at forslaget ikke berører § 2-9 tredje ledd, slik at politiet fortsatt vil ha adgang til å få utlevert abonnentinformasjon, også IP-adresser, i den grad disse er lagret med en annen begrunnelse enn den nye lagringsplikten i høringsnotatet.

Riksadvokaten har ingen synspunkter på bruk av opplysninger i sivile saker isolert sett, men understreker med styrke at regelverket på dette punktet bør utformes slik at det ikke går utover forhold som har betydning for kriminalitetsbekjempelsen.

Det nasjonale statsadvokatembetet viser til de garantier som er innbakt i åndsverksloven § 87, og har ikke betenkeligheter med at det fortsatt skal være adgang til sikring av bevis og bevisføring i sivile saker.

Oslo statsadvokatembeter viser til at EMK artikkel 8 ikke bare gjelder på strafferettens område: EMDs vurdering av forholdsmessighet ved utlevering til bruk i sivile saker, eksempelvis med bakgrunn i overtredelser av åndsverkloven, vil kunne bli annerledes enn ved vurderingen i forbindelse med kriminalitetsbekjempelse.

Politidirektoratet støtter vurderingen i høringsnotatet om at gjeldende rett bør videreføres på dette punktet, selv om innføring av en plikt til å lagre IP-adresser vil innebære lengre lagring.

Statens sivilrettsforvaltning viser til at forslag til ny voldsoffererstatningslov legger opp til at fornærmede må ta ut sivilt søksmål. Dette aktualiserer spørsmålet om å føre denne type opplysninger som bevis i erstatningssaker. Hensynet til sakens opplysning og fornærmedes mulighet til å forfølge sitt erstatningskrav, tilsier etter SRFs syn at det ikke bør innføres ytterligere begrensninger for bruk av informasjon om IP-adresse i sivile krav om erstatning, enn det som gjelder i forslaget for øvrig.

Stine Sofies Stiftelse mener det bør være adgang til å bruke bevisene i sivile saker, under de begrensninger som ellers følger av tvistelovens regler om bevisforbud. At det åpnes for bruk i sivile saker blir svært viktig dersom forslag til ny lov om voldsoffererstatning blir vedtatt. Ved krav om dom i erstatningssak for at voldsutsatte skal kunne kreve voldsoffererstatning, vil det være av stor betydning at innhentede IP-adresser kan brukes som bevis i den sivile saken.

9.4 Departementets vurdering

9.4.1 Utlevering av IP-adresser i medhold av tvisteloven § 22-3 og åndsverkloven § 87

I henhold til tvisteloven § 22-3 andre og tredje ledd kan det etter en nærmere avveining gis unntak fra bevisforbudet for opplysninger undergitt lovbestemt taushetsplikt i første ledd, herunder opplysninger om IP-adresser. Tilsvarende unntaksregler finnes i åndsverkloven § 87.

Innføring av en lagringsplikt for IP-adresser med formål å bekjempe alvorlig kriminalitet, vil medføre at informasjonen om IP-adresser lagres lenger enn etter gjeldende rett. Tilgangen til IP-adresser i medhold av bestemmelsene i tvisteloven § 22-3 andre og tredje ledd og åndsverkloven § 87, vil dermed kunne bli utvidet sammenlignet med i dag. I høringsnotatet drøftet departementene derfor en utvidelse av tilgangen i sivile saker, til informasjon om IP-adresser lagret i tolv måneder etter forslag til ny § 2-8 a.

Ved vurderingen av om opplysninger lagret i medhold av forslag til ny § 2-8 a med formål å

bekjempe alvorlig kriminalitet, også skal kunne tillates brukt i sivile saker, har departementet tatt utgangspunkt i de rammer som er oppstilt i kommunikasjonsverndirektivet artikkel 15, med de presiseringer som er gjort for lagring av IP-adresser i *La Quadrature du Net*-dommen. Utgangspunktet her er at lagring av de angitte opplysningene bare skal kunne begrunnes i nærmere angitte hensyn, blant annet i bekjempelse av alvorlig kriminalitet, se for eksempel dommens avsnitt 156. Det er videre uttalt i avsnitt 112 i dommen at oppregningen av de formål som er fastsatt i artikkel 15 er uttømmende, slik at en rettsregel som er vedtatt i medhold av denne bestemmelsen kun kan benyttes til å oppfylle de formål som er angitt.

Formålet med den foreslåtte bestemmelsen i ekomloven § 2-8 a er å etterforske alvorlig kriminalitet. Det er dette som begrunner den foreslåtte lagringen av opplysningene hos ekomtilbyderne. Erfaringsmessig vil det imidlertid ofte oppstå ønske om å benytte opplysninger som allerede ligger lagret, til andre formål. Dette ønsket vil ventelig bli større når lagringstiden for opplysningene blir lengre.

Flere av høringsinstansene peker på faren for formålsutglidning dersom man åpner for bruk av de lagrede opplysningene også i sivile saker. I denne sammenheng er det også blant annet anført at når det oppstilles strengere materielle vilkår for utlevering av opplysninger til politiet, kan det være en risiko for at parter i sivile saker vil kunne få tilgang på informasjon som politiet ikke har tilgang til i en straffesak knyttet til samme hendelse. Departementet viser her til at en utlevering i sivile tvister i medhold av tvistloven § 22-3 andre og tredje ledd og etter åndsverkloven § 87 skal være basert på en konkret avveining av de relevante hensynene. Departementet har likevel kommet til at det ikke bør være tilgang til opplysninger om IP-adresser som er pålagt lagret med formål om å bekjempe alvorlig kriminalitet, i sivile saker. Tilgangen i sivile saker etter ekomloven § 2-9 til IP-data lagret for tilbydernes eget formål, foreslås imidlertid ikke endret, og disse opplysningene vil derfor fremdeles kunne benyttes i sivile saker.

Departementet foreslår på bakgrunn av det ovenstående at opplysninger som kun er lagret for å oppfylle lagringsplikten etter § 2-8 a, bare skal kunne utleveres etter § 2-8 b, det vil si til politi- og påtalemyndigheten når det er nødvendig i saker om etterforsking av alvorlig kriminalitet. Dette vil hindre utlevering av data lagret etter § 2-8 a til politiet i etterforsking av andre saker. Videre vil det hindre utlevering til andre offentlige myndigheter, og det vil også sikre at det ikke kan hentes ut IP-adresser lagret etter § 2-8 a som bevis i sivile saker etter unntakene fra bevisforbudet i tvisteloven § 22-3 og åndsverksloven § 87. Departementet foreslår at det tas inn en avgrensing i § 2-8 b for å klargjøre dette.

Departementet finner grunn til å presisere at man ved dette ikke har ment å gjøre endringer i adgangen til bruk av straffesaksdokumenter i sivile saker, eksempelvis i erstatningssaker etter overgrep. Departementet legger videre til grunn at tilbyderne ved valg av teknisk løsning etter kapittel 8.3, tar tilstrekkelig hensyn til at opplysninger lagret i medhold av § 2-8 a bare skal kunne utleveres til formålene som er nærmere angitt.

9.4.2 Utlevering av IP-adresser til politi og påtalemyndighet, samt annen myndighet etter ekomloven § 2-9

Når det pålegges lagringsplikt for IP-adresser i tolv måneder, må det vurderes om det er behov for endringer i ekomloven § 2-9 tredje ledd. Departementet foreslår ingen endringer i § 2-9 på det nåværende tidspunkt. Behovet for endringer i denne bestemmelsen er ikke tilstrekkelig utredet. Departementet vil arbeide videre med denne problemstillingen, og komme tilbake ved en senere anledning.

At det ikke foreslås endringer i ekomloven § 2-9, innebærer for det første at tilgangen etter § 2-9 tredje ledd i sivile saker ikke endres, jf. kapittel 9.4.1. Videre vil politi og påtalemyndighet samt andre myndigheter ha samme tilgang til abonnementsdata, inkludert IP-adresser, lagret i tilbyders driftslager som i dag. Dette innebærer for politiets og påtalemyndighetens del at de vil få tilgang til IP-adresser lagret etter ekomloven § 2-7 femte ledd nummer 1, også i saker som ikke gjelder alvorlig kriminalitet. Det samme gjelder andre myndigheter når dette følger av særskilt lovhjemmel.

10 Kostnadsfordeling

10.1 Gjeldende rett

Det følger av ekomloven § 2-8 første ledd at tilbyder skal tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres. Etter dagens kostnadsfordeling belastes ekomtilbyderne for investeringskostnadene for slik tilrettelegging fordi det er tilbyder som selv har behov for dataene til kommunikasjons- og faktureringsformål, og derfor uansett måtte ha dataene tilgjengelig i perioden politiet kan få tilgang.

Det følger av § 2-8 andre ledd 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-data til politiet. Dette er avtaleregulert mellom politiet og de forskjellige tilbyderne i en rekke enkeltavtaler mellom partene.

10.2 Forslaget i høringsnotatet

I departementenes vurdering av hvilken kostnadsfordelingsmodell som er mest hensiktsmessig, ble hensynet til kriminalitetsbekjempelse og kommunikasjonsvern vektlagt. I tillegg måtte modellen ivareta konkurransen i ekommarkedet og understøtte samfunnsøkonomisk kostnadseffektivitet. Siden forslaget til lagring av IP-adresser først og fremst er begrunnet i kriminalitetsbekjempelse, forventet ikke departementene at tilbyderne skal dekke alle kostnadene.

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 kostnadsfordelingsmodellene nedenfor.

Forslaget i høringsnotatet er til dels basert på tidligere arbeid med kostnadsfordeling mellom ekomtilbydere og politi, blant annet Kostnadsutvalgets utredning «*Forslag til kostnadsfordelingsmodell i forbindelse med innføring av datalagringsdirektivet i norsk rett»,* som ble fremlagt 1. februar 2012.

10.2.1 Alternative fordelingsmodeller

Det er tre ulike utgangspunkt 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 når det gjelder investeringskostnadene for tilrettelegging for lovbestemt tilgang til informasjon, jf. ovenfor, fordi tilbyder utelukkende lagrer til egne behov. Det kan imidlertid argumenteres for at kostnadene som følger av lovendringen, forventes å bli større enn dagens kostnader, og det vil medføre uheldige virkninger i markedet dersom tilbyderne skal dekke disse selv. På den andre siden vil en modell hvor staten fullt ut dekker kostnadene, ikke gi tilbyderne insentiv til å velge kostnadseffektive løsninger, og dermed kunne 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 fastsatt fordelingsnøkkel. Staten dekker faste driftskostnader og uthentingskostnader.
e. Investeringskostnader og faste driftskostnader deles mellom staten og tilbyderne i henhold til en fastsatt fordelingsnøkkel. Staten dekker uthentingskostnader.

Fordelingsnøkkelen ble i forslag til bestemmelse i høringen eksemplifisert med at tilbyders merkostnader for investeringer som påløper for å oppfylle lagringsplikten, dekkes av tilbyder med 20 prosent. Tilsvarende eksempel ble også brukt for modell E.

Tabell 10.1 viser en oversikt over hvem som dekker de ulike kostnadskategoriene i de ulike modellene.

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.

10.2.2 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 B, C eller D 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 etterspurt IP-data. I tillegg kan noe av prisvariasjonen skyldes at tilbyderne benytter forskjellig utstyr og løsninger. Ulik størrelse på tilbyderne og ulikt antall

Tabell 10.1 Oversikt over alternative kostnadsfordelingsmodeller

	Investeringskostnader	Faste driftskostnader	Uthentingskostnader
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

forespørsler medfører trolig variasjoner i prosesser og rutiner for uthenting av IP-data, noe som igjen resulterer i varierende uthentingskostnader mellom tilbydere.

Dersom en av modellene B, C eller D skal benyttes, bør det derfor vurderes om det bør utdypes hvilke kostnader som inngår i de ulike kategoriene. Dette kan spesifiseres på et detaljeringsnivå som er lettere å forholde seg til både for tilbyderne og for staten. I den grad det skulle være hensiktsmessig, kan dette eventuelt reguleres i forskrift. 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 modellene D og E deles én eller flere av kostnadskategoriene i henhold til en fordelingsnøkkel. I Kostnadsutvalgets utredning vises det til at selv en liten andel av kostnadene tillagt tilbyderne gir dem insentiv til å velge en kostnadseffektiv løsning.

På bakgrunn av at 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 at kostnadene derfor i hovedsak dekkes av staten, med de uheldige virkningene som er beskrevet ovenfor, knyttet til insentiv for å vri kostnader over på staten. 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 mindre behov for å kontrollere valgt løsning, ettersom tilbyderne selv har insentiver til å velge den mest kostnadseffektive løsningen. Denne fordelen er størst i modell A og E.

10.2.3 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 lagringsplikten. Dette vil kunne være til hinder for etablering, og det 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. 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-data i alle modellene. Dette er begrunnet i 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-data.

Det antas at større tilbydere som kan fordele sine merkostnader over mange kunder, lettere kan bære en lagringsplikt enn små tilbydere med langt færre kunder.

10.2.4 Nærmere om uthentingskostnader

En sentral del av formålet med lovforslaget er å legge til rette for at politiet skal kunne innhente IP-data 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-data 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-data i flere saker enn i dag. Departementene forutsetter at politiet begrenser uthentingen av IP-data til det som er nødvendig for politiets arbeid, slik at hensynet til kommunikasjonsvernet ivaretas i enkeltsaker.

Som det fremkommer i kapittel 11 om økonomiske og administrative konsekvenser, er det relativt stor variasjon i prisene hos tilbyderne ved utlevering av IP-data 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 foren-

klinger 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.

10.3 Høringsinstansenes syn

Ekomtilbyderne og deres organisasjoner mener at staten må dekke merkostnadene som oppstår ved lagring av IP-adresser til bekjempelse av alvorlig kriminalitet, fordi dette utelukkende er til statens formål og ikke gir noen fordeler for ekomtilbyderne. Dersom ekomtilbyderne må velge mellom de hørte modellene, peker de på modell D.

IKT-Norge påpeker at tilbyderne «*(..) pålegges plikter som ikke er knyttet til deres egne formål, prioriteringer og ønsker – men som tvert imot står i kontrast til den sentrale forpliktelsen og forventningen som påhviler dem om kommunikasjonsvern. I slike saker er det prinsipielt viktig at det offentlige tar ansvar for og finansierer merutgiftene ved ordningen.*» IKT-Norge fremhever videre at markedet er konkurranseutsatt, og at tilbyderne vil ha forskjeller i kostnader ved ordningen, blant annet på grunn av forskjellig innretning av virksomhetene og størrelse/antall sluttbrukere, og at det i motsetning til den gjeldende tilretteleggingsplikten etter ekomloven § 2-8, her er snakk om investeringskostnader som ikke er knyttet til egne behov. IKT-Norge viser også til at allokering av utgiftene til staten kan føre til en modererende effekt på antall utleveringsbegjæringer, og dermed styrke nødvendighetsvurderingen og hensynet til kommunikasjonsvernet i den enkelte sak hvor politi/påtalemyndighet vurderer å begjære utlevering. IKT-Norge mener at en kostnadsdelingsmodell mellom tilbydere og staten for investeringskostnader kan være et fornuftig virkemiddel, dersom en lav andel dekket av tilbyder kan erstatte omfattende oppfølging i form av rapportering og revisjoner. *Bredbåndsfylket (Troms) AS* og *Enivest AS* stiller seg i sine høringssvar bak denne uttalelsen.

Abelia viser til at forslaget om lagring av IP-adresser er bistand til løsning av myndighetsoppgaver, og at selskapenes utgifter må dekkes av staten. Innføring av lagringsplikt må ikke få utilsiktede konkurransemessige effekter i ekommarkedet, eller utilsiktede, uheldige og unødvendig fordyrende konsekvenser for næringslivet. Abelia mener videre at ingen av de foreslåtte modellene for kostnadsfordeling er tilstrekkelige, men at modell D er å foretrekke dersom en av de fremlagte modellene må velges. Valg av kostnadsfordelingsmodell bør imidlertid utredes nærmere i dialog med bransjen.

Prinsipielt mener *Telenor* og *Telia* at når staten pålegger private aktører utvidede oppgaver av ulik art, bør også staten ta kostnadene både for investering og drift i tilknytning til disse. *Telenor* mener at ingen av de foreslåtte modellene reflekterer at staten bør bære alle kostnadene. I valg mellom modellene mener Telenor at det kan være aktuelt å diskutere videre alternativ D, under forutsetning av at private aktører ikke pålegges en urimelig byrde. Modell D legger opp til at «*Investeringskostnader deles mellom staten og tilbyderne i henhold til en fordelingsnøkkel. Staten dekker faste driftskostnader og uthentingskostnader*». Telenor understreker videre at automatisering og forenkling – for eksempel med en API-lignende ordning ved utlevering til politiet – ikke bør pålegges ISPene, selv om Telenor i sitt interne arbeid stiller seg positive til automatisering og forenkling i den grad dette er praktisk gjennomførbart.

Telia fremhever at kostnader for politiets uthentinger bør dekkes av staten, fordi dette kan bidra til å moderere antall utleveringsbegjæringer og dermed styrke nødvendighetsvurderingen i den enkelte sak hvor politi/påtalemyndighet vurderer å begjære opplysninger utlevert. Selskapet viser videre til at dersom staten dekker alle kostnader vil en lagringsplikt heller ikke medføre konkurransevridende effekter i ekommarkedet. Av modellene som er skissert i høringsnotatet fremholder selskapet at modell D sammenfaller best med Telias vurderinger.

Altibox mener det klare utgangspunktet er at utleveringskostnadene bør dekkes av staten, fordi dette kan ha en modererende effekt for antall utlevering av denne type opplysninger. I valget mellom de foreslåtte modellene, er modell D å foretrekke.

GlobalConnect viser til at en plikt til å lagre IP-adresser i 6–12 måneder ikke har noen form for egenverdi for ekomtilbyderne, og mener at staten bør dekke alle investerings-, drifts- og uthentingskostnader. Dette vil også disiplinere de som

ber om tilgang, og gi insentiver til at ordningen ikke blir mer omfattende, komplisert og inngripende enn nødvendig. Eventuelle bekymringer for at tilbyderne kan påføre staten ekstra kostnader, kan løses gjennom avtaler, forhåndsgodkjenning eller etterfølgende kontroll. Av de fem skisserte modellene mener GlobalConnect at modell D er den eneste akseptable, men fordelingsnøkkelen bør justeres slik at staten dekker 90 prosent, og ikke kun 80 prosent av de relevante merkostnadene.

Politiet og påtalemyndigheten mener at tilbyderne må dekke merkostnadene ved investeringer- og drift av IP-lagringen, dvs. modell A, med bakgrunn i at kriminalitetsbekjempelse er en del av tilbydernes samfunnsansvar. Det pekes videre på at det er utfordrende å skille mellom investerings- og driftskostnader, og dersom det velges en løsning hvor staten skal dekke annet enn rene uthentingskostnader, bør man gå for en modell der det ikke skilles mellom investerings- og driftskostnader, jf. modell E.

Politidirektoratet (inkludert høringsinnspill fra politidistriktene *Sør-Øst*, *Innlandet*, *Sør-Vest*, *Nordland*, *Øst*, *Oslo*, og *Trøndelag*, samt fra *Kripos*, *Politihøgskolen* og *Politiets utlendingsenhet*) støtter *Kripos'* vurdering om at kostnader knyttet til lagring, herunder investering i og drift av løsninger, må dekkes av tilbyderne selv. Kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn, og staten bør kunne pålegge næringer tilretteleggingskrav uten kompensasjon, slik som for eksempel finansnæringene er pålagt å dekke kostnadene knyttet til hvitevaskingsregisteret. Politidirektoratet og Kripos mener videre at det er utfordrende å skille mellom investeringskostnader og driftskostnader, for eksempel dersom man inngår leasingavtale istedenfor innkjøp av serverpark. Disse høringsinstansene mener videre at dersom det velges en løsning hvor staten skal dekke annet enn rene uthentingskostnader, bør man gå for modell E, der det ikke skilles mellom investerings- og driftskostnader. Politidirektoratet viser til at det store antall tilbydere tilsier at individuelle refusjonsavtaler vil være ressurskrevende å drifte, og at en fast fordelingsnøkkel derfor er bedre. Kripos peker i sitt innspill på at uthentingskostnader bør begrenses til å gjelde rene kostnader med å hente ut lagrede data og overføre disse til politiet. Valget av kostnadsfordelingsmodell må ikke få konsekvenser for om politiet faktisk velger å innhente data, og lage utfordringer for de innarbeidede ordningene som gjelder for innhenting av trafikkdata og tilrettelegging for kommunikasjonskontroll. Politidirektoratet tiltrer disse vurderingene.

Det nasjonale statsadvokatembetet mener at ekomtilbyderne skal dekke 50 prosent av merkostnadene for investeringer som følge av lovendringen, fordi ekomtilbyderne hvert år omsetter for betydelige beløp. Det vises til at Telenor alene skal utbetale utbytte på 12,4 milliarder kroner til sine aksjonærer i 2020, og det anføres at det er rom for en likedeling av utgiftene, ikke en skjevdeling.

Politiets Fellesforbund mener at tilbyderne må ta utgiftene, og at det vil være prinsipielt feil å overføre kostnadene til politiet, noe som kan føre til en svekket polititjeneste, stikk i strid med intensjonen.

KS er dypt bekymret for at økte kostnader for små, lokale bredbåndsutbyggere som følge av lagringsplikten, kan gå utover god dekning og robusthet i ekominfrastrukturen i alle landets kommuner. KS mener videre at det er viktig å unngå uheldige konkurransevridende effekter i ekommarkedet når merkostnader for den nye lagringsplikten skal fordeles mellom staten og tilbydere. KS er særlig bekymret for at økte kostnader for små, lokale bredbåndsutbyggere som følge av lagringsplikten, kan gå utover god dekning og robusthet i ekominfrastrukturen i alle landets kommuner, og fremhever at lokale bredbåndtilbyderes nettutbygging er viktig i mange kommuner for å sikre at flest mulige innbyggere, bedrifter og offentlige lokasjoner får tilbud om høykapasitetsbredbånd de nærmeste årene. Dersom ikke staten dekker det meste av kostnadene for lagringsplikten, vil merkostnader kunne utgjøre en større kostnads- og konkurranseulempe for små lokale aktører, enn for de store nasjonale bredbåndstilbyderne, som har flere kunder å fordele en merkostnad på. KS påpeker at mange lokale bredbåndsutbyggere har vært viktige «motorer» for regional utvikling og kompetansearbeidsplasser utenfor sentrale strøk de senere årene, og de er bekymret for at dette kan skape utfordringer for det videre digitaliseringsarbeidet i mange kommuner. Staten bør dekke det meste av kostnadene ved etablering og drift av den nye lagringsplikten for IP-adresser, og Modell D vil best understøtte behovet for god dekning og robusthet i ekominfrastrukturen i det videre digitaliseringsarbeidet i kommunal sektor.

10.4 Departementets vurdering

Departementet viser til at formålet med lovendringen er å gi politiet et effektivt verktøy i kampen

mot alvorlig kriminalitet, hvor de kan innhente IP-data i de sakene de faglig sett har behov for det. Samtidig er det viktig å ivareta hensynet til kommunikasjonsvern, konkurransen i ekommarkedet og samfunnsøkonomisk kostnadseffektivitet når kostnadene skal fordeles mellom stat og tilbyder. I alle kostnadsfordelingsmodellene i høringsnotatet er det lagt til grunn at staten dekker uthentingskostnadene. Dersom tilbyderne hadde blitt pålagt å dekke alle eller deler av uthentingskostnadene, ville det påført tilbyderne enda større kostnader, avhengig av antall utleveringsbegjæringer fra politiet hos hver enkelt tilbyder, noe de selv ikke kan påvirke. Departementet merker seg at *IKT-Norge*, *Abelia*, *Telenor*, *Telia*, *Altibox*, *GlobalConnect*, *Bredbåndsfylket (Troms) AS* og *Enivest AS*, mener at det vil være mer rettferdig at staten dekker alle utgiftene, fordi lagring av IP-adresser er bistand til løsning av myndighetsoppgaver. Departementet er imidlertid opptatt av at en modell der staten dekker alle kostnader, ikke vil gi tilstrekkelige insentiver til kostnadseffektive investeringer. Departementet mener at denne utfordringen ikke kan løses gjennom avtaler, forhåndsgodkjenning eller etterfølgende kontroll slik *GlobalConnect* fremholder. Bakgrunnen er at prisene fastsettes gjennom forhandlinger mellom tilbyder og leverandør, og det er grunn til å anta at forhandlingene vil påvirkes av om tilbyder selv skal dekke en andel av kostnadene. I et slikt tilfelle legger departementet dessuten til grunn at leverandørene vil gi bedre inngangstilbud dersom det på forhånd er klart at tilbyder har en egeninteresse i kostnadene.

Når det gjelder Abelias innspill om at valg av kostnadsfordelingsmodell bør utredes nærmere i dialog med bransjen, viser departementet til at kostnadsfordeling mellom ekomtilbydere og politi, har vært utredet i Kostnadsutvalgets utredning *Forslag til kostnadsfordelingsmodell i forbindelse med innføring av datalagringsdirektivet i norsk rett* som ble fremlagt 1. februar 2012. Både Telenor og IKT-Norge deltok i utvalget. Selv om IP-lagring er mindre omfattende enn datalagring, vil en ny utredning ikke nødvendigvis gi så mange flere svar at det ville rettferdiggjøre en ny utredning med en tilhørende utsettelse av lovforslaget. Tilbyderne har dessuten gjennom høringen fått anledning til å inngi sine syn på saken.

Departementet merker seg at alle ekomtilbyderne, *IKT-Norge* og *Abelia* fremhever at utgifter som selskapene har som følge av at det innføres lagringsplikt for IP-adresser for bekjempelse av alvorlig kriminalitet, må dekkes av staten, men at disse høringsinstansene foretrekker modell D, dersom de må velge mellom de fremlagte modellene. Dette fordi modell D i størst grad tar hensyn til at lagringsplikten ikke gir fordeler for tilbyder og gjenspeiler at lagringsplikten først og fremst er til nytte for politiet. *KS* påpeker i sitt høringsinnspill at en modell som pålegger tilbyderne kostnader knyttet til IP-lagring, vil kunne gi konkurranseskadelige effekter i ekommarkedet, både ved å hindre etablering og å drive mindre aktører ut av markedet.

Departementet merker seg at politiet mener kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn hvor staten bør kunne pålegge næringer tilretteleggingskrav uten kompensasjon, herunder at investerings- og driftskostnader knyttet til lagring, derfor må dekkes av tilbyderne som i modell A. Høringsinstansene fra politisiden viser også til at dette er tilfellet for finansnæringen, som er pålagt å dekke kostnadene knyttet til hvitvaskingsregisteret. Departementet merker seg dette samtidig som det også vises til at aktørene i finansnæringen har fordeler av og egeninteresse i registreringen, fordi de kan holdes strafferettslig ansvarlig for gjennomføring av transaksjoner med midler som kommer fra straffbare handlinger. Departementet har også merket seg at *Politiets Fellesforbund* i sitt høringsinnspill argumenterer for at dersom politiet påføres merkostnader, kan det føre til en svekket polititjeneste, stikk i strid med intensjonen i lovforslaget.

Departementet er enig i at kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn hvor staten bør kunne pålegge næringer tilretteleggingskrav, og viser til at dette er tilfellet for finansnæringen som er pålagt å dekke kostnadene knyttet til hvitvaskingsregisteret, selv om situasjonen ikke er direkte sammenlignbar med en ordning for lagring av IP-data. Til tross for at det vil være ulikheter mellom finansnæringen og ekomtilbyderne knyttet til henholdsvis hvitvaskingsregisteret og IP-lagringsplikten, viser departementet til at dette trekker i retning av at næringer i visse tilfeller må kunne pålegges tilretteleggingskrav uten kompensasjon.

Departementet viser også til at enkelte av våre naboland praktiserer lignende ordninger. I både Sverige og Danmark må tilbyderne bære kostnadene ved å innrette sine systemer slik at de kan levere nødvendig informasjon til politiet, altså dekker de selv investerings- og driftskostnadene. Når det gjelder uthentingskostnader, er det i Sverige fastsatt en prisliste, differensiert etter hvilken informasjon politiet ber om og om uthenting skjer innenfor ordinær kontortid. Prisintervallet strekker seg fra 150 til 790 svenske kroner. I Danmark

er det inngått avtale med de største selskapene om at de leverer informasjonen som politiet etterspør, inkludert IP-data, mot at de får et fast årlig beløp. Departementet har ikke lykkes med å finne ut eksakt hvor mye av totalbeløpet som kan tilskrives utlevering av IP-data. I Finland er det politiet som betaler for investeringskostnadene og deler av driften, mens tilbyder betaler for personalkostnader ved drift og for uthentingen. Våre naboland har med andre ord forskjellige ordninger, men alle ordningene inneholder kostnadsfordelingsmodeller der merkostnadene ved IP-lagring er delt mellom staten og tilbyder, noe som også gjenspeiles i større eller mindre grad i alle forslag til kostnadsmodeller i dette lovforslaget.

Departementet legger til grunn at modell A i størst grad ivaretar hensynet til samfunnsøkonomisk kostnadseffektivitet, ved at tilbyderne har størst insentiv til å velge kostnadseffektive løsninger når de selv må bære investerings- og driftskostnadene. Behovet for en egen kontrollenhet/ordning for å ettergå kostnader ved valgte løsninger, bortfaller med modell A, til forskjell fra de andre modellene.

Etter en totalvurdering av innspillene som er kommet inn, mener departementet at kostnadsfordelingsmodell A bør velges.

11 Økonomiske og administrative konsekvenser

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

11.1 Dagens situasjon

Tilbyder har som nevnt en plikt etter ekomloven § 2-7 femte ledd til å slette eller anonymisere trafikkdata, lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren, så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. Politiet og påtalemyndigheten kan imidlertid få tilgang til slike data så lenge de er lagret etter nærmere regler i straffeprosessloven og ekomloven § 2-9.

11.1.1 Omfang

Kripos opplyser at det ikke foreligger en nasjonal oversikt over antall anmodninger om IP-adresser fra politiet til ekom- 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 tilbyderne. 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-data 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. Tilbakemeldingen fra enkelte av tilbyderne indikerer samtidig at de rene uthentingskostnadene ligger noe lavere enn stykkprisintervallet skulle tilsi.

Det er altså relativt stor variasjon i prisene hos tilbyderne ved utlevering av IP-data til politiet, og det indikerer at det er betydelig variasjon i hva tilbyderne inkluderer i utleveringskostnader og hvor kostnadseffektive systemene og prosessene til de ulike tilbyderne er.

11.2 Ved innføring av lovendringen

11.2.1 Omfang

Det er vanskelig å anslå hvor ofte politiet og påtalemyndigheten vil be om utlevering av IP-adresser og eventuelt portnumre i fremtiden, som følge av lovendringen. Politiet forventer imidlertid en betydelig økning ved innføring av en lagringsplikt.

11.2.2 Kostnader

Det ble før høringen innhentet anslag på hva en lagringsplikt for IP-adresser 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 departementet skissert kostnadsintervaller for hva det vil koste for en 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 11.1).

Tabell 11.1 Kostnadsintervall ved lagring av IP-adresser 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 millioner kroner. Årlige driftskostnader vil være på mellom 100 000 kroner og 3 millioner kroner avhengig av lagringstiden.

Nasjonal kommunikasjonsmyndighet 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 kroner 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-teknologi og hvilke tekniske løsninger som velges hos den enkelte tilbyder. Bruk at NAT-teknologi krever at man lagrer mer data, noe som gir høyere kostnader. Kostnadene ved NAT-teknologi kan ikke angis presist og vil variere med omfanget av bruken, og hvilke tekniske løsninger som er valgt.

Departementet 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 følgelig må anskaffe disse.

Videre er det viktig at politiet har gode systemer for å motta, dekode, presentere og lagre data fra tilbyderne. *Politidirektoratet* opplyser i sitt høringsinnspill at kostnader knyttet til tilpasninger i politiets system for å motta, dekode, presentere og lagre data er avhengig av hvilke systemløsninger som velges, og derfor ikke kan kostnadsfestes på nåværende tidspunkt. *Politidirektoratet* presiserer at kostnader til slike tilpasninger ikke er hensyntatt i dagens utviklingsportefølje i politiet.

Som vist ovenfor er det stor variasjon i kostnadene knyttet til lagring og utlevering av IP-data hos de ulike tilbyderne. Forslaget til lovendring er forventet å berøre alle tjenestetilbydere. Det er på det nåværende tidspunkt ikke mulig å angi nøyaktig hva den samlede investeringskostnaden vil utgjøre, og heller ikke den samlede 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 millioner kroner. I og med at politiet forventer at behovet vil øke fremover, vil altså uthentingskostnadene som staten må dekke, kunne bli betydelig høyere enn 40 millioner kroner, gitt at politiet anmoder om IP-data når de faglig sett har behov for det. Det er usikkerhet knyttet til hvor store disse kostnadene vil bli i tiden fremover, men estimatene ovenfor indikerer at kostnadene vil bli betydelige. Uthentingskostnadene dekkes innenfor politiets til enhver tid gjeldende budsjettrammer.

Som det fremkommer av kapittel 8.6.4, jf. forslag til bestemmelse i ny § 2-8 b, skal anmodninger fremmes skriftlig i et enhetlig format, og politiet skal utarbeide en årlig oversikt over anmodninger som sendes Nasjonal kommunikasjonsmyndighet. Politiet opplyser at det eksisterende systemet for telefoni kan utvikles til å støtte innhenting og statistikk for IP-anmodninger, og at dette i liten grad vil medføre kostnader for politiet. Eventuelle merkostnader for politiet som følge av disse lovendringene, dekkes innenfor politiets gjeldende budsjettrammer.

11.2.3 Gevinster

Innføring av lagring av IP-adresser og portnumre på abonnentsiden i en tidsperiode på 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 straffesaker, noe som gjør at politiet og påtalemyndigheten vil kunne behandle flere saker med samme ressursinnsats. Departementet vurderer at en tallfesting av spart tid, og dermed økt kapasitet på området, vil være utfordrende og lite hensiktsmessig å fremstille

som følge av at en rekke usikre faktorer ville påvirket et slikt estimat. Eksempelvis ville et estimat hvor man regner om akkumulert tid spart per sak, multiplisert med antall etterforskingssaker, være svært sårbart for selv små justeringer (minutter spart). Usikkerheten gjør det altså lite hensiktsmessig å fremstille kvantitative estimater for gevinstene ved lovendringen. Formålet og gevinsten er altså at politiet får et effektivt verktøy i kampen mot alvorlig kriminalitet.

Forslaget om å innføre en lagringsplikt vil ikke komme tilbyderne til gode, og vil følgelig ikke gi gevinster for ekomtilbyderne.

12 Merknader til lovforslaget

Til endringer i § 2-7 femte ledd

Det foreslås en tilpasning i § 2-7 femte ledd *nummer 2* for å klargjøre forholdet mellom sletteplikten i § 2-7 femte ledd og lagringsplikten i § 2-8 a.

Til ny § 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 ekomtjenester. Formålet med bestemmelsen er at de lagrede opplysningene skal kunne brukes til å identifisere personer ved etterforsking av alvorlig kriminalitet.

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, jf. § 1-5.

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 er nødvendige for å identifisere abonnenten ut ifra offentlig IP-adresse og et tidspunkt for kommunikasjon, jf. *bokstav a*. Dette vil 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 er presisert i bestemmelsen at formålet med lagringen er etterforsking av alvorlig kriminalitet. Etter første ledd *siste punktum* går det klart frem at lagringsplikten ikke omfatter destinasjonsinformasjon. Med destinasjonsinformasjon menes informasjon om offentlig IP-adresse og portnummer tilhørende abonnentens kommunikasjonsmotpart, dvs. informasjon om hvem det kommuniseres med. Kravet legger kun føringer på hva som ikke skal lagres, og ikke føringer på de tekniske løsningene som benyttes. Dette betyr blant annet at dersom det anvendes NAT-løsninger som også differensierer mellom ulike abonnenter ved hjelp av kommunikasjonsmotpartens IP-adresse og portnummer, skal slikt informasjon ikke lagres. Konsekvensen av en eventuell bruk av NAT-løsninger som også anvender informasjon om kommunikasjonsmotparten for å skape en entydig binding, er at man ikke kan identifisere en enkelt abonnent, men kun flere abonnenter som har delt samme IP-adresse og portnummer på abonnementssiden på samme tidspunkt.

Det skal heller ikke lagres opplysninger om innholdet i abonnentens internettkommunikasjon. Departementet viser for øvrig til kapittel 4.1.

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

Tredje ledd regulerer kostnadsfordelingsmodellen. Tilbyder må selv dekke investerings- og driftskostnader som påløper for å oppfylle lagringsplikten. Staten dekker kostnadene for utlevering av informasjon etter § 2-8 b første ledd. Investeringskostnader er normalt merkostnader til anskaffelse og oppgradering av maskinvare og programvare for å kunne oppfylle lagringsplikten. Faste driftskostnader omfatter drift, vedlikehold, testing, avskriving av investeringer, lisens- og supportkostnader, leiekostnader og tilhørende personellkostnader. Kostnader for utlevering av informasjon omfatter kostnader knyttet til selve uthentingen av data, og inkluderer blant annet personell- og administrasjonskostnaden for behandling av utleveringsbegjæringer.

Fjerde ledd gir hjemmel for ytterligere regulering i forskrift om lagringsplikten og om kostnader for tilbyderne. Det kan blant annet gis bestemmelser som presiserer nærmere hvilke opplysninger som er omfattet av lagringsplikten og nærmere om fordelingen av merkostnader ved IP-lagringen. I tillegg kan det gis forskrift om revisorbekreftede regnskaper for kostnader som staten skal dekke dersom det viser seg å bli nødvendig. Det kan også gjøres unntak fra lagringsplikten ved enkeltvedtak eller forskrift dersom lagringsplikten ikke er hensiktsmessig, for eksempel for tilbydere som ikke tilbyr tjenester til sluttbruker, jf. § 1-5 nummer 14.

Til ny § 2-8 b

Bestemmelsens *første ledd* gir regler om utlevering av opplysninger lagret etter § 2-8 a. Bestemmelsen åpner kun for utlevering til politi og påtalemyndighet. Opplysninger kan utleveres 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.

Når vilkårene for utlevering er oppfylt, plikter tilbyder å utlevere opplysningene etter skriftlig anmodning fra politiet eller påtalemyndigheten, uten hensyn til taushetsplikt etter § 2-9. Det ligger til politiet eller påtalemyndigheten å ta stilling til om vilkårene for utlevering er oppfylt i det enkelte tilfellet, herunder kravet til nødvendighet. Tilbyder skal derfor ikke foreta noen selvstendig vurdering av vilkårene i bestemmelsen.

Bestemmelsens første ledd oppstiller et generelt nødvendighetskrav, og angir uttømmende hvilke formål opplysningene kan utleveres til. Kravet om nødvendighet innebærer at det ikke kan innhentes flere opplysninger enn det som trengs for formålet i det enkelte tilfellet. Vilkåret skal ikke tolkes så strengt at utlevering av opplysningene må være den eneste løsningen. På den annen side vil det ikke være tilstrekkelig at opplysningene bare vil kunne lette arbeidet. Det må foretas en konkret vurdering av behovet for opplysningene, som må veies mot hensynet til kommunikasjonsvernet. Dette kan innebære at vurderingen kan falle forskjellig ut avhengig av inngrepet i kommunikasjonsvernet i den enkelte sak.

Opplysningene skal utleveres når det er nødvendig for å etterforske en handling som etter loven kan medføre straff av fengsel i tre år eller mer. Strafferammekravet innebærer at saken må inkludere minst én handling som alene kan medføre denne straffen. Bestemmelsen omfatter straffebud som åpner for fengsel «inntil» tre år. 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.

I tillegg åpnes det for at opplysninger kan utleveres for å etterforske nærmere angitte straffebud med lavere strafferamme enn fengsel i tre år. De angitte straffebudene er lovbrudd der IP-data er av særlig stor betydning for etterforskingen. Opplistingen av straffebud med lavere strafferamme er uttømmende.

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

Bestemmelsens *andre ledd* oppstiller krav til anmodningen. Anmodninger om utlevering av opplysninger skal være skriftlige, og skal så vidt mulig opplyse om hva saken gjelder, formålet med anmodningen og hva den omfatter. Begrensningen «så vidt mulig» tar høyde for at det i enkelte tilfeller ikke vil kunne gis fullstendige opplysninger, for eksempel av etterforskingshensyn eller fordi opplysningene er graderte. Vurderingen av hvilke opplysninger som kan gis ved den enkelte anmodningen ligger til politiet og påtalemyndigheten. Det skal fremgå av anmodningen at kravet om nødvendighet etter første ledd er vurdert. Dette kravet gjelder ubetinget. Kravene til anmodningen gjør at det kan etableres et enhetlig system for utforming av anmodningene, og at det går klart frem at vilkårene for utlevering er tilstrekkelig vurdert i forkant av anmodningen. Både politiet og påtalemyndigheten kan anmode om utlevering av opplysninger etter bestemmelsen.

Det følger av *tredje ledd* at politiet og påtalemyndigheten skal sende en årlig rapport om uthentingen av IP-data til myndigheten. Det kan gis nærmere regler i forskrift om rapporteringen, herunder for eksempel om hensiktsmessig nivå og format på rapporteringen, jf. femte ledd.

Fjerde ledd presiserer at opplysninger fra IP-lageret etter § 2-8 a ikke skal utleveres til andre enn politi og påtalemyndighet til formål som er angitt i første ledd. Dette utgjør et unntak fra muligheten til bevisføring av IP-adresser i tvisteloven § 22-3 andre og tredje ledd og åndsverkloven § 87. Unntaket i fjerde ledd medfører at det ikke skal uthentes IP-data fra det nye lageret i medhold av disse lovene. Fjerde ledd presiserer også at det heller ikke kan utgis data fra det nye lageret i medhold av andre lover eller i andre tilfeller enn det som er angitt i første ledd. Dette innebærer at kravene for utlevering til politi- og påtalemyndighet i § 2-8 b første ledd, må være oppfylt for utlevering av IP-data lagret i medhold av § 2-8 a. Bakgrunnen for dette er at det nye lageret av IP-adresser etableres kun for å bekjempe kriminalitet som angitt i bestemmelsen her.

Det følger av *femte ledd* at myndigheten kan gi forskrift om utlevering av data etter § 2-8 b. Forskriftshjemmelen kan blant annet benyttes for å presisere rekkevidden av utleveringsplikten eller til å fastsette nærmere bestemmelser om hvordan utlevering skal skje.

Kommunal- og moderniseringsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i ekomloven (lagring av IP-adresser mv.)

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i lov om elektronisk kommunikasjon (lagring av IP-adresser mv.) i samsvar med et vedlagt forslag.

Forslag
til lov om endringer i lov om elektronisk kommunikasjon (lagring av IP-adresser mv.)

I

I lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon gjøres følgende endringer:

§ 2-7 femte ledd skal lyde:

Trafikkdata, lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren skal slettes eller anonymiseres så snart de ikke lenger er nødvendig:

1. til kommunikasjons- eller faktureringsformål
2. for å oppfylle plikten etter § 2-7 a *og § 2-8 a* eller
3. for å oppfylle andre krav fastsatt i medhold av lov.

Annen behandling av slike data krever samtykke fra bruker.

Ny § 2-8 a skal lyde:

§ 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 til bruk for etterforsking av alvorlig kriminalitet, 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.

Det skal ikke lagres destinasjonsinformasjon.

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

Tilbyder skal dekke investerings- og driftskostnader som påløper for å oppfylle lagringsplikten. Staten dekker kostnadene for utlevering av informasjon etter § 2-8 b første ledd.

Myndigheten kan gi forskrift om lagringsplikten, om et nærmere system for kostnadsfordelingen og om bruk av revisor for kostnader som dekkes av staten. Myndigheten kan ved enkeltvedtak eller forskrift gi unntak fra lagringsplikten.

Ny § 2-8 b skal lyde:

§ 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 for å etterforske en handling som etter loven kan medføre straff av fengsel i 3 år eller mer, eller som rammes av straffeloven §§ 125, 168, 184, 201, 202, 204, 205, 251, 263, 266, 297, 298, 305, 306 eller 309, eller åndsverkloven § 104 jf. § 79.

Anmodninger om utlevering etter første ledd skal fremsettes skriftlig og skal så vidt mulig opplyse om hva saken gjelder, formålet med anmodningen og hva den omfatter. Det skal fremgå at kravet om nødvendighet etter første ledd er vurdert.

Politiet og påtalemyndigheten skal oversende en årlig rapport om uthentingen av IP-adresser til myndigheten.

Opplysninger som kun er lagret etter § 2-8 a kan ikke gis ut i medhold av tvisteloven § 22-3 andre og tredje ledd eller åndsverkloven § 87, eller andre lover eller i andre tilfeller enn angitt i første ledd.

Myndigheten kan gi forskrift om utlevering av data etter denne bestemmelsen og om politiet og påtalemyndighetens rapportering om innhenting av opplysninger.

II

1. Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til ulik tid.
2. Kongen kan gi nærmere overgangsregler.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: Departementenes sikkerhets- og serviceorganisasjon – 04/2021