Høringsnotat

Utlevering av IP-data til forebygging av alvorlig kriminalitet

Høringsfrist 6. oktober 2025

Innhold

1. Sammendrag

Med IP-data menes i dette høringsnotatet de opplysninger som er nødvendige for å identifisere en abonnent basert på offentlig IP-adresse (Internet Protocol Address) og tidspunkt, eventuelt også portnummer dersom flere deler samme IP-adresse. I dette høringsnotatet foreslår Digitaliserings- og forvaltningsdepartementet og Justis- og beredskapsdepartementet (departementene) at det, innenfor nærmere angitte rammer åpnes for utlevering av IP-data til PST og politiet for øvrig for å forebygge alvorlig kriminalitet.

Utlevering av IP-data til forebyggingsformål vil bare være tillatt dersom inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig. For at opplysninger skal kunne utleveres til dette formålet foreslår departementene et vilkår om at det må være *grunn til å undersøke om noen forbereder nærmere bestemte straffbare handlinger*. Dette innebærer blant annet at det må være konkrete objektive omstendigheter som tilsier at noen forbereder en straffbar handling.

Departementene foreslår ulike terskler for når opplysningene kan utleveres, avhengig av om det er PST eller politiet for øvrig som anmoder om opplysningene. Departementene foreslår at PST skal kunne få utlevert IP-data som ligger inntil 12 måneder tilbake i tid. Videre foreslår departementene at IP-data skal kunne utleveres for å forebygge alle straffbare handlinger som hører under PSTs mandat, jf. politiloven § 17 b. Dette er begrunnet i at PST skal forebygge straffbare handlinger med svært alvorlige samfunnsmessige konsekvenser dersom de inntreffer. Ettersom PST primært arbeider forebyggende, er det viktig å sette slike rammer for PSTs uthenting av IP-data som gjør tiltaket til et egnet verktøy i det forebyggende arbeidet.

For politiet for øvrig foreslår departementene at IP-data fra inntil 6 måneder tilbake i tid skal kunne utleveres. Det foreslås at IP-data skal kunne utleveres til politiet for å forebygge overtredelse av straffebud med strafferamme på 6 år eller mer, med nærmere angitte unntak der IP-data vurderes å være særlig viktig for å kunne forebygge handlingen. De straffebudene med lavere strafferamme som foreslås inkludert gjelder i hovedsak seksuallovbrudd, men det foreslås også å gjøre unntak fra strafferammekravet for enkelte straffebud som gjelder handlinger som begås helt eller delvis på nett og gjerne i stort omfang, som datainnbrudd og utpressing.

IP-data til forebygging skal etter forslaget bare kunne utleveres på bakgrunn av en IP-adresse, ikke med utgangspunkt i abonnent. Dette innebærer at det til forebyggende formål, etter forslaget, ikke vil kunne utleveres informasjon om hvilke IP-adresser en gitt abonnent var tildelt på et gitt tidspunkt eller i en gitt tidsperiode.

1.1. Bakgrunn

Norge er et av verdens mest digitaliserte land og ligger i verdenstoppen når det gjelder bruk av internett. Samfunnet har aldri vært mer avhengig av digital infrastruktur. Bedrifter og forvaltning over hele landet blir stadig mer digitalisert, og ny teknologi benyttes til nye funksjoner av folk i alle aldersgrupper. Den teknologiske utviklingen gjenspeiles samtidig i kriminalitetsbildet. Kriminalitet skjer i stadig større grad ved hjelp av digitale verktøy. Det er i tillegg en generell trend at kommunikasjon i økende grad blir internettbasert, for eksempel ved at nettbaserte kommunikasjonstjenester tar over for telefonoppringninger og SMS.

Muligheten til å kunne ettergå aktivitet på internett kan være sentralt for forebygging av kriminalitet. Tilgang til informasjon om hvem som kan knyttes til bruk av en konkret IP-adresse vil kunne være avgjørende for å sette inn målrettede og effektive tiltak. Samtidig har personvern og vern av borgernes kommunikasjon (kommunikasjonsvern) stor verdi i et demokratisk samfunn. Brukerne av internett, mobilkommunikasjon og bredbånd mv. må kunne ha tillit til at de trygt kan bruke tjenestene uten å måtte gi fra seg mer informasjon enn nødvendig, og uten at uvedkommende får tilgang til kommunikasjonen. Retten til privatliv, respekt for personlig kommunikasjon og ytringsfrihet er vernet i Grunnloven og EMK. Både person- og kommunikasjonsvern og ytringsfrihet, herunder pressens kildevern, er forutsetninger for et velfungerende demokrati.

Regulering av politiets tilgang til IP-data for forebyggende formål må balansere behovet for effektiv kriminalitetsbekjempelse og hensynet til person- og kommunikasjonsvernet. Tiltak som griper inn i borgernes rett til konfidensiell elektronisk kommunikasjon må oppfylle kravene til nødvendighet og forholdsmessighet som følger av blant annet EMK. Når inngrepet skjer på et stadium der det ikke foreligger konkret mistanke om en straffbar handling, blir denne balansen særlig viktig.

I 2021 ble det vedtatt regler om lagring av IP-adresser til bruk for etterforsking av alvorlig kriminalitet i den tidligere ekomloven av 2003, jf. Prop. 167 L (2020-2021). Disse bestemmelsene er nå videreført i gjeldende ekomlov §§ 3-13 og 3-14. I det forutgående høringsnotatet til endringen i 2021 foreslo departementene at IP-data skulle kunne utleveres både for å forebygge og etterforske alvorlige straffbare handlinger. Utgangspunktet var 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. Av høringsinstansene var særlig Advokatforeningen og Datatilsynet kritiske til å åpne for utlevering av IP-data for forebyggingsformål. Disse pekte blant annet på at det vil være vanskeligere å kontrollere behovet for opplysningene, samt at begrepet «forebygging» ikke har noen klar definisjon og ble ansett som lite egnet som vilkår for utlevering. På bakgrunn av disse høringsinnspillene konkluderte departementet i Prop. 167 L (2020-2021) s. 53 med 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.

I Prop. 93 LS (2023-2024) punkt 6.1.5 uttalte departementet:

> I lys av den teknologiske utviklingen, kriminaliteten på internett og særlig PSTs behov, vil departementet nå utrede om IP-data skal utleveres i saker der skadepotensialet er så stort at det av hensyn til samfunnet må anses som proporsjonalt innenfor tydelige og gode rammer, å gi tilgang til slike data for å forebygge alvorlige hendelser, og tilsvarende i visse saker der IP-data er særlig viktig for muligheten til å forebygge lovbruddet.

For å utrede spørsmålene nærmere ble det våren 2024 nedsatt en arbeidsgruppe med deltakere fra DFD, JD og Nasjonal kommunikasjonsmyndighet (Nkom) som fikk i oppgave å vurdere hvorvidt utlevering av IP-data skulle utvides til å omfatte utlevering til forebyggingsformål og foreslå rammer for en eventuell utlevering. Arbeidsgruppen anbefalte at det åpnes for utlevering av IP-data for å forebygge alvorlig kriminalitet, innenfor nærmere angitte rammer. Arbeidsgruppens anbefalinger ligger til grunn for forslaget som presenteres i høringsnotatet.

2. Om IP-adresser

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

Når en internettilbyder gir en abonnent tilgang til internett, tildeler nettilbyderen abonnenten en IP-adresse. Denne kan enten være tildelt fast (statisk) eller midlertidig (dynamisk). Med fast tildelt IP-adresse vil abonnentens IP-adresse alltid være den samme. Abonnenter med dynamisk tildelt IP-adresse vil midlertidig tildeles en IP-adresse, for eksempel når man kobler seg opp til nettet hjemme, eller basert på tidsintervaller. Dynamiske tildelinger er mye brukt overfor privatpersoner. Dynamisk tildeling av IP-adresser brukes av flere grunner, blant annet fordi det forenkler tildelingsprosessen og administrasjonen av nettverket for tilbyderen, for eksempel ved bruk av DHCP (Dynamic Host Configuration Protocol).

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.

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 også ved deling av IP-adresser kunne være mulig å identifisere en enkeltabonnent. 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 (Network Address Translation) gjør at det ikke nødvendigvis er mulig å identifisere én enkelt abonnent utelukkende på grunnlag av en IP-adresse og et tidspunkt for kommunikasjonen. IP-adressen og tidspunktet vil imidlertid kunne gi en liste over alle abonnentene som benyttet IP-adressen på det aktuelle tidspunktet. Versjonen av internett-protokollen som er mest utbredt i dag, IPv4, blir gradvis erstattet av den nye standarden IPv6. Innenfor IPv6 finnes det et langt større antall unike IP-adresser. Det er forventet at bruken av dynamisk tildeling av IP-adresser vil fortsette etter overgangen til IPv6, men at behovet for dagens bruk av NAT på grunn av adressemangel, vil falle bort. Det må imidlertid legges til grunn at IPv4 4 og IPv6 vil sameksistere i lang tid fremover, og at noen av overgangsmekanismene kan kreve NAT-lignende loggbehov.

3. Gjeldende rett om lagring og utlevering av IP-adresser

3.1. Tilbydernes taushetsplikt

Det følger av ekomloven § 3-10 at tilbyder og installatør plikter å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter. Taushetsplikten omfatter en plikt til å bevare taushet om abonnentinformasjon, herunder opplysninger om abonnenters disponering av IP-adresser.

I ekomloven § 3-10 tredje ledd første og andre punktum gis det samtidig unntak fra taushetsplikten for utlevering av enkelte, bestemte opplysninger (abonnementsopplysninger) til politi, påtalemyndighet og ved vitnemål for retten, herunder også opplysninger om elektronisk kommunikasjonsadresse. Politiet eller påtalemyndigheten kan etter dette få informasjon om navn, adresse og telefonnummer tilknyttet en elektronisk kommunikasjonsadresse, jf. Prop. 93 LS (2023-2024) (ekomloven).

Ekomloven § 3-11 angir at trafikkdata, lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren skal slettes eller anonymiseres så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål, eller for å oppfylle andre krav fastsatt i lov. I praksis har man lagt til grunn at IP-adresser kan lagres inntil 21 dager for driftsrelaterte formål, og ifølge opplysninger fra noen av de største internettilbyderne lagres IP-adresser normalt i 21 dager.

IP-adresser som for en kort periode er lagret for tilbyders egen drift og som faller inn under unntaket i § 3-10 tredje ledd første punktum, utleveres til politiet uten forutgående kjennelse fra retten eller fritak fra taushetsplikten fra Nkom.

3.2. Lagringsplikt og utlevering av abonnementsinformasjon

Tilbyder av elektroniske kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, og tilbyder av slik tjeneste, skal etter ekomloven § 3-13, til bruk for etterforsking av alvorlig kriminalitet, lagre de opplysninger som er nødvendige for å identifisere abonnentene med utgangspunkt i

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

Bestemmelsens tredje ledd angir at opplysningene skal lagres i 12 måneder fra den dagen kommunikasjonen avsluttes. Videre fastsetter bestemmelsen at tilbyder skal dekke investerings- og driftskostnader som påløper for å oppfylle lagringsplikten, mens staten dekker kostnadene for utlevering av informasjonen.

I merknadene til bestemmelsen påpekes det at «kravet om nødvendighet innebærer at det ikke skal lagres flere opplysninger enn det formålet krever.» Det pekes videre på at «formålet med lagringen er etterforsking av alvorlig kriminalitet» og at «lagringsplikten ikke omfatter destinasjonsinformasjon.» Med destinasjonsinformasjon menes informasjon om offentlig IP-adresse og portnummer tilhørende abonnentens kommunikasjonsmotpart, det vil si informasjon om hvem det kommuniseres med.[1]

Ekomforskriften §§ 3-5 og 3-6 gir nærmere regler om tilbyders plikter i forbindelse med lagring og krav om utlevering av IP-adresser, og om politiet og påtalemyndighetens årlige rapportering. Etter forskriften § 3-5 tredje ledd kan anmodninger fra politi- og påtalemyndighet ta utgangspunkt i IP-adresser og abonnenter.

Etter ekomloven § 3-14 skal tilbyderne, uten hinder av taushetsplikten etter § 3-10, utlevere IP-data 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 straffeloven §§ 125, 168, 184, 201, 202, 204, 205, 251, 263, 266, 267 a første ledd, 267 b, 297, 298, 305, 306 eller 309, eller åndsverkloven § 104, jf. § 79.» Enkelte av disse straffebudene gjelder lovbrudd der IP-data kan være av særlig stor betydning for etterforskingen.

De nevnte straffebudene har alle en strammeramme på bot eller fengsel inntil 1 eller 2 år, og gjelder følgende handlinger:

Strl. § 125 (uaktsom avsløring av statshemmelighet), § 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), § 267 a første ledd (deling av krenkende bilder mv.), § 267 b (grov

deling av krenkende bilder mv.), § 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) eller § 309 (kjøp av seksuelle tjenester fra mindreårige), eller åndsverkloven § 104 jf. § 79 (retten til eget bilde).

Om kravet om nødvendighet understrekes det i merknadene til bestemmelsen at abonnementsinformasjon kan være nødvendig i en etterforsking for andre formål enn å identifisere ukjente gjerningspersoner, for eksempel 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.[2]

Ekomloven § 3-14 fjerde ledd presiserer at opplysninger som kun er lagret etter § 3-13, ikke kan utleveres 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. Etter § 3-14 annet ledd skal anmodninger om utlevering fremsettes skriftlig og 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.

I merknadene til bestemmelsen fremgår det at 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. 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.

Etter ekomforskriften § 3-5 tredje ledd andre til femte punktum skal tilbyder «utlevere liste over alle abonnenter som har vært tilordnet en IP-adresse på aktuelt tidspunkt når anmodninger ikke inneholder informasjon om portnummer på abonnentssiden. Tilbyder skal utlevere all tilgjengelig abonnentinformasjon knyttet til identifiserte abonnenter i forbindelse med anmodningen. Tilbyder skal ikke utlevere opplysninger om abonnement og abonnentens utstyr etter bestemmelsen her med unntak av tidspunktet for når abonnementet ble opprettet. Tilbyder skal utlevere informasjon om tidspunkt og tidsperiode abonnenten har vært tilordnet IP-adressen og portnummer om dette har vært benyttet.»

Politiet og påtalemyndigheten skal oversende en årlig rapport om uthentingen av IP-adresser til Nkom, jf. ekomloven § 3-14 tredje ledd og forskriften § 3-6 første ledd.

Det er utarbeidet en standardisert løsning for politiets anmodning av IP-data og svar fra tilbyderne. Løsningen forutsetter at alle tilbydere etter § 3-13 første ledd registreres i politiets portal for innsending av ekomopplysninger. Hver tilbyder har sin egen side i portalen, hvor de kan motta og besvare anmodninger enten direkte i portalen eller via en API-løsning. Løsningen sørger for sikker overføring gjennom kryptering, autentisering og autorisasjon.

3.3. Straffeprosessloven og politilovens regler om forebygging og etterforsking

Verken straffeprosessloven eller politiloven har bestemmelser som definerer forebygging eller angir når politiet kan sies å handle forebyggende. Dette har sammenheng med at politiets forebyggende virksomhet etter sin art er vanskelig å definere og omfatter en rekke ulike situasjoner og virkemidler.

Vilkårene for å åpne etterforsking følger av straffeprosessloven § 224 første ledd. Bestemmelsen angir at etterforsking «foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige», jf. straffeprosessloven § 224 første ledd. Riksadvokatens rundskriv RA-1999-3 presiserer nærmere hva som skal anses som etterforsking. Av punkt II 2 fremgår at virksomhet som har som siktemål å «avklare om straffbart forhold finner eller har funnet sted, og i tilfelle hvor, når og hvem som er ansvarlig», er å anse som etterforsking. De sentrale momentene i vurderingen av om det er «rimelig grunn» er sannsynligheten for at det er begått et straffbart forhold, om forholdets alvor bærer den etterforskingsinnsats som saken krever (proporsjonalitet, og om etterforskingen er saklig begrunnet, jf. rundskrivet punkt III 3.

PST er, som eneste politiorgan, gitt anledning til å benytte skjulte tvangsmidler, som skjult beslag, skjult utleveringspålegg, kommunikasjonskontroll, dataavlesing og romavlytting, i forebyggende øyemed. Etter politiloven § 17 d kan PST få rettens godkjenning til å bruke skjulte tvangsmidler dersom det er «grunn til å undersøke om noen forbereder en handling» som rammes av nærmere bestemte straffebud. Vilkåret «grunn til å undersøke» ble tilføyd av justiskomiteen, jf. Innst. O. nr. 113 (2004–2005) punkt 9.2. I innstillingen uttales det at grunnen til å undersøke etter flertallets syn må være “forankret i objektive holdepunkter, for eksempel saksopplysninger i form av spanings- eller infiltrasjonsopplysninger, tips, dokumentfunn eller andre bevis som indikerer at noen kan være i ferd med å forberede for eksempel en terrorhandling”. Flertallet i komiteen uttalte videre at vilkåret har klare likhetstrekk med vilkåret i straffeprosessloven § 224 første ledd om når etterforsking skal settes i verk, som gjennom praksis har fått et klart definert innhold, særlig gjennom rundskriv RA-1999-3 fra riksadvokaten. Forståelsen av vilkåret i straffeprosessloven § 224 gir derfor også veiledning for forståelsen av uttrykket «grunn til å undersøke» i politiloven § 17 d. Kravet om «grunn til å undersøke» innebærer ifølge innstillingen både et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling, og et krav til forholdsmessighet. Det må være konkrete objektive omstendigheter som tilsier at noen forbereder en handling som angitt.

4. Rettslige rammer for regler om lagring og utlevering av IP-data

4.1. Retten til privatliv og vern av kommunikasjon etter Grunnloven og EMK

Retten til privatliv og respekt for personlig kommunikasjon er vernet gjennom Grunnloven § 102. Første ledd første punktum lyder: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.» En tilsvarende rettighet følger av EMK artikkel 8, som gir enhver rett til respekt for sitt privatliv og familieliv. Inngrep fra offentlige myndigheter i utøvelsen av denne rettigheten kan bare skje dersom tiltaket er hjemlet i lov, skal beskytte nærmere bestemte formål og er forholdsmessig. Grunnloven § 102 første ledd første punktum har klare likhetstrekk med EMK artikkel 8 og må tolkes i lys av denne, jf. Prop. 167 L (2020–2021) Endringer i ekomloven (lagring av IP-adresser med videre) kapittel 5.2.

EMK artikkel 8 nr. 2 angir at inngrep i retten til privatliv kan være begrunnet i hensynet til å forebygge uorden eller kriminalitet. Prinsippet om at myndighetenes inngrep overfor den enkelte innbygger må ha hjemmel i lov (legalitetsprinsippet), innebærer at inngrepshjemler må være tydelige og presise. Det følger videre av proporsjonalitetsprinsippet at lovgivningen må være klar og begrenses til det som er strengt nødvendig. Det innebærer at både lagringen av IP-data og vilkårene for utlevering må være forholdsmessige.

I Prop. 167 L (2020-2021) 5.2 er det nærmere redegjort for relevant rettspraksis fra EMD om retten til privatliv og vern av kommunikasjon. Departementene har ikke avdekket nyere rettspraksis av direkte relevans for forslagene i dette høringsnotatet.

I *Podchasov mot Russland,* saksnr. 33696/19, 13. februar 2024, uttalte domstolen at rettshåndhevende myndigheters tilgang til lagrede opplysninger i enkeltsaker må ledsages av de samme garantier som hemmelig overvåking (avsnitt 72). Dommen gjaldt imidlertid en langt mer omfattende plikt for tilbyderne til å lagre og utlevere opplysninger enn forslaget i høringsnotatet her. Russiske tilbydere var pålagt ved lov å lagre alle kommunikasjonsdata i ett år og innholdet i all kommunikasjon i seks måneder, og utlevere dette til myndighetene i nærmere angitte tilfeller. Tilbyderne var også pålagt å utlevere informasjon som var nødvendig for å dekryptere kryptert informasjon. Uttalelsene i dommen har dermed ikke direkte overføringsverdi til en klart avgrenset plikt til å lagre og utlevere IP-data.

4.2. Ytringsfrihet, herunder pressens kildevern

Ytringsfriheten er vernet av både Grunnloven § 100, EMK artikkel 10 og SP artikkel 19. Vernet etter disse bestemmelsene er i det alt vesentlige sammenfallende. Inngrep i retten til ytringsfrihet etter EMK artikkel 10 nr. 1 må kunne rettferdiggjøres etter vilkårene i nr. 2, som krever at inngrepet har tilstrekkelig hjemmel, har et legitimt formål og er forholdsmessig. Forebygging av kriminalitet er et formål som kan begrunne inngrep i ytringsfriheten etter EMK artikkel 10.

Pressefriheten er et viktig element i retten til ytringsfrihet etter EMK artikkel 10. Selv om det ikke fremgår direkte av ordlyden, følger det av EMDs praksis at pressens ytringsfrihet også omfatter retten til kildevern, jf. blant annet *Goodwin mot Storbritannia,* saksnr. 17488/90, 27. mars 1996, avsnitt 39. Kildevernet etter EMK artikkel 10 medfører blant annet begrensninger i adgangen til å pålegge journalister å avsløre en kildes identitet eller fremlegge dokumenter som indirekte medfører at kildens identitet avsløres. Det vil utgjøre et inngrep i kildevernet hvis myndighetene pålegger journalister å utlevere dokumenter eller materiale. 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,* saksnr. 50001/12, 30. januar 2020, 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.

I Prop. 167 L (2020-2021) punkt 5.3 er det nærmere redegjort for relevant rettspraksis fra EMD om ytringsfrihet, herunder pressens kildevern. Kildevernet er også drøftet i proposisjonen punkt 8.7. Departementene har ikke avdekket nyere rettspraksis av direkte relevans for forslagene i dette høringsnotatet.

4.3. Kommunikasjonsvern etter EØS-retten

EUs bestemmelser om kommunikasjonsvern er i hovedsak fastsatt i kommunikasjonsverndirektivet (2002/58/EF) med senere endringer. Direktivet er innlemmet i EØS-avtalen. Direktiv 2009/136/EF, som endret kommunikasjonsverndirektivet, er ikke innlemmet i EØS-avtalen, men innholdet er i all hovedsak gjennomført i norsk rett gjennom ekomloven.

Tilbyders plikt til å bevare taushet om innholdet av elektronisk kommunikasjon er en grunnleggende forutsetning for kommunikasjonsvernet. Bestemmelser om taushetsplikt finnes i kommunikasjonsverndirektivet artikkel 5. Kommunikasjonsverndirektivet artikkel 6 og 9 gir som hovedregel en plikt for tilbyder til å slette eller anonymisere trafikkdata, inkludert lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren, så snart det ikke lenger er nødvendig å beholde dataene for å oppfylle visse angitte formål. Et unntak følger av kommunikasjonsverndirektivet artikkel 15, der det fremgår 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 (…)». Kommunikasjonsverndirektivet artikkel 15 åpner dermed for at forebygging av kriminalitet kan begrunne inngrep i kommunikasjonsvernet.

Rekkevidden av unntaket i artikkel 15 er tolket i flere avgjørelser fra EU-domstolen. Av særlig interesse er de to La Quadrature du Net-dommene. I den første, de forente sakene C-511/18, C-512/18 og C-520/18 *av* 6. oktober 2020 (*La Quadrature du Net - LQdN1),* ble det innledningsvis i avsnitt 141 slått fast at generell og udifferensiert lagring av trafikk- og lokaliseringsdata for å bekjempe alvorlig kriminalitet, går lenger enn det som er strengt nødvendig, og ikke kan forsvares i et demokratisk samfunn. Domstolen nyanserte så dette ved å vise til at data som kun er egnet til å identifisere en person, er mindre sensitive enn andre data. Domstolen viste videre til at det skal tas hensyn til de tilfeller der IP-data er eneste mulighet for å identifisere en abonnent. På denne bakgrunn uttalte domstolen at det

kunne åpnes for generell lagring av IP-data, men under forutsetning av at dette er "betinget af en streng overholdelse af de materielle og proceduremæssige betingelser, der skal gælde for brugen af disse data" (avsnitt 155). Domstolen la til grunn at IP-adresser blant annet kan brukes til "at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktivitete", og at lagring av IP-adresser som muliggjør slik sporing utgjør et alvorlig inngrep (avsnitt 153). Det ble deretter presisert at slik lagring 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, jf. avsnitt 156.

EU-domstolen i full rett avsa 30. april 2024 avgjørelse i sak C-470/21 L*a Quadrature du Net mfl. mot Premier ministre og Ministre de la Culture (LQdN2)*. Saken gjaldt det franske systemet for forebygging og håndheving av brudd på opphavsrettskrenkelser på nett, der et forvaltningsorgan, uten uavhengig forhåndskontroll, innhentet IP-data fra tilbyderne for å sende varsler til abonnenter om at deres internettilgang var blitt brukt til opphavsrettskrenkelser. Ved tre varsler innenfor en gitt tidsperiode ville saken kunne oversendes påtalemyndigheten med henblikk på å innlede straffeforfølgning. Det sentrale spørsmålet i saken var om en offentlig myndighets tilgang til identitetsdata knyttet til en IP-adresse er blant de trafikk- og lokaliseringsdata som prinsipielt må underlegges uavhengig forhåndskontroll.

I dommen justerer domstolen sine tidligere uttalelser i avgjørelsen i LQdN1. I avsnitt 79 uttales at enhver generell og udifferensiert lagring av IP-adresser ikke nødvendigvis utgjør et alvorlig inngrep. Domstolen viser til at tidligere avgjørelser har berørt regelverk som pålegger lagring av flere typer opplysninger, herunder både avsender- og mottakeradresser (destinasjons-IP). Lagring av IP-adresser innenfor slik lovgivning kan, hensett til andre lagringspliktige opplysninger og mulighet til å kombinere opplysningskategorier, gjøre det mulig å trekke presise slutninger om en persons privatliv, jf. avsnitt 80 og 81.

Domstolen åpner deretter i avsnitt 82 for at IP-adresser kan lagres for bekjempelse av alminnelig kriminalitet, dersom det utelukkes at lagringen kan utgjøre et alvorlig inngrep ved å gjøre det mulig å trekke presise konklusjoner om personens privatliv ved å koble de lagrede IP-adressene med andre opplysninger som er underlagt lagringsplikt. Domstolen oppstiller deretter krav som må være oppfylt for at lagring av IP-adresser i slike tilfeller ikke skal anses som et alvorlig inngrep, blant annet at ulike kategorier lagringspliktige data lagres atskilt fra hverandre med vanntette skott, at eventuell kobling mellom sivil identitet og IP-adresser må skje på en måte som ikke uthuler effekten av skottene, og at den tekniske løsningen for separasjon må kontrolleres jevnlig av en annen offentlig etat enn den som ber om opplysninger (avsnitt 86 til 89). Dersom disse kravene er oppfylt, er tilgang i prinsippet ikke betinget av forutgående uavhengig kontroll (avsnitt 134). Domstolen uttaler likevel at det ikke kan utelukkes at opplysninger som myndighetene får tilgang til i systemer som det franske, i atypiske situasjoner kan avsløre opplysninger som gjør det mulig å trekke presise slutninger om en persons privatliv (avsnitt 135). For det franske systemet måtte det derfor på et gitt stadium i prosessen foretas en uavhengig forhåndskontroll for å utelukke risiko for uforholdsmessige inngrep (avsnitt 141). Domstolen uttalte at slik forhåndskontroll måtte skje i den tredje fasen der myndigheten vurderte om saken skulle oversendes påtalemyndigheten for strafforfølging (avsnitt 142-143).

5. Utenlandsk rett

5.1. Sverige

Den svenske lagen (2022:482) om elektronisk kommunikation 9. kap. 19 § pålegger tilbydere å lagre bl.a. abonnementsopplysninger. Dette omfatter bl.a. opplysninger om abonnentens nummer, navn og adresse. Også opplysninger om faste og dynamiske IP-adresser regnes som abonnementsopplysninger dersom formålet med opplysningene er å identifisere en abonnent eller en registrert bruker, jf. Prop. 2018/19:86 s. 93. Opplysningene skal lagres i ti måneder, jf. 9 kap. 22 § stk. 1 andre strekpunkt. Et forslag om å utvide lagringstiden til 12 måneder har vært på høring, med frist 17. januar 2025.[1]

Etter 9. kap. 33 § stk. 1 nr. 2 skal tilbyderne etter begjæring utlevere abonnementsopplysninger i tilfeller som gjelder «brottslig verksamhet eller misstanke om brott» til bl.a. Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, eller Åklagarmyndigheten. Det stilles ikke krav til lovbruddets alvorlighet.
Av forarbeidene fremgår det at bestemmelsen ikke er begrenset til etterforsking («förundersökning»), men også får anvendelse i de kriminalitetsbekjempende myndighetenes etterretningsvirksomhet. Etterretningsvirksomhet omfatter bl.a. arbeidet med innsamling, bearbeiding og analyse av informasjon med sikte på å forhindre eller oppdage «brottslig verksamhet» når det ennå ikke er mistanke om at et konkret lovbrudd er begått, jf. Prop. 2021/22:183 s. 61.

Abonnementsopplysninger kan også utleveres til andre myndigheter i nærmere bestemte tilfeller uten at det er knyttet til en pågående etterforsking, jf. 9. kap. 33 § stk. 1 nr. 1 bokstav a til l. Dette omfatter bl.a. utlevering til legemiddelverket ved tilsyn med markedsføringsreglene etter legemiddelloven (bokstav g), til politiet i forbindelse med ulykker (bokstav h) eller lokalisering av personer som er dømt til fengsel mv. (bokstav i) samt til skattemyndighetene i sak om kontroll av skatt eller avgift (bokstav k).

[1] Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information - Regeringen.se

5.2. Danmark

Det er i dansk rett ikke åpnet for utlevering av lagringspliktig informasjon utenfor etterforsking.

Den danske retsplejeloven § 786 f pålegger tilbydere å foreta generell og udifferensiert lagring av opplysninger om en sluttbrukers adgang til internett. Opplysningene skal lagres i ett år.

Opplysninger om *dynamisk* IP-adresse utleveres etter reglene om edition, jf. retsplejeloven § 804. Etter denne bestemmelsen kan det, som ledd i etterforsking av et lovbrudd som er underlagt offentlig påtale, gis pålegg om å fremvise eller utlevere gjenstander som kan tjene som bevis. Avgjørelse om pålegg om edition treffes av retten ved kjennelse etter begjæring

fra politiet, jf. retsplejeloven § 806 stk. 1 og 2. Det stilles ikke krav til lovbruddets alvorlighet ut over at det må være underlagt offentlig påtale.

Opplysninger om *statisk* IP-adresse utleveres på begjæring fra politiet uten krav om rettslig kjennelse, jf. retsplejeloven § 804 b. Utleveringen må skje som ledd i etterforskingen av et lovbrudd som er underlagt offentlig påtale, eller en krenkelse som nevnt i § 2 stk. 1 nr. 1 i lov om tilhold, opholdsforbud og bortvisning (brudd på oppholdsforbud). Det stilles ikke krav til lovbruddets alvorlighet ut over at det må være underlagt offentlig påtale.

5.3. Finland

Den finske lag om tjänster inom elektronisk kommunikation (917/2014) 19. kap. 157 § pålegger lagringspliktige foretak å lagre nærmere bestemte opplysninger for myndighetenes behov. Dette omfatter bl.a. opplysninger om internettaksesstjenester, jf. 157 § annet ledd nr. 3. I Föreskrift om teleföretagens skyldighet att lagra uppgifter för myndigheternas behov (Kommunikationsverket 53B/2014 M) 6 § er det angitt at lagringsplikten bl.a. omfatter statisk og dynamisk IP-adresse og abonnentens identitetsopplysninger.

Opplysningene skal lagres i ni måneder.

Opplysningene kan bare brukes for å etterforske og påtale («utreda och åtalspröva) lovbrudd som nevnt i tvångsmedelslagen (806/2011) 10. kap. 6 § annet ledd. Dette omfatter lovbrudd med en strafferamme på fengsel i minst 4 år, eller som omfattes av nærmere angitte lovbruddskategorier.

Lovens ordlyd åpner ikke for utlevering i forebyggende øyemed.

6. Departementenes vurderinger

6.1. Bør utlevering av IP-data utvides til å omfatte utlevering til forebyggingsformål?

6.1.1. Innledning

Det er ulike hensyn som taler for og mot å åpne for utlevering av IP-data i forebyggende øyemed. På den ene siden har politiet behov for IP-data i kriminaltetsbekjempende øyemed også utenfor etterforsking. Hensynet til å forebygge alvorlig kriminalitet er et legitimt hensyn som kan begrunne inngrep i flere grunnleggende rettigheter. Samtidig taler hensynet til retten til privatliv, personvern, kommunikasjonsvern og ytringsfrihet for tilbakeholdenhet med å utvide adgangen til å utlevere IP-data til nye formål. Når det foreslås at IP-data skal kunne utleveres til nye formål, må hvilke formål dataene skal lagres for også utvides.
Ved avveiningen må det ses hen til hvilke vilkår som i tilfelle kan eller må stilles for at utlevering skal være forholdsmessig, noe som omtales i punktene nedenfor.

6.1.2. Hensynene til retten til privatliv, vern av kommunikasjon og ytringsfriheten

Forslaget om å åpne for utlevering av IP-data for å forebygge alvorlig kriminalitet reiser prinsipielle spørsmål om inngrep i retten til privatliv, personvern og kommunikasjonsvern.

Prinsippet om vern av kommunikasjon står sterkt både i norsk rett og i internasjonale menneskerettighetskonvensjoner. Kommunikasjonsvernet utgjør en del av retten til privatliv og personvern, da det er vanskelig å tenke seg et effektivt personvern uten at kommunikasjon mellom to eller flere parter kan være fortrolig. Kommunikasjonsvernet omfatter også informasjon som kommer fra juridiske personer og som derfor ikke faller inn under kategorien "personopplysninger", som for eksempel forretningssensitiv informasjon.

Kommunikasjonsvernet innebærer at den enkelte i størst mulig grad skal kunne kommunisere elektronisk uten inngrep fra myndigheter eller andre aktører, med mindre det foreligger et klart og legitimt grunnlag for slik inngripen. Vern av kommunikasjon er en grunnleggende forutsetning for en fri og åpen debatt i ethvert demokratisk samfunn, og det vil kunne ha negativ innvirkning på den frie meningsdannelsen hvis kommunikasjonsvernet ikke respekteres. Hvordan en stat ivaretar denne grunnleggende rettigheten har også betydning for borgernes tillit til og bruk av digitale tjenester. Slikt sett er kommunikasjonsvern en forutsetning for digitaliseringen av samfunnet. Ettersom den teknologiske utviklingen har ført til at borgerne legger igjen flere digitale spor enn tidligere, er behovet for effektivt kommunikasjonsvern blitt desto viktigere.

I ekomsektoren er kommunikasjonsvernet forankret i regler om blant annet taushetsplikt og sletteplikt, som skal hindre unødvendig lagring og utlevering av opplysninger om brukernes elektroniske kommunikasjon. IP-adresser er en type trafikkdata, som i utgangspunktet gir begrenset informasjon om abonnentenes bruk av internett. Informasjon om en tildelt IP-adresse viser i seg selv bare at en abonnent har hatt tilgang til internett på et gitt tidspunkt. Det lagres ikke opplysninger om innholdet i kommunikasjonen, hvilke nettsteder som er besøkt, eller hvem brukeren har kommunisert med. Samtidig er formålet med å lagre og utlevere IP-data til kriminalitetsbekjempelse, enten det er forebygging eller etterforsking, at politiet skal kunne koble opplysninger om kommunikasjon til en bestemt abonnent.
Selv om utlevering av IP-data vil gjøre det mulig å identifisere den konkrete *abonnenten*, vil det som regel ikke være mulig å identifisere en konkret *bruker* gjennom å koble en IP-adresse til en abonnent. Det er ikke gitt at abonnenten og brukeren er samme person. Abonnentinformasjon, kombinert med data fra andre kilder, vil imidlertid kunne bidra til å identifisere brukeren og gi innsikt i brukerens nettbruk og handlingsmønstre. En utvidelse av plikten til å utlevere IP-adresser til å også gjelde forebygging av alvorlig kriminalitet, vil derfor gripe inn i person- og kommunikasjonsvernet.

Et annet sentralt hensyn ved vurderingen er hvilken betydning en plikt til å utlevere IP-data til forebygging av alvorlig kriminalitet vil ha for ytringsfriheten.

Ytringsfrihet er en grunnleggende rettighet som gir individer frihet til å uttrykke sine meninger og tanker uten frykt for represalier. Selv om ytringsfrihet er en forutsetning for demokratiet, er den likevel ikke absolutt. Ytringsfriheten kan begrenses av andre viktige samfunnsinteresser.

Selv om forslaget ikke direkte begrenser noen ytring, kan en plikt til å utlevere IP-data for forebyggende formål ha en nedkjølende effekt på ytringsfriheten. Dette gjelder særlig i digitale fora hvor brukere forventer en viss grad av anonymitet, som for eksempel i diskusjoner om kontroversielle eller politisk sensitive tema. Berettigede forventninger om å kunne være anonym på nett er også et personvernhensyn. For enkelte kan en hjemmel for myndighetene til å koble nettaktivitet til identitet, selv der det ikke er mistanke om straffbare handlinger, føre til at personen avstår fra å ytre seg.

Videre er et sterkt kildevern avgjørende for at pressen skal kunne fylle sin samfunnsfunksjon, som også er nødvendig i et velfungerende demokrati. Dette er et grunnleggende hensyn som må ivaretas i lovverket. Reglene til vern om journalisters anonyme kilder, må ikke kunne omgås, slik at kilders identitet avsløres.

Det at lovforslaget, hvis vedtatt, vil utgjøre inngrep i kommunikasjonsvernet og ytringsfriheten, gjør det nødvendig å vurdere tiltakets proporsjonalitet. Jo større inngrepene er, jo tyngre må de hensynene som begrunner tiltaket veie. Det må derfor vurderes hvordan utlevering av IP-data til forebyggingsformål skal balanseres mot kommunikasjonsvernet og retten til ytringsfrihet.

Et sentralt element i vurderingen er at utlevering til forebygging innebærer at informasjon innhentes før en straffbar handling begås eller er begått. Det betyr at det må gjøres en vurdering av hva slags handlinger en person antas å ville foreta seg. En slik fremoverrettet vurdering vil nødvendigvis være usikker. Det kan for eksempel være glidende overganger fra når noe går fra å være en politisk ytring, til radikalisering eller straffbare hatytringer. Dette skiller seg fra utlevering av IP-data til etterforskingsformål, hvor en handling antas å ha overskredet grensen for det straffbare. Utlevering av IP-data til forebyggingsformål vil dermed utgjøre et større inngrep i kommunikasjonsvernet og ytringsfriheten enn utlevering til etterforskingsformål.

6.1.3. Hensynet til politiets behov for tilgang til IP-data i forebyggende øyemed

Det å kunne koble en IP-adresse opp mot en abonnent, kan - som nevnt innledningsvis - være av stor betydning for å bekjempe alvorlig kriminalitet. Dette gjelder ikke bare ved etterforsking av straffbare forhold, men også ved forebygging av lovbrudd.
Formålet med å identifisere abonnenten bak en IP-adresse er i hovedsak å kunne vurdere informasjonens troverdighet, om den gir grunn til bekymring, om det er grunn til å sette inn tiltak og hvem det i så fall skal settes inn forebyggende tiltak overfor. Det å avklare om nye hendelser kan tilskrives en person som allerede er kjent for politiet, er viktig i forebyggende individrettet arbeid, for å ha grunnlag for å vurdere om innsatsen mot personen bør vedvare, trappes opp eller reduseres. I mange tilfeller er IP-data lagret hos tilbyderne eneste mulighet til å identifisere personen.

Ved vurderingen av betydningen av tilgang til IP-data i forebyggende øyemed er det grunn til å nyansere noe mellom PST og politiet for øvrig.

PSTs behov

PST arbeider primært forebyggende. Dette har sammenheng med at de straffebudene som faller innenfor PSTs ansvarsområde, jf. politiloven § 17b, er av svært samfunnsskadelig karakter. Det er derfor svært viktig at disse oppdages og stanses allerede på forberedelsesstadiet. Mange av de handlingene PST er satt til å forebygge, som terror, trusler mot myndighetspersoner, angrep på de høyeste statsorganene og på viktige samfunnsinstitusjoner, er for øvrig handlinger som – dersom de gjennomføres - vil kunne påvirke borgernes grunnleggende rettigheter, herunder ytringsfriheten.

Behovet for tilgang til IP-data i forebyggende øyemed vil kunne aktualiseres på flere måter. PST mottar blant annet et stort antall tips og mye informasjon fra publikum og samarbeidende tjenester knyttet til aktivitet på nett. PST kan også selv avdekke informasjon på nett som gir grunn til bekymring. Et eksempel kan være informasjon om at en norsk IP-adresse er blitt brukt til å hylle en terroraksjon i utlandet og gi uttrykk for at lignende aksjoner bør gjennomføres i Norge. Videre kan det avdekkes diskusjoner om bombeingredienser, truende eller ekstreme ytringer, herunder trusler mot myndighetspersoner, eller deltakelse i voldsforherligende og ekstreme fora. Dette kan være informasjon som indikerer at personen som står bak ytringen forbereder en straffbar handling.

Et fellestrekk ved truslene fra ekstreme miljøer er at stadig mer foregår på digitale plattformer og at svært få bruker sine reelle navn.

Videre vil nettverksoperasjoner mot Norge som regel alltid bestå av datatrafikk mellom ulike IP-adresser hvor skadevare sendes fra et fremmed lands etterretningstjeneste, gjerne via IP-adresser i andre land, før nettverksoperasjonen utføres mot det norske målet og den stjålne informasjonen sendes tilbake, gjerne gjennom et annet nettverk av IP-adresser.
Det vil derfor være av avgjørende betydning å identifisere brukerne bak IP adressene for at PST skal kunne analysere informasjonen og ved behov iverksette forebyggende tiltak.

Politiet for øvrig

Politiet for øvrig opplever også at teknologiutviklingen innebærer en stadig større mulighet for å begå kriminalitet som rammer bredt, og som derfor er svært samfunnsskadelig. Digitale plattformer brukes i stor utstrekning i den organiserte kriminaliteten, bl.a. for å rekruttere barn og unge til kriminalitet og som kanal for tilbydere av spesifikke kriminelle aktiviteter og tjenester som utvikler ekspertise innen handel med kriminalitet («kriminalitet som handelsvare», se Politiets trusselvurdering 2025 s. 33[1]). Dette er kriminalitet der målrettet tilgang til IP-data kan være av særskilt betydning i forebyggende øyemed. Etterforsking i etterkant kan være krevende når sporene er digitale, fordi teknologiutviklingen innebærer at politiets tilgang til informasjon som er digitalt lagret er stadig vanskeligere tilgjengelig (bl.a. på grunn av ende-til-ende kryptering og teknologiselskaper lokalisert til lite samarbeidsvillige jurisdiksjoner). Opplysninger knyttet til nettrelatert aktivitet blir dermed samlet sett stadig viktigere også for forebygging.

Politiet kan få informasjon om IP-adresser på mange forskjellige måter, for eksempel i form av tips fra publikum og andre offentlige organer, informasjon fra samarbeidende tjenester (både innenlands og utenlands), eller de kan avdekkes som ledd i politiets egen virksomhet.

Ideelle organisasjoner som *NCMEC* (National Center for Missing & Exploited Children) videreformidler tips til politiet om aktivitet på internett som kan utsette barn for fare. Tilsvarende informasjon kan politiet komme over gjennom åpen og skjult patruljering på internett gjort i forebyggende øyemed, eller ved tips fra andre. Tipsene kan typisk gå ut på varsel om deltagere som viser seksuell interesse for barn, personer som med seksuelle undertoner tilbyr kontakt med barn eller som får tilsendt materiale som tilsier seksuell interesse for barn. Grensen for straffbart forsøk på seksuelle overgrep er ikke nødvendigvis overtrådt.

I tilfeller der politiet ser en person bli tiltakende radikalisert i diskusjonsfora på internett, eller nærmer seg grensen for straffbare ytringer i kommentarfelter, kan identifisering gjøre det mulig å sette i verk forebyggende tiltak, eksempelvis samtale med den aktuelle personen. Identifiseringen vil på denne måten kunne bidra til å forebygge lovbrudd. Det samme gjelder der det på sosiale medier eller nettsteder snakkes om å utføre vold mot enkeltpersoner eller grupper i befolkningen.

I datakrimsaker oppdages det stadig at unge personer står i fare for å begå datainnbrudd gjennom sin aktivitet på internett. Abonnementsinformasjon knyttet til IP-adresser vil være viktig for å identifisere denne type hackere og iverksette forebyggende tiltak for å unngå lovbrudd. I DDoS-saker (Distribuert tjenestenektangrep) kan flere enheter (servere, datamaskiner, osv.) være infisert med skadevare som gjør det mulig for gjerningspersonene å benytte enhetene til å utføre angrep, uten at eier nødvendigvis kjenner til det. Et forebyggende tiltak kan være å informere eierne om at de kan ha skadevare på sin maskin, slik at denne kan fjernes, dersom politiet får informasjon om hvem som er tildelt IP-adressen.

Internasjonale forpliktelser utløser også behov for tilgang til IP-data i forebyggende øyemed. Nye EU-regelverk som TCO-forordningen, Digital Services Act (DSA) og forslaget til CSAM-forordning inneholder forpliktelser som skal sikre at ulovlig innhold på nett avdekkes, anmeldes og fjernes i større grad enn i dag. Blant annet pålegger DSA artikkel 18 hostingtjenester å varsle rettshåndhevende myndigheter om informasjon «giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place». Denne informasjonen vil kunne komme til politiet i form av en IP-adresse.

Norge er gjennom EUs fjerde hvitvaskingsdirektiv forpliktet til å forebygge og bekjempe hvitvasking og terrorfinansiering. Dette arbeidet har ofte en forebyggende karakter, og ender ikke nødvendigvis i anmeldelse, etterforsking og sak for domstolen. Norges Financial Intelligence Unit (FIU), som er lokalisert ved ØKOKRIM, mottar jevnlig forespørsler fra andre land om abonnementsinformasjon knyttet til IP-adresser. Norske myndigheter kan ikke svare ut slike forespørsler når forholdet er eldre enn 21 dager.

Tilgjengelig her: Politiets trusselvurdering 2025

6.1.4. Samlet vurdering

Plikten til å lagre og utlevere IP-data utgjør et inngrep i den enkeltes person- og kommunikasjonsvern, og i retten til privatliv etter Grunnloven § 102 og EMK artikkel 8. Tiltaket innebærer også et inngrep i ytringsfriheten etter EMK artikkel 10. En utvidelse av hvilke formål IP-data skal lagres og utleveres for, vil utgjøre et ytterligere inngrep i disse rettighetene.

Lagring og utlevering av IP-data til forebyggingsformål vil bare være tillatt dersom inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig. Kommunikasjonsverndirektivet artikkel 15 og praksis fra EU-domstolen åpner for at inngrep i kommunikasjonsvernet kan være begrunnet i forebygging av kriminalitet, gitt at vilkårene i artikkelen ellers er oppfylt. Forebygging kan derfor være et legitimt formål.

Det må imidlertid foretas en konkret vurdering av om lagring og utlevering av IP-data til forebyggingsformål vil være et proporsjonalt inngrep, som både tar hensyn til politiets behov for dataene til kriminalitetsbekjempelse og hensynet til vern av kommunikasjon og ytringsfrihet. Departementene mener det er av betydning for vurderingen at uthenting av informasjon om en abonnents identitet på bakgrunn av en IP-adresse, ikke i seg selv avslører noe om innholdet i abonnentens kommunikasjon eller hvem abonnenten har kommunisert med. Opplysninger om abonnenten bak en IP-adresse vil kunne bidra til å avdekke hvem som står bak en aktivitet, men opplysningene som gir grunn til å undersøke om noen forbereder visse straffbare handlinger, må politiet få andre steder. Dette kan for eksempel være gjennom egen virksomhet, tips, informasjon fra samarbeidende tjenester eller annet hold. Departementene mener det også er av betydning at identiteten til en abonnent er mindre inngripende for kommunikasjonsvernet enn om uthentingen skulle omfatte annen type trafikkdata, som kunne gitt informasjon om abonnentens personlige forhold.

Datatilsynet har ved tidligere anledninger uttrykt at utlevering av IP-data til forebygging er et svært inngripende tiltak som berører mennesker som ikke har begått kriminelle handlinger. Tilsynet mener også at tiltaket ikke bare innebærer oversikt over kommunikasjon, men kan brukes til å finne lokasjon.

Departementene er enig i at utlevering til forebygging stiller seg annerledes enn ved utlevering til etterforsking, og innebærer en utvidelse av gruppen personer som vil bli omfattet. Dette innebærer en risiko for innhenting av informasjon om personer som ikke har til hensikt å begå kriminelle handlinger. Dette, og den «nedkjølingseffekten» dette kan ha for ytringsfriheten, gjør at en eventuell utvidelse av utleveringsplikten må underlegges grundig vurdering.

Når det gjelder lokasjon, oppfatter departementene at det særlig er «sporing» av en bruker som kommuniserer via mobilnettene, Datatilsynet er bekymret for. Som det fremgår av Prop. 167 L (2020-2021) punkt 8.2.4, vil det være «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».

Departementene påpeker imidlertid at dette kun vil gi upresis informasjon om abonnentens geografiske posisjon, normalt på fylkesnivå eller et større geografisk område.

Forutsetninger for å utvide utleveringsplikten til et nytt formål, er at det oppstilles klare rammer for inngrepet og at utlevering begrenses til det som er nødvendig og forholdsmessig. Informasjon om abonnenten som har vært tildelt en IP-adresse, gir i seg selv ikke tilgang til kommunikasjonens innhold, og gjør det normalt ikke mulig å identifisere enkeltpersoner direkte. Kommunikasjonsvernet må imidlertid vurderes i lys av at opplysningene kan, og som regel vil, bli koblet med annen informasjon. Departementet mener derfor at det er grunn til å være varsom med å utvide plikten til utlevering av slike data til nye formål, men at dette likevel kan være aktuelt dersom tiltaket begrenses til forebygging av alvorlig kriminalitet, og innenfor rammer som ivaretar person- og kommunikasjonsvernet og retten til ytringsfrihet.

Informasjon om hvilken abonnent som er tildelt en IP-adresse i et aktuelt tidsrom kan bidra til å identifisere hvem som kommuniserer. Dette vil kunne være av stor betydning for å bekjempe alvorlig kriminalitet, både ved etterforsking og ved forebygging av lovbrudd. Forebygging av alvorlig kriminalitet utgjør et tungtveiende samfunnsmessig hensyn. Departementene understreker viktigheten av å kunne forebygge alvorlige straffbare handlinger der det er mulig, med de fordeler det har for både fornærmede og samfunnet for øvrig.

Samlet sett mener departementene at det bør åpnes for utlevering av IP-data til forebygging av alvorlig kriminalitet, men at det må settes nærmere rammer og vilkår som sikrer at tiltaket ikke utgjør et uforholdsmessig inngrep i retten til privatliv, person- og kommunikasjonsvernet og ytringsfriheten. Disse forutsetningene omtales i de følgende punktene.

6.2. Vilkår for utlevering av lagrede opplysninger

6.2.1. Innledning – generelle vilkår

Som omtalt i forrige punkt har departementene kommet til at det bør åpnes for utlevering av IP-data i forebyggende øyemed i visse tilfeller og på nærmere vilkår. Spørsmålet i det følgende er hvilke vilkår som må stilles for å sikre at inngrepet er begrenset til det som er nødvendig og forholdsmessig, samtidig som hensynet til å forebyggealvorlig kriminalitet ivaretas.

Departementene mener at det er særlig viktig at PST får mulighet til å innhente IP-data i forebyggende øyemed. PST skal forebygge kriminalitet med særlig alvorlige konsekvenser dersom den finner sted. PST er også gitt flere virkemidler i sitt forebyggende arbeid enn politiet for øvrig.

Samtidig kan også alvorlig kriminalitet som politiet skal forebygge, som overgrep mot barn og dataangrep, ha et så stort skadepotensial at utlevering av IP-data for å forebygge handlingen vil kunne være forholdsmessig innenfor gitte rammer. Både politiet og PST står overfor utfordringer som følge av den teknologiske utviklingen og kriminaliteten på internett. Det er forventet at politiet skal kunne utføre sine lovpålagte oppgaver, herunder forebygge lovbrudd, også i det digitale rom. Viktigheten av å forebygge alvorlige straffbare handlinger der det er

mulig gjør seg gjeldende for alle former for alvorlig kriminalitet, ikke bare den som ligger innenfor PSTs ansvarsområde.

Departementene mener derfor at det bør åpnes for at både politiet og PST skal kunne innhente IP-data i forebyggende øyemed. Departementene har samtidig kommet til at det kan være grunn til å skille noe på vilkårene for utlevering til PST og til politiet for øvrig. Dette gjelder i all hovedsak kravene til forholdets alvorlighet (strafferamme) og utleveringstid. Kravene omtales nærmere i punkt 6.2.2 og 6.2.3.

Etter gjeldende ekomforskrift § 3-5 tredje ledd fremgår det at politiets og påtalemyndighetens anmodninger for etterforskingsformål kan ta utgangspunkt i både IP-adresse og abonnent. For utlevering i forebyggende øyemed har politiet og PST behov for å identifisere abonnenten bak en IP-adresse, og det er i liten grad behov for å innhente alle IP-adresser en abonnent har vært tildelt i en gitt periode. En slik utlevering omfatter atskillig mer informasjon, og er dermed også mer inngripende. Departementene foreslår derfor at anmodningene om utlevering i forebyggende øyemed bare kan ta utgangspunkt i en IP-adresse. At formålet med anmodningene er bestemmende for hva anmodningene kan ta utgangspunkt i, er imidlertid såpass sentralt skille mellom de to formålene at departementene mener at dette bør fremgå av ekomloven heller enn ekomforskriften. Se forslag til ekomloven § 3-14 nytt tredje ledd.

«Grunn til å undersøke»

Adgangen til å innhente IP-data i forebyggende øyemed må rammes inn på en måte som sikrer at inngrepet i ytringsfriheten og kommunikasjonsvernet ikke blir større enn det som er nødvendig for å oppnå formålet med hjemmelen.

Forebygging er et vidt begrep som kan romme en rekke ulike situasjoner og handlinger, både generell forebyggende virksomhet og mer individrettede tiltak. I Prop. 167 L (2020–2021) punkt 8.5.4.2 ble det uttalt at et vilkår om «nødvendig for å forebygge» vil kunne skape uklarheter om hva som skal til for at politiet kan anmode om informasjon. Begrepet «forebygge» egner seg ikke nødvendigvis som et utløsende vilkår. Departementene viser også til at i de tilfeller der det er behov for IP-data i forebyggingsøyemed, har politiet og PST allerede fått tilgang til informasjon som gir grunn til bekymring på annen måte. Det anses dermed verken nødvendig eller forholdsmessig å åpne for tilgang til IP-data for forebygging generelt, kun dersom det er konkrete forhold som utløser behov for IP-data i forebyggende øyemed. Lovbestemmelsen må utformes på en måte som sikrer dette.

Ved vurderingen av hva vilkårene for utlevering bør være, har departementene sett hen til de vilkårene som gjelder for at PST skal kunne benytte skjulte tvangsmidler i forebyggende øyemed etter politiloven § 17 d. Etter denne bestemmelsen kan PST, som nevnt i punkt 3.3, få rettens tillatelse til å benytte skjulte tvangsmidler dersom det er «grunn til å undersøke» om noen forbereder nærmere bestemte straffbare handlinger. Departementene vurderer at «grunn til å undersøke» om noen forbereder en straffbar handling vil være et egnet inngangsvilkår også for uthenting av IP-data i forebyggingsøyemed. Formuleringen konkretiserer i hvilke tilfeller opplysninger kan utleveres, og synliggjør at utleveringen er begrenset til individrettet forebygging.

I vilkåret «grunn til å undersøke» ligger som nevnt i punkt 3.3 et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling, og et krav til forholdsmessighet. Det må være konkrete objektive omstendigheter som tilsier at noen forbereder en straffbar handling. Det er ikke tilstrekkelig å vise til informasjon, erfaringer og vurderinger mer generelt. Vilkåret er relativt i forhold til handlingens alvor, slik at det skal mindre til for at kravet er oppfylt dersom det dreier seg om svært alvorlige handlinger (som terror, drap, seksuallovbrudd og grove narkotikalovbrudd mv.) enn handlinger av lavere alvorlighetsgrad (som trusler, hatefulle ytringer mv.). Hva som skal til for at kravet er oppfylt må vurderes konkret i det enkelte tilfelle. Momenter i vurderingen kan blant annet være innholdet i og omstendighetene rundt den konkrete ytringen som gir grunn til bekymring, hvem informasjonen kommer fra (etablert samarbeidspartner, offentlig organ eller en privatperson), tipserens troverdighet dersom informasjonen kommer fra et tips, og hvor gammel informasjonen er.

Vilkåret om «grunn til å undersøke» er det samme som for at PST skal kunne opprette såkalt «forebyggende sak», jf. politiregisterloven § 64 tredje ledd nr. 1 og politiregisterforskriften § 20-3 nr. 2. Departementene viser også til at samme vilkår er foreslått for PSTs pålegg om utlevering av kundeopplysninger fra datasenteroperatører i høringsnotat 29. januar 2025 om forslag til endringer i datasenterforskriften, som er utarbeidet i samarbeid med Justis- og beredskapsdepartementet. Det er hensiktsmessig med samme inngangsvilkår i ulike bestemmelser om utlevering av opplysninger, så fremt det ikke er særlige hensyn som taler for avvikende vilkår. Det å etablere en egen terskel i ekomloven for når opplysninger kan utleveres i forbindelse med forebygging, som ikke har noen parallell i politiets eget regelverk, vil videre kunne skape betydelig mer usikkerhet og høyere risiko for at det fremmes flere anmodninger enn nødvendig. Selv om det i den enkelte situasjonen kan være krevende å vurdere om opplysningene gir grunn til å undersøke, er innholdet i begrepet utpenslet både i Innst. O nr. 113 (2004–2005) og Riksadvokatens etterforskingsrundskriv. Departementene mener derfor at det vil være tilstrekkelig klart hva som skal til for å få opplysninger utlevert dersom dette begrepet benyttes.

Departementene understreker at dersom vilkårene for utlevering til forebygging etter de foreslåtte endringene i ekomloven § 3-14 ikke er oppfylt, vil politiet fremdeles kunne anmode om opplysninger som er lagret for tilbydernes egne formål etter § 3-10 tredje ledd, så fremt de ikke er slettet etter § 3-11.

Proporsjonalitet – nødvendighetskravet

Det knytter seg enkelte utfordringer til å det anvende «nødvendighet» som et utløsende vilkår for at PST og politiet for øvrig skal kunne innhente IP-data i forebyggende øyemed. Forebyggende tiltak er fremtidsrettede av natur, og vil ofte bygge på indikasjoner, bekymringer eller risikovurderinger – heller enn dokumenterte eller nært forestående straffbare handlinger. Når politiet får utlevert IP-data i en etterforsking, kan man kanskje i ettertid se at dataene bidro til å bringe etterforskingen videre og dermed til å oppklare saken. Dette vil stille seg annerledes ved forebygging, fordi man ikke på forhånd kan vite om tilgangen faktisk vil forebygge en straffbar handling. Man kan heller ikke vite sikkert om tiltaket virket – eller ville virket – fordi det handler om hypotetiske fremtidige hendelser. Dette

vil, iallfall ved en streng forståelse av kravet til nødvendighet, gjøre det det vanskelig å si at tilgang til IP-data er nødvendig for å forebygge en straffbar handling, fordi man ikke kan påvise en klar årsakssammenheng mellom tiltaket og det man ønsker å forebygge.

Departementene er følgelig noe i tvil om hvordan lovbestemmelsene best kan utformes på en måte som sikrer at kravet til nødvendighet ivaretas, uten at dette tas uttrykkelig inn i ordlyden i bestemmelsen.

Det er imidlertid viktig å presisere at selv om nødvendighetskravet ikke er foreslått uttrykkelig tatt inn i den foreslåtte lovteksten, vil dette likevel måtte innfortolkes som et overordnet rettslig krav. Grunnloven § 102 og EMK artikkel 8 stiller krav om at inngrep i privatlivet må være nødvendige og forholdsmessige i et demokratisk samfunn. Det samme følger av kommunikasjonsverndirektivet som angir at 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»* må være «*nødvendig, egnet og rimelig i et demokratisk samfunn».* Disse kravene vil altså gjelde uavhengig av om de er uttrykkelig lovfestet i den aktuelle bestemmelsen. Dette innebærer blant annet at det ved anmodning om tilgang til IP-data i forebyggende øyemed må foretas en konkret vurdering av behovet for opplysningene, som må veies mot hensynet til kommunikasjonsvernet, og at det ikke skal anmodes om eller utleveres flere opplysninger enn det som trengs for formålet i det enkelte tilfellet. I Prop. 167 L (2020-2021) s.54 pekes det på at nødvendighetskravet i bestemmelsen om utlevering av IP-data til etterforsking, allikevel ikke skal «tolkes så strengt at utlevering av opplysningene må være den eneste løsningen». Samtidig vises det til at det «på den andre siden (…) ikke [vil] være tilstrekkelig at opplysningene bare vil kunne lette arbeidet.» Videre vises det til at det av proporsjonalitetskravet følger at inngrepet i kommunikasjonsvernet også må tas med i vurderingen, og at «dette kan innebære at vurderingen kan falle forskjellig ut avhengig av inngrepet i kommunikasjonsvernet i den enkelte sak.» Departementene mener det er hensiktsmessig å legge til grunn en tilsvarende forståelse av kravet om nødvendighet som vil gjelde ved utlevering av IP-data i forebyggende øyemed.

Oppsummert understreker departementene at de overordnede kravet om nødvendighet uansett vil gjelde for utlevering av IP-data i forebyggende øyemed, selv om det ikke fremgår uttrykkelig i lovteksten. Departementene vil derfor fremheve dette i forarbeidene til bestemmelsene. Meningen er at dette skal gi tilstrekkelige rettssikkerhetsgarantier, samtidig som bestemmelsen forblir praktisk anvendelig. Departementene ber samtidig høringsinstansene om innspill til hvordan lovbestemmelsene best kan utformes på en måte som sikrer at kravet om nødvendighet synliggjøres og ivaretas på best mulig måte.

Departementene ser det imidlertid som hensiktsmessig at kravet til forholdsmessighet kommer klart til uttrykk i lovbestemmelsen. I både politiloven og straffeprosessloven er kravet til forholdsmessighet ved politiets inngrep lovfestet, i henholdsvis politiloven § 6 annet ledd og straffeprosessloven § 170 a. Kravet til forholdsmessighet er også inntatt i politiloven § 17 d annet ledd for PSTs tvangsmiddelbruk i forebyggende øyemed. Ettersom hjemmelen for utlevering av IP-data finnes i ekomlovgivningen, er det en fordel at kravet om forholdsmessighet inntas også her. Kravet til forholdsmessighet gjelder også for utlevering til

etterforsking, og bestemmelsen er derfor formulert slik at det gjelder uavhengig av hvilket formål opplysningene utleveres til.

6.2.2. Rammer for utlevering til PST

PST skal forebygge noen av de mest alvorlige og samfunnstruende straffbare handlingene. Av den grunn er PST gitt tilgang til en rekke inngripende virkemidler i det forebyggende sporet, herunder skjulte tvangsmidler som kommunikasjonskontroll og dataavlesing, som er langt mer inngripende enn utlevering av IP-data. I Prop. 93 LS (2023–2024) punkt 6.1.5 er PSTs behov særlig trukket frem i begrunnelsen for å utrede utlevering av IP-data til forebyggende formål. Departementene mener det er særlig viktig at man setter rammer som gjør uthenting av IP-data til et egnet verktøy i PSTs forebyggende arbeid.

Ekomloven § 3-14 åpner for utlevering til etterforsking av alle straffebud innenfor PSTs mandat. De fleste straffbare handlinger PST skal etterforske har en strafferamme på minst tre år, og alle straffebud PST skal forebygge og etterforske som har en lavere strafferamme er inntatt i bestemmelsen. Sett hen til de særskilte behovene som gjør seg gjeldende for PST, mener departementene at det bør åpnes for utlevering i forebyggende øyemed for alle straffbare handlinger innenfor PSTs mandat. All kriminalitet PST skal forebygge er svært alvorlig og kan true nasjonale sikkerhetsinteresser, også den kriminaliteten som har en strafferamme på fengsel i 3 år eller lavere. Eksempelvis har straffeloven § 121 om etterretningsvirksomhet mot statshemmeligheter, § 123 om avsløring av statshemmeligheter og § 126 om annen ulovlig etterretningsvirksomhet en strafferamme på fengsel i inntil 3 år. Straffeloven § 251 om tvang og § 263 om trusler har en strafferamme på inntil henholdsvis 2 og 1 års fengsel. PST skal forebygge slike handlinger rettet mot myndighetspersoner. Innenfor PSTs ansvarsområde er dermed ikke strafferammen et egnet avgrensningskriterium for å vurdere handlingens alvorlighet. Departementene viser også til at PST etter politiloven § 17 d kan benytte skjulte tvangsmidler dersom det er grunn til å undersøke om noen forbereder nærmere bestemte straffbare handlinger, der flere av straffebudene har en relativt lav strafferamme.

Departementene ser det verken som nødvendig eller hensiktsmessig å differensiere etter strafferamme for utlevering av IP-data til PSTs forebyggende virksomhet. Det foreslås derfor at ekomloven § 3-14 første ledd ny bokstav c viser til handlinger som nevnt i politiloven § 17 b, som regulerer hvilke straffbare handlinger PST skal forebygge og etterforske.

Departementene mener videre at PSTs bør få tilgang til IP-data lagret etter ekomloven § 3-13 inntil 12 mnd tilbake i tid. Forberedelsen av alvorlig kriminalitet som etterretningsvirksomhet, sabotasje og terrorisme kan pågå i lang tid, også over år. PSTs forebyggende arbeid har derfor et langsiktig perspektiv, og opplysninger av eldre dato kan også være av betydning for forebygging av fremtidige handlinger. For eksempel kan slik informasjon bidra til å avdekke hittil ukjente personer som det bør settes i verk forebyggende tiltak mot. Der det gjennom innhenting av IP-data viser seg at personen allerede er i PSTs søkelys, kan eldre informasjon bidra til å avklare om nye tiltak bør iverksettes eller eksisterende tiltak trappes opp eller ned. Når PST mottar tips og informasjon fra samarbeidende tjenester, kan denne være av eldre dato. Opplysningene kan likevel gi grunn til å undersøke om noen forbereder en straffbar

handling. PST sine behov for tilgang til IP-data i forebyggende øyemed tilbake i tid er derfor det samme som i etterforsking.

PSTs forebyggende virksomhet skal ikke bare forebygge straffbare handlinger, men også ivareta hensynet til nasjonal sikkerhet. Utlevering til PSTs forebyggende virksomhet vil dermed være begrunnet i flere legitime formål etter kommunikasjonsverndirektivet artikkel 15 nr. 1. Sett hen til de tungtveiende samfunnsinteresser PST skal ivareta, og de øvrige rammene som vil gjelde for uthentingen, mener departementene derfor at det vil være forholdsmessig å åpne for at PST kan innhente IP-data i forebyggingsøyemed i de samme tilfellene som tjenesten kan få utlevert IP-data til etterforsking, og like langt tilbake i tid. Kravene om skriftlighet mv. etter § 3-14 nåværende annet ledd vil gjelde også for pålegg om utlevering i forebyggende øyemed. For PSTs forebyggende virksomhet vil begrunnelsen imidlertid måtte gis på et overordnet nivå for ikke å røpe graderte opplysninger, for eksempel kun at det gjelder utlevering etter § 3-14 første ledd bokstav c. Videre vil det også være krav om årlig rapportering, se nærmere om hvem som skal motta rapporten og innholdet i den i punkt 6.3.3.

6.2.3. Rammer for utlevering til politiet

Krav til strafferamme

Departementene mener som nevnt i punkt 6.2.1 at også politiet bør kunne få utlevert IP-data i forebyggende øyemed, men at det er grunn til å etablere en høyere terskel for utlevering til politiet enn til PST. Hensikten med strengere rammer er å sikre at tiltaket ikke går lenger enn nødvendig. Etter ekomloven § 3-14 kan opplysninger utleveres når det er nødvendig for å etterforske straffbare handlinger som har en strafferamme på fengsel i 3 år eller mer, eller som rammes av nærmere bestemte straffebud. Dersom det skal stilles et høyere generelt krav til strafferamme, må dette settes til fengsel i inntil seks år, ettersom straffeloven ikke inneholder andre strafferammer mellom tre og seks år.

Departementene har kommet til at det bør settes et krav om seks års strafferamme for utlevering til politiet i forebyggingsøyemed, for å sikre at inngrepet ikke går lenger enn nødvendig. I *La Quadrature du Net II,* som gjaldt håndheving av opphavsrettskrenkelser med en lav strafferamme, åpner EU-domstolen for at IP-data på nærmere vilkår kan utleveres også for å bekjempe alminnelig kriminalitet. Det franske systemet, med flere varsler før en eventuell straffeforfølging, hadde blant annet et forebyggende formål. En høyere strafferamme for utlevering til forebygging enn til etterforsking er dermed ikke et krav som kan utledes av kommunikasjonsverndirektivet. Departementene peker også på at det på det forebyggende stadiet kan være vanskelig å fastslå om det man ønsker å forhindre, vil rammes av et straffebud med høy eller lavere strafferamme dersom forebyggingen ikke lykkes. Eksempelvis kan det ved forebygging av seksuelle overgrep være vanskelig å forutse hvilke konkrete seksuallovbrudd en person kan komme til å begå dersom handlingen først finner sted. Departementene mener likevel at man bør begrense uthentingen i forebyggende øyemed til de mest alvorlige straffbare handlingene. Politiets forebyggende virksomhet er et område som i liten grad er regulert, og politiet har ellers få virkemidler av inngripende karakter for forebyggende formål. Dette gjør at man etter departementenes syn bør være tilbakeholden med å åpne for utlevering av IP-data i for stort omfang på dette området.

Straffebud med lavere strafferamme der IP-data er særlig viktig for å forebygge handlingen

Et krav om seks års strafferamme for utlevering i forebyggingsøyemed, gjør at mange straffbare handlinger som kan ha alvorlige konsekvenser vil falle utenfor. Det må derfor vurderes hvilke straffebud med en lavere strafferamme som bør inntas særskilt, fordi IP-data vurderes å være særlig viktig for å forebygge handlingen. Som omtalt i punkt 6.1.3 blir opplysninger knyttet til nettrelatert aktivitet, på grunn av samfunns- og teknologiutviklingen, samlet sett stadig viktigere også for forebygging, uavhengig av hvilken handling det dreier seg om. Dette gjør at avgrensningen av hvilke straffebud som skal inkluderes er krevende.

Departementene ser likevel at det er enkelte kriminalitetsområder der IP-data fremstår som særlig viktig for å kunne forebygge handlingen, også der strafferammen er lavere enn 6 år. I Prop. 167 L (2020–2021) ble det uttalt at: «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.» Som eksempel ble det særlig trukket frem seksuelle overgrep mot barn, der flere straffebud har en lavere strafferamme enn fengsel i inntil 3 år. Disse straffebudene ble derfor inkludert i bestemmelsen.

Behovet for å kunne etterforske nettrelaterte seksuallovbrudd, særlig mot mindreårige, var en viktig del av begrunnelsen for å innføre IP-lagring til etterforsking, jf. Prop. 167 L (2020–2021) punkt 2.1. Departementene mener at seksuallovbrudd er et område der også forebygging er særlig viktig. Selv om flere av seksuallovbruddene har en relativt lav strafferamme, er konsekvensene for de som utsettes for handlingene ofte store, og mange ofre kan bli rammet av samme gjerningsperson. Mørketallene er også store.

Departementene mener derfor at det bør åpnes for uthenting av IP-data for å forebygge seksuallovbrudd med en lavere strafferamme enn fengsel i seks år. Som omtalt i forrige punkt er det vanskelig å vite hvilke straffbare handlinger som kan bli begått der opplysninger gir grunn til å undersøke om noen forbereder seksuallovbrudd mot mindreårige. Selv om bekymringen isolert sett er knyttet til et straffebud med lav strafferamme, som seksuelt krenkende atferd, kan det likevel være en risiko for at mer alvorlige handlinger på sikt kan finne sted. I lys av viktigheten av å forebygge seksuelle overgrep, foreslås det derfor å inkludere alle seksuallovbrudd som har en strafferamme på 3 år, samt de seksuallovbruddene med lavere strafferamme som i dag er inntatt i ekomloven § 3-14. Det foreslås imidlertid ikke å inkludere straffeloven §§ 267 a og 267 b om alminnelig og grov deling av krenkende bilder mv. For disse to straffebudene synes det mindre praktisk at IP-data vil være nødvendig for å forebygge lovbruddet.

Dette innebærer at følgende straffebud kan begrunne uthenting av IP-data i forebyggende øyemed:

§ 297 Seksuell handling uten samtykke
§ 298 Seksuelt krenkende atferd offentlig eller uten samtykke
§ 304 Seksuell handling med barn under 16 år
§ 305 Seksuelt krenkende atferd mv. overfor barn under 16 år
§ 306 Avtale om møte for å begå seksuelt overgrep

§ 309 Kjøp av seksuelle tjenester fra mindreårige
§ 310 Fremvisning av seksuelle overgrep mot barn eller fremvisning som seksualiserer barn
§ 311 Fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn

I tillegg vurderer departementene at enkelte andre konkrete straffebud som gjelder kriminalitet som begås helt eller delvis på nett, og som gjerne skjer i stort omfang, bør inkluderes. Teknologiutviklingen innebærer en mulighet for å begå kriminalitet som rammer bredt, og som derfor er svært samfunnsskadelig, også i form av at tilliten til digitale løsninger svekkes dersom det ikke reageres mot denne typen kriminalitet. For personene som rammes av identitetskrenkelser, datainnbrudd og utpressing kan konsekvensene være store, selv om strafferammen for enkeltovertredelser ikke nødvendigvis er høye. Politiet vil ofte være avhengig av IP-data for å kunne vurdere og sette i verk tiltak for å forebygge denne typen kriminalitet. Ettersom omfanget er stort og mulighetene for å straffeforfølge personene bak kan være små, blir forebyggende tiltak særlig sentralt.

Den digitale utviklingen gjør at infrastruktur i Norge kan benyttes av utenlandske aktører til å utføre kriminalitet, eksempelvis datainnbrudd, identitetstyverier eller utpressing. Aktørene kan selv eie utstyret, men det kan også være andre personers utstyr som er hacket eller infisert med skadevare, som gjør det mulig for gjerningspersonene å benytte enhetene til å utføre kriminalitet uten at eier kjenner til det. Slik kriminalitet kan pågå over lang tid, og gjerne i stort omfang. Forebyggende tiltak som å identifisere og lokalisere det elektroniske utstyret og eventuell eier for å unngå fremtidige straffbare forhold, kan i slike saker være viktigere og mer formålstjenlig enn å etterforske saken. En svært stor andel av slike saker vil resultere i henleggelse uten oppklaring.

Departementene foreslår derfor at også følgende straffebud inkluderes i bestemmelsen:
§ 201 Uberettiget befatning med tilgangsdata, dataprogram mv.
§ 202 Identitetskrenkelse
§ 204 Innbrudd i datasystem
§ 330 Utpressing

I tillegg vurderer departementene at det er grunn til å inkludere straffeloven § 371 om bedrageri, som har en strafferamme på fengsel inntil 2 år, men at dette bør inkludere utlevering til både forebygging og etterforsking. Dette omtales nærmere i punkt 6.4.

Det bes særlig om høringsinstansenes syn på hvilke straffebud med en lavere strafferamme enn fengsel i seks år som bør kunne begrunne utlevering av IP-data i forebyggende øyemed.

Utleveringstid

Selv om lagringstiden etter ekomloven § 3-13 er satt til 12 måneder etter at kommunikasjonen ble avsluttet, kan det tenkes at utleveringstiden gjøres kortere enn dette. En kortere utleveringstid vil redusere antall anmodninger/pålegg, og bidra til at tiltaket rammes ytterligere inn. En kortere utleveringstid vil innebære at politiet bare kan spørre med

utgangspunkt i en IP-adresse (og eventuelt portnummer) og et tidspunkt for kommunikasjonen som ligger et gitt antall måneder tilbake i tid, selv om tilbyderne har lagret informasjon i 12 måneder.

Det er vanskelig å konkretisere hvor stort politiets behov for utlevering av IP-data som er eldre enn eksempelvis 3, 6 eller 9 måneder i forebyggingsøyemed, er. I en del tilfeller vil antakeligvis behovet for IP-data i forebyggende øyemed være knyttet til opplysninger som relativt sett er av nyere dato, ettersom det for en del straffbare handlinger vil kunne gå kort tid fra planlegging til utførelse.

Samtidig kan IP-adressene politiet mottar fra andre være av eldre dato, og behovet for identifisering kan først vise seg etter noe tid. Der politiet mottar informasjon fra samarbeidende tjenester om norske IP-adresser knyttet til bekymringsverdig innhold på nett, kan det ha gått tid siden innholdet ble publisert eller lastet ned. Informasjonen kan likevel gi grunn til å undersøke om noen forbereder en alvorlig straffbar handling, for eksempel dersom det dreier seg om straffbare handlinger der planleggingen kan gå over tid. I saker med internasjonale forgreininger, for eksempel ved organisert kriminalitet, kan det også være behov for samarbeid over landegrenser, noe som kan være omfattende og tidkrevende. For å kunne avdekke og stanse bakmenn, som gjerne befinner seg i utlandet, fra å begå ny kriminalitet, må politiet ofte se informasjon fra flere saker i sammenheng. Dette blir vanskelig hvis informasjonen er lagret i for kort tid. Politiet har heller ikke kapasitet til å vurdere og reagere umiddelbart på all innkommen informasjon.

At informasjonen ligger tilbake i tid kan bety at en straffbar handling allerede er begått. Informasjonen kan likevel være viktig for å forebygge fremtidige lovbrudd. Eksempelvis vil informasjon om seksuell interesse for barn kunne være av stor betydning for å forebygge fremtidige overgrep, selv om den ligger tilbake i tid. Politiet vil ut fra opplysningene ikke vite om personen faktisk har utført noen seksuelle overgrep, bl.a. fordi anmeldelsesprosenten er lav og det tar lang tid før de fornærmede anmelder. At et overgrep allerede kan være begått, betyr heller ikke at det ikke er fare for at personen vil begå nye straffbare handlinger. For seksuallovbrudd på nett kan antallet fornærmede være svært stort, og aktiviteten kan pågå i lang tid. Forebyggende arbeid for å unngå fremtidige lovbrudd blir dermed svært viktig. Også for annen nettrelatert kriminalitet, som datainnbrudd, bedrageri, identitetstyveri og utpressing, vil informasjon tilbake i tid kunne være viktig. Som nevnt pågår slik kriminalitet ofte i stort omfang med mange fornærmede. Mulighet for identifisering tilbake i tid vil dermed kunne være viktig ikke bare for å etterforske allerede begåtte lovbrudd, men også for å forebygge fremtidige lovbrudd.

Hvor gammel informasjonen er, vil som omtalt i punkt 6.2.1 være et moment i vurderingen av om det er grunn til å undersøke om en person forbereder et straffbart forhold. Ved informasjon av eldre dato som gjelder mulig kriminalitet som normalt forberedes og begås i et kort tidsperspektiv, vil dette kravet ofte ikke være oppfylt. Dette gjør det etter departementenes syn mindre betenkelig å åpne for utlevering også tilbake i tid.

Hvor ofte det er behov for eldre informasjon for å forebygge fremtidige handlinger, og hvor viktig denne informasjonen vil være, er imidlertid usikkert og vanskelig å vurdere. For å sikre

at inngrepet i privatlivet og kommunikasjonsvernet ikke går lenger enn nødvendig, har departementene etter en samlet vurdering kommet til at det bør åpnes for at politiet bare kan innhente IP-data i forebyggingsøyemed der tidspunktet for kommunikasjonen ikke ligger mer enn 6 måneder tilbake i tid. Fristen beregnes fra tidspunktet politiet sender anmodningen til tilbyderne, og innebærer at det bare kan spørres med bakgrunn i en IP-adresse (og eventuelt portnummer) og et tidspunkt som ligger inntil seks måneder før anmodningen sendes.

Det foreslås også en justering i ekomforskriften § 3-5 annet ledd for å sikre beredskap hos tilbydere for på kort varsel å kunne behandle anmodninger i saker der det ved opphold er stor fare for at muligheten til å forebygge den straffbare handlingen vil gå tapt. Departementene ber særlig om høringsinstansenes tilbakemelding på terskelen som er foreslått for anmodninger utenfor arbeidstid.

6.3. Kontrollmekanismer

6.3.1. Forhåndskontroll

I Prop. 167 L (2020-2021) ble det foretatt en vurdering av behovet for forhåndskontroll ved utlevering av IP-data til etterforsking i lys av praksis fra EMD og EU-domstolen. Kommunal- og moderniseringsdepartementet la vekt på at dataene er mindre sensitive enn annen kommunikasjonsdata og at dataene som lagres ikke kan gi presise slutninger om folks privatliv, og at kravet til prosessuelle garantier derfor er lavere. Departementet konkluderte med at det ikke var nødvendig å innføre et generelt krav om forhåndskontroll for utlevering av IP-adresser på grunnlag av EU-domstolens praksis, jf. proposisjonen punkt 8.6.4.

Departementene mener at spørsmålet om behovet for forhåndskontroll ikke har endret seg i lys av EU-domstolens avgjørelse siste avgjørelse (sak C-470/21 *La Quadrature du Net II)*. Avgjørelsen er nærmere omtalt i punkt 4.3.

I *La Quadrature du Net II* oppstiller domstolen nærmere krav til lagringen av abonnementsopplysninger og opplysninger om IP-adresser for at inngrepet ikke skal anses alvorlig og for at det ikke skal være nødvendig med uavhengig forhåndskontroll. Kravene knytter seg til systemer der tilbyderne også er pålagt å lagre andre typer opplysninger, jf. dommen avsnitt 80 flg. Det er ulike kategorier lagringspliktige opplysninger som må skilles fra hverandre med vanntette skott, ettersom kobling av ulike typer lagringspliktige opplysninger vil kunne gjøre det mulig å trekke presise slutninger om en persons privatliv. Kravene synes derfor ikke overførbare til det norske systemet for IP-lagring, som kun pålegger lagring av informasjon som er nødvendig for å identifisere hvilken abonnent som er tildelt en IP-adresse på et gitt tidspunkt.

Departementene mener at heller ikke andre avsnitt i dommen kan tolkes slik at det må innføres uavhengig forhåndskontroll for uthenting av IP-data for å forebygge alvorlig kriminalitet. Riktig nok mener domstolen at det i det franske systemet for håndheving av opphavsrettskrenkelser på nett var behov for forhåndskontroll på et visst stadium i prosessen, fordi det ikke kunne utelukkes at den samlede informasjonen myndigheten hadde, gjorde det mulig å trekke presise slutninger om en persons privatliv (avsnitt 135 flg.). I forbindelse med kriminalitetsbekjempelse generelt vil informasjonen politiet kobler

abonnenten bak en IP-adresse med, kunne gjøre det mulig å trekke slike presise slutninger. Uttalelsene i dommen er imidlertid knyttet spesifikt til det franske systemet og den "gradvise prosessen" med flere varsler, som ikke har noen parallell til politiets kriminalitetsbekjempende virksomhet. Departementene mener derfor at man bør være varsom med å gi uttalelsene overføringsverdi til politiets kriminalitetsbekjempende virksomhet mer generelt.

Departementene har videre lagt vekt på at kommunikasjonsverndirektivet ikke stiller andre krav til inngrep som er begrunnet i hensynet til forebygging av kriminalitet, enn for de som er begrunnet i hensynet til etterforsking av kriminalitet. Når det ikke kreves forhåndskontroll for utlevering til etterforsking, er det derfor lite naturlig, og heller ikke behov for, å stille et slikt krav for utlevering til forebygging.

I lys av hvor inngripende tiltaket er, de rammer som er satt for uthentingen, reglene for politiets behandling av opplysningene og at behandlingen er underlagt tilsynskompetansen til Datatilsynet og EOS-utvalget, mener departementene at uavhengig forhåndskontroll ikke er en nødvendig sikkerhetsmekanisme for at uthenting av IP-data i forebyggingsøyemed skal være forholdsmessig.

6.3.2. Behandling av opplysninger

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

Politiets behandling av opplysninger er underlagt Datatilsynets tilsynskompetanse, jf. lovens § 58. Tilsynskompetansen omfatter all behandling av opplysninger i politiet og påtalemyndigheten, herunder for behandling av opplysninger i den enkelte straffesak, med unntak av opplysninger som behandles av Politiets sikkerhetstjeneste eller opplysninger som er underlagt kompetansen til kontrollutvalget for kommunikasjonskontroll. For PST er det EOS-utvalget som er tilsynsmyndighet, jf. politiregisterloven § 68 og EOS-kontrolloven.

Det er ikke etablert særskilte regler om behandling av IP-data som innhentes til etterforskingsformål. I Prop. 167 L (2020-2021) punkt 8.6.4 konkluderte departementet med at de alminnelige reglene i politiregisterlovgivningen var tilstrekkelige for å sikre kontrollen med behandlingen av opplysningene etter at de er utlevert til politiet.

Departementene vurderer at gjeldende regelverk er tilstrekkelig også for den videre behandlingen av opplysninger som utleveres i forebyggende øyemed, og at det ikke er

behov for særskilte regler for behandlingen. Departementene understreker samtidig viktigheten av at kravet om at opplysninger ikke skal lagres lenger enn det som er nødvendig for formålet med behandlingen, jf. politiregisterloven § 50, etterleves.

6.3.3. Rapportering

Etter ekomloven § 3-14 tredje ledd skal politiet og påtalemyndigheten oversende en årlig rapport til departementene om uthenting av IP-adresser. Hva rapporteringen skal inneholde er nærmere regulert i ekomforskriften § 3-6, der det også er presisert at rapporteringen skal skje til Nasjonal kommunikasjonsmyndighet.

Når det nå foreslås å åpne for uthenting av IP-data i forebyggingsøyemed, er det behov for justeringer i disse bestemmelsene, både av hensyn til å kunne få pålitelige data om bruken av de nye bestemmelsene og for å skjerme om PSTs forebyggende virksomhet. PSTs forebyggende arbeid er i all hovedsak gradert etter sikkerhetsloven, og det er EOS-utvalget som er kontrollorgan for PST. EOS-utvalget skal blant annet sikre at PSTs virksomhet holdes innenfor rammen av tjenestens fastlagte oppgaver og skal føre kontroll med tjenestens behandling av forebyggende saker og dens innhenting av informasjon og behandling av personopplysninger, jf. EOS-kontrolloven § 6 annet ledd og fjerde ledd nr. 1.

Rapportering på i hvilket omfang PST henter ut IP-data i forebyggende øyemed, og til hvilke straffebud, kan røpe både PSTs kapasiteter og hvilke områder de særlig retter sin forebyggende innsats mot. Dersom uvedkommende får tilgang til denne informasjonen, kan det ha svært negative konsekvenser. Departementene ser det derfor som mest nærliggende at rapportering knyttet til PSTs uthenting av IP-data i forebyggende øyemed sendes EOS-utvalget og Justis- og beredskapsdepartementet, og foreslår at dette presiseres i ekomloven § 3-14, i tillegg til at det foreslås et nytt tredje ledd i ekomforskriften § 3-6 om hva rapporteringen skal inneholde.

Departementene foreslår videre justeringer i ekomforskriften § 3-6 annet ledd bokstav a og d slik at politiets årlige rapportering vil synliggjøre både omfanget av anmodninger til henholdsvis etterforsking og forebygging, og hvilke straffebud som ligger til grunn for uthenting til hvert av de to formålene. Dette vil kunne gi nyttig informasjon om bruken av den nye hjemmelen.

6.4. Særlig om bedrageri

Av Politidirektoratet og riksadvokatens fellesrapport for straffesaksbehandlingen for 2024 fremgår det at bedrageri utgjorde nærmere 86 prosent av alle anmeldte økonomilovbrudd i 2024. Dette er en økning på 13,5 prosent sammenlignet med året før. Den store majoriteten av disse sakene er ansett som alminnelige bedragerier. Flertallet av disse bedrageriene, 83 prosent, er registrert med en digital fremgangsmåte. To tredjedeler av bedrageriene er registrert med ukjent gjerningsmann. En svært stor andel av sakene henlegges uten oppklaring. Økokrim opplyser i sin årsrapport for 2024 at av 30 000 anmelder om bedrageri som politiet mottok i 2024, gjaldt 77 prosent digitale bedragerier.

Selv om disse sakene enkeltvis kan fremstå mindre alvorlige, kan de ha store personlige og samfunnsmessige konsekvenser når de ses i sammenheng. Handlingene utføres ofte av

organiserte kriminelle grupper på tvers av landegrenser. Politiets har i mange tilfeller liten mulighet til å komme i mål med etterforsking. Forebyggende innsats bør derfor være hovedfokus.

Økokrim har nylig etablert en egen bedragerienhet som har som mål å få i en stand en mer effektiv og strukturert bedrageribekjempelse på tvers av landets politidistrikt. Enheten skal først og fremst være en forebyggende enhet. Forebygging skal imidlertid være tett integrert i etterforskingen. I bedragerienheten er det mulig å gripe fatt i sakene på en annen måte, med sikte på blant annet å avdekke mønster og bakmenn.

Både ved etterforsking og forebygging av digitale bedragerier vil det være et godt verktøy for politiet å få tilgang til IP-data. Slike data kan eksempelvis brukes til å se sammenheng mellom en større mengde bedragerier og herunder avdekke om aktiviteten er organisert.

Selv om alminnelige bedragerier kun har en strafferamme på 2 år, jf. straffeloven § 371, mener departementene det kan være grunn til å inkludere dette straffebudet i oversikten av bestemmelsen som skal kunne gi grunnlag for utlevering av IP-data til forebyggende formål. Når omfanget av denne kriminaliteten er så stort blir konsekvensene både for enkeltpersoner og samfunnet som helhet svært alvorlige. Dersom politiet er henvist til å henlegge flertallet av saker, vil det på sikt kunne få konsekvenser for tilliten til myndighetene. Det vises til at grovt bedrageri har en strafferamme på seks år, jf. straffeloven § 372 og følgelig vil være omfattet direkte av det foreslåtte strafferammekravet. Det vil imidlertid ofte være vanskelig å vite om ett bedrageri bør ses i sammenheng med andre, noe som kan innebære at forholdet samlet sett vil anses som grovt. Om forholdet inngår i organisert virksomhet er også vanskelig å ha en klar formening om før man kan se flere saker i sammenheng.

For å sikre en god sammenheng i bestemmelsen, og ettersom etterforsking og forebygging i noen grad fremstår som en integrert virksomhet på dette området, kan det være grunn til å inkludere bedrageribestemmelsen også som grunnlag for utlevering av IP-data til etterforskingsformål. Departementene ber særskilt om høringsinstansenes syn på inkludering av dette.

7. Økonomiske og administrative konsekvenser

Digitaliserings- og forvaltningsdepartementet vil ikke ha økte kostnader som følge av dette lovforslaget.

For lagringspliktige tilbydere vil en utvidelse ikke medføre økte kostnader med selve lagringen. Uthenting til forebygging vil kreve justeringer i den tekniske løsningen for utlevering av data. Et usikkert anslag tilsier kostnader til tekniske endringer hos politiet på om lag 1. mill. kr. Det må også legges til rette for datatekniske løsninger hos PST.

For staten vil uthenting av flere IP-data medføre økte uthentingskostnader, både for PST og politiet for øvrig. Basert på dagens uthenting til etterforskingsformål kan det legges til grunn en gjennomsnittlig uthentingspris på ca. kr 500 pr anmodning. I 2024 sendte politiet totalt 4815 anmodninger til etterforskningsformål etter nåværende § 3-14. Som følge av forslaget om en høyere strafferamme og kortere uthentingstid antas antallet anmodninger fra politiet til

forebygging å bli vesentlig lavere. For PST er det grunn til å forvente at antallet anmodninger om IP-data vil øke vesentlig, noe som vil kunne medføre et merbehov på 5 årsverk, som tilsvarer merutgifter på 6,25 mill. kroner årlig.

At politiet får slike data, forventes imidlertid å bidra positivt i kriminalitetsbekjempelsen, til gode for samfunnet.

Kostnadene forslagene medfører for politiet og PST vil dekkes innenfor Justis- og beredskapsdepartementets til enhver tid gjeldende budsjettrammer.

8. Forslag til lov- og forskriftsbestemmelser

Ekomloven § 3-13 første ledd innledningen skal lyde:

Tilbyder av elektroniske kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal til bruk for etterforsking *og forebygging* av alvorlig kriminalitet, lagre de opplysninger som er nødvendige for å identifisere abonnentene med utgangspunkt i…

Ekomloven § 3-14 skal lyde:

§ 3-14 *Utlevering av IP-adresser*

Opplysninger lagret etter § 3-13 skal uten hinder av taushetsplikt etter § 3-10 utleveres til*:*

a. *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 straffeloven § 125, § 168, § 184, § 201, § 202, § 204, § 205, § 251, § 263, § 266, § 267 a første ledd, § 267 b, § 297, § 298, § 305, § 306, § 309 eller § 371, eller åndsverkloven § 104, jf. § 79*
b. *politiet når det er grunn til å undersøke om noen forbereder en handling som etter loven kan medføre straff av fengsel i seks år eller mer, eller som rammes av straffeloven § 201, § 202, § 204, § 297, § 298, § 304, § 305, § 306, § 309, § 310, § 311, § 330 eller § 371*
c. *Politiets sikkerhetstjeneste når det er grunn til å undersøke om noen forbereder en handling som nevnt i politiloven § 17 b*

Anmodning om utlevering etter første ledd skal fremsettes skriftlig og så vidt mulig opplyse om hva saken gjelder, formålet med anmodningen og hva den omfatter. *Det skal fremgå av anmodningen at vilkårene for utlevering av opplysningene er vurdert.*

Det kan bare anmodes om utlevering etter første ledd dersom det etter sakens art og forholdene ellers vil være forholdsmessig.

Anmodning om utlevering etter første ledd bokstav a kan ta utgangspunkt i både IP-adresser og abonnenter. Anmodning om utlevering etter første ledd bokstav b og c kan bare ta utgangspunkt i IP-adresser.

Anmodning om utlevering etter første ledd bokstav b kan ta utgangspunkt i et tidspunkt som ligger inntil 6 måneder tilbake i tid.

Politiet og påtalemyndigheten skal oversende en årlig rapport til departementet om uthentingen av IP-adresser *etter første ledd bokstav a og b. PST skal oversende en årlig*

rapport til EOS-utvalget og Justis- og beredskapsdepartementet om uthentingen av IP-adresser etter første ledd bokstav c.

Opplysninger som kun er lagret etter § 3-13 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.

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

Ekomforskriften § 3-5 annet ledd tredje punktum skal lyde:

Utenfor normal arbeidstid skal tilbyder ha beredskap for på kort varsel å kunne behandle anmodninger i saker som haster av hensyn til liv eller helse eller dersom det ved opphold er fare for at etterforskingen vil lide *eller det ved opphold er stor fare for at muligheten til å forebygge den straffbare handlingen vil gå tapt.*

Ekomforskriften § 3-5 tredje ledd første punktum oppheves.

Ekomforskriften § 3-6 skal lyde:

§ 3-6 *Årlig rapportering om uthenting av opplysninger om IP-adresser*

Politi- og påtalemyndigheten skal oversende årlig rapportering om uthentingen av lagringspliktige opplysninger etter ekomloven § 3-14 første ledd *bokstav a og b*. Rapporteringen skal sendes Nasjonal kommunikasjonsmyndighet innen 1. mars hvert år. Rapporteringen skal inneholde oversikt over

a. det totale antallet anmodninger som er sendt lagringspliktige tilbydere per kalenderår *etter henholdsvis ekomloven § 3-14 første ledd bokstav a og b*, antallet som er besvart av tilbyder og dokumentasjon på at kravene til utlevering i ekomloven § 3-14 annet ledd er oppfylt for anmodningene,
b. det totale antallet abonnenter politiet har fått utlevert informasjon om per kalenderår, og varigheten av det etterspurte tidsintervallet for den enkelte anmodningen om dette er benyttet. Dersom det anmodes om informasjon gjentatte ganger i løpet av kalenderåret med utgangspunkt i samme abonnent når denne er en fysisk person, skal antallet abonnenter dette gjelder oppgis. I slike tilfeller skal også det totale antallet utleveringer og den totale varigheten på eventuelle tidsintervall benyttet oppgis per abonnent,
c. den årlige fordelingen av besvarte anmodninger med utgangspunkt i henholdsvis IP-adresse eller abonnent og,
d. hvilke straffebud som ligger til grunn for det årlige uttaket av lagringspliktig informasjon *etter henholdsvis ekomloven § 3-14 første ledd bokstav a og b.*

Politiets sikkerhetstjeneste skal oversende rapportering om uthenting etter ekomloven § 3-14 første ledd bokstav c til EOS-utvalget og Justis- og beredskapsdepartementet. Rapporteringen skal inneholde oversikt over

a. det totale antallet anmodninger som er sendt lagringspliktige tilbydere per kalenderår, antallet som er besvart av tilbyder og dokumentasjon på at kravene til utlevering i ekomloven § 3-14 annet ledd er oppfylt for anmodningene,

b. hvilke straffebud som ligger til grunn for det årlige uttaket av lagringspliktig informasjon.