Svein Willassen AS

DATALAGRINGSDIREKTIVET –

VERDI I ETTERFORSKNING
OG
RISIKOFAKTORER FOR PERSONVERN

Oslo, 07.04.2010

Svein Y. Willassen
siv.ing., ph.d.

Steinhammerveien 3, 1177 OSLO, Norway
phone: +47 92449678, email: svein@willassen.no, web: www.willassen.no

Sammendrag

Ved innføring av pliktig lagring av trafikkdata som opprettes ved elektronisk kommunikasjon er det av interesse å foreta en avveining av verdien slike data vil ha i etterforskning sammenholdt med risikofaktorer for personvern forbundet med slik lagring. En slik vurdering må utføres for seg for hver datatype som kreves lagret.

Denne utredningen beskriver hver datatype som kreves lagret i henhold til EUs datalagringsdirektiv, og vurderer nytte i etterforskning og risikofaktorer for personvern for hver datatype, samt gjør en avveining av disse hensynene. Det er funnet at datatypene som kreves lagret i direktivet kan grupperes i tre grupper som ved en avveining gir ulikt resultat:

Gruppe A – logg over internettilgang og logg over tilgang til epostkasse: Slike data kan være avgjørende i etterforskningssammenheng og lagring medfører få risikofaktorer for personvern. En avveining tilsier at slike data bør lagres.

Gruppe B – trafikkdata fra mobil-, fast- og ip-telefoni: Slike data er nyttig i etterforskningssammenheng, men lagring medfører fremtredende risikofaktorer for personvern. Utfallet av en avveining avhenger av en demonstrasjon av i hvilken grad slike bevis vektlegges i forhold til andre bevis i saker der slike data er benyttet.

Gruppe C – logg over hvem som har sendt epost til hvem. Slike data har liten nytte i etterforskningssammenheng, og lagring medfører betydelige risikofaktorer for personvern. En avveining tilsier at slike data ikke bør lagres.

For alle de nevnte datatyper er det mulig å redusere risikofaktorer for personvern ved å stille tekniske krav til implementasjon av datalagring. Et mulig teknisk tiltak som vil redusere risikofaktorer for personvern betydelig er kryptering av lagrede data med offentlig-nøkkel kryptografi. Med en slik implementasjon vil tilgangen til lagrede data være begrenset til politiets tilgang til individualiserte data ved rettslig kjennelse.

1. Innledning

EUs datalagringsdirektiv vurderes innført i norsk rett. Direktivet innfører en plikt for tilbydere av elektronisk kommunikasjon til å lagre nærmere spesifiserte data om kommunikasjon om formidles. [1] Samferdselsdepartementet, Justisdepartementet og Fornyings- og Administrasjonsdepartementet har sendt ut et høringsnotat som beskriver en mulig implementering av datalagringsdirektivet i norsk rett. [2] Notatet foreslår at direktivet implementeres gjennom endringer i ekomloven og ekomforskriften. Formålet med å innføre en slik plikt er å sikre politiets tilgang til data som har nytteverdi i forbindelse med etterforskning og påtale av straffesaker. I tillegg foreslås endringer i straffeprosessloven som innfører et strengere krav for politiets tilgang til slike data enn det som foreligger i dag.

Høringsnotatet inneholder i punkt 4.4.1 – 4.4.5 en liste over hvilke data som kreves lagret ved ulike former for elektronisk kommunikasjon. Listen er basert på en oppregning av hvilke datatyper som kreves lagret i artikkel 5 selve direktivteksten. Dataene som kreves lagret gjelder kommunikasjon med ulike teknologier; telefoni (herunder mobil-, fast- og ip-telefoni), internettilgang og epost-kommunikasjon. Disse teknologiene er av sin art forskjellige, og brukes på forskjellig måte av brukerne. Dette resulterer i at dataene som kreves lagret for de ulike kommunikasjonsteknologiene skiller seg fra hverandre både i form, innhold og hva innholdet forteller om brukerens kommunikasjon. Disse forskjellene medfører at de ulike datatypene som kreves lagret har ulik nytteverdi i etterforskningssammenheng, samt at risikofaktorer for personvern ved innføring av lagringsplikt vil være ulik for de forskjellige datatypene.

Ved en vurdering av innføring av lagringsplikt, er det av interesse å foreta en vurdering av hvilken nytte dataene har i etterforskningssammenheng. Denne nytten bør vurderes opp mot risikofaktorer for personvern ved å innføre pliktig lagring av data om all kommunikasjon som foretas gjennom tilbyderne. Som følge av at dataene er relatert til forskjellige kommunikasjonsformer, vil en slik vurdering kunne slå ulikt ut for hver av datatypene som omhandles i direktivet. Det er derfor av interesse å foreta en slik vurdering og sammenligning for hver kommunikasjonsform for seg. En slik vurdering av hver kommunikasjonssform for seg vil kunne avdekke forskjeller mellom forholdet mellom nytteverdi i

etterforskningssammenheng og risikofaktorer for personvern mellom de ulike kommunikasjonsformene som bør hensyntas i vurderingen av om datalagringsdirektivet bør implementeres, og eventuelt i hvilken form.

Det foreliggende dokument har som mål å utrede forholdet mellom nytte i etterforskning og risikofaktorer for personvern ved lagringsplikt for hver kommunikasjonsform som omhandles av datalagringsdirektivet. Utredningen er utarbeidet i februar og mars 2010 av ph.d. Svein Y. Willassen på oppdrag fra Datatilsynet i forbindelse med høring om datalagringsdirektivet.

2. Metode

Det er tatt utgangspunkt i de ulike kommunikasjonsformene som det foreslås innført lagringsplikt om. Hver kommunikasjonsform og hvilke data som skal lagres er beskrevet. Videre er omfang av bruk av slik kommunikasjon i Norge beskrevet. Det er for flere av kommunikasjonsformene gitt eksempler på hvilke data som opprettes og lagres av eksisterende kommunikasjonssystemer. Disse dataene sammenholdes så med sletteplikten etter ekomloven §2-7, samt eventuell innføring av lagringsplikt.

For å vurdere hvilken nytte de lagrede data fra de ulike kommunikasjonsformene har i etterforskningen er det gjennomført samtaler med personer i politiet om hvilken nytte de ulike kommunikasjonsformene har, og innenfor hvilke kriminalitetsområder. Det er gjennomført samtaler med Ketil Haukaas, John Ståle Stamnes og Erik Trønnes-Hansen i Kripos. Politiet har i dag ikke selv statistikk over sine henvendelser til kommunikasjonsleverandører. For å få et bilde omfanget av utlevering til politiet er det derfor rettet forespørsler til Telenor, NetCom og NextGenTel om opplysninger om antall henvendelser de mottar fra politiet. Disse henvendelsene ble alle besvart, og statistikken er tatt inn i det følgende. Utreder har også hatt glede av egne erfaringer fra arbeid i Økokrim i perioden 1999-2002, samt egen forskning innen området digitale bevis.

For å vurdere risikofaktorer for personvern ved innføring av lagringsplikt er det gjennomført samtaler med ansatte ved Datatilsynet, i tillegg til egne vurderinger. Arbeidet er gjennomført i Datatilsynets lokaler, og utreder har på denne måten fått et godt innblikk i hvilke utfordringer

som ligger i at data lagres og hvilke utfordringer innføring av lagringsplikt reiser, både av prinsipiell og praktisk art.

3. Generelt om nytte i etterforskningssammenheng

3.1. Kommunikasjonsdata og lokasjonsdata

Det er et hovedinntrykk at data om de ulike kommunikasjonsformene som omhandles i datalagringsdirektivet brukes ulikt innen de ulike kriminalitetsområdene. Eksempelvis har informasjon om internettoppkobling betydning innen noen kriminalitetsområder, mens informasjon om mobilkommunikasjon har større betydning i andre kriminalitetsområder.

Ved bruk av lagrede data ser det ut til å gå et skille mellom bruk av *kommunikasjonsdata* og *lokasjonsdata*. Med kommunikasjonsdata menes her informasjon som forteller hvem som har kommunisert med hvem, hvilken type kommunikasjon som er utført, hvor lenge kommunikasjonen varte og så videre. Med lokasjonsdata menes informasjon som plasserer brukeren på et bestemt sted på et bestemt tidspunkt. Lokasjonsdata kan utledes fra data som lagres av kommunikasjonsleverandører. Dette fordi kommunikasjonsleverandørene for noen datatyper eksplisitt lagrer data om lokasjon i forbindelse med kommunikasjonen, slik som for eksempel celleid som lagres ved oppringninger i mobilnettet. Videre kan lokasjonsdata også utledes fra implisitt lokasjonsinformasjon, når kommunikasjonen skjer fra et fast anlegg som er levert til et bestemt sted.

Både kommunikasjonsdata og lokasjonsdata slik det er definert her, kan ha verdi for politiet i en etterforskning. Det synes å være slik at det i noen sakstyper primært er kommunikasjonsdata som er av interesse, mens det i andre saker primært er lokasjonsdata som er av interesse. Lokasjonsdata i forbindelse med elektronisk kommunikasjon kan i forbindelse med straffesaker brukes som bevis på at vedkommende som kommuniserte oppholdt seg på et bestemt sted til et bestemt tidspunkt, uavhengig av hvem vedkommende kommuniserte med og i hvilken form. Brukt på denne måten blir trafikkdata fra kommuniksjonsleverandører et bevis for oppholdssted på lik linje med vitneobservasjoner, bilder fra overvåkningskamera, fingeravtrykk, biologiske spor og andre tekniske bevis. Dette

kan ha stor verdi i mange saker der den straffbare handlingen har skjedd på et konkret sted. Det kan imidlertid innvendes at når lokasjonsdata fra elektronisk kommunikasjon brukes på denne måten, så er ikke bruken relatert til selve den elektroniske kommunikasjonen som er foretatt. Den elektroniske kommunikasjonen som er foretatt trenger ikke å ha noe med forholdet som etterforskes å gjøre. Det er utelukkende informasjon om lokasjonen til den som kommuniserte man er ute etter.

I andre sakstyper kan det være selve kommunikasjonsdataene som er av interesse. Det kan for eksempel være av interesse å kartlegge hvem som har vært i kommunikasjon med hvem, for å kartlegge et nettverk av personer. I et slikt tilfelle er lokasjonen som er knyttet til kommunikasjonen mindre interessant. Her er man ute etter å finne bevis for tilknytning mellom personer. Da er det hvem som har hatt kontakt med hvem, i hvilken form og hvor lenge som er interessant, ikke hvor vedkommende tilfeldigvis befant seg når kontakten fant sted.

Basert på det overnevnte bør man derfor skille mellom nytteverdi i etterforskning forsåvidt gjelder kommunikasjonsdata og lokasjonsdata. Det er ikke gitt at en avveining mellom nytteverdi i etterforskning og risikofaktorer for personvern vil falle likt ut for henholdsvis kommunikasjonsdata og lokasjonsdata.

3.2. Sporing og annen bevisuthenting

Når det gjelder politiets forespørsler om utlevering av data fra kommunikasjonsleverandører kan det videre oppstilles et skille mellom *sporing* og *annen bevisuthenting*. Ved *sporing* er situasjonen den at man forsøker å finne ut hvem som har vært motparten i en kommunikasjon. Det kan for eksempel dreie seg om en epost med innhold som etter sin art er straffbart å besitte eller sende, og hvor politiet i etterforskningen forsøker å avdekke identiteten til den som sendte eposten. Dette gjøres ved å rette en henvendelse til internettleverandøren som har levert internettoppkoblingen som er benyttet, med forespørsel om hvilken abonnent det var som benyttet ip-adressen som er oppgitt i epostmeldingen på det tidspunktet eposten ble sendt. Leverandøren vil da slå opp i loggen over hvilke ip-adresser som er benyttet på ulike tidspunkt, og utlevere navnet på abonnenten som brukte den aktuelle ip-adressen på det aktuelle tidspunktet. I sporingstilfellet følger man altså sporene direkte fra bevisene tilbake til opphavspersonen.

Ved *annen bevisuthenting* er inngangen motsatt: her har man et kjent informasjonselement, for eksempel et telefonnummer eller en lokasjon. Man ber så om utlevering av alle data som er knyttet til dette informasjonselementet – for eksempel alle oppringninger til og fra et telefonnummer, eller all telefonaktivitet som er utført på en bestemt lokasjon. Når disse dataene utleveres av leverandøren, kan politiet gå gjennom dataene og lete etter andre elementer som kan ha betydning i saken – for eksempel andre telefonnumre av interesse som det har blitt ringt til eller alle telefoner som har foretatt oppringinger eller mottatt samtaler innenfor dekningen til en bestemt basestasjon. Ved annen bevisuthenting er det altså politiet som selv leter gjennom de data som er utlevert med tanke på å avdekke sammenhenger som kan ha betydning i saken.

Et skille mellom sporingstilfeller og bevisuthentingstilfeller tydeliggjør forskjeller mellom utlevering av ulike typer data på flere ulike plan. Når det gjelder nytte i etterforskningen, så er det ved *sporing* som regel slik at identifikasjon av gjerningsperson avhenger av at sporingen kan gjennomføres, det vil si at leverandøren besitter en logg som de kan slå opp i for å gjennomføre sporingen. I slike tilfeller kan informasjonen som utleveres fra leverandøren være avgjørende for at politiet kommer videre, for hvis man ikke kan identifisere noen gjerningsperson kan det være vanskelig å vite hvordan man skal gå frem for å samle inn ytterligere bevis. Ved annen bevisuthenting er situasjonen som regel den at en eller flere gjerningspersoner allerede er kjent, og bevisene som hentes ut skal tjene som dokumentasjon på tilknytning mellom dem eller tilknytning til en bestemt lokasjon. Det er på det rene at slik informasjon kan være nyttig i etterforskningen, men de er neppe i de fleste tilfeller avgjørende.

Når det gjelder risikofaktorer for personvern, synes det å være forskjell på data som må være lagret for å understøtte sporing, og data som må være lagret for å understøtte annen bevisuthenting. For å understøtte sporing er det tilstrekkelig om det er lagret data om koblingen mellom abonnent og den kommunikasjonsadresse som benyttes ved kommunikasjonen, slik som ip-adresse eller telefonnummer. Denne koblingen er tilstrekkelig for å kunne slå opp hvilken abonnent som benyttet en bestemt kommunikasjonsadresse på et bestemt tidspunkt – og dermed hvem som er kommunikasjonsmotparten. Lagring av slike data vil medføre langt færre risikofaktorer for personvern enn lagring av alle data om hvem som har satt seg i forbindelse med hvem, som er den type data som oftest hentes ut ved annen bevisinnhenting.

Skillet mellom sporing og annen bevisinnhenting synes derfor å være en nyttig abstraksjon for politiets uthenting av bevis i de ulike tilfeller, og vil bli drøftet nærmere under hver enkelt datatype i det følgende.

4. Generelt om risikofaktorer for personvern

4.1. Utgangspunkt – risikofaktorer for personvern ved datalagring

Lagringsplikt for trafikkdata har implikasjoner for personvernet for dem de lagrede dataene omhandler. Implikasjonene ligger i at informasjon om hvilken kommunikasjon den enkelte har foretatt blir lagret, slik at de potensielt kan være tilgjengelig for andre. Hvis informasjonen ikke hadde vært lagret, eller eventuelt overhodet ikke innsamlet, hadde det ikke vært mulig å hente ut noen oversikt over den enkeltes kommunikasjon, hverken for politiet eller andre. Risikofaktorer for personvern ved datalagring henger altså sammen med hvem dataene er eller kan være tilgjengelig for. Dette betyr at man med en vurdering av risikofaktorer for personvern ved datalagring må vurdere hvem dataene vil være tilgjengelig for. Lagring av data på en slik måte at datainnholdet ikke kan leses av noen medfører ingen risikofaktor for personvernet. (For eksempel ved kryptering med en tilfeldig nøkkel som ikke lagres.) Motsatt vil publisering av data medføre en betydelig risikofaktor for personvernet for den dataene omhandler.

På bakgrunn av overnevnte kan den foreliggende vurderingen av risikofaktorer for personvern sies å ha en praktisk tilnærming. Dette i motsetning til en prinsipiell tilnærming der enhver lagring av data sees på som skadelig for personvernet uansett om dataene kan leses av noen eller ikke.

Dataene er i utgangspunktet tilgjengelig for kommunikasjonsleverandørene selv. Etter utlevering, vil dataene også være tilgjengelig for politiet og andre aktører i forbindelse med straffesaken. Men det er ikke tilstrekkelig å vurdere hvem som skal ha rettmessig tilgang til dataene. Ved en vurdering av lagringplikt, må også muligheten for urettmessig tilgang vurderes. Hvis dataene ikke hadde vært lagret, hadde det heller ikke være mulig å hente ut dataene enten det skjedde ved rettmessig eller urettmessig tilgang. Muligheten til urettmessig tilgang kan reduseres ved å stille krav til informasjonssikkerhetstiltak i forbindelse med innføring av lagringsplikten. Det er imidlertid umulig å oppnå absolutt sikkerhet med

informasjonssikkerhetstiltak, slik at det alltid vil være større risiko for at data kommer uvedkommende i hende når data er lagret enn om de ikke var det.

4.2. Kommunikasjonsleverandørenes egen tilgang til data

Lov om elektronisk kommunikasjon §2-9 gir bestemmelser om taushetsplikt for leverandører av elektronisk kommunikasjon. Bestemmelsene er til hinder for at leverandører utleverer data om elektroniske kommunikasjon til andre. Videre er bestemmelsen til hinder for at leverandøren benytter slike data i sin egen virksomhet, med unntak av statistikk som er anonymisert og som ikke gir informasjon om innretninger eller tekniske løsninger. Dette gjelder også for ansatte hos leverandørene.

Det er imidlertid på det rene at leverandørene rent faktisk lagrer data slik at de er tilgjengelig for leverandørens egne ansatte. Ansatte hos leverandørene har dermed rent faktisk en mulighet for å gjøre søk i de lagrede dataene, og trekke ut informasjonssammenstillinger for egne formål. På denne måten kan det for eksempel være mulig for ansattte hos leverandørene å avdekke hvem som har kommunisert med hvem og hvilke lokasjoner bestemte personer har oppholdt seg på. Denne muligheten er en risikofaktor for personvern. Det er mulig å forhindre slik tilgang ved å stille krav til teknisk implementasjon for lagringen, men så langt har det ikke vært stilt krav om en slik teknisk implemtasjon for lagring av data.

4.3. Tilgang til data i forbindelse med utlevering i straffesaker

Politiet kan hente ut data fra kommunikasjonsleverandørene i straffesaker. Hvilken prosedyre som benyttes for å hente ut data, varierer med hvilke data det er snakk om. Resultatet av uthentingsprosedyren er en beslutning som oversendes kommunikasjonsleverandøren. Denne beslutningen inneholder en identifikasjon av hvilke data som skal utleveres. Identifikasjonen må være tilstrekkelig presis til å individualisere et datasett som kan identifiseres med den hendelse eller person som etterforskes. Det kan eksempelvis være tale om et telefonnummer eller en ip-adresse som er brukt på et bestemt tidspunkt. Kommunikasjonsleverandøren bruker så denne identifikasjonen til å gjøre et uttrekk av individualiserte data fra dataene som er lagret hos dem. Dette uttrekket sendes så tilbake til politiet og inngår i straffesaksdokumentene.

Trafikkdata som blir en del av straffesaksdokumentene gjøres tilgjengelig for flere aktører. For det første vil straffesaksdokumentene normalt leses av politiets etterforskere og påtalejurister. Videre vil andre innenfor påtalemyndigheten normalt ha tilgang til dokumentene i forbindelse med påtale. Dokumentene vil også oversendes til forsvarere i saken, og forsvarer vil normalt foreholde opplysningene i saken til sin klient. Dersom det er flere siktede i saken vil vanligvis alle dokumenter bli oversendt alle forsvarere. Endelig vil de data som påberopes som bevis i saken bli lagt frem i forbindelse med hovedforhandling og eventuelle ankeforhandlinger, og kan dermed gjengis offentlig. Data som er hentet ut i forbindelse med etterforskningssaker kan dermed i ytterste konsekvens kan gjøres kjent for mange, noe som utgjør en risikofaktor for personvernet for den det gjelder.

Det må imidlertid understrekes at data som politiet får utlevert er begrenset til å gjelde data som er individualisert i en konkret sak. Det er altså et relativt begrenset uttrekk av de data som faktisk er lagret som er tilgjengelig for aktørene i straffesaken. Videre er det vanligvis bare en begrenset del av dataene som er hentet ut som har konkret betydning som bevis og som dermed blir presentert i retten. De øvrige data er overskuddsinformasjon som normalt ikke vil bli kjent for offentligheten.

Risikofaktorer for personvern ved utlevering i forbindelse med straffesaker kan neppe reduseres med tekniske løsninger, i det selve formålet med lagringsplikten nettopp er å gi tilgang til slik utlevering og bruk.

4.4. Andres tilgang til data

Det kan også forekomme at andre får tilgang til data fra kommunikasjonsleverandørene. Dette kan skje ved at data urettmessig blir hentet ut eller utlevert fra kommunikasjonsleverandøren eller fra aktører som har tilgang på straffesaksdokumentene.

4.4.1. Andres tilgang hos leverandøren

Urettmessig tilgang hos leverandøren er den potensielt mest alvorlige formen for urettmessig tilgang. Alle data om kommunikasjon er lagret her, ikke bare et uttrekk som er gjort for

etterforskning av konkrete saker som vil være tilfelle hos politiet og påtalemyndigheten. Urettmessig tilgang kan skje ved datainnbrudd eller ved at data utleveres urettmessig av ansatte hos kommunikasjonsleverandøren. Begge typer forhold kan motvirkes ved informasjonssikkerhetstiltak hos leverandøren. Slike informasjonssikkerhetstiltak kan og bør bestå i tekniske sikkerhetstiltak som beskytter de datasystemer som er involvert i selve lagringen. I tillegg bør det være etablert regler og rutiner for hvem som har tilgang, som reduserer risikoen for at ansatte utleverer informasjon fordi de blir satt under press eller får belønning. Risikoen for utlevering kan reduseres med slike informasjonssikkerhetstiltak, men kan neppe fjernes helt så lenge det faktisk er mulig for ansatte hos leverandøren å få fysisk tilgang til dataene.

Avsnitt 4.5 i det følgende beskriver et system hvor ansatte hos leverandøren ikke har tilgang til dataene. Et slikt system vil redusere risikoen for urettmessig tilgang til data hos leverandøren til et minimum, ettersom slik urettmessig tilgang også forutsetter at vedkommende som skaffer seg tilgang har skaffet seg adgang til politiets hemmelige nøkkel.

4.4.2. Andres tilgang til data fra straffesaker

Det har forekommet tilfeller av at data som er utlevert i forbindelse med etterforskning av straffesaker har tilkommet uvedkommende. Eksempelvis har det forekommet at opplysninger som er hentet ut fra kommunikasjonsleverandører har blitt gjengitt i pressen på et stadium i etterforskninger hvor opplysninger enda ikke har vært gjengitt offentlig i forbindelse med rettssak. Hvem som har utlevert opplysningene kan variere, men det bør påpekes at aktørene i en straffesak kan ha interesse av å få opinionen på sin side, og derfor kan se seg tjent med å gi ut opplysninger til pressen. Dette vil krenke personvernet til den opplysningene handler om, som ikke nødvendigvis er den mistenkte. Dette er imidlertid et generelt problem som ikke er begrenset til opplysninger som er utlevert av kommunikasjonsleverandører. Også andre opplysninger som fremkommer i en straffesak, slik som vitneforklaringer og tekniske bevis, kan medføre risikofaktorer for personvern ved utlevering. Urettmessig utlevering av opplysninger fra straffesaksaktørene er derfor et problem som må håndteres uansett om data lagres eller ikke.

4.5. Begrensning av leverandørens egen tilgang til lagrede data

ETSI TR 102 661 er en teknisk rapport som beskriver informasjonssikkerhetstiltak som kan gjennomføres i forbindelse med kommunikasjonskontroll og datalagring. [7] Rapporten beskriver ulike trusselscenarier, og dokumenterer tiltak som kan gjennomføres ved implementasjon av lagringssystem som gjør at informasjonssikkerhet kan ivaretas ved gjennomføring av datalagring. Det heter i rapportens innledning at tiltakene som beskrives er *anbefalinger*.

Av spesiell interesse i denne sammenheng er tiltakene som er beskrevet i rapportens appendiks C under overskriften "Protection of retained data". Her beskrives et system som muliggjør at data lagres uten at ansatte hos operatøren som lagrer data har tilgang til dataene, men hvor politiet fortsatt kun har tilgang til individualiserte data ved at operatøren henter ut data for dem i henhold til rettslig beslutning. Systemet er bygget på offentlig-nøkkel kryptografi og består av følgende elementer:

- Et system for datalagring som er separat fra lagringssystem for andre formål (fakturering e.l.)
- Ved lagring krypteres hvert logginnslag med politiets offentlige nøkkel
- I tillegg til det krypterte logginnslaget lagres det hashverdier for hver nøkkel som skal kunne brukes til oppslag (IP-adresse, telefonnummer o.l.), og tidspunkt for logginnslaget
- Etter at logginslaget er lagret i systemet blir klartekstdataene slettet, slik at det bare er krypterte logginnslag med tilhørende hashverdier som lagres
- Logginnslag som er eldre enn lagringstiden slettes fra systemet (Dette er mulig fordi tidspunktet er lagret i klartekst)
- Ved uthenting av data må politiet skaffe en beslutning som utpeker hvilken nøkkelverdi det skal hentes data for. Leverandøren lager så en hashverdi for denne nøkkelverdien, og henter ut de krypterte logginnslagene som sendes over til politiet. Politiet kan så dekryptere disse med sin private nøkkel.

I nevnte rapport er dette systemet foreslått som en løsning på hvordan lagring kan skje hos en tredjeparts lagringsleverandør på vegne av mindre operatører. Det er imidlertid intet i veien for at operatørene kan benytte en slik fremgangsmåte i sitt eget system.

I forhold til risikofaktorer for personvern, vil en slik lagringsmetode ha flere fordeler. For det første vil de lagrede dataene ikke være tilgjengelige for leverandøren eller ansatte hos leverandøren. Dette vil forhindre trusler mot personvernet som oppstår som følge av at leverandøren eller ansatte hos operatøren kan analysere data for egne formål. For det andre, vil oversendelsen av data fra operatøren til politiet automatisk være sikret, slik at risikoen for at andre får tilgang til dataene under oversendelsen vil være redusert. For det tredje vil dataene rent faktisk fortsatt være lagret hos operatøren. Dette innebærer at politiet fortsatt kun vil få tilgang til korrekt individualiserte data, og kun på bakgrunn av en beslutning som sjekkes av leverandøren. En ytterligere fordel i forhold til risikofaktorer for personvern, er at man med dette systemet må bestemme på implementasjonstidspunktet hvilke nøkler det skal være mulig å hente ut data for. Det er altså ikke i ettertid mulig å hente ut data på en måte som man ikke så for seg på det tidspunkt systemet ble implementert. Denne egenskapen kan sies å innebære en resistens mot en glidning hvor man kan hente ut data på stadig nye måter fordi dataene uansett allerede er lagret. Videre forhindrer systemet også at andre enn politiet henter ut data, da bruk av politiets private nøkkel er nødvendig for å få tilgang til dataene.

Metoden som skisseres er altså en teknisk løsning som fjerner noen av de personvernmessige utfordringene med datalagring. Samtidig er det på det rene at et krav om innføring av en slik metode vil stille ytterligere krav til operatørene i form av funksjonelle krav til implementasjon. Innføring av kryptering av data som beskrevet i TR 102 661 vil etter all sannsynlighet gjøre implementasjon av datalagring hos operatørene dyrere. En løsning som innebærer at operatøren krypterer data på denne måten ser ikke ut til å ha vært vurdert i forbindelse med kostnadsvurderingen som er utført av Teleplan.

5. Trafikkdata fra internettoppkobling

5.1. Beskrivelse

Datalagringsdirektivet krever at data som blir opprettet ved internettoppkobling blir lagret. Data som skal lagres er: [2]

- brukers IP-adresse
- abonnentinformasjon, registrert brukerinformasjon
- dato og tidspunkt for pålogging og avlogging av internettjenesten
- type internettoppkobling

- informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg

Det er verdt å merke seg at data om kommunikasjonsmotparter (hvem som har satt seg i forbindelse med hvem) ikke kreves lagret. Dette skiller seg fra lagring av telefonilogger, der det skal lagres hvem som har satt seg i forbindelse med hvem. Dette medfører at det ikke er mulig å trekke ut informasjon om hvilken aktivitet som er utført av brukeren på internett, slik som hvilke websider som er besøkt eller liknende. Dataene som skal lagres er utelukkende relatert til brukerens egen tilgang til internett. Lagring av slike data gjør det mulig å identifisere en abonnent når det foreligger informasjon fra en av abonnentens kommunikasjonsmotparter i form av ip-adresse og tidspunkt.

Hos leverandørene vil lagring av slike data normalt være implementert på to nivåer:

1. Et abonnentregister som inneholder brukernavn for alle brukerne og annen informasjon som blir registrert av leverandøren når abonnementsforholdet opprettes. Et slikt register inneholder vanligvis abonnentens navn og adresse, teknisk informasjon om abonnementet, samt informasjon om betalingsvilkår og betalingsstatus.
2. En logg over når brukeren koblet seg opp, og hvilken ip-adresse brukeren ble tildelt av leverandøren ved oppkoblingen, samt identifikasjon av brukerutstyret som ble benyttet. Sistnevnte kan for eksempel være i form av MAC-adresse (fast adresse tilordnet et nettverkskort) tilhørende kommunikasjonsutstyret. Denne loggen vil også vise når brukeren koblet seg ned.

Informasjonen under punkt 1 over er normalt nødvendig for leverandøren å beholde så lenge abonnementet er aktivt. Informasjonen under punkt 2 er derimot ikke nødvendig for leverandøren å ta vare på med mindre brukerene betaler for tiden de er oppkoblet, noe som er mindre vanlig i dag. Begge typer informasjon er imidlertid nødvendig for å kunne identifisere en abonnent på bakgrunn av ip-adresse og tidspunkt.

De nevnte trafikkdata må sees i sammenheng med at svært mange internettleverandører i dag benytter dynamiske ip-adresser. Ved bruk av dynamiske ip-adresser blir abonnenten tildelt en ip-adresse ved oppkobling, og denne benyttes til kommunikasjon så lenge abonnenten er

oppkoblet. Når abonnenten kobler ned blir adressen frigitt, og den kan da tas i bruk av andre abonnenter. En ip-adresse kan altså ha blitt brukt av flere forskjellige abonnenter over et tidsrom, så for å identifisere hvem som brukte adressen på et bestemt tidspunkt er det nødvendig å gjøre oppslag i loggen som registrerer hvilken abonnent som var tildelt hvilken adresse på hvilket tidspunkt. Hos de fleste leverandører er dette tilfelle selv om abonnenten har en bredbåndsoppkobling som tillater abonnenten å være tilkoblet kontinuerlig, slik som ADSL eller fibernettverk. Ved slik oppkobling vil ruteren hos abonnenten bli tildelt en ip-adresse når den kobler seg opp. Denne adressen kan forandre seg når abonnenten kobler seg ned og kobler seg opp igjen, for eksempel fordi strømmen til ruteren blir brutt i en kortere periode.

Bakgrunnen for at leverandørene bruker dynamiske adresser er primært at ip-adresser er en begrenset ressurs. Dersom det var uendelig mange ip-adresser hadde det ikke vært problematisk å la alle brukere ha sine egne ip-adresser som var tilordnet dem hele tiden selv om de ikke var oppkoblet. En slik løsning ville hatt mange fordeler, og hadde sannsynligvis vært løsningen som hadde vært valgt dersom mangel på ip-adresser ikke hadde vært et problem. Med en slik løsning hadde det ikke vært behov for noen logg over tildeling av ip-adresser til brukere på ulike tidspunkt, da denne tildelingen hadde fulgt direkte av opplysningene som var registrert i abonnementsregisteret. Faktum er imidlertid at ip-adresser er en begrenset ressurs. Det er ikke ønskelig å "sløse" med ip-adressene ved å la abonnenter som ikke er oppkoblet legge beslag på dem.

Det har ikke tidligere vært noen lagringsplikt for logger som opprettes ved internettoppkoblinger. De fleste norske internettleverandørene har likevel ønsket å lagre disse opplysningene for å kunne identifisere sine egne abonnenter av sikkerhetshensyn. Dette er for eksempel aktuelt når internettleverandørene mottar informasjon om spredning av datavirus og spam. I slike tilfeller må leverandøren slå opp i loggen over abonnent/ip-adresse for å finne ut hvilken abonnent det er som er infisert av virus eller som sender ut spam, for å varsle vedkommende om at datamaskinen hans er infisert. Ekomloven §2-7 oppstiller imidlertid en sletteplikt for data som ikke er nødvendig for kommunikasjons- eller faktureringsformål. Inntil 2009 tolket de fleste leverandørene dette slik at de på grunn av overnevnte i hvert fall kunne ta vare på disse loggene i den tiden som konsesjon fra Datatilsynet tillot dem å ta vare på logger for faktureringsformål, det vil si 3 måneder. Dette ble imidlertid innskjerpet i et

vedtak fra Datatilsynet i 2009, hvor lagringstiden for denne type logger ble satt til maksimalt tre uker. Dette virker å ha blitt fulgt opp av leverandørene, slik at politiet i dag ikke har mulighet til å identifisere hvilken abonnent som har brukt en ip-adresse når det er gått mer enn tre uker siden den aktuelle adressen ble brukt. Det er videre opplyst at enkelte leverandører ikke fører noen slik logg i det hele tatt, hverken nå eller før vedtaket i 2009.

5.2. Omfanget av lagringsplikten

En eventuell innføring av lagringsplikt vil omfatte alle abonnenter av norske internettleverandører. Dette omfatter ifølge Post- og Teletilsynets årlige markedsundersøkelse ca 1.6 millioner bredbåndsabonnenter. [3] Det store flertall av disse er private abonnenter. Antall husholdninger i Norge er ca 2 millioner. [8] Tallene tilsier altså at over 80% av norske husholdninger har et bredbåndsabonnement. Internet World Stats oppgir at internettpenetrasjonen i Norge er 90,9%. [9] Dette er det nest høyeste tallet i Europa, etter Island. Det fremgår ikke hvordan dette tallet er beregnet, men det er rimelig å anta at det også inkluderer internettabonnement som ikke er levert over bredbånd.

Basert på overnevnte er det ingen overdrivelse å si at lagringsplikten vil omfatte det store flertall av norske borgere.

5.3. Verdi i etterforskning

Ettersom data som skal lagres om internettoppkobling ikke inneholder detaljert informasjon om hvem som har satt seg i forbindelse med hvem, er verdien til disse dataene i etterforskningssammenheng utelukkende knyttet til å avdekke hvilken abonnent som har benyttet en bestemt ip-adresse på et bestemt tidspunkt. Det er altså snakk om *sporing*, jamfør drøftelsen i punkt 3.2. Siden dataene som loggføres av kommunikasjonsleverandøren ikke avslører noe om hvilken kommunikasjon som har foregått over internettforbindelsen, er dette informasjon som må komme fra andre kilder.

Etter det som er opplyst fra Kripos, er abonnentsporing ved internettoppkobling relevant ved alle typer kriminalitet som har foregått over internett. Den typiske situasjonen i slike saker er at det foreligger informasjon om data som en bruker har sendt ut på nettet. Det kan for

eksempel være epost som er sendt ut av brukeren, bruk av en ekstern epostadresse, bruk av chattesystemer, eller innlogging på en webside eller server. Ved slik bruk, vil det bli registrert hos kommunikasjonsmotparten hvilken ip-adresse som ble benyttet, og på hvilket tidspunkt kommunikasjonen skjedde. Disse dataene kan bli fremlagt for politiet som del av en anmeldelse, eller den kan være avdekket i forbindelse med politiets etterforskning. Politiet kan så avdekke hvilken internettleverandør som innehar den aktuelle ip-adressen ved å gjøre oppslag i offentlig tilgjengelige registre. For så å finne ut hvilken abonnent det var som foretok kommunikasjonen må man rette en henvendelse til internettleverandøren som må slå opp i sin logg for å finne ut hvilken abonnent som var tilkoblet. Når politiet får utlevert abonnentens navn kan man gå videre med ytterligere søk etter bevis hos vedkommende, i form av ransaking og avhør dersom vedkommende er mistenkt i saken, eller i form av vitneavhør og andre undersøkelser dersom den identifiserte er vitne i saken.

Som nevnt er sporing av internettbruk aktuelt i alle typer saker der det forholdet som etterforskes har skjedd via internett. Ifølge det opplyste er dette spesielt aktuelt i saker om datakriminalitet og saker om seksuelle overgrep. I mange saker av denne type, har det straffbare forholdet utelukkende skjedd via internett. Den eneste måten å finne frem til gjerningspersonen er da å spore vedkommende på internett. Ved bruk av oppkobling med dynamisk ip-adresse kan dette bare gjennomføres dersom det finnes en logg over kobling mellom ip-adresse og abonnent. Når abonnenten først er identifisert, vil politiet kunne utføre ytterligere undersøkelser, for eksempel ved å undersøke datautstyr hos abonnenten. På denne måten vil det kunne avdekkes hvorvidt det var abonnenten selv som hadde utført det straffbare forholdet, noen andre i abonnentens husstand, eller eventuelt andre. (for eksempel naboer ved oppkobling til abonnentens trådløse nettverk) Slike undersøkelser fordrer imidlertid at abonnenten kan identifiseres. Dersom dette ikke er tilfelle, vil det som regel ikke finnes noen mulighet til å komme videre i etterforskningen.

Telenor har opplyst om antall henvendelser fra politiet i forbindelse med utlevering av abonnentinformasjon knyttet til ip-adresse. Tallene er opplistet i tabell 1.

År	*Telenor Internett*	*Avidi / Canal Digital*
2004	130	6
2005	213	3

2006	274	38
2007	208	28
2008	221	36
2009 (første 9 mnd.)	149	27

Tabell 1 – IP-sporing hos Telenor

Tallene for 2005-2009 vurderes å ligge på et relativt jevnt nivå. Ifølge Post- og Teletilsynet har Telenor ca 45% av bredbåndsmarkedet. [3] Dette tilsier at totalt antall ip-sporinger som utføres av norsk politi ligger på rundt 500 per år.

NextGenTel har opplyst at de i 2009 mottok 111 henvendelser fra politiet om IP-sporing. Ifølge Post- og Teletilsynet har NextGenTel ca 10% av bredbåndsmarkedet. [3] Dette tilsier at antall ip-sporinger som utføres av norsk politi ligger på rundt 1000 per år. Det er ikke funnet noen spesiell grunn til at NextGenTel skal motta flere slike henvendelser i forhold til sitt kundegrunnlag enn Telenor. I mangel av annen informasjon antas det derfor at det totale antall ip-sporinger som utføres årlig av norsk politi ligger et sted mellom ca 500 og ca 1000.

5.4. Risikofaktorer for personvern

En vurdering av risikofaktorer for personvern ved lagring av logger ved internettilgang må basere seg på hvilke konsekvenser det får for brukeren at data om internettilgang finnes lagret og kan være tilgjengelig for ansatte hos leverandøren, for politiet og eventuelt for andre gjennom urettmessig tilgang. Slike konsekvenser avhenger av hvilket innhold det er i de aktuelle loggene som eventuelt vil bli avslørt, og hva dette innholdet sier om vedkommende bruker.

Som nevnt over, inneholder loggene over internettoppkobling utelukkende ip-adresser og oppkoblingstidspunkt, koblet med brukernavn som identifiserer abonnenten som har benyttet oppkoblingen. Informasjon om brukerens bruk av systemet er derfor begrenset til når vedkommende var oppkoblet. Det kunne hevdes at dette avslører når internett blir brukt og derfor sier noe om vedkommendes bruksmønster, men dette er ikke tilfelle. Som nevnt over, er oppkobling via bredbånd den dominerende oppkoblingformen i dag. Ved en slik

oppkoblingsform er de fleste abonnenter normalt oppkoblet hele tiden, og tidspunkter for opp- og nedkobling er mer styrt av tilfeldigheter (strømbrudd og liknende) enn av når brukeren faktisk bruker nettet. Abonnentet er som regel oppkoblet også når det ikke er noen brukere tilstede, og opp- og nedkobling kan skje også da. I det hele tatt sier loggen over ip-adresser svært lite om bruksmønsteret til abonnenten.

Basert på det overnevnte er risikofaktorer for personvern ved lagring av ip-logg primært knyttet til tilfeller der informasjonen kobles mot ekstern informasjon om hvilke handlinger som er utført på internett ved bruk av et abonnement. Slik ekstern informasjon vil som regel være spredt ut over et stort antall kommunikasjonsmotparter, slik at det ikke er mulig for noen å skaffe seg oversikt over hvilke handlinger som er utført gjennom internettabonnementet. Heller ikke politiet kan gjøre dette for historisk informasjon. Den eneste bruken som da gjenstår, er nettopp den bruken som politiet gjør av opplysningene, nemlig sporing av konkret kommunikasjon for å finne ut hvilken avsender den ble sendt fra. Spørsmålet blir da hvor stor risiko dette i seg selv medfører for brukernes personvern.

Det er normalt bare kommunikasjonsmotparten som kjenner ip-adressen som kommunikasjonen er sendt fra. De eventuelle risikofaktorer for personvern ved at slike logger føres er dermed begrenset til tilfeller hvor kommunikasjonsmotparten søker å avdekke identititeten til den det kommuniseres med gjennom å få utlevert informasjon fra internettleverandøren. Det er i dag ikke mulig for andre enn politiet og påtalemyndigheten å få utlevert slik informasjon. Undertegnede er kjent med at det i skrivende stund står en sak for Høyesterett vedrørende spørsmålet om også private rettighetshavere til åndsverk kan få utlevert slik informasjon. Utfallet av denne saken er foreløpig ikke kjent, men vurderes ikke som avgjørende for i hvor stor grad brukeres personvern vil være berørt av at det lagres informasjon om kobling mellom ip-adresse og abonnentinformasjon. Det legges til grunn at utlevering uansett bare vil skje på bakgrunn av konkrete krenkelser. Det vil bare være kommunikasjonsmotparter som har tilgjengelig informasjon som kan si noe om bruken av en adresse, og denne informasjonen vil være begrenset til det den aktuelle kommunikasjonsmotparten har mottatt. Det man eventuelt vil kunne oppnå med å få utlevert abonnentinformasjon er dermed begrenset til å få identifisert hvem det var man kommuniserte med.

Behovet for en logg som kobler ip-adresser og abonnentinformasjon skyldes utelukkende løsningen med dynamiske ip-adresser. Dersom statiske ip-adresser hadde vært benyttet, hadde koblingen mellom abonnent og ip-adresse fulgt direkte av abonnentregisteret. Sånn sett medfører loggens eksistens ikke noe annet enn at bruken av abonnementet er like sporbar som den hadde vært med en statisk adresse. Løsningen med sporing via logg medfører ikke flere risikofaktorer for personvern i forhold til om det var brukt statiske ip-adresser i kommunikasjonen. Så lenge det ikke lagres en logg hos leverandøren over hvilke motparter brukeren har kommunisert med, vurderes derfor risikofaktorene for personvern ved føring av en ip-logg for å være få.

5.5. Vurdering

Det er opplyst fra politiet at sporing av ip-adresse er av stor viktighet ved oppklaring av internettkriminalitet, og i særdeleshet datakriminalitet og seksuelle overgrep. Uten å kunne følge internettsporet kan man normalt ikke oppklare slike saker. Tallene som er utlevert fra internettleverandørene viser at det skjer en del slike sporinger årlig, men signifikant færre enn antall utleveringer som gjelder telefonilogger. Mens antall utleveringer kan si noe om hvor mange slike saker som etterforskes årlig, sier det ikke så mye om hvilken betydning opplysningene har i hver enkelt sak. Etter utreders oppfatning må det vektlegges at disse opplysningene er avgjørende i de sakene det gjelder. Sammenholdt med det faktum at risikofaktorene for personvern ved slik lagring er få, ser det ut til behovet for at en slik logg lagres er tilstede.

Et separat spørsmål er hvorvidt det er behov for å innføre en *plikt* til å lagre slike data, eller om det er tilstrekkelig å *tillate* lagring av slike data. Sistnevnte kunne for eksempel skje ved en lempning i sletteplikten etter ekomloven §2-7. Et moment av betydning for en slik vurdering er om internettleverandørene vil ønske å føre en slik logg av eget tiltak. Det er ikke innhentet utfyllende informasjon om dette, men leverandørenes holdning før Datatilsynets vedtak i 2009 om tre ukers lagringstid kan gi en indikasjon. Spesielt det forhold at enkelte leverandører ikke lagrer noen slik logg i det hele tatt, hverken nå eller før 2009, tyder på at det kan være behov for en *plikt* til å lagre slike data.

6. Trafikkdata fra mobiltelefoni

6.1. Beskrivelse

Datalagringsdirektivet krever at data som blir opprettet ved mobiltelefoni blir lagret. Data som skal lagres er: [2]

- A-nummer (oppringers telefonnummer)
- B-nummer (nummer til den som blir oppringt)
- C-nummer (nummer en samtale blir viderekoblet til)
- IMSI-nummer som identifiserer abonnent for A- B- og C-nummer
- IMEI-nummer som identifiserer håndsettet som ble brukt for A-, B- og C-nummer
- Identitet og registrerte brukerdata for innehaver av A-, B- og C-nummer
- Dato og tidspunkt for start og avslutning av kommunikasjon
- Informasjon om hvilken tjeneste som er benyttet
- Lokaliseringsinformasjon ved start og avslutning av kommunikasjon

Det følger av dette at det som kreves lagret er en fullstendig logg over hvem som ringte til hvem, og hvem som sendte SMS til hvem, inkludert dato og tidspunkt, abonnentsinformasjon og lokaliseringsinformasjon. Slike data kalles "Call Detail Records". (CDR) Det kreves også lagret informasjon om hvilket håndsett som ble benyttet. Denne informasjonen er av interesse, fordi abonnementet i moderne mobilsystemer ikke er direkte knyttet mot håndsettet som benyttes. Istedet er abonnementet knyttet til SIM-kortet, som er et smartkort som inneholder opplysninger som er nødvendig for å kommunisere, blant annet IMSI-nummeret som er brukerens identitet i mobilsystemet. SIM-kortet kan flyttes fra håndsett til håndsett. Håndsettet identifiseres med IMEI-nummeret. Gjennom om kreve lagret både IMSI og IMEI, oppstår en dokumentasjon for hvilke SIM-kort som har benyttet i hvilket håndsett. Denne dokumentasjonen kan være av interesse i etterforskningssammenheng.

Når det gjelder telefonsamtaler og SMS følger det direkte av kravene hva som skal lagres. Pakkeorientert datatrafikk er imidlertid ikke omtalt. Man må imidlertid se dette i sammenheng med hva som kreves lagret i forbindelse med internettaksess. Ettersom det for internettaksess ikke kreves at man logger hvilke ip-adresser data sendes til eller mottas fra kan dette heller ikke være noe krav ved pakkeorientert datatrafikk fra mobiltelefon. Det antas imidlertid at

lagringsplikten innebærer at det lagres når den pakkeorienterte forbindelsen ble opprettet, og hvor lenge den varte.

Lokaliseringsinformasjon er i direktivet artikkel 5 presisert til celleid. [1] Dette er en unik id som identifiserer hvilken basestasjon som benyttes ved kommunikasjonen. Presisjonsnivået for lokaliseringsinformasjon avhenger dermed av hvor stort område som dekkes av hver enkelt basestasjon. I dagens mobilsystemer kan dette variere fra flere titalls kilometer ned til enkeltgater i urbane strøk, og i særlige tilfelle enkeltbygninger. [10] Direktivet krever også at det tas vare på geografisk informasjon knyttet til hver enkelt celle, slik at historisk informasjon om geografisk lokalisering av bestemte celleider er tilgjengelig selv om det skulle bli gjort endringer i nettet som innebærer at celleider endrer plassering.

Når det gjelder lokaliseringsinformajon krever høringsnotatet at det lagres lokaliseringsinformasjon både ved start *og avslutning* av kommunikasjonen, mens direktivet i artikkel 5 bare krever at lokaliseringsinformasjonen lagres ved kommunikasjonens start. Dette ser ut til å innebære en utvidelse av hva som kreves lagret i høringsnotatet i forhold til direktivet, men utvidelsen er ikke nærmere begrunnet i høringsnotatet. Det er derfor vanskelig å vite hva som er begrunnelsen for utvidelsen, og om den i det hele tatt er tilsiktet. Det synes imidlertid klart at det ikke kreves at det skal lagres lokaliseringsinformasjon for alle basestasjoner som benyttes underveis i kommunikasjonen. Ved telefonoppringninger, er det celleid på basestasjon som ble benyttet når samtalen ble koblet opp og eventuelt når den ble koblet ned som skal lagres. Celleid på eventuelle basestasjoner som samtalen går over underveis i samtalen er det ikke noe krav om å lagre. SMS-meldinger blir alltid sendt over kun en basestasjon, så celleid for denne basestasjonen skal lagres. Det er imidlertid vanskeligere å tolke ut fra direktivet og høringsnotatet hvorvidt det oppstår noen plikt til å lagre lokaliseringsinformasjon ved pakkeorientert dataoppkobling. Siden betaling for slik oppkobling skjer per mengde data sendt og motattt, er de fleste mobilterminaler oppkoblet i lengre perioder av gangen. De sender og mottar data fra nettverket når det behøves, for eksempel for å sjekke om det er kommet noen ny epost til epostserveren. Mange moderne mobiltelefoner (slik som feks iPhone), beholder dataoppkobling til nettverket til enhver tid og benytter denne til å sjekke epost osv med få minutters mellomrom. Dersom systemet skulle lagre lokaliseringsinformasjon for enhver dataoverføring, ville det for slike telefoner bli lagret en fullstendig logg over hvor brukeren har vært lokalisert til enhver tid. Det er etter

undertegnedes oppfatning vanskelig å tolke direktivet slik at dette kreves. Kravene som er angitt i artikkel 5 kan neppe innebære noe annet enn at lokasjonen må lagres når dataoppkoblingen opprettes, men ikke hele tiden mens den er oppkoblet.

Det har ikke tidligere vært noen lagringsplikt for logger fra mobiltelefoni. Leverandørene lagrer likevel i stor utstrekning de data som direktivet krever lagret i dag. Data benyttes til faktureringsformål, og kan derfor tas vare på i en lengre periode enn rene tekniske hensyn tilsier. Det kan hevdes at leverandørene i så fall kun skal ta vare på data som behøves til faktureringsformålet, det vil si hva som ringte til hvem, type og varighet. Det er imidlertid en kjensgjerning at de fleste leverandører også lagrer data som det egentlig ikke er behov for å lagre for dette formålet, slik som IMEI og lokasjonsdata. En mulig forklaring på dette er at all denne informasjonen i utgangspunktet blir lagret av svitsjene i telesystemet. I tilfelle man ønsker å ikke lagre for eksempel lokasjonsinformasjon, må man i så fall fjerne denne informasjonen eksplisitt ved å vaske dataene som blir produsert av telesystemet som skal lagres for fakturering. I tillegg til å være ekstraarbeid, vil en slik datavask introdusere en feilkilde. Det er derfor normalt ikke ønskelig for leverandøren å utføre slik datavask.

6.2. Omfanget av lagringsplikten

Lagringsplikten omfatter alle norske mobilabonnement. Det var i 2009 over 5.2 millioner mobilabonnement i Norge, inklusive kontantkort. [3] Basert på dette er det neppe noen overdrivelse å si at det i dag kun er en liten andel nordmenn som ikke har mobiltelefon. Dette gjelder særlig blant voksne og ungdommer. Lagringsplikten vil dermed omfatte all kommunikasjon som alle disse brukerne foretar med sine mobiltelefoner.

6.3. Verdi i etterforskning

Ved sporing av telefonioppkoblinger er det normalt tilstrekkelig å finne innehaveren av et bestemt telefonnummer. Dette kan normalt gjøres ved å hente ut abonnentinformasjon direkte fra teleoperatøren. Verdien av trafikkdata fra mobiltelefoni i etterforskningssammenheng ligger derfor normalt ikke i sporing, men i *annen bevisuthenting*, jf drøftelsen under punkt 3.2.

Det kan oppstilles et skille mellom tilfeller der de aktuelle dataene er interessante fordi de gir bevis for hvem som har vært i kontakt med hvem (kommunikasjonsdata) og tilfeller der de gir bevis for en persons lokasjon (lokasjonsdata), jf drøftelsen under punkt 3.1. Kripos opplyser at førstnevnte primært er interessant i saker der det er flere personer har vært involvert. Eksempelvis er slike kommunikasjonsdata av primær interesse i saker med kriminelle nettverk. Det kan for eksempel være snakk om et nettverk som organiserer narkotikaomsetning, ran, spritsmugling, menneskehandel eller gjengkriminalitet. Ved etterforskning av slike saker er situasjonen ofte den at en eller flere spesifikke personer mistenkes for konkrete straffbare handlinger, men at man ikke vet hvem andre som står bak de aktuelle straffbare handlinger, eller om de samme og andre personer utfører lignende straffbare handlinger jevnlig. I slike tilfeller er det ønskelig å rulle opp hele nettverket for å forhindre at ytterligere straffbare handlinger gjennomføres. Trafikkdata fra mobilkommunikasjon benyttes ofte til dette. Ved å hente ut trafikkdata, kan politiet identifisere hvem som har kommunisert med de personer som mistenkes for konkrete straffbare handlinger. Ved å undersøke kommunikasjonsmønsteret nærmere kan man identifisere andre telefonnummer som kan være involvert i forbindelse med de straffbare handlingene, og kommunikasjonsdata kan hentes ut også for disse. På denne måten kan politiet etterhvert skaffe seg oversikt over det kriminelle nettverket og samle bevis for de straffbare handlingene som pågår. Til en viss grad er det slik at uthenting av lagrede kommunikasjonsdata i slike saker kombineres med kommunikasjonskontroll. Kommunikasjonsdata kan da benyttes til å finne ut hvilke telefoner som bør avlyttes, og for å dokumentere at brukeren av aktuelle telefon er tilstrekkelig involvert i straffbare handlinger til å begrunne kommunikasjonskontroll. Kommunikasjonsinnholdet som blir fanget opp ved kommunikasjonskontroll kan være med å ytterligere belyse hvem som er involvert i det kriminelle nettverket, og hvilken rolle de har.

Det kriminelle miljøet er i stor grad kjent med at det foretas kommunikasjonskontroll og uthenting av kommunikasjonsdata i forbindelse med politiets etterforskning. Dette har resultert i mottiltak mot slik bevisuthenting fra de kriminelles side. Slike mottiltak kan involvere bruk av kontantkort som er registrert på falske navn, jevnlig bytte av kontantkort og telefoner, samt at man jevnlig kvitter seg med telefoner og kontantkort for å forhindre at disse blir avdekket ved beslag. Disse mottiltakene er imidlertid ressurskrevende å gjennomføre, og lider av den svakhet at det nye nummeret må kommuniseres til alle

kommunikasjonspartene hver gang man bytter nummer. Erfaring viser at det ofte er mulig å benytte kommunikasjonsdata som bevis på aktivitet i kriminelle nettverk selv om brukerne har foretatt nevnte mottiltak.

Når det gjelder bruk av lokasjonsdata, så er det opplyst at dette i prinsippet kan være interessant i enhver sak som berører en bestemt lokasjon. Uthenting av lokasjonsdata benyttes imidlertid av ressursmessige og proporsjonalitetsmessige årsaker primært i de mest alvorlige sakene. Således er det saker om grov vold, drap og ran som er de mest aktuelle. I disse sakene blir data om mobiltelefoni hentet ut jevnlig, og tjener da som bevis på lokasjonen vedkommende som benyttet telefonen befant seg på. Slik uthenting kan gjøres på bestemte telefonnummer, for eksempel fordi et bestemt telefonnummer er benyttet av en mistenkt. Det er også mulig å hente ut telefondata som er knyttet til en bestemt lokasjon. For eksempel er det mulig å hente ut en liste over alle samtaler som er knyttet til en bestemt basestasjon. Dette innebærer at politiet får en liste over alle telefoner som utførte eller mottak anrop eller sms via den aktuelle basestasjonen. Dette er en aktuell fremgangsmåte i alvorlige saker med ukjent gjerningsperson, for eksempel drap. Listen over mobiltelefonnummer som fremkommer på denne måten er med å dokumentere hvem som befant seg på lokasjonen på dette tidspunktet og er dermed et mulig utgangspunkt i et søk etter mulige gjerningspersoner. I praksis er det imidlertid så mye arbeid forbundet med en slik fremgangsmåte at den bare brukes i de mest alvorlige sakene.

Telenor har utlevert statistikk over antall henvdendelser om utlevering de har mottatt fra politiet angående trafikkdata fra mobil. Tallene er oppsummert i tabell 2, og omfatter antall fakturerte enheter. Det er verdt å merke seg at dette tallet kan være betydelig høyere enn antall saker.

År	Nummersøk	Basestasjonssøk	Identitet/IMEI
2004	2441	1312	3725
2005	2397	2040	1402
2006	2624	1924	2085
2007	2196	2534	2438
2008	3321	2561	2181
2009 (9 mnd)	2571	2067	1921

Tabell 2 – Utlevering av mobildata fra Telenor

NetCom har utlevert statistikk over antall henvendelser om utlevering de har mottatt fra politiet. Tallene er oppsummert i tabell 3. Tallene omfatter kun henvendelser om utlevering knyttet til mobiltelefoni, og omfatter både nummersøk og basestasjonssøk. Dataene for NetCom gjelder antall henvendelser, og det er opplyst av hver henvendelse ofte gjelder flere basestasjoner/telefonnummer. Tallene samsvarer ikke nødvendigvis med antall saker / sakskomplekser, da det ofte gjøres flere henvendelser i samme sak.

År	*Henvendelser*
2005	1288
2006	1501
2007	1513
2008	1693
2009	1730

Tabell 3 – Utlevering av mobildata fra NetCom GSM

Tallene fra Telenor og NetCom er ikke direkte sammenlignbare. For å kunne avdekke hvordan de eventuelt kunne sammenlignes måtte det vært gjort ytterligere undersøkelser av hvordan registreringen foregår i de to virksomhetene. Det ansees ikke formålstjenlig å gjennomføre en slik undersøkelse. Tallene gir uansett et bilde av i hvilket omfang det foregår utlevering til politiet av slike data. Det er opplyst fra politiet at man primært spør henholdsvis Telenor og NetCom om slike data, da disse også besitter data for virtuelle operatører som er tilknyttet deres nett.

Overnevnte tall viser at uthenting av trafikkdata fra mobiltelefoni benyttes i et visst omfang. Tallene er større enn tilsvarende tall for sporing av IP-adresser. Dette har trolig sammenheng med at de sakene hvor slike data brukes gjennomgående er alvorlige saker, med et høyt etterforskningstrykk. I slike saker hentes gjerne ut data om mange ulike telefoner eller basestasjoner i hver sak.

Ut fra det som er opplyst er vanskelig å få inntrykk av i hvor stor grad trafikkdata for mobiltelefoni faktisk bidrar til å oppklare saken. Trafikkdata fra mobil som regel en ekstra beviskilde i tillegg til andre beviskilder som er tilgjengelig. Dette er forskjellig fra IP-sporing, hvor sporingen som regel er avgjørende for å finne gjerningspersonen. Bevisene fra trafikkdataene som er hentet ut presenteres i retten sammen med andre bevis som er avdekket gjennom etterforskningen. Ettersom retten som regel fatter en beslutning ut fra et helhetsbilde av alle bevis som er tilgjengelig kan det derfor være vanskelig å avgjøre hvilken betydning trafikkdata fra mobil har hatt for avgjørelsen. For å få nærmere informasjon om dette måtte man eventuelt gå nærmere inn på avgjørelser hvor trafikkdata for mobiltelefoni hevdes å ha hatt sentral betydning. Dette er ikke gjort i forbindelse med den foreliggende utredning.

6.4. Risikofaktorer for personvern

En vurdering av risikofaktorer for personvern ved lagring av mobiltelefonlogger må basere seg på hvilke konsekvenser det får for brukeren at data om mobilkommunikasjon finnes lagret og kan være tilgjengelig for ansatte hos leverandøren, for politiet og eventuelt for andre gjennom urettmessig tilgang. Slike konsekvenser avhenger av hvilket innhold det er i de aktuelle loggene som eventuelt vil bli avslørt, og hva dette innholdet sier om vedkommende bruker.

Også i en vurdering av innholdet i loggene kan det være formålstjenlig å skille mellom kommunikasjonsdata og lokasjonsdata. Innholdet i kommunikasjonsdata er hvem som har hatt kontakt med hvem, på hvilken måte (telefon eller sms) og varighet av eventuelle telefonsamtaler. I tillegg lagres knytning mellom abonnement og telefon, slik at det kan utledes hvilken telefonmodell som benyttes, og når eventuelle skifter av telefon er gjennomført. Den som har disse dataene tilgjengelig kan altså skaffe seg oversikt over hvem som har hatt kontakt med hvem. Spesifikt er det mulig å foreta søk på bestemte nummer for å avdekke hvem en spesifikk person har hatt kontakt med i et bestemt tidsrom. Dette kan si mye om vedkommendes handlemønster. Spesielt om dataene analyseres over tid, vil det være mulig å trekke slutninger om personen som bruker telefonnummeret som analyseres. Sett over tid vil det være mulig å utlede hvilken personkrets vedkommende omgås, og andre som vedkommende har behov for å ha kontakt med i løpet av en dag. Ut fra dette kan det neppe

være noen tvil om at tilgjengelighet av kommunikasjonsdata fra mobiltelefoni utgjør en risikofaktor for personvern.

Når det gjelder lokasjonsdata, så medfører disse at lokasjonen vedkommende bruker befant seg på lagres på de tidspunkter vedkommende sender eller mottar et anrop eller en sms. Tidspunktene for lagring av lokasjon er utenfor brukerens kontroll, ettersom lokasjon vil bli lagret også ved mottak av samtale og sms. Som nevnt vil nøyaktigheten på lokasjonen variere etter størrelsen på basestasjonens dekningsområde. Dette er også utenfor brukerens kontroll, ettersom valg av basestasjon avhenger av hvordan nettverket er satt sammen og andre kriterier som last, værforhold og så videre. Det er likevel klart at den som har oversikt over hvilke basestasjoner som er brukt til sending og mottak for et bestemt personnummer, har forholdsvis god oversikt over hvor vedkommende som bruker den aktuelle telefonen befinner seg. Denne informasjonen er klart personvernsensitiv.

Basert på det overnevnte, jamført med drøftelsen under punkt 4 kan det neppe være noen tvil om at lagring av trafikkdata for mobiltelefoni medfører en risikofaktor for personvern.

6.5. Vurdering

Det er i det overnevnte beskrevet hvordan trafikkdata fra mobiltelefoni hentes inn i straffesaker. Det er beskrevet hvilken nytte slik informasjon kan ha, men det er ikke foretatt en inngående analyse om hvordan slike bevis vurderes opp mot andre bevis som vanligvis foreligger i saker hvor trafikkdata er presentert for retten. Det er derfor vanskelig å konkludere sikkert med hvor avgjørende slike data faktisk er i etterforskningssammenheng.

Det er utvilsomt at et pålegg om lagring av slike data medfører en risikofaktor for personvern. Denne kan i stor grad sies å være proporsjonal med hvor mange av dataene (lokasjon mv) som lagres og med lagringstiden. Risikoen kan også sies å være proporsjonal med hvor mange dataene er tilgjengelige for. Som nevnt under punkt 4.5 er det mulig å redusere sistnevnte ved hjelp av tekniske midler.

7. Trafikkdata fra fasttelefoni og ip-telefoni

7.1. Beskrivelse

Data som skal lagres ved fasttelefoni er i stor grad de samme som for mobiltelefoni, med unntak av celleid, som ikke er relevant for fasttelefoni. Lokasjon for anropet vil likevel fremkomme ut fra abonnentopplysningene, ettersom oppkoblingen ved fasttelefoni skjer til en fast adresse.

Ved ip-telefoni skal følgende lagres: [2]

- ip-adresser som identifiserer oppringer og den som blir oppringt
- tildelt brukeridentitet
- navn og adresser til abonnent, registert brukers ip-adresse eller telefonnummer
- brukeridentitet eller telefonnummer som tildeles mottaker
- informasjon som identifiserer kommunikasjonsutstyr

Dette innebærer at sender og mottaker for hvert enkelt anrop skal registreres, slik at det opprettes en logg over alle anropene på tilsvarende måte som for vanlig telefoni. Det spesielle ved ip-telefoni ligger i hva som skal registreres som identifiserer sender og mottaker. Kravene må tolkes slik at både brukeridentitet, ip-adresse, telefonnummer og adresser til kommunikasjonsutstyr skal lagres for både sender og mottaker, i den utstrekning disse er kjent for ip-telefonileverandøren. Videre skal det lagres navn og adresser tilhørende registrerte brukeridentiteter.

Formålet med å kreve lagring av ip-adresser må være å kunne spore avsender tilbake til kommuniserende oppkobling også i tilfeller der det ikke er tildelt noe bestemt telefonnummer eller brukeridentitet, samt å kunne avdekke lokasjonen anropet er gjort til eller fra. De fleste leverandørene av ip-telefoni på det norske markedet tilbyr imidlertid tjenesten slik at abonnenten får et vanlig telefonnummer, og at oppringninger skjer ved hjelp av bestemt terminalutstyr. Når ip-telefontjenesten er levert på denne måten, vil identifikasjon av brukeren følge av brukeridentiteten som også logges. Det antas derfor at bruken av ip-adresser fra ip-telefonilogger i praksis vil være begrenset til å avdekke hvilken lokasjon oppkoblingen ble gjort fra. Dette må da gjøres ved hjelp av sporing av ip-adressen som fremkommer av ip-telefoniloggen.

7.2. Omfanget av lagringsplikten

I 2009 er det i Norge ca 1.8 millioner abonnenter av fasttelefoni og ca 500 000 abonnenter av bredbåndstelefoni. En tilsvarende betraktning som for bredbåndsabonnement gjør seg gjeldende her, slik at man kan konkludere at lagringsplikten som innføres for fasttelefoni og bredbåndstelefoni gjelder det alt vesentlige av den norske befolkning.

7.3. Verdi i etterforskning

Verdi i etterforskningsammenheng av trafikkdata fra fasttelefoni og ip-telefoni vil i det alt vesentlige tilsvare verdien av trafikkdata fra mobiltelefoni, forsåvidt gjelder *kommunikasjonsdata*. Således vil data om hvem som ringer til hvem på fast- og ip-telefon kunne brukes i opprullingen av kriminelle nettverk på samme måte som tilsvarende data fra mobiltelefoninettverk. *Lokasjonsdata* fra fasttelefoni vil derimot ha langt mindre interesse enn for trafikkdata fra mobiltelefoni. Denne typen abonnement er levert til en fast lokasjon, og brukes gjerne av flere enn abonnenten. Foretatte anrop sier derfor ikke så mye om lokasjonen til abonnenten. Det samme vil i det alt vesentlige gjelde ip-telefoni. Man kan imidlertid se for seg noen unntak som ikke er så fremtredende i dag, men som kan bli viktigere i fremtiden:

- Abonnenten har tatt med seg terminalutstyret til en annen adresse, for eksempel utenlands, og bruker det derfra.
- Terminalutstyret består i et dataprogram som kjører på abonnentens mobiltelefon.

Telenor har utlevert statistikk over antall henvdendelser om utlevering de har mottatt fra politiet angående trafikkdata fra fastnettet. Tallene er oppsummert i tabell 4, og omfatter antall fakturerte enheter. Tallene viser en bemerkelsesverdig nedgang i antall utleveringer i perioden 2004 til 2009. Nedgangen er trolig et uttrykk for en nedadgående relevans av denne tjenesten. Dette kan skyldes at brukerne i større grad benytter mobiltelefoni og ip-telefoni istedenfor fasttelefoni. En annen mulig årsak er en redusert etterspørsel fra politiet fordi data fra mobiltelefon kan gi den samme informasjonen og også inneholder lokasjon.

År	Nummersøk	Identitet

2004	1514	199
2005	746	67
2006	537	77
2007	484	44
2008	408	18
2009 (9 mnd)	232	11

Tabell 4 – Utlevering av trafikkdata for fastnett fra Telenor

7.4. Risikofaktorer for personvern

En vurdering av risikofaktorer for personvern ved fasttelefoni og ip-telefoni vil i det alt vesentlige tilsvare vurderingen for mobiltelefoni forsåvidt gjelder *kommunikasjonsdata*, men ikke lokasjonsdata. Risikofaktorene er altså færre for fast- og ip-telefoni enn for mobiltelefoni, men muligheten for å finne ut hvem som har kontakt med hvem utgjør fortsatt en risikofaktor for personvernet ved slik lagring.

7.5. Vurdering

Som for mobiltelefoni er det ikke foretatt en analyse av hvilken nytte trafikkdata fra fast- og ip-telefoni har som bevis i konkrete straffesaker, og hvordan slike bevis vurderes opp mot andre bevis som foreligger i saker der trafikkdata er presentert for retten. Det er derfor vanskelig å konkludere sikkert med hvor avgjørende slike data faktisk er i etterforskningssammenheng.

Det er utvilsomt at et pålegg om lagring av slike data medfører en risikofaktor for personvernet. Risikofaktoren kan i stor grad sies å være proporsjonal med lagringstiden. Risikoen kan også sies å være proporsjonal med hvor mange dataene er tilgjengelige for. Som nevnt under punkt 4.5 er det mulig å redusere sistnevnte ved hjelp av tekniske midler.

8. Trafikkdata fra epost

8.1. Beskrivelse

Data som skal lagres ved formidling av epost omfatter følgende: [2]

- avsender og mottakers epostadresser og ip-adresser
- abonnentinformasjon og registrert brukerinformasjon
- dato og tidspunkt for pålogging og avlogging til eposttjenesten

Trafikkdata ved formidling av epost opprettes på flere ulike trinn i epost-systemet. Hvilke data som eksisterer på hvert trinn er forskjellig. Således er i prinsippet følgende servere involvert i formidling av epost:

1. Server som mottar epost fra sluttbruker for videreformidling. (*smtp-server*) Her er avsender og mottakers epostadresse tilgjengelig, samt sluttbrukers ip-adresse og dato/tidspunkt for sending av epost. Hvis serveren krever autentisering er også brukerinformasjon tilgjengelig.
2. Server som mottar epost fra andre epostservere for videreformidling. (*smtp-server*) Her er normalt bare avsender og mottakers epostadresse, samt dato og tidspunkt tilgjengelig.
3. Server som samler opp epost på vegne av en sluttbruker og gjør den tilgjenglig med protokoller for nedlasting av epost (*pop/imap*) eller gjennom en web-basert epostklient. Her er avsenders og mottakers epostadresse tilgjengelig, samt dato og tidspunkt når eposten ble sendt. I tillegg vil selve innholdet i eposten være tilgjenglig inntil den eventuelt slettes av brukeren. Denne serveren kan også loggføre dato og tidspunkt for påloggінger til eposttjenesten og hvilke ip-adresser som er benyttet til dette.

Det er verdt å merke seg at mye av den overnevnte informasjon også legges inn i selve eposten av serverene som formidler epost. Dette gjelder avsenders og mottakers epostadresse, dato og tidspunkt for sending og avsenders ip-adresse. Denne informasjonen er således tilgjengelig for mottaker, og kan beslaglegges eller overleveres frivillig til politiet. Følger man en slik fremgangmåte, vil politiet også få tak i innholdet i selve eposten, noe som ikke er tilgjengelig ut fra loggene som føres på overnevnte epostservere.

Et annet forhold av betydning for lagring av trafikkdata om epost er hvem som omfattes av det foreslåtte regelverket. I henhold til forslaget er det kun *tilbyder av offentlig kommunikasjonstjeneste* som omfattes. [2] Hvem som omfattes vil da bero på en tolkning av hvem som er en slik tilbyder. Det legges opp til at vedtak om hvem som faller inn under tilbyderbegrepet skal gjøres av ekommyndigheten. (Post- og Teletilsynet) I tillegg foreslås det en hjemmel for å pålegge andre enn dem som faller inn under tilbyderbegrepet å lagre trafikkdata. Slike vedtak vil også kunne utføres av Post- og Teletilsynet.

Siden avgjørelsen om hvem som omfattes i stor grad overlates til ekommyndigheten, er det på det nåværende tidspunkt vanskelig å si hvilke leverandører av overnevnte tjenester som vil falle inn under det foreslåtte regelverket. Når leverandør av eposttjenester også tilbyr internettilgang er dette ikke tvilsomt. Dette vil være tilfelle for eposttjenester som leveres sammen med internettabonnement. De fleste norske internettleverandører leverer en slik tjeneste, og har i den sammenheng servere som tar imot utgående epost for videresending (punkt 1 over), samt servere som tar imot epost på vegne av brukeren (punkt 3 over). Mange brukere benytter imidlertid eposttjenester som leveres av andre. De største leverandørene av slike tjenester, Yahoo Mail, Google GMail og Microsoft Hotmail, er lokalisert utenfor Europa og omfattes dermed ikke av regelverket. Men det finnes også norske leverandører som tilbyr slike tjenester. I tillegg finnes det leverandører av eposttjenester som utelukkende benyttes til formidling av epost mellom andre leverandører. Hvorvidt disse omfattes synes å være usikkert.

8.2. Omfanget av lagringsplikten

Lagringsplikten omfatter enhver sending og mottak av epost gjennom norske leverandører. Statistisk sentralbyrå oppgir i 2009 at 81% av nordmenn i alderen 16 – 79 brukte internett til å sende og motta epost i en tremånedersperiode. [11] Det antas at antallet brukere av epost i stor grad er sammenfallende med antall brukere av internett, jamfør drøftelsen under punkt 5.2.

8.3. Verdi i etterforskning

Når det gjelder verdi i etterforskning er det formålstjenlig å skille mellom to typer trafikkdata:

1. Logg som viser hvem som har sendt epost til hvem og når.
2. Logg som viser når bruker har logget inn for å lese epost og fra hvilken ip-adresse

Førstnevnte er tilgjengelig både på avsenderserver, mellomliggende servere og mottakende servere. Sistnevnte er utelukkende tilgjengelig på mottakende epostserver.

Når det gjelder logg som viser hvem som har sendt epost til hvem og når, så det opplyst fra politiet at denne type logg ikke etterspørres i særlig grad. Årsaken er primært at det ikke er behov for å hente ut en slik logg i etterforskningssammenheng, fordi den samme informasjonen er tilgjengelig på annet vis. I tilfeller hvor man ønsker å spore en epost tilbake til kilden kan man ganske enkelt gå gjennom epostmeldingens meldingshoder og finne ip-adressen meldingen er sendt fra. Det er ikke nødvendig med noen utlevering av trafikkdata for å gjennomføre dette. Når ip-adressen er funnet, kan opprinnelsen av epostmeldingen spores ved hjelp av ip-sporing, jamfør drøftelsen under punkt 5. Dersom situasjonen er den at man ønsker å kartlegge epostaktiviteten til en mistenkt, vil politiet som regel gå frem på en annen måte enn å hente ut en logg over epostaktiviteten. I slike tilfeller begjærer man heller en ransakingsbeslutning, slik at datamaskinen som er benyttet kan beslaglegges. Her vil man finne en fullstendig oversikt over inn- og utgående epost, som regel for et lengre tidsrom enn det som finnes lagret hos leverandøren. Ved denne fremgangsmåten får man også tilgang til innholdet i eposten. Det kan være at epost er slettet på datamaskinen som er benyttet, men erfaring viser at slik slettet epost ofte kan rekonstrueres når innholdet på den beslaglagte maskinen analyseres. Den teknologiske utvikling ser ut til å gå i en retning hvor mer og mer data er lagret i nettverket og ikke på brukerens personlige datamaskin. En slik utvikling må nødvendigvis medføre at politiet må beslaglegge epost hos kommunikasjonsleverandøren og ikke på brukerens personlige datamaskin. Det vil imidlertid ikke medføre noe økt behov for pliktig datalagring. Ved sentral lagring må dataene nødvendigvis uansett være lagret på en server et sted, og det er derfor ikke et behov for en plikt til slik lagring.

Når det gjelder logg som viser hvem som har logget seg inn på en epostkonto for å lese epost og fra hvilken epostadresse, så er det opplyst fra politiet at denne typen trafikkdata etterspørres i noen grad. Formålet med å hente inn slike data er som regel å identifisere hvem som benytter den spesifikke epostkontoen. Slik innhenting er derfor spesielt aktuelt i

forbindelse med epostleverandører som ikke foretar noen kontroll med identiteten til kunden ved registrering av aktuelle epostkonto, slik at kunden kan skrive inn falske opplysninger om navn og adresse. Dette synes i særlig grad å være tilfelle for eposttjenester som tilbys på internett uten å ha noen tilknytning til andre abonnement. Det synes i mindre grad å være tilfelle for norske internettleverandører. For disse er navn og adresse til innehaver av epostabonnement som regel kjent, fordi eposttjenesten leveres i tilknytning til et bredbåndsabonnement som leveres til en fast adresse. Således er det opplyst fra politiet at man i særlig grad etterspør slike opplysninger fra utenlandske leverandører slik som Hotmail og GMail. Når disse trafikkdataene utleveres, kan politiet identifisere hvem som bruker den aktuelle epostkontoen ved hjelp av ip-sporing, jamfør drøftelsen under punkt 5. Ifølge det opplyste fra politiet er slik identifisering særlig aktuelt ved etterforskning av seksuelle overgrep og datakriminalitet.

Telenor opplyser at det kun har vært et fåtall henvendelser fra politiet om utlevering av trafikkdata for epost siden politisvarsenteret ble opprettet på begynnelsen av 2000-tallet. NetCom GSM og NextGenTel opplyser at de ikke kjenner til at det har vært forespørsler om utlevering av slike data i det hele tatt.

8.4. Risikofaktorer for personvern

Spørsmålet ved en vurdering av risikofaktorer for personvern for trafikkdata fra epost er hva dataene sier om brukeren, samt hvor mange dataene er tilgjengelig for. Det som kreves lagret er en logg over hvem som har sendt epost til hvem, samt dato og tidspunkt for hver enkelt epost. Den som har tilgang til en slik logg kan finne ut hvem som kommuniserer med hvem, og kan skaffe seg en oversikt over kommunikasjonsmønster. Dette medfører klart en risikofaktor for personvern. Informasjonen som kan trekkes ut av disse dataene tilsvarer informasjonen som kan trekkes ut av kommunikasjonsinformasjonen i trafikkdata fra mobiltelefon, jamfør drøftelsen under punkt 6.4. Hvem disse dataene er tilgjengelig for er imidlertid forskjellig. Mens trafikkdata fra mobiltelefon i utgangspunktet kun er tilgjengelig for ansatte hos leverandøren av mobiltelefoni, er trafikkdata fra epost tilgjengelig for ansatte både hos den primære epostleverandøren, samt operatører hos eventuelle sekundære epostservere som de aktuelle epostene blir rutet innom. Dette medfører en større risikofaktor for personvern.

Når det gjelder logg over når det ble foretatt innlogging på epostserver og fra hvilken ip-adresse, så stiller det seg anderledes. Denne loggen avslører ikke informasjon om hvem som har kommunisert med hvem, eller annet som kan sier noe direkte om brukerens kommunikasjonsmønster. Det loggen eventuelt kunne avsløre er når brukeren leser epost, men heller ikke dette trenger å være tilfelle, da mange epostapplikasjoner sjekker epost med jevne mellomrom, slik at antallet innlogginger ikke nødvendigvis er sammenfallende med at brukeren leser epost, eller i det hele tatt er til stede ved terminalen. Loggen er imidlertid egnet til å trekke ut informasjon om brukerens lokasjon, dersom informasjonen benyttes til ip-sporing. Denne muligheten må imidlertid sammenholdes med hvem som kan foreta slik ip-sporing. En må derfor kunne si at det foreligger en viss risikofaktor for personvern ved lagring av slik logg, men den er begrenset i omfang.

8.5. Vurdering

Når det gjelder logg over hvem som har sendt epost til hvem, synes det klart at dette er en type data som politiet har liten bruk for, og som utgjør en risikofaktor for personvern å lagre. For denne typen data er det derfor klart at risikofaktorene for personvern overstiger nytte i etterforskning.

Når det gjelder logg over hvem som har logget inn på epostkonto, så foreligger det kun begrensede risikofaktorer for personvern ved lagring av slike data, mens dataene også til en viss grad kommer til nytte i etterforskningsammenheng. Det synes som om nytten i etterforskningsammenheng i stor grad er knyttet til utlevering fra utenlandske leverandører som ikke er omfattet av datalagringsdirektivet. Det foreligger ikke informasjon som tyder på at slike data fra norske leverandører har vært nyttig, men det kan ikke utelukkes at dette i større grad vil skje i fremtiden dersom norske leverandører av eposttjenester får en større markedsandel.

Skillet mellom de to typene trafikkdata for epost korresponderer med data som er nødvendig for *sporing* og *annen bevisuthenting* som drøftet i avsnitt 3.2.

9. Oppsummering

En vurdering av nytte i etterforskning sett i forhold til personvernkonsekvenser ved en innføring av plikt til datalagring i norsk rett vil slå ulikt ut for de forskjellige datatypene som kreves lagret. Basert på resultatet av vurderingen, kan en gruppere dataene i tre grupper A-C. Beskrivelse av disse tre gruppene er gjort i det følgende:

Datatypegruppe A:
Logg over internettilgang, jf punkt 5.5, samt logg over tilgang til epostkasse jf punkt 8.5.

Disse data vurderes som viktig i etterforskningssammenheng, da mange saker ikke kan løses dersom slike data slettes. Risikofaktorer for personvern ved lagring av slike data vurderes som begrenset, da de kun i svært liten grad avslører brukerens egen aktivitet. En avveining mellom hensynene tilsier dermed at slike data lagres.

Datatypegruppe B:
Trafikkdata fra mobiltelefoni, fastnett og ip-telefoni jf punkt 6.5 og 7.5.

Disse data vurderes som nyttig i etterforskningssammenheng, men det foreligger ikke klar informasjon om i hvilket omfang disse data er avgjørende for å oppklare saker. Bevisene fra slike data som regel inngår i en større bevismengde, og det kan være vanskelig å skille ut hvor stor vekt som er lagt på trafikkdatabevisene. Risikofaktorer for personvern knyttet til lagring av slike data vurderes som betydelig. En avveining av hensynene bør gjøres når det foreligger informasjon om i hvilket omfang disse datatypene er avgjørende for å oppklare saker.

Datatypegruppe C:
Logg over hvem som har sendt epost til hvem, jf punkt 8.5.

Disse data vurderes som lite nyttig i etterforskningssammenheng. Risikofaktorer for personvern knyttet til lagring av slike data vurderes som betydelig. En avveining av hensynene tilsier dermed at slike data ikke lagres.

For alle datatyper som er nevnt over er det mulig å redusere risikofaktorer for personvern ved hjelp av tekniske tiltak. Et mulig teknisk tiltak som vil redusere risikofaktorer for personvern

betydelig er kryptering av lagrede data med offentlig-nøkkel kryptografi som beskrevet i punkt 4.5.

Referanser

[1] European Union, "Directive 2006/24/EC of the European Parliament and of the Council", 15.3.2006

[2] Samferdselsdepartementet m. fl., "Høringsnotat – datalagring", januar 2010

[3] Post- og Teletilsynet, "Det norske ekommarkedet 1. halvår 2009", Publisert 14.10.2009

[4] Teleplan, "Økonomisk utredning av konsekvensene knyttet til innføring av EUs datalagringsdirektiv", 25.02.2008

[5] ETSI, "ETSI TS 102 656, Lawful Interception; Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data", versjon 1.2.1, desember 2008

[6] ETSI, "ETSI TS 102 657, Lawful Interception; Retained data handling; Handover interface for the reques and delivery of retained data", versjon 1.4.1, desember 2009

[7] ETSI, "ETSI TR 102 661, Lawful Interception; Security framework in Lawful Interception and Retained Data environment", versjon 1.2.1, november 2009

[8] Statistisk Sentralbyrå, "Folke- og boligtellingen 2001", www.ssb.no/fob/

[9] Internet Usage Statistics, www.internetworldstats.com

[10] Willassen, S. "A Method for implementing Mobile Station Location in GSM", NTNU, desember 1998.

[11] Statistisk Sentralbyrå, statistikkbanken, http://statbank.ssb.no/statistikkbanken/Default_FR.asp?PXSid=0&nvl=true&PLanguage=0&tilside=selectvarval/define.asp&Tabellid=06998

Om Svein Willassen AS

Svein Willassen er utdannet sivilingeniør i informasjonssikkerhet ved Norges Teknisk Naturvitenskapelige Universitet. Etter studiene har Willassen jobbet som spesialetterforsker ved Datakrimteamet i ØKOKRIM. Her har han utført etterforskning av datainnbruddssaker, samt sikring og analyse av databevis i alle typer straffesaker. Gjennom jobben i ØKOKRIM har Willassen deltatt i internasjonalt arbeid, blant annet som medforfatter av Interpol Computer Crime Manual, samt utarbeidelse av retningslinjer for sikring og analyse av databevis i regi av International Organization on Computer Evidence.

Willassen har siden vært ansatt i Ibas AS. Her ledet han oppbyggingen av det nye forretningsområdet sikring og analyse av databevis. Som dataetterforskningssjef var Willassen ansvarlig for et stort antall undersøkelser i sivile tvister i hele Europa, og bygget også opp kursvirksomhet i dataetterforskning. Fra 2005 til 2008 jobbet Willassen med forskning innen dataetterforskning i forskningsprosjektet *Timestamps in Digital Forensics* ved NTNU. Willassen fullførte sin doktorgrad innenfor dette temaet i 2008. Willassen driver i dag egen virksomhet innen databevis og dataetteforskning gjennom sitt selskap Svein Willassen AS.