NTNU
Det skapende universitet

Datalagringsdirektivet

Eystein Huse Leren

Master i kommunikasjonsteknologi
Oppgaven levert: Mai 2009
Hovedveileder: Stig Frode Mjølsnes, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Datalagringsdirektivet EU 2006/24/EF pålegger registrering av kommunikasjonstrafikk og skal innføres i 2009. Dette innebærer lagring av trafikkinformasjon om e-post, fast- mobil- og IP-telefoni samt internettrafikk fra 6 til 24 måneder.

Denne oppgaven vil forsøke å kartlegge hvilke tekniske krav direktivet stiller og hvilke praktiske konsekvenser dette får for norske tjenestetilbyderne. Oppgaven vil ta for seg lignende lovgivning og implementering av datalagringsdirektivet i andre land.

Datalagringsdirektivet har som intensjon å bidra til bekjempelsen av kriminalitet og terrorisme. Oppgaven vil derfor undersøke om data som blir lagret vil være et effektivt verktøy i henhold til intensjonen og hvilke utfordringer som finnes i forhold til krypterte og forfalskede data.

Oppgaven gitt: 13. januar 2009
Hovedveileder: Stig Frode Mjølsnes, ITEM

Forord

Oppgaven er skrevet på bakgrunn av et forslag til masteroppgave gitt av professor Stig Frode Mjølsnes ved Institutt for Telematikk. Det rettes en stor takk til Professor Mjølsnes, som har vært veileder og bidratt mye til retningen oppgaven har fått. Ivan Langhelle takkes for å ha bidratt med korrekturlesning og faglige innspill.

Oppgaven har til hensikt å undersøke konsekvensene ved en innføring av datalagringsdirektivet, noe arbeidet underveis har gitt undertegnede et godt innblikk i. Dersom direktivet skal innføres i Norge, krever dette ulike grader av systemendringer hos tjenestetilbyderne. Det er i denne sammenheng undersøkt hvilke fordeler og ulemper en innføring vil ha, samt foreslått en mulig løsning for sentralisert lagring av trafikkdata.

En rekke kilder har bidratt ved å stille opp til intervju og svare på henvendelser og fortjener en stor takk i denne sammenheng. Flere av disse kan ikke nevnes ved navn grunnet konkurransemessige forhold i bransjen, og har derfor blitt anonymisert i oppgaven.

Innhold

Figurer

Tabeller

Forkortelser

DLD Datalagringsdirektivet

DSL Digital Subscriber Line

PT Post- og teletilsynet

EMK Den europeiske menneskerettskonvensjonen

FRA Försvarets radioanstalt

CDR Call Detail Record

IMSI International Mobile Subscriber Identity

IMEI International Mobile Equipment Identity

PSTN Public Switched Telephone Network

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

Sammendrag

Datalagringsdirektivet EU 2006/24/EF har til hensikt å harmonisere lovgivningen som gjelder lagring av trafikkdata gjennom hele EU området, og gjennom dette gjøre medlemslandene bedre rustet til å bekjempe alvorlig kriminalitet. Direktivet er svært spesifikt for de ulike teknologiene og tjenestene. Innføringen har ført til en politisk kontrovers og samfunnsdebatt som har vært preget av frykten for et storebrorsamfunn på den ene siden og kriminalitetsbekjempelse på den andre.

Hvis direktivet skal innføres i Norge så vil dette ha varierende konsekvenser avhengig av hvilken teknologi eller tjeneste man skal lagre trafikkdata for. I det ene ytterpunktet har man de typiske telefontjenestene som baserer fakturering på samtaledata som lagres i dag. Forskjellen ved en innføring er at man vil få en noe lengre lagringstid. I det andre ytterpunktet har man e-post som aldri vært underlagt en slik form for lagringskrav og fører med seg noe helt nytt både i forhold til personvern og teknisk implementasjon. Den tekniske løsningen vil hverken være krevende eller dramatisk, men representerer et skille hvor man går fra å lagre trafikkdata av nødvendighet til å lagre de av potensiell nytteverdi i en kriminaletterforskning. Jeg foreslår en løsning for å sentralisere lagringen av trafikkdata, løsningen vil kunne bedre påliteligheten, integriteten og personvernet men vil også øke kompleksiteten.

Trafikkdata har i mange konkrete eksempler bidratt til etterforskningen og oppklaringen av det som kan kalles alvorlig kriminalitet. Dette er illustrert gjennom en rekke eksempler.

Det finnes et stort antall måter å forsøke å unngå registrering av trafikkdata på. De mest vanlige metodene og tjenestene har blitt undersøkt hvorvidt de er effektive og satt i en sammenheng med direktivet.

1 Innledning

1.1 Problemstilling

Datalagringsdirektivet skal innføres i Norge som en del av EØS-avtalen, direktivet skulle vært innført i mars 2009, men det er i skrivende stund ikke avgjort om direktivet skal implementeres eller stoppes ved hjelp av et veto.

Oppgaven skal kartlegge tekniske konsekvenser for tjenestetilbyderne av offentlig tilgjengelige kommunikasjonstjenester ved en eventuell innføring av datalagringsdirektivet. En konsekvens av at direktivet ennå ikke er implementert i Norsk lov er at arbeidet er basert på den informasjonen som har vært tilgjengelig, og en begrensning som følge av dette er at det ikke er mulig å gå ned på detaljnivå på flere punkter. Dette er for eksempel hva slags formater data som lagres skal ha, og nøyaktig innhold i data som lagres.

Direktivet vil pålegge tjenestetilbydere å rette administrative rutiner og drift inn etter de kravene som stilles. Lagring av trafikkdata gjøres av tjenestetilbydere i dag for fakturering- og driftsformål, men direktivet har en grunnleggende forskjell i hensikt og vil sette en ny standard for hvordan datalagring skal foregå. Direktivet vil medføre kostnader for implementering og drift, men denne kan ikke beregnes nøyaktig uten et nasjonalt regelverk som spesifiserer kravene som tjenestetilbydere må forholde seg til. Ved å pålegge tjenestetilbydere kostnader og plikter kan man endre konkurransesituasjonen, og i verste fall gi enkelte aktører fortrinn og virke konkurransehemmende.

Potensielle endringer som følge av en innføring er for eksempel lengre lagringstid og lagring av mer personidentifiserbar data, noe som kan ha en negativ konsekvens for personvernet til brukere. I hvilken grad personvernet kan bli påvirket og hvor alvorlig endringen er kommer til å bli undersøkt i oppgaven.

Direktivet er ikke implementert i Norsk lov og det kan være relevant å plassere det i forhold til dagens lovverk. Hensikten med direktivet i tillegg til å harmonisere lovgivningen innen EU er å bekjempe alvorlig kriminalitet,

det er da naturlig å undersøke hvordan trafikkdata brukes i en etterforskning og finne ut hvordan forutsetningene for denne bruken av trafikkdata endres ved en innføring.

En utfordring relatert til bruken av trafikkdata i etterforskninger er forfalskning av data, og omgåelse av systemene som skal sørge for datalagringen. Det er i denne sammenheng interessant å undersøke de teknikkene som kan brukes for å omgå datalagring eller forfalske data, og om disse vil ha noen reell betydning.

1.2 Avgrensning

Datalagringsdirektivet vil ha en rekke økonomiske og juridiske konsekvenser, disse er tatt med som del av bakgrunnen, men får liten oppmerksomhet i kjernen av oppgaven da fokuset er på de tekniske løsningene og konsekvensene. Gjeldende lover, både nasjonale og internasjonale, er gjennomgått for å sette direktivet i en sammenheng. Det ligger utenfor oppgaven å gjøre vurderinger rundt lovverket.

Lagringstiden kan innen de gitte rammene på 6 og 24 måneder bestemmes av landene som skal innføre direktivet. Dette er en av forutsetningene for en kostnadsberegning og har vært gjenstand for debatt. I oppgaven er det referert til synspunkter på ønsket lagringstid og gjort rede for dagens praksis, men det er ikke gjort vurderinger rundt hvor lang lagringstid som vil være hensiktsmessig.

Trafikkdata som samles inn med grunnlag i direktivet skal brukes til å bekjempe alvorlig kriminalitet. Hvordan dette kan gjøres er undersøkt ved å se på en rekke case studies hvor det er undersøkt om trafikkdata var til hjelp eller ikke. Dette kunne vært undersøkt ved å gjennomgå de ulike formatene på data og se på hva slags informasjon man kan få ut av disse, men bruken av case studies framstod som mer hensiktsmessig for å illustrere hvordan trafikkdata bidrar til etterforskning i praksis.

Oppgaven skal undersøke hva slags teknikker som kan være effektive for å omgå datalagringsdirektivet. Undersøkelsene er basert på analyser av dokumentasjonen til systemer og ikke på eksperimenter da dette ikke ville gitt ytterligere relevant informasjon.

1.3 Organisering av oppgaven

Innledningskapittelet inneholder problemstillingen, avgrensingen, oppsummeringen og metoden som er brukt i oppgaven. Det er dette kapittelet som legger grunnlaget for hva som er målsetningen for oppgaven og hvordan den målsetningen skal nås.

Bakgrunnskapittelet forklarer hva datalagringsdirektivet er og hensikten med det. Direktivet settes i en sammenheng ved å se på eksisterende lovgivning, tilsvarende lover, andre typer informasjonslagring og hvordan samfunnsdebatten rundt direktivet har vært. Arbeidet i kapittelet er resultatet av en bred litteraturstudie.

Implementering i teknologiene er en kartlegging av hva slags konsekvenser datalagringsdirektivet vil få ved en innføring. Denne kartleggingen er basert på intervjuer med aktører i bransjen og eget arbeid, noen underkapitler er basert på litteratur.

Bruk av trafikkdata i etterforskning undersøker hvordan trafikkdata kan bidra til å oppklare kriminelle handlinger. Arbeidet er basert på en litteraturstudie som er satt i sammenheng med datalagringsdirektivet og supplert med egne vurderinger.

Omgåelse av datalagring skal vise hvilke metoder som kan brukes for å unngå lagringen som pålegges i henhold til direktivet. Kapittelet inneholder et bredt utvalg av metoder som er dokumentert ved hjelp av litteratur og vurdert opp i mot hvorvidt metoden kan brukes effektivt for å unngå datalagring.

Konklusjonen oppsummerer funnene i oppgaven og svarer på problemstillingen.

1.4 Metode

Den metodiske tilnærmingen er avhengig av hva en ønsker å undersøke. Den er et hjelpemiddel for å få kunnskap og en dypere forståelse av et fenomen. I dette tilfellet var den kvalitative tilnærmingen den som virket mest hensiktsmessig.

Arbeidsmetoden bestod av intervjuer med nøkkelpersoner og bruk av informasjon som finnes i offentlige kilder. Dette arbeidet la grunnlaget for en diskusjon og konklusjon.

Den kvalitative metoden som ble benyttet beskrives i [53] som; "Kvalitativ metode er en metode for innhenting av opplysninger hvor man istedenfor å undersøke flest mulig forekomster (kvantitativ metode) konsentrerer seg om noen få, og undersøker disse svært grundig. Innenfor forskjellige fag er det utviklet metoder og teknikker for å samle inn informasjon, og for å bearbeide dem. I metodelæren er det vanlig å skille mellom kvantitative og kvalitative metoder."

En ulempe med den kvalitative metoden er at de data man samler inn er mindre formaliserte og at man samler inn uten noen spesifiserte regler. Når man jobber med kvantitative data fins det klare anbefalinger som søker å sikre validiteten til disse.

Man kan skille mellom "harde" kvantitative data og "myke" kvalitative data. De harde er offentlige dokumenter som for eksempel standarder og lovtekster. Disse data lar seg lett referere til og er lett tilgjengelige for ettersyn. Myke kvalitative data kan for eksempel være et intervju, disse er også lette å referere til, men er mye vanskeligere å verifisere. I denne oppgaven har det blitt brukt både harde og myke datakilder.

Intervjuene som har blitt gjennomført var ansikt til ansikt, telefonintervju og over e-post. De intervjuene som ble utført ansikt til ansikt eller over telefon var halvstrukurerte.

Et halvstrukturert intervju blir definert som: "et intervju som har som

mål å innhente beskrivelser av den intervjuedes livsverden, med henblikk på fortolkning av de beskrevne fenomenene, har en bestemt **hensikt**(å forstå sider ved intervjupersonens dagligliv, fra den intervjuedes eget perspektiv), har en bestemt **struktur**."[56]

Fordelen med å bruke denne typen intervju er at man har et sett med punkter man skal belyse og står ellers fritt til å snakke om temaer i den grad og detalj som intervjuerne og intervjuobjektene ønsker. Dermed kan en bruke tid på emner som viser seg å være viktige, men som man ikke visste om på forhånd. Det ble brukt notater til å dokumentere alle gjennomførte intervju, og disse ble brukt som kilder i det videre arbeidet med oppgaven.

Intervjuene på e-post var mer strukturerte og ga mindre rom for intervjuobjektet å svare utover spørsmålet med mindre han/hun valgte dette selv. Fordelen med e-post er at det er enklere å få stilt oppfølgningsspørsmål og den asynkrone kommunikasjonen gir tid til å komme med gjennomtenkte og fyldige svar.

Utvalget av kilder var svært sammensatt. Veilederen kom med enkelte anbefalinger, mens andre kilder ble funnet gjennom å ta kontakt med de etatene og bedriftene som direkte er berørt av innføringen av direktivet.

Enkelte kilder er unntatt kildehenvisning da de har oppgitt informasjon som er bedriftsintern og kilden har bedt om å ikke bli oppgitt grunnet konkurransehensyn. Dette gjelder teknisk informasjon og begrenser seg til kapitlene 3.1-3.3.

Feilkilder i intervjuene og kildene kan være mange og ha ulik grad av betydning. I offentlige dokumenter som ligger på lett tilgjengelige internettsider, vil feilen primært begrense seg til tolkningen og bruken av dokumentene. Dette gjelder også for de andre offentlige kildene som har blitt brukt. I intervjuene er inntrykkene og notatene de viktigste kildene en baserer seg på når man skal benytte seg av informasjonen en har fått. I [56] står det; "det finnes ingen sann, objektiv oversettelse fra muntlig til skriftlig form." Oppgaven må da bli å skaffe informasjon fra intervjuobjektene og bruke denne på en mest mulig objektiv måte. Måten dette ble gjort på var blant annet ved å stille

minst mulig ledende spørsmål. Spørsmålene som ble stilt var åpne for å la intervjuobjektet poengtere det han/hun syntes var vesentlig. [36][1]

Deler av oppgaven har benyttet artikler som grunnlag for arbeidet. Artiklene varierte fra vitenskapelige artikler publisert som et ledd i forskning til artikler i tabloidaviser og internettaviser. De sistnevnte inneholder langt mer subjektive synspunkter og vinklinger, dette er ikke et problem når man skal kartlegge motstand og støtte i en samfunnsdebatt, men de kan ikke brukes ukritisk. Artikler i tabloidaviser og andre kilder som ikke er vitenskapelige må utsettes for mer kildekritikk enn forskningsartikler.

[1] Kapittelet er en omskrivning av tilsvarende kapittel fra [36].

2 Bakgrunn

2.1 Datalagringsdirektivet

Datalagringsdirektivet (DLD) EU 2006/24/EF [35] er et direktiv som ble vedtatt 15. mars 2006, og omhandler datalagring av offentlig tilgjengelig elektroniske kommunikasjonstjenester.

Direktivet spesifiserer at data som beskriver kommunikasjon skal lagres, men ikke dens innhold. Lagringstiden skal bestemmes av landene som innfører det, men det er satt en minimumstid på 6 måneder og en maksimumstid på 24 måneder. Data som er definert til å beskrive kommunikasjonen er ulik for kommunikasjonsmåten og ordlyden i direktivet kan oversettes til: "Direktivet gjelder trafikk- og lokasjonsdata både for juridiske enheter og personer og de data som er nødvendige for å identifisere abonnent eller registrerte bruker."

For telefoni betyr dette at telefonnumrene det ringes fra og til, tidspunktet og lengden på samtalen, samt ubesvarte anrop skal registreres. Direktivet tar også høyde for viderekobling og presiserer at det ved viderekobling må registreres hvor samtalen overføres. Spesielt for mobiltelefoni er at lokasjonsdata og Cell ID skal lagres i tillegg til IMSI og IMEI både for den som ringer og den som blir oppringt.

Ved bruk av Internett skal tidspunkt for inn- og utlogging av aksesstjenesten sammen med IP-adresse og bruker-ID som tilhører abonnenten logges. Hvis aksesstypen er oppringt Internett skal telefonnummeret det ringes fra lagres og hvis det er Digital Subscriber Line (DSL) eller annet endepunkt må dette identifiseres og lagres. E-post har fått spesiell oppmerksomhet som del av internettrafikken og underlegges separat registrering. I forbindelse med e-post skal senders og mottakers navn og adresser registreres samt tidspunkt og type tjeneste. IP-telefoni på lik linje med e-post registreres separat med tid, varighet og identifisering av brukeren som ringer om mottar samtale, samt hvilken tjeneste som er benyttet.

EU vedtok DLD 15. mars 2006 med et krav om at nødvendige lover og

administrative rutiner måtte være på plass 15. september 2007. Medlemslandene kunne utsette datalagring i forbindelse med internettoppkobling, IP-telefoni og e-post til 15 mars 2009.

DLD skal innføres i alle landene som er med i EØS-avtalen. Dette har resultert i motstand mot direktivet, blant annet et søksmål på grunn av personvern i Irland [17] og tvil om hvorvidt direktivet er gyldig som del av EØS-avtalen [18]. Tvilen rundt gyldigheten er beskrevet i [58] og kan oppsummeres med at DLD er hjemlet i feil del av EØS-avtalen og derfor ikke gyldig. Regjeringen valgte å avvente til EU-domstolens dom forelå. Dommen kom 10. Februar 2009 og ga ikke Irland og Slovakia medhold. Dette gjør at regjeringens eneste tiltak for å unngå innføring er å nedlegge veto mot direktivet. Regjeringen har per mai 2009 ikke tatt stilling til om eller hvordan eventuelt DLD skal implementeres i norsk rett. Det er mye kontrovers rundt DLD som er mer samfunnsmessig enn juridisk og dette vil bli videre diskutert i kapittelet om motstanden mot DLD.

Hvis DLD blir innført i Norge, vil dette berøre majoriteten av befolkningen. Alle som bruker elektroniske kommunikasjonstjenester vil få lagret trafikkdata opp mot sitt abonnement eller bruker. Tjenestetilbydere vil få et ansvar for å samle inn, lagre og gjøre data tilgjengelige for relevante etater som har myndighet til innsyn i disse.

DLD har som formål å være en del av politisamarbeidet og terrorbekjempelsen innen EU. DLD skal harmonisere lovgivningen i medlemslandene og være et verktøy i forbindelse med bekjempelsen av "alvorlig kriminalitet". Definisjonen av hva som er alvorlig kriminalitet skal ligge i hvert enkelt lands nasjonale lovgivning.

Kostnaden som blir en følge av DLD er av IKT-Norge beregnet til å bli 300 MNOK årlig. Dette er en kostnad justisministeren har uttalt skal dekkes av teleoperatørene selv. IKT-Norge har uttalt at dette vil kunne svekke konkurransen i telemarkedet til fordel for store operatører. [14]

Direktivet stiller krav til at data som lagres har den samme graden av beskyttelse som når de er i nettet. Det er interessant i og med at all IPv4-

og GSMtrafikk er ukryptert i nettet. Den eneste formen for beskyttelse ligger enten i kryptering i applikasjoner for IP-trafikk og adressering for begge teknologiene. Adressering er ikke i seg selv et beskyttelsestiltak, men beskytter mot enkle trusler som for eksempel tilfeldig avlytting.

2.2 Eksisterende lovgivning

Formålet med DLD er å harmonisere lovgivningen til medlemslandene med tanke på datalagring. Det er da hensiktsmessig å se på allerede eksisterende og relevant nasjonal og internasjonal lovgivning. I norsk sammenheng finnes det få lover som direkte omhandler kommunikasjonskontroll og datalagring. Majoriteten av de relevante lovene og reglene dreier seg om personvern og spesifiserer hva som ikke er lov, i motsetning til DLD som pålegger hva som skal lagres, hvor lenge og av hvem.

Nasjonal lovgivning

De nasjonale lovene og reglene rundt personvern og kommunikasjonskontroll består av:

Personopplysningsloven som er den generelle loven for behandling av personopplysninger. I motsetning til DLD som spesifikt beskriver de ulike teknologiene er personopplysningsloven laget for å være teknologinøytral og mer rettet mot de tilfeller der personopplysninger er systematisk lagret. Et av de svært sentrale punktene i loven er at registrere med sensitive opplysninger er underlagt krav om konsesjon.[66]

Ekomloven [75] har kort sagt som formål å sikre brukerne gode elektroniske kommunikasjonstjenester. Dette gjør loven ved å regulere en rekke forhold, blant annet kommunikasjonsvern hvor det beskrives hvor lenge en tjenestetilbyder kan lagre trafikkdata. Loven regulerer også hvem som skal dekke kostnadene av tilretteleggingsplikt som gir tilgang til informasjon om sluttbruker - dette skal i henhold til Ekomloven dekkes av staten. Det er også en paragraf som omhandler taushetsplikten en tjenestetilbyder er underlagt.

Straffeprosessloven kapittel 216a og 216b gir hjemmel til kommunikasjonskontroll, også kjent som avlytting. Dette er myndighetenes adgang til å avskjære, høre og lagre kommunikasjon til og fra en gitt person eller organisasjon. Kommunikasjonskontroll har en egen forskrift som beskriver detal-

jene rundt utførselen av denne typen informasjonsinnhenting. [65]

Helselovgivningen har flere lover som omhandler personvern. Disse er i liten grad relevante i denne sammenhengen, selv om de ofte omhandler data lagret i forbindelse med en gitt person. Lovene innen helselovgivningen som omhandler personvern er helseregisterloven, helseforskningsloven og helsepersonelloven, og nevnes i denne sammenheng for å bidra til helhetsbildet. [63, 64, 62]

Internasjonal lovgivning

Det internasjonale lovverket er beskrevet i [71][2]. I tillegg til å beskrive de relevante lovene, så kommer [71] med flere påstander rundt betydningen av disse. En konsekvens av lovene er at enkeltlandene får mindre frihet til å utforme sitt eget personvern, da lovene nedsetter minstekrav og begrensninger. Det er også en stor variasjon fra lov til lov med tanke på detaljer og anvendelsesområde.

De lovene som er nevnt i [71], er:

FNs Verdenserklæring om menneskerettigheter av 1948, artikkel 12: "Ingen må utsettes for vilkårlig innblanding i privatliv, familie, hjem og korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike angrep." FN-konvensjonen om sivile og politiske rettigheter artikkel 17 lyder omtrent likt som artikkel 12 i Verdenserklæringen.

Den europeiske menneskerettskonvensjonen (EMK) av 1950 ble vedtatt den 4. november 1950 og trådte i kraft den 3. september 1953. Artikkel 8 lyder som følger:

1. "Enhver har rett til respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse.

2. Offentlig myndighet skal ikke gjøre noe inngrep i utøvelsen av denne

[2]Kapittelet er en i all hovedsak hentet fra kap 7 i [71]

rett med mindre dette inngrep er i samsvar med loven og i et demokratisk samfunn er en nødvendig forholdsregel for den nasjonale eller offentlige sikkerhet, for landets økonomiske velstand, for å forebygge uorden eller forbrytelser, beskytte helse eller moral eller beskytte andres rett og friheter.“

I DLD er det spesifikt nevnt at direktivet skal være i henhold til denne artikkelen. Dette er en av årsakene til mye kontrovers.

EUs charter om grunnleggende rettigheter (Charter of Fundamental Rights of the European Union (2000/C 364/01)) av 2000 inneholder to bestemmelser med særskilt relevans for personvern og personopplysningsvern. Den første er artikkel 7, som lyder:

”Everyone has the right to respect for his or her private and family life, home and communications.“

Den andre er artikkel 8, som direkte angår personopplysningsvern. Bestemmelsen består av tre ledd:

1. ”Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.“

Charteret er i seg selv ikke rettslig bindende, men det utgjør likevel et viktig utgangspunkt for utvikling av regulatorisk politikk innenfor EU.

Europarådets konvensjon om personvern i forbindelse med elektronisk behandling av personopplysninger ”Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data“ er den eneste konvensjonen som direkte omhandler personopplysningsvern. Konvensjonen er blitt ratifisert av de aller fleste land som er medlemmer

av Europarådet, deriblant Norge. Ved ratifikasjon forplikter en stat seg til å inkorporere konvensjonens prinsipper i sitt nasjonale regelverk (jf. artikkel 4(1)). Konvensjonen inneholder ellers ikke rettigheter som direkte kan anvendes av enkeltindivider. Den etablerer heller ikke et eget håndhevelsesorgan. Hovedformålet med konvensjonen er å sikre personvernet mot trusler ved elektronisk databehandling (jf. artikkel 1). Den nedfeller et sett med prinsipper som fastsetter minstestandarder for all elektronisk behandling av personopplysninger (jf. artikkel 5 flg.). Prinsippene gjelder i utgangspunktet kun elektronisk eller automatisert behandling, men kan utvides til også å omfatte manuelle prosesser.

OECD vedtok den 23. september 1980 retningslinjer for beskyttelse og utveksling av personopplysninger over landegrenser (Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data). Retningslinjene er ikke rettslig bindende, men har hatt stor innflytelse på utviklingen av nasjonalt regelverk, særlig i ikke-europeiske medlemsland av OECD, eksempelvis Canada, Australia og New Zealand.

FN har laget retningslinjer for elektroniske personregistre (Guidelines Concerning Computerized Personal Data Files). Retningslinjene inneholder prinsipper for behandling av personopplysninger og er stort sett like de som finnes i OECDs retningslinjer av 1980 og Europarådets konvensjon av 1981, men utfyller likevel disse på enkelte punkter.

EU vedtok den 24. oktober 1995 et direktiv om personopplysningsvern (direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger). Direktivet ble den 25. juni 1999 tatt inn i avtalen om det europeiske økonomiske samarbeid av 1992, EØS-avtalen, og ble dermed gjort folkerettslig bindende for Norge. Direktivet utgjør en sentral premissleverandør for norsk regulatorisk politikk på feltet, ikke bare på grunn av EØS-avtalen, men også fordi direktivet er betydelig mer detaljert og omfattende enn øvrige internasjonale regelsett som for eksempel Europarådets konvensjon av 1981 og OECDs retningslinjer av 1980. Direktivet er implementert i norsk lovverk primært i personopplysningsloven. Direktivet er langt mer ambisiøst når det

gjelder harmonisering av nasjonalt regelverk enn Europarådets konvensjon av 1981 og OECDs retningslinjer av 1980. Dette gjelder både fastsettelse av grunnprinsipper, begrepsapparat, tilsynsordninger og anvendelsesområdet for regulering. På visse punkter tillates likevel medlemsstater et spillerom ved implementering av direktivet.

Tilsyn

Tilsyn med lover og regler er fordelt på en rekke offentlige organer, hvor de mest relevante er beskrevet under.

Politiet skal etterforske og påtale eventuelle brudd på lover og forskrifter. I spesielle tilfeller skal egne avdelinger ta over enkelte saker. Dette er relevant ved en eventuell innføring av DLD da "alvorlig kriminalitet" skal etterforskes av Kripos.[72] Enkelte andre former for alvorlig kriminalitet som miljø- og økonomisk kriminalitet blir etterforsket av Økokrim.[47] Politiets behov for kommunikasjonskontroll og holdning til DLD er omtalt i kapittel 2.3.

Post- og teletilsynet (PT) skal føre tilsyn med konkurransen i telemarkedet og at relevante lover regler og pålegg følges. PT har ved flere anledninger reagert ovenfor aktører som ikke har overholdt reglene som angår personvern. På PT sine hjemmesider står det at: "PT er eit frittståande forvaltningsorgan som ligg under Samferdselsdepartementet. Hovudansvarsområda for etaten er å regulere og overvake post- og telekommunikasjonssektoren i Noreg. PT er sjølvfinansiert, primært gjennom gebyr frå teleoperatørane." [68]

Datatilsynet har spesielle oppgaver angående personvern. "Datatilsynet skal medverke til at den einskilde ikkje vert krenka gjennom bruk av opplysningar som kan knyttast til han eller henne. Datatilsynet er oppretta for å sjå til at personopplysningslova vert fulgt. Formålet med lova er å verne den einskilde mot krenking av personvernet gjennom bruk av personopplysningar. Datatilsynet er både tilsyn og ombud. Datatilsynet er eit uavhengig forvaltningsorgan administrativ underordna Kongen og departementet." [24]

Datatilsynet håndhever oppgaven ved å gi konsesjoner til databaser i henhold til personopplysningsloven og gi pålegg til de som bryter den. Datatilsynet er også ofte framme i media og kommer med synspunkter på saker som angår personvern og DLD har vært gjenstand for mange uttalelser fra datatilsynet.

Avsluttende kommentar om lovverk

Dette kapittelet har vært en gjennomgang av hvilke relevante lover og regler som finnes i dag. Det er ikke uttømmende, ikke nødvendigvis fordi at det fins flere relevante lover, men fordi at lover og regler også eksisterer i sammenheng med forskrifter og rettspraksis som setter lovens teori om til praksis. Ved en eventuell innføring av DLD, vil norske lover måtte endres i henhold til direktivets hensikt om å harmonisere europeisk lovverk rundt datalagring.

2.3 Motstanden mot datalagringsdirektivet

Motstanden mot DLD er veldig variert, alt fra nær tverrpolitisk motstand til folkeaksjoner på Facebook og sterke innsigelser fra miljøene som må implementere direktivet. Dette kapittelet skal se nærmere hva denne motstanden er basert på.

Det er en sterk politisk motstand mot DLD. Høyre[42], Kristelig Folkeparti[48], Senterpartiet[103], Sosialistisk Venstreparti[49], Fremskrittspartiet og Venstre [102] er motstandere, mens Arbeiderpartiet enda ikke har kommet med en uttalelse. Flere partier har landsstyrevedtak mot DLD og jobber for å nedlegge et veto mot at direktivet blir innført. Samtlige ungdomspartier har gått sammen mot direktivet i et brev til Stortinget. [52]

Det finnes motstand mot DLD i media og samfunnsdebatten. Eksempler på dette er dekning i internettavisen Liberaleren og bloggen Vox Populi som begge har hatt en kritisk holdning til DLD. Et annen reaksjon på direktivet er Facebookgruppen mot DLD som p.t. har over 18 000 medlemmer og gruppen mot EU-direktiv 2006/24 som har over 6000 medlemmer. En internettside som ønsker å bidra med informasjon angående direktivet, www.datalagringsdirektivet.no, har samlet mye informasjon og gjennomfører intervjuer som blir publisert.

Flere faglige instanser har innvendinger mot direktivet. Forbrukerombudet mener at DLD truer personvernet og rettsikkerheten. [37] Datatilsynet har både i media og i egne uttalelser gått hardt ut mot innføringen og innholdet i DLD. [7, 23]

Landets to største teleoperatører, Telenor og Netcom, ser begge store problemstillinger knyttet til innføringen av DLD. [22, 21] Blandt bekymringene er kostnadene, tillitsforholdet til kunder, utformingen av lovverk og regler samt håndhevingen av disse.

Personvernkommisjonen skriver i sin uttalelse om DLD, som er vedlegg 1 i [71], at behovet for lagringen direktivet pålegger ikke er dokumentert. Dagens regelverk ansees å være uoversiktlig og vanskelig. Kommisjonen stiller

seg også spørrende til om trafikkdata vil bidra til oppklaringen av kriminalitet. Et annet poeng som kommer fram i uttalelsen er at fakturering fra teleoperatører går fra å være forbruksbasert til å være tilgangsbasert. Dette vil medføre at man på enkelte områder, som telefoni, må man beholde gamle registreringsrutiner. På andre, som datatrafikk over EDGE/GRPS/HSDPA eller DSL, må det innføres nye lagringsrutiner som tilfredsstiller kravene til registrering som stilles i DLD.

IKT-Norge ser på innføringen av DLD med bekymring og mener at teleoperatørene blir pålagt politiarbeid. De er spesielt kritiske til hvordan små teleoperatører skal kunne lagre sensitive data på en trygg måte. [20] Det er også IKT-Norge som innhentet en juridisk vurdering av hvorvidt direktivet er relevant i henhold til EØS-avtalen. Denne vurderingen konkluderer med at Norge kan reservere seg mot direktivet og at bakgrunnen for en slik er politisk i stedet for juridisk.

Irland og Slovakia anla et søksmål mot EU-kommisjonen på grunnlag av at de mente at hjemmelsgrunnlaget for direktivet ikke var korrekt og gjorde at direktivet var ugyldig. Den europeiske domstolen i Luxemburg kom den 10. Februar 2009 fram til at direktivet er korrekt plassert og må implementeres av medlemslandene i EU. [26]

Motargumentene til skepsisen og kontroversen mot DLD er en blanding av faglige og politiske. De faglige argumentene kommer fra blant annet Kripos[20], som sier at trafikkdata har løst flere saker som omhandler blant annet narkotika og barnepornografi. De legger til at flere av disse sakene ville vært uløste om man ikke hadde fått tilgang til trafikkdata og kommunikasjonskontroll. Konkrete eksempler på bruk av trafikkdata og innhold i kommunikasjon er Baneheia- og Knutbysakene. Disse sakene fører til en opinion som er positiv til datalagring. De politiske grunnene er at et veto mot direktivet vil kunne svekke Norges stilling innen EØS-samarbeidet. Det har vært noe debatt rundt konsekvensene av et slikt veto.

Artikkel 8 i EMK omhandler som tidligere beskrevet personvernet. I 2006/24/ECdokumentet stadfestes det i avsnitt 9, før selve direktivet, at

datalagring er et behov for å kunne oppklare alvorlig kriminalitet og dermed i overensstemmelse med artikkel 8 i EMK. I avsnitt 22 i samme del av dokumentet presiseres det spesifikt at direktivet respekterer de grunnleggende menneskerettigheter beskrevet i EMK. Direktør i Datatilsynet, Georg Apenes, er uenig og uttaler; "Samtlige personvernmyndigheter innenfor EØS-området har for lengst påpekt at lagringsdirektivet frontkolliderer med Den Europeiske Menneskerettighetserklæringens artikkel 8 om retten til en respektert privat sfære. Når det likevel blir innført i nasjonal lovgivning, skyldes det at politikerne mener at hensynet til lov og orden må gå foran hensynet til de - etter hvert åpenbart nokså gammelmodige - borgerlige frihetsidealer." [50] Personvernkommisjonen sier i sin uttalelse om direktivet at det i henhold til artikkel 8 kreves et sterkt grunnlag for å gripe inn i personvernet og at kommisjonen ikke ser at nødvendighetsprinsippet og proposjonalitetsprinsippet overholdes i direktivet.

2.4 Lover tilsvarende datalagringsdirektivet

Det finnes flere eksempler på lover som ligner på DLD i funksjon og det kan være fornuftig å se på disse i sammenheng med DLD. Det finnes to profilerte lover som er naturlige å se på i denne sammenheng: den svenske Signalspaningslagen som ble vedtatt i 2008 og den amerikanske USA PATRIOT Act som ble vedtatt i 2001. Disse lovene ligner i varierende grad på DLD, men danner et interessant sammenligningsgrunnlag.

Signalspaningslagen

Signalspaningslagen, også kjent som FRA-loven, ble vedtatt 19. juni 2008 og trådte i kraft 1. januar 2009. [25, 97] Loven går i korte trekk ut på at Försvarets radioanstalt (FRA) har fått som oppgave å drive spaning på all trafikk innen Sveriges grenser som ferdes i kabler. Dette vil i realiteten si mesteparten av all data- og teletrafikk som ferdes innen eller gjennom Sverige.

Bakgrunnen for loven er nesten den samme som for DLD; å bekjempe terrorisme og internasjonal kriminalitet. En av forskjellene er at myndigheten legges til den sivile etaten FRA, som ligger under det svenske forsvarsdepartementet. FRAs formål er å støtte svensk utenriks-, sikkerhets-, og forsvarspolitikk. Dette er en helt annen plassering av utøvende ansvar enn i DLD, hvor det er gjort klart at det er politiet som skal bruke de innsamlede data for etterforske terrorisme og alvorlig kriminalitet. En annen vesentlig forskjell er at innholdet i kommunikasjonen er underlagt kontroll med denne loven. Kommunikasjonen skal i henhold til loven kontrolleres automatisk, men hvordan dette skal skje er ikke offentlig kjent. [27]

Konsekvensene av Signalspaningslagen er at mye av trafikken fra Norge vil bli kontrollert av svenske myndigheter, da majoriteten av tele- og internettrafikken som skal utenlands, og deler av den nasjonale teletrafikken rutes via Sverige. [86, 67] Et konkret eksempel på dette er SMS som sendes av Tele2-abonnenter som routes via Sverige av økonomiske årsaker. En konsekvens av dette er at innholdet i alle SMS sendt av Tele2-kunder vil bli underlagt

kontroll av svenske myndigheter.

Loven utløste mye kontrovers i Sverige med debatter og en liten margin ved avstemningen i Riksdagen. Kritikken mot loven kom ikke bare i media og samfunnsdebatten, men også som til dels svært krass kritikk fra andre etater. Det svenske Justisdepertamentet skriver at "Forslaget... innebærer et integritetsbrudd som savner sidestykke i internasjonalt perspektiv." [5] Rikspolitiet skriver i sitt svar at "Forslaget tyder på en skremmende mangel på forståelse av de krav om beskyttelse av integritet som kommer av grunnloven og Europakonvensjonen." [4] Det svenske sikkerhetspolitiet beskriver innholdet i loven som "massiv telefonavlytting og en krenking av integritet... forslaget kan umulig gjennomføres uten at Justisdepertamentets endringsforslag innføres"[77] I lys av at norsk data- og teletrafikk rammes av lovforslaget har både Datatilsynet og Post- og teletilsynet kommet med vurderinger av konsekvensene. Stort sett all internasjonal telefoni- og datatjenester rutes via Sverige, mens begrensede mengder går via Danmark. Post- og teletilsynet har funnet leverandører som har kapasitet på sjøkabler som vil rute trafikken gjennom Storbritannia eller Danmark, men det er ikke gjort undersøkelser eller anbefalinger om man bør legge trafikken over på disse. Det er reist er søksmål mot loven i menneskerettighetsdomstolen, søksmålet får støtte blant annet av den norske avdelingen for juristkommisjonen. [28] Georg Apenes er sitert i samme artikkel: "Etter min mening tilsier sakens fundamentale alvor at den prøves for menneskerettighetsdomstolen i Strasbourg. Det er ikke første gang forholdet mellom grunnleggende menneskerettigheter og nasjonal lovgivning blir rettslig prøvet, og det blir ganske sikkert heller ikke siste."

USA PATRIOT act

USA PATRIOT act, som er en forkortelse for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, ble vedtatt og trådte i kraft 26. oktober 2001. Loven har som hensikt å være et verktøy for å bekjempe terrorisme og bruker innsamling av

data for å gjøre dette.

Forskjellene er store i forhold til Signalspaningslagen og DLD. PATRIOT act gir myndighetene tilgang til å overvåke innholdet i telefontrafikk, e-post, legejournaler, finansielle data, lånedata fra offentlige bibliotek m.m. Det er også gitt åpning for ransaking av eiendom og tilbakeholding av personer. Alt dette kan skje uten en rettslig kjennelse eller skjellig grunn til mistanke. Utlevering av for eksempel lånedata fra biblioteket medfører også at de som utleverer informasjonen ikke har rett til å informere om at lånedata er blitt utlevert. [73, 60, 2, 3, 99] Lovhjemmelen for praksisen med å kunne kreve hemmelighold om at informasjon hadde blitt utlevert ble i 2007 bestemt til å være grunnlovsstridig av en amerikansk domstol. [1]

USA PATRIOT act har vært kilden til mye diskusjon, og grupper som jobber med borgerrettigheter har reagert kraftig på enkelte avsnitt i lovteksten. Avsnitt 215 er et av disse og er den hjemmelen som gir myndighetene adgang til å innhente informasjon uten skjellig grunn.

Avsluttende kommentar om tilsvarende lover

Dette kapittelet har vist at det finnes en rekke lover som ligner på DLD i hensikt, men som har en noe annen tilnærming. Spesielt med tanke på utførelsen og graden av fullmakter som gis, finnes det store forskjeller. DLD gir medlemslandene ansvaret for å definere alvorlig kriminalitet og la politiet bruke trafikkdata til å oppklare denne. Signalspaningsloven er ment til å være et verktøy for etterretningstjenestene for å kunne bekjempe terrorisme og er underlagt en etat innen forsvarsdepartementet. USA PATRIOT act går mye videre enn de to andre angående hvilken informasjon som kan hentes inn uten en rettslig kjennelse. Felles for lovene og direktivet er at de er sterkt kritiserte for å bryte med de grunnleggende rettighetene som borgere av moderne demokratier skal nyte godt av.

2.5 Innføring av datalagringsdirektivet i andre land

Direktivet er i EU-domstolen kjent gyldig og må derfor innføres i alle medlemsland og i land som er del av EØS-avtalen. Direktivet kan stoppes i EØS-land dersom man nedlegger veto. Innføringen skal ferdigstilles mars 2009. Enkelte land har lovgivning som går utover det DLD pålegger dem å ha. Et eksempel som er beskrevet tidligere er Sverige, men også Danmark, Italia og Storbritannia har lovgivning utover det som spesifiseres i direktivet. [70]

Danmark har en lov som går utover DLD, hvor de pålegger å logge datastrømmene med tilhørende trafikkdata på hoteller, lufthavner, campingplasser o.l. I systemer der dette ikke er teknisk mulig skal minst én av 500 pakker lagres. [81]

Som del av antiterrorlovgivningen har Storbritannia innført et frivillig lagringssystem som data- og teletjenestetilbydere kan benytte seg av. Kostnaden av datalagringen blir dekt av staten men de som får innvilget innsyn skal betale en avgift. I Norge skal trafikkdata slettes etter at den ikke trengs til fakturering, denne sletteplikten er fjernet i Storbritannia.

I mange EU- og EØS-medlemsland har det vært stor kontrovers rundt innføring av DLD og tilsvarende lovgivning. I Ungarn er DLD tatt til grunnlovsretten. I Tyskland prøvde opposisjonen å få stemt gjennom et forslag om å bli med på Slovakias og Irlands søksmål som motstand mot direktivet. Alt dette er i tillegg til en generell misnøye blant befolkningen og organisasjoner. [13]

2.6 Andre typer informasjonslagring

Datalagringsdirektivet har fått oppmerksomhet siden det lagrer informasjon om brukere og hva de foretar seg. Informasjonslagring er på ingen måte begrenset til direktivet, og derfor kan det være relevant å se på andre områder hvor det blir lagret informasjon knyttet til privatpersoner.

Autopass er et system for å kjøre gjennom bomstasjoner og betale ved hjelp av en RFID-brikke plassert i kjøretøyet. Selskapet bak Autopass har for tiden pilotprosjekter for å utvide systemet til bruk ved parkering og ferge, og det har vært diskutert hvorvidt systemet kan brukes til betaling ved fylling av drivstoff m.m. I dag er Autopassystemet pålagt sletting av data ikke senere enn 72 timer etter passering av et betalingspunkt. Hvis systemet i framtiden utvides er det ikke naturlig at dette må revurderes med tanke på at fakturaene skal kunne kontrolleres og etterprøves. Dette vil bidra til økte mengder av lagret informasjon om bevegelses- og forbruksmønster som lagres og knyttes opp til enkeltpersoner eller husstander eller firmaer. [8, 71]

Storbritannia har vurdert å innføre et system for bilovervåkning ved hjelp av kameraer som skal settes opp langs veier, bensinstasjoner, bysentre og kjøpesentre. Formålet med dette å å stanse uvettig kjøring, biltyverier, kjøring med uforsikret bil og biler det ikke er betalt veiavgift på. Kritikken er at man samtidig vil overvåke majoriteten av bilførere som følger lovene. Tilgangen til data som lagres i systemet vil være tilgjengelig for politiet ved tillatelse fra overordnede. [69]

Flyselskap har fått et ansvar med å overlevere passasjerdata til EU ved flyreise fra land utenfor unionen, noe som også innebærer Norge da det ikke er gjort unntak for land som er med i EØS- eller Schengensamarbeidet. Disse data er passasjernavn og -adresse, telefonnummer, e-postadresser, all kredittkortinformasjon, reisedatoer, hele reiseruten, bonuskortinformasjon, regningsadresse, opplysninger om reisebyrå, all billettinformasjon, all bagasjeinformasjon, setenummer og navn på andre i samme reisefølge. Informasjonen skal lagres i 13 år før den slettes. [11]

Dersom man skal reise til USA skal det på forhånd fylles ut en innreisesøknad hvor man må oppgi personopplysninger. Denne er gyldig i to år etter at den er innvilget. Det står ikke eksplisitt at informasjonen lagres, men tatt i betraktning at en innvilget søknad er gyldig i to år er dette en naturlig antakelse. [33]

Dette er noen eksempler på at informasjon lagres utover det man er vant til, som legejournaler, bankinformasjon, offentlige registre og lignende. Disse eksemplene har likhetstrekk med datalagringslover i at personidentifiserbare data lagres, men skiller seg i at det i mange tilfeller er frivillig og ofte et ønske fra forbrukere. Forbrukere ønsker å forenkle egne reiser ved hjelp av å bruke køfribrikker og registrere kredittkort og lignende informasjon for å komme raskere gjennom innsjekking. Bakdelen med dette er konsekvensene av at informasjonen blir stjålet eller misbrukt, noe som har medført en viss skepsis til slike løsninger.

2.7 Oppsummering

Kapittelet har gitt en bred introduksjon til ikke bare datalagringsdirektivet, men også satt det i en sammenheng. Direktivet må ikke vurderes isolert sett men må sees i lys av hensikten, bakgrunnen, alternativene og argumentene både for og imot. Direktivet har til hensikt å harmonisere lovgivningen som regulerer lagring av trafikkdata for å bidra til å stanse alvorlig kriminalitet. Dette vil kreve endring av nasjonale lover og representerer et skille fra å lagre trafikkdata på grunn av fakturering- eller driftsformål til å lagre de av hensyn til etterforskningen av kriminalitet. Det er dette skillet som har vært kilden til kontrovers, noe som i liten grad har preget de andre formene for datalagring som eksisterer i dag. Direktivet har møtt ikke bare motstand blant interessegrupper men også tverrpolitisk motstand med unntak av noen partier som har valgt å ikke uttale seg.

Datalagringsdirektivet er del av en ny trend innen lovgivning som regulerer kontroll og lagring av kommunikasjon og informasjon. Flere eksempler på lignende lover har blitt gått gjennom i kapittelet for å sette direktivet i sammenheng. Innføringen av direktivet i andre land er også tatt med da Norge er i en særstilling og må innføre direktivet som del av EØS-avtalen og ikke som EU-medlem.

3 Implementering i teknologiene

Dette kapittelet vil dreie seg om implementeringen av DLD i aksessteknologiene. Kapittelet vil ta for seg hvor stor endring som må til i de tekniske løsningene for å kunne lagre trafikkdata ved bruk av mobiltelefoni, datatrafikk over Internett, IP-telefoni og e-post. I tillegg til de tekniske løsningene vil endringen i graden av personvern bli vurdert. Deretter vil de tekniske konsekvensene av datalagringen bli oppsummert og konsekvensene av et eventuelt misbruk av data vil bli vurdert. Til slutt vil en modell for sentralisert lagring av trafikkdata bli foreslått.

3.1 Telefoni

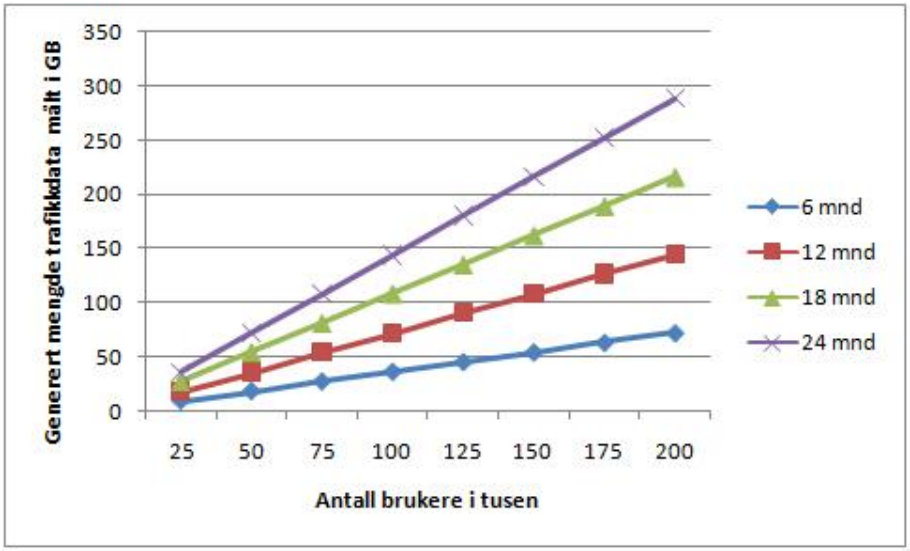
Lagring av trafikkdata i forbindelse med telefoni er velkjent og mye brukt. Trafikkdata kalles innen telefoni Call Detail Record (CDR) og inneholder alle punktene som datalagringsdirektivet nevner. Det er dette som brukes som et grunnlag for fakturering. En trend innen telefoni er teknologimigrering - kunder migrerer i stor grad fra fasttelefon til mobiltelefon og fra vanlig fasttelefon til IP-basert fasttelefon. En annen migrering er at brukere bytter fra betaltjenester fra en teleoperatør til gratistjenester over Internett, som Skype og lynmeldingsklienter. Disse tjenestene har ikke tatt over telefonmarkedet ennå, men representerer en mulig utvikling som også vil ha konsekvenser for verdien og tilgjengeligheten av trafikkdata.

Mobiltelefoni

Implementeringen av DLD for mobiltelefoner vil kreve lagring av en del ulike data. Det som skal lagres er nummeret som ringer, med abbonementdata og nummeret som mottar, også med abonnementdata. Tidspunkt og lengden av samtalen skal registreres, samt ubesvarte anrop. I tillegg skal type tjeneste som er brukt bli registrert. Et eksempel på dette er viderekobling av samtaler. International Mobile Subscriber Identity (IMSI) og International Mobile Equipment Identity (IMEI) er globalt unike identifikasjonsnummer for henholdsvis abonnent og telefon, og skal også lagres. For å registrere lokasjonsdata skal Cell ID registreres.

Størrelsen på denne datamengden er i dag ca 300 byte pr logginnslag. [51] Det betyr at hver gang det gjennomføres en samtale vil operatøren lagre ca. 300 byte. Denne informasjonen lagres i dag i forbindelse med faktureringsformål i henhold til Ekomloven. Teknisk sett må lagringstiden endres fra dagens praksis med tre til fem måneder, til den tiden som blir satt i regelverket. [82]

Figur 1 viser mengden data som vil bli generert ved lagring av trafikkdata fra mobiltelefoni. X-aksen er antall brukere i tusen, og Y-aksen er antall GB



Figur 1: Lagring av trafikkdata for mobiltelefoni.

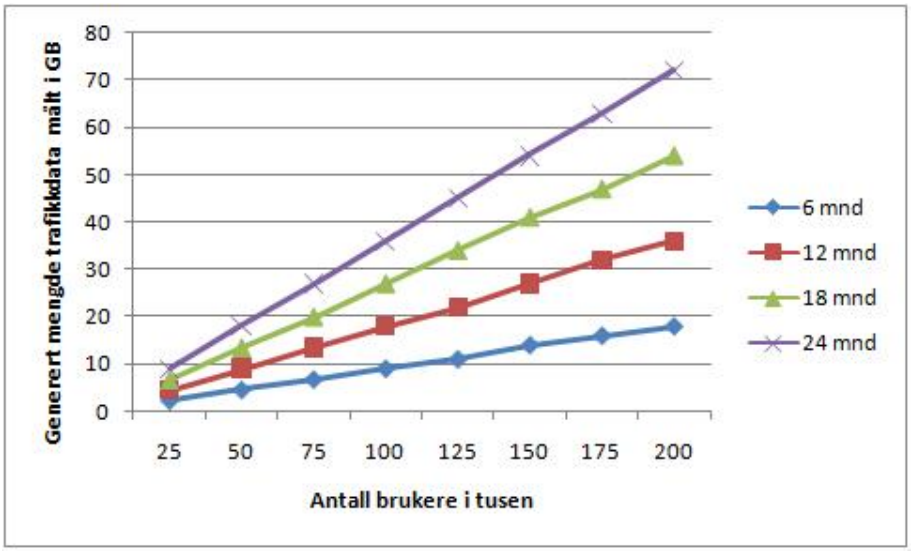
med genererte loggdata. De ulike funksjonene representerer antall måneder med lagring. Grunnlaget for utregningen er at hvert logginnslag er på 300 byte og at både telefonsamtaler, sms og mms genererer et logginnslag som er like stort. Forbruket er basert på tall fra telepriser.no, som er en pris- og forbrukskalkulator for teletjenester laget av Post- og Teletilsynet. Det er tallene fra et middels forbruk som er lagt til grunn. Middel forbruk for mobiltelefoni er 68 samtaler, 119 sms og 5 mms per måned.

En implementering av DLD vil medføre en marginal endring, og kan således sies å ha lite påvirkning i forhold til personvernet. Informasjonen lagres allerede, og det er i forbrukeres egen interesse at slik lagring finner sted da det vil kunne bidra til å kontrollere og etterprøve faktureringen fra tjeneste- og innholdsleverandører. Denne typen informasjon har allerede blitt brukt i etterforskningen av kriminalsaker, og har blant annet bidratt til oppklaring av Baneheia- og Knutby-sakene. Disse to sakene vil bli nærmere redegjort for i kapittel 4.

PSTN

Public Switched Telephone Network (PSTN) er det offentlige telefonnettet basert på oppkobling via kobbertråder, som i Norge er eid av Telenor. Nettet vil bli underlagt den samme registreringsplikten som for mobiltelefoni. Den eneste forskjellen er at dette systemet er stasjonært og derfor er ikke Cell ID, IMEI eller IMSI relevant.

PSTN er på samme måte som mobiltelefoni fakturert på bakgrunn av forbruk, og dermed er data som DLD beskriver allerede lagret, dog med en kortere lagringstid enn rammene direktivet fastsetter. Telefoni og mobiltelefoni behøver omtrent samme mengde data for å loggføre en samtale.



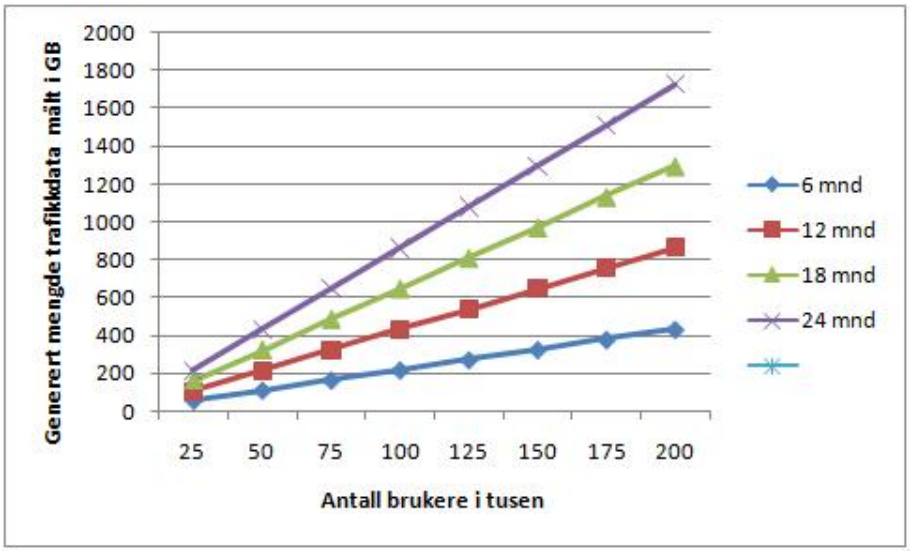
Figur 2: Lagring av trafikkdata for fasttelefoni.

Ut fra figur 2, ser man at uansett lagringstid og abonnenttall så er datamengden beskjeden i databasesammenheng. Grunnlaget for dette er at middels forbruk for fasttelefoni på telepriser.no er 51 samtaler i måneden. Et lite antall samtaler kombinert med en liten størrelse på logginnslaget gjør lagring av trafikkdata for fasttelefoni svært effektivt i forhold til datamengden. Dette står i sterk kontrast til logging av IP-telefonsamtaler, som kan kreve opptil ti ganger så stor lagringsplass. [51] Endringen i personvernspørsmålet for PSTN

ved en innføring av DLD vil være det samme som for mobiltelefon, det vil si en forholdsvis liten endring i fra dagens praksis. Dagens ordning med lagring av trafikkdata i tre-fem måneder har ikke blitt grunnlag for debatt hittil.

IP-telefoni

Loggstørrelsene for IP-telefoni varierer noe fra kilde til kilde, noe som kan forklares med at det er opp til tjenestetilbyderen hvilke felt som logges og med hvilken størrelse. Tallene på loggstørrelser varierer fra 3kB til 6kB, hvor det største tallet er hentet fra en norsk teleoperatør. I beregningen er som er grunnlaget for figur 3 er en loggstørrelse på 6kB lagt til grunn, sammen med forbruksdata fra telepriser.no som er det samme for fasttelefoni som for IP-telefoni, 51 samtaler i måneden.



Figur 3: Lagring av trafikkdata for IP-telefoni.

Figuren har antall brukere på X-aksen og antall GB med trafikkdata på Y-aksen. Mengden trafikkdata for 200 000 brukere lagret i to år vil bli i underkant av 1,8 terabyte med data, som er en betraktelig men overkommelig mengde data for en database. På lik linje med mobiltelefoni er lagring av

CDR for PSTN noe som foregår i dag, og har en rekke funksjoner relatert til forretningssiden av virksomheten. Denne lagringen er ikke utviklet med bistand til myndigheter som grunntanke, men kan også benyttes til dette. Lagring av CDR framstår som en fornuftig praksis som bør fortsette. IP-telefoni har derimot en spesiell utfordring, og det er at adressedata sendes over Internett, noe som gjør at det er mye enklere å avlytte og fange opp enn for de andre telefonteknologiene. Dette er blant annet fordi det ikke trengs spesielt utstyr, noe som tilsier at dette bør være et fokus om man skal vurdere personvernet blant de ulike IP-telefontilbyderne.

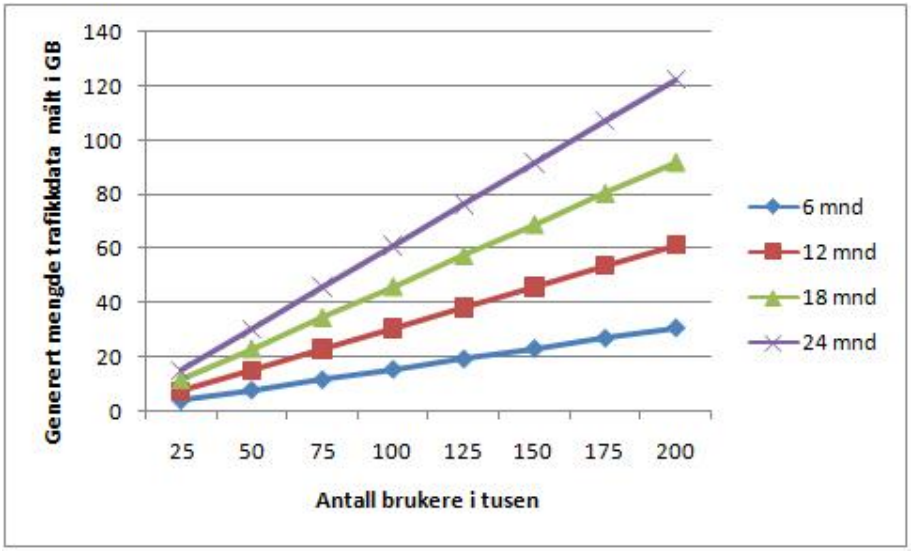
3.2 Internett

Internettrafikk skal logges ved hjelp av å knytte IP-adressene til avsender og mottaker opp mot brukerkontoer med navn og adresse samt tidspunkt og varighet av sesjonen.

IP-logger er det viktigste verktøyet for å etterforske kriminalitet hvor datatrafikk er av interesse. Det er også i tjenestetilbydernes interesse å ha disse loggene, ikke bare for å kunne bistå politiet, men også i forbindelse med fakturering ved en forbruksbasert tjeneste, samt for å kunne kontrollere at tjenestevilkårene overholdes. En mer detaljert diskusjon av bruken av denne typen data i forbindelse med etterforskning kommer i kapittel 4.

I direktivet står det spesifisert at det er IP-adressen som skal lagres. Dette fører til at en identifiserer hvilken juridisk eier som har hatt en IP-adresse på et gitt tidspunkt, men det identifiserer ikke hvem som har brukt tjenesten. Man identifiserer ikke brukeren fordi man kan ha mange brukere og ulikt brukerutstyr koblet til et aksesspunkt som gir internettilgang. For å entydig identifisere brukerutstyret måtte man lagret termineringsadressen, ikke bare for modemet, men også termineringsadressene til alt brukerutstyret som fantes i det lokale nettverket brukeren har. Når termineringsadresser ikke lagres gir dette en trygghet i forhold til personvern, men en utfordring i forhold til etterforskningen av kriminalitet, spesielt nå som trådløse aksesspunkt er blitt vanlige. Temaet blir diskutert videre i kapittel 4 og 5.

Logger over internettilgang kjennetegnes ved mye lavere antall innslag i loggene enn for de andre kommunikasjonstjenestene. Dette er på grunn av at teknologien som brukes til bredbånd angir samme IP-adresse til en bruker over lengre tid, gjerne flere døgn. Tallene som er lagt til grunn i utregningen er logginnslag på 1,7kB og 15 innslag pr bruker pr måned. Det er viktig å påpeke at dette gjelder bredbåndskunder og ikke trådløs Internett via for eksempel WiMAX eller internettilgang via teleoperatørene. WiMAX er ennå lite utbredt og derfor fins det lite erfaringsgrunnlag å gjøre beregninger ut i fra. Internettilgang via teleoperatører er stadig mer populært og økningen av telefoner som er i stand til å sende og motta datatrafikk gjør at datat-



Figur 4: Lagring av trafikkdata for IP-aksess.

jenester via teleoperatører øker i omfang. Disse datatjenestene har typisk korte sesjoner, noe som kan være et resultat av flere årsaker, både at flere abonnementstyper tar betalt for datamengden man laster ned, og at datatrafikk for håndholdt brukerutstyr er for strømkrevende til å stå på hele tiden. En konsekvens av dette er at det kan bli flere logginnslag. I motsetning til tradisjonelt bredbånd, gis IP-adresser rett til brukerutstyret. Dette gir en sikkerhetsmessig gevinst, ved at det er langt mindre sannsynlig at oppkoblingen kan misbrukes eller deles blant flere brukere. IP-adressen vil typisk assosieres med termineringsadressen til nettverkskortet i en mobiltelefon eller annet utstyr. Dette kan igjen benyttes til å spre internettilgang til andre brukere, men dette er langt mindre vanlig enn for vanlig bredbånd. Det vil derfor være vesentlig lettere å koble bruker til IP-adresse og relevant aktivitet enn for bredbånd.

Å implementere kravene i DLD vil være enklere for de store aktørene enn for de små. Det kreves kompetanse for både å implementere, utvikle og drifte denne typen løsninger. Det er enklere for store aktører å tilegne seg og beholde denne kompetansen enn de små, og en av utfordringene er finansiering av løsningene. I dag dekkes tilrettelegging av tilgang til informasjon

og elektronisk kommunikasjon av staten i henhold til ekomloven, men det er uttalt at kostnadene for DLD skal dekkes av tjenestetilbyderne. [14, 75]

En spesiell utfordring i forhold til internettrafikk er Community Networks, som baserer seg på at man tilbyr internettilgang, e-post og andre tjenester gratis til brukere. [96] Dette kan i stor grad sammenlignes med den gratis tilgang og bruk av Internett som norske biblioteker tilbyr, bare på en større skala. Denne typen tjenestetilbud har i mange tilfeller ikke registrering eller svært liten grad av registrering ved bruk av tjenester. Dette vil føre til at det kan finnes tilbydere hvor data lagres, men at disse ikke kan knyttes opp mot en bruker som lett kan identifiseres. Denne typen nett har liten utbredelse, men er like fullt en gråsone i henhold til direktivet.

En problemstilling som er spesielt interessant for internettrafikk er at DLD omfatter *offentlige kommunikasjonsnett*, noe som betyr at tilbydere som for eksempel universitet og bedriftsnett er ikke omfattet av direktivet. Denne definisjonen står i Ekomloven [75] §1-5, definisjon nr 7. Dette medfører at et stort antall brukere ikke er underlagt direktivet, men kan likevel rammes av det dersom trafikken logges hos mottakerens tjenestetilbyder, såfremt denne er en offentlig tilbyder. Dette kan bli eksempelvis bli et smutthull dersom ansvaret for logging tillegges tjenestetilbyderen hos den som tar initiativet til kommunikasjonen. Universiteter logger av egeninteresse både med tanke på brukervilkår og kvalitetskontroll av tjenestene, men det vil kunne bli en ulikhet i lovgivningen for aktører som i realiteten tilbyr samme tjeneste.

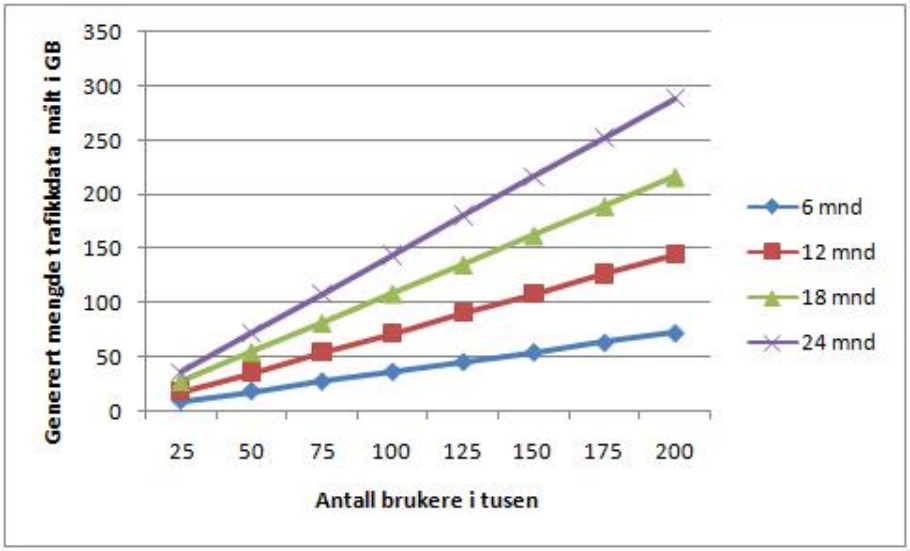
3.3 E-post

Lagring av trafikkdata for e-post er noe som ikke gjøres i dag og formatet er også ulikt det som lagres for andre kommunikasjonsteknologier, da adresseinformasjonen i seg selv inneholder brukerdata. Grunnen til at adresseinformasjonen i større grad inneholder brukerdata er at trenden for e-postadresser viser at man går bort fra konvensjonen brukernavn@bedrift.no. Det kan være problematisk å finne frem til brukeren av denne typen adresser, kontra en standard som for eksempel fornavn.etternavn@bedrift.no. Dette gjør at kommunikasjonskartlegging av e-post vil bli svært enkelt og at brukere ikke uten videre kan dra nytte av anonymiseringen beskrevet i kapittel 3.6.

Trafikklogger for e-post er normalt sett lite brukt som bevis [101], noe som kan forklares ved at datautstyr normalt sett beslaglegges som et ledd i etterforskningen. Politiet kan dermed få direkte tilgang til all relevant e-post. Logging av e-posttrafikk er i langt større grad en inngripen i privatlivet enn loggingen av andre tekologier. Som nevnt over vil loggene i større grad inneholde informasjon om hvem som snakker med hvem i klartekst, uten behov for oppslag av hvem som er brukeren av e-postkontoen. Det eneste positive er at denne typen logger vil være en tredjeparts bekreftelse på at e-poster som blir funnet på beslaglagte datamaskiner faktisk er sendt og mottatt.

Figur 5 viser et anslag på datamengden som vil bli generert ved lagring av trafikkdata for e-post. Beregninger for e-post er, i langt større grad enn ved andre kommunikasjonsteknologier, basert på basert på forutsetninger som kan endre seg i takt med forbruksmønster. De relevante forutsetningene er at en privat bruker sender ca 120 e-poster i måneden hvor mengden relevante trafikkdata er ca 2kb pr e-post. Tallene er definert med bakgrunn i *privat* bruk av e-post, noe som er vesentlig for blant annet antall mottakere som er en vesentlig del av logginformasjonen.

Direktivet sier ikke noe om lagring av trafikkdata for søppelpost, bedre kjent som "spam". Dette er svært vesentlig, da rundt 85% [39] av all e-post som sendes globalt er spam. Det finnes en rekke teknikker for å be-



Figur 5: Lagring av trafikkdata for e-post.

grense mengden spam og en av disse er å be e-posttjeneren som sender om å vente på grunn av stor trafikk. Dette medfører at man unngår å motta søppelposten, da en tjener som sender søppelpost vil normalt kun vil prøve en gang. Spørsmålet er om dette skal loggføres som e-post som er blitt forsøkt sendt, eller om det skal ignoreres. Dette er den type problemstillinger man typisk ikke finner i lovtekster eller forskrifter, men som er svært vesentlige. En annen teknikk er filtrering, hvor man sorterer posten som kommer inn under seriøs post og søppelpost. Et interessant spørsmål er om man skal logge søppelposten eller om denne er unntatt? I den hensikt å etterforske kriminalitet relatert til søppelpost, kan det være nytteverdi i å loggføre den. Man må i den sammenheng vurdere kost- mot nytteeffekt, sett i lys av den enorme mengden søppelpost. Kriminaliteten relatert til spam er masseutsendelse, innbrudd i e-postservere, tyveri av e-postkontoer og svindel med mail.

3.4 Konsekvenser av innføring

Den største konsekvensen av en innføring av DLD, er at lagring av trafikkdata blir satt i system og underlagt et større regelverk enn i dag. Det vil også settes en klar begrensning på hvor lenge logger skal beholdes. For både telefonitjenester og internettilgang vil det bli utvidet lagringstid, men ingen større endringer utover dette. Internettilgangslagringen settes i system i større grad enn tidligere. E-post er den teknologien som utsettes for den største endringen og er den som er minst forutsigbar i datavolum. Det er også denne teknologien hvor det kan stilles det største spørsmålstegnet ved om har en reell nytteverdi, selv om det teknisk sett ikke vanskelig å få tak i og lagre de relevante data.

Systemene for å lagre og gjøre oppslag i alle disse data kommer til å bli en kostnad. Inntil man får et norsk regelverk som spesifiserer hvilke data og metadata som skal lagres, er det vanskelig å fastslå mengden data som må lagres. Dette er viktige forutsetninger for kostnaden på systemene som enten skal anskaffes eller utvikles. Det finnes svært mange tilbydere av løsninger for å håndtere CDRdata og flere aktører som har laget helhetlige løsninger som er spesifikt myntet på å tilfredsstille kravene i DLD. To eksempler blant mange tilbydere er HP DRAGON [40] og løsninger fra SUN [79]. HP DRAGON er det systemet har mest tilgjengelig dokumentasjon og skriver i [41] at systemet i dag håndterer 800 millioner CDR per dag hos en mobiloperatør i Spania. I forsøk med oppslag som kan være relevant for politiet, leverte systemet jevnt resultater på under 5 minutter i et datasett på 20 milliarder CDR.

Egenutvikling av løsninger eller anskaffelse av kommersielle systemer kan til en viss grad være konkurransevridende i favør av de store aktørene. Dette kan reduseres ved å innføre en sentralisert lagring som beskrevet i 3.7. Den foreslåtte løsningen vil også kunne forenkle tilsynet med lagringen av trafikkdata og standardisere formatene på logger. En bakdel er at datamengden vil bli mye større når den samles i ett system.

Databasesystemer har flere ressursbegrensninger enn harddiskstørrelsen, det viktigste i et databasesystem er å få skrevet og lest data til og fra harddisker, noe som stiller krav til kapasiteten som må være tilgjengelig inn og ut av systemet.

Hvis tallene fra IP-telefoni i kapittel 3.1 legges til grunn da denne tjenesten har den absolutt største datamengden og vil kreve mest båndbredde, så kan et anslag settes opp. Trafikkdata for 100 000 brukere av IP-telefoni over 12 måneder vil bli 450GB, på en måned utgjør dette 37,5GB. Dersom man også antar at 70% av samtalene vil skje innen en 8 timers periode så blir det $\frac{1{,}25GB/dag \cdot 70\%}{8t} = 112mb/t$, $\frac{(112MB \cdot 10^6)}{(1000 \cdot 3600)} = 31,1kBps$ med input til databasesystemet.

I 3.1 ble det fastslått at et logginnslag for IP-telefoni er 6kB som vil si at databasesystemet må klare 5,2 transaksjoner per sekund i snitt.

Hvis forbrukstallene for mobiltelefon legges til grunn, siden disse har høyest antall transaksjoner på en måned, så utgjør det 192 transaksjoner/måned som blir 6,4 transaksjoner/dag. Dersom en tjenestetilbyder har 100 000 brukere og 70% av trafikken er innenfor 8 timer så er resultatet 15,5 transaksjoner/sekund.

En SATA harddisk har 11 millisekunders søketid, overføringshastighet på 300 MBps og vil trenge 3 skrive- og leseoperasjoner per innslag i databasen. Lagring av et innslag for IP-telefoni på 6kB vil da kreve $3 \cdot 11ms + \frac{6kB}{300MBps}$, resultatet blir 34ms. 5,2 slike operasjoner trenger 178ms. Tilsvarende tall for 15,5 innslag for mobiltelefondata blir 512ms.

Anslagene basert på tall som er relevante for norske forhold illustrerer at databasesystemer for datalagring ikke vil være problematisk. Databasesystemer vil benytte seg av høyhastighets harddisker, RAID og flere servere i parallell for å øke kapasiteten langt utover tallene som er brukt i eksempelet.

3.5 Misbruk

Lagring av data om kunder og deres bruk av ulike tjenester fører til et potensial for misbruk. Konsekvensene av dårlig sikring av lagrede data, utro tjenere og usikrede nettverk kan bli misbruk, noe det finnes flere eksempler på.

Et godt eksempel på manglende sikring av brukerdata som førte til misbruk, er de ca 100 000 navn, fødselsnummer, kredittkortinformasjon og adresser som ble tappet fra brukerdatabasene til Combitel, Telenordic og Tele2 i august 2007. Saken fikk et etterspill og pågår ennå. Sakene mot teleoperatørene for brudd på personopplysningsloven §13 ble henlagt på grunn av mangel på bevis. Det graverende i denne saken er at operatørene ble varslet av PT på forhånd om svakheten, uten at denne ble rettet på før misbruket fant sted. [16, 15, 19]

Misbruk av datamaskiner ved hjelp av fjernstyring kan føre til at en datamaskin kan bli delaktig i et dataangrep uten at maskinens eier er klar over det. Denne typen fjernstyring utnytter prosesseringskraften og båndbredden datamaskinen har, maskinen blir del av et såkalt botnet, som kan samle tusenvis av maskiner i målrettede angrep. Dette fører til en interessant juridisk problemstilling om hvor langt eierens ansvar strekker seg. Kan det kalles uaktsomt å ikke ha antivirusprogramvare på datamaskinen, eller er det bare uvitende?

Utro tjenere er en trussel som vil eksistere uavhengig av hva slags organisasjon det er snakk om. Utro tjenere er en spesiell trussel å beskytte seg mot, da de kan omgå sikkerhetsmekanismer som i utgangspunktet er gode nok for eksterne angrep. Et godt eksempel på salg av lagrede data, er tilfellet der kredittkortinformasjon tilhørende kongehuset ble solgt til ukebladet Se og Hør. Dette tilfellet kan sees på som direkte overførbart til teledata. Hvor og hva en person handler kan være like interessant som hvem vedkommede snakker med. [57]

Innbrudd og misbruk av trådløse nettverk med internettforbindelse er en relevant problemstilling. Det finnes en rekke måter å sikre disse nettverkene

på, som Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) og WPA2. WEP-beskyttelse har vist seg å være svært enkel å omgå, og gjør at individer med rett utstyr og programvare, kan få adgang til nettverk og andres brukerdata. Det er funnet svakheter i WPA, og konsekvensen er at det er i dag mulig å få tilgang til nettverk som bruker denne metoden for å sikre trådløse nettverk. [83] Det ansees i dag som forsvinnende sannsynlig at en angriper vil kunne få tilgang til nettverk beskyttet med WPA2. Dette er svært relevant i forhold til misbruk, da vanlige forbrukere i svært liten grad setter seg inn i hvordan trådløse nettverk sikres best. I [84] er det gjort en undersøkelse av hva slags beskyttelsestiltak brukere benytter for å sikre trådløse nettverk. Resultatene er gjengitt i tabell 1, og resultatet viser at det er enkelt å bryte seg inn i majoriteten av nettverkene.

Tabell 1: Metoder brukt for å sikre trådløse nettverk

Time	No Encryption	WEP	WPA1/2
March 2007	21,8%	46,3%	31,9%
Middle of 2006	23,3%	59,4%	17,3%

3.6 Anonymisering

Anonymisering av data kan være en måte å tilfredsstille både Politiets behov for trafikkdata ved etterforskninger, og Datatilsynets krav til personvern. Det er flere måter å anonymisere data på. En artikkel som er svært relevant på dette området er [34], som beskriver flere måter å anonymisere data på, samtidig som de blir signert for å sikre validiteten.

Den store fordelen med anonymisering er at den kan filtrere innholdet i en database ut i fra hvem som skal se hva. Dette, sammen med å gi brukeren et pseudonym, gjør at personvernet potensielt kan beskyttes mye bedre enn i dag. Dette er et eksempel gjengitt fra artikkelen:

Tabell 2: Opprinnelig tabell

Name	Race	Birth Date	Gender	ZIP	Medical Diagnosis
Frank Miller	white	June 2, 1970	male	45873	chest pain
Mary Ross	white	Apr 10, 1964	female	45875	obesity
Howard Wu	Asian	Jan 17, 1958	male	45875	hypertension
Frank Miller	white	June 2, 1970	male	45873	HIV-related symptoms
Cathy Dunne	black	Sep 20, 1975	female	45874	short of breath

Tabell 3: Redusert tabell

Name	Race	Birth Date	Gender	ZIP	Medical Diagnosis
Patient 1	white	1970		4587*	chest pain
Patient 2	white	1964	female	45875	obesity
Patient 3	Asian	1958		4587*	hypertension
Patient 1		1970	male	4587*	HIV-related symptoms
Patient 4		1975	female	45874	short of breath

Den reduserte tabellen kan fremdeles gjengi mye relevant data, men ingenting som er personidentifiserbart uten å kombinere den med oversikten over pseudonymer. Denne teknikken gir derfor et sterkt personvern, såfremt

listen over pseudonymer gjøres mindre tilgjengelig enn den reduserte tabellen. Den samme artikkelen oppgir at 87% av befolkningen i USA entydig kan identifiseres ved hjelp av kjønn, fødselsdato og postnummer. Dette har bidratt sterkt til å motivere forskning innen denne typen informasjonsutvanning, i den hensikt å beskytte personvernet. Innspillene fra artikkelen kan direkte overføres til datalagringen, og en mulig bruk er foreslått i 3.7.

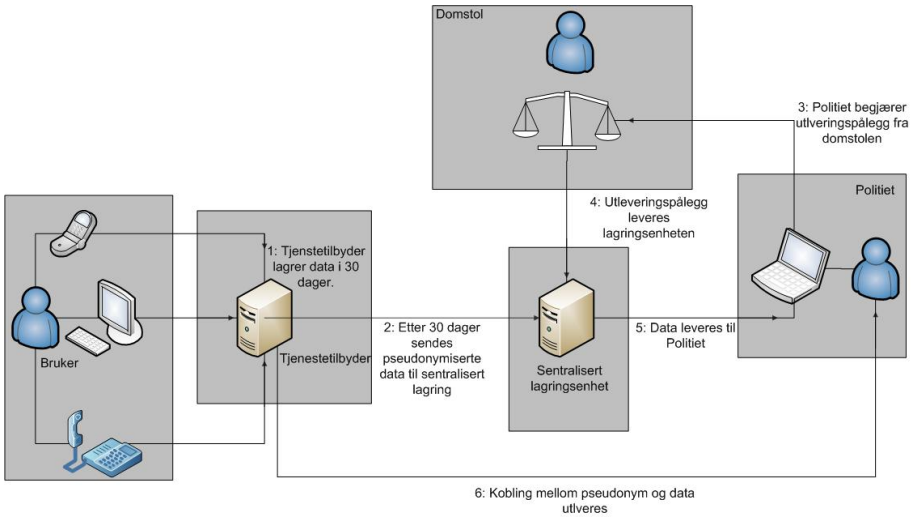
Bakdelen med pseudonymisering og gradvis vasking av informasjon i et databaseinnslag, er at man kan få mye mer data som må lagres i databasen. En kobling mellom navn og pseudonym betyr at man får to navn i stedet for ett. Skal man for eksempel gradvis vaske fødselsdato, kan dette gjøres med flere teknikker. Artikkelen nevner et eksempel hvor 2.juni 1970 kan bli til juni 1970, 1970 eller 1970-1979 og så videre. Poenget med denne gradvise vaskingen er primært personvern, men den kan også bidra til at tilgang til en database kan gis til forskningsformål i større grad en hva man ville gjort om data var i klartekst og så nøyaktige som mulig.

Et kjent problem med databaser er såkalt "function creep", noe som betyr at databasen benyttes til flere formål enn den var opprinnelig ment for. Mange av konsekvensene av function creep kan elimineres ved å vaske informasjon og benytte pseudonymisering. En database med helseopplysninger kan eksempelvis benyttes til forskning uten å bryte med personvernet, men det kan likevel være ytterligere problemstillinger knyttet til om man har vasket *nok* til at man etisk kan gå god for sikkerheten.

3.7 Sentralisert lagring

Det er oppgitt i flere publikasjoner at lagringen av innsamlede data skal ivaretas av tjenestetilbyderne. Dette kan ha sine fordeler og bakdeler. Fordelene er at tjenestetilbyderne til enhver tid har kontroll over de data som deres kunder genererer, og at skaden begrenser seg til en enkelt tjenestetilbyder i tilfelle innbrudd i systemene. Dette kan sees på som naturlig, i og med at disse tilbyderne må registrere og lagre trafikkdata for tekniske- og faktureringsformål uansett. Bakdelen er at kostnaden vil kunne være konkurransevridende ved lengre lagring og at data lagres hos aktører som har telekommunikasjon og ikke datalagring som primæroppgave. Ved et pålegg om lagring hindrer man tjenestetilbyderne fra å rasjonalisere bort store deler av registreringen og loggingen ved overgang fra fakturering basert på forbruk til fakturering av tilgang.

Et alternativ til dette er sentralisert lagring. Det vil her bli foreslått en slik modell som benytter den tidligere diskuterte metoden med pseudonymisering.



Figur 6: Mulig løsning for sentralisert datalagring

Denne modellen er et kompromiss mellom lagringen som foregår i dag, som har en norm på 1-5 måneder, og de 6 - 24 månedene som er lagringsrammene i DLD. Modellen tar bort ansvaret for sikker lagring data fra teleoperatørene.

Data sikres ytterligere mot misbruk ved pseudonymisering før de overføres til det sentrale lageret. Denne modellen gjør at det må opprettes en sentral lagringsenhet samt rutiner for overføring til den. Den sentrale lagringsenheten kan realiseres på hovedsaklig to ulike måter som enten en offentlig eller en privat instans. Dersom det blir opprettet en offentlig instans vil dette øke tilliten til uavhengigheten samt at finansieringen av driften vil være forutsigbar. Bakdelen med en offentlig instans er at det kan ta tid å opprette, samt at det må finnes en politisk vilje til å iverksette og gjennomføre denne endringen. Et alternativ er et privat initiativ til en sentralisert løsning. Dette kan være en av to varianter - enten at det offentlige pålegger operatørene å bruke en slik tjeneste og denne legges ut på anbud, eller at operatørene går sammen og oppretter enheten på eget initiativ. Fordelene med de private løsningene er at de kan komme i gang raskere enn de offentlige og trenger ikke vente på lovpålegg, men heller tilby en tjeneste som det er opp til operatørene å benytte seg av. Denne enheten vil også ha en rendyrket rolle som potensielt kan fjerne hele implementasjonen og driften av dataloggingen fra tjenestetilbyderne. Tilliten til både en offentlig og privat løsning for sentralisert lagring kan økes betraktelig hvis hele systemet gjennomført bruker digital signering av data som lagres og kryptering av data som overføres og lagres mellom alle aktørene i løsningen, inkludert politiet.

Det sentrale lageret skal motta og lagre data fra alle tjenestetilbydere som er pålagt logging. En fordel med et sentralisert lager er at det vil kunne strømlinjeforme og kvalitetssikre formatet på data. Et sentralisert lager vil bidra til å kontrollere at de som skal innhente og lagre trafikkdata gjør dette i henhold til regelverket. En slik løsning vil også ta bort risikoen for at data går tapt dersom en tjenestetilbyder skulle gå konkurs.

Data som lagres i det sentrale lageret skal på ingen måte kunne være personidentifiserbare. Dette er en ekstra utfordring i forhold til e-post da trafikkdata for denne tjenesten i seg selv vil kunne inneholde personidentifiserbar informasjon. En løsning på denne problemstillingen kan være å gi både brukeren og e-postadressen pseudonymer.

Når politiet ønsker å få tak i trafikkdata i forbindelse med en etterforskn-

ing så vil man på samme måte som i dag måtte be domstolene om et utleveringspålegg. Gitt at denne blir innvilget så blir tjenestetilbyderen pålagt å utlevere abonnementsinformasjon, pseudonym og trafikkdata som ennå ikke er sendt til det sentrale lageret, eller eventuelt deler av denne informasjonen avhengig av utleveringspålegget. Den sentrale lagringsenheten blir pålagt å utlevere data som tilhører de pseudonymer som politiet melder inn sammen med kjennelsen fra domstolen dersom utleveringspålegget omfatter dette.

En person som har flere abonnement, for eksempel et mobilabonnement og et bredbåndsabonnement, må ha ulike pseudonymer selv om leverandøren av begge tjenestene er den samme. Dette er fordi at politiet vil be om å få utlevert data enten på grunn av mistanke mot en person eller grunn av trafikk som sees på som interessant. Ber politiet om å få utlevert trafikkdata for en person innebærer dette at man ønsker tilgang på all trafikkdata koblet til personens pseudonymer. Hvis man allerede vet hvilken trafikk som er interessant så kan identiteten til den juridiske eieren av abonnementet være informasjonen som man er ute etter, og eventuelt en dokumentasjon fra tjenestetilbyderen på at brukeren faktisk har generert trafikken. Å gi en person et pseudonym for hver tjeneste som han eller hun får kan virke tungvindt, men er et tiltak for å ivareta og styrke personvernet.

Systemene hos tjenestetilbyderne må takle loggføring av datamengdene beskrevet tidligere i kapittelet. Mengden data vil variere mellom de ulike tilbyderne avhengig av kundemasse og hvilke tjenester som tilbys. Majoriteten av datainnsamlingen som er beskrevet i direktivet gjøres av systemer hos tjenestetilbyderne allerede, men et nasjonalt regelverk som implementerer direktivet kan stille nye krav til oppbevaring av de innsamlede data og hva slags informasjon som lagres. Det finnes kommersielle systemer som er laget spesifikt for å tilfredsstille kravene i DLD, disse ble beskrevet i 3.4. Denne typen systemer er beregnet for bruk av enkeltoperatører og basert på dokumentasjonen så virker et samvirke mellom denne typen systemer og et sentralt lager realistisk. I motsetning til tjenestetilbyderne trenger ikke det sentrale lageret å tilfredsstille kravene om lagring i sanntid og derfor kan også rutinene for samvirke mellom tjenestetilbydernes databaser og det sentrale lageret ta

hensyn for å minimere forstyrrelsen av driften hos tjenestetilbyderne.

Tidspunkt og hyppigheten av overføring av data mellom tjenestetilbydere og det sentrale lageret er praktiske problemstillinger som bør avgjøres ved en eventuell realisering av et sentralt lager, de 30 dagene som er oppgitt i figur 6 er ment som et eksempel.

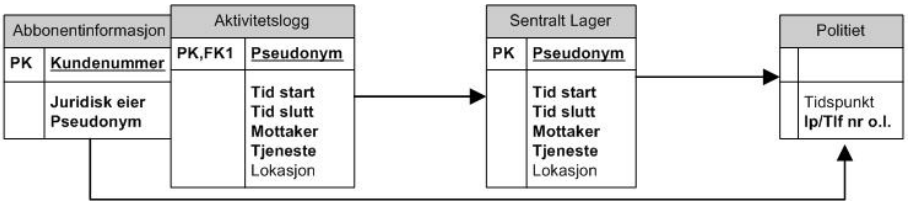
Bakdelen med pseudonymiseringen og sentraliseringen er at man fremdeles må ha en database hos tjenestetilbyderne med en kobling mellom pseudonym og bruker, samt rutiner for å utlevere disse til politiet. Personvernmessig er dette en bedre løsning enn å ha trafikkdata og brukerdata samlet i samme organisasjon gjennom hele levetiden såfremt de sikres mot insidere.

Realisering

En sentralisert lagring kan realiseres på mange forskjellige måter og med mange ulike teknologier. Det vil her bli foreslått en løsning generisk nok til å kunne dekke alle de ulike aksessteknologiene som er tatt med i DLD.

Figur 7 viser et mer detaljert eksempel på innholdet i databasene enn i forrige figur. Tjenestetilbyderen har de to databasene helt til venstre, hvor den ene inneholder kundeinformasjon, kundenummer og pseudonym. For å gjøre det mer oversiktlig er all kundeinformasjon samlet til ett felt, juridisk eier, som i reelle implementasjoner vil bestå av navn, adresse, betalingsinformasjon og lignende. Den andre databasen hos tjenestetilbyderen inneholder en aktivitetslogg for hvert pseudonym med den informasjonen DLD pålegger. Innholdet av denne databasen overføres med jevne mellomrom til den sentraliserte lagringsenheten som tar vare på anonymiserte trafikkdata fra alle tjenestetilbydere underlagt direktivet. Koblingene mellom aktørene foregår ved hjelp av sikre tilkoblinger, for eksempel SSL, og all data som overføres signeres digitalt for å sikre dataens integritet.

Politiet vil ikke ha en database slik som det er skissert i figuren, men vil basere etterforskninger på generert trafikk i enten et gitt tidsrom, telefonnummer eller IP-adresse. Alternativt vil all trafikkdata en person har generert



Figur 7: Forslag til databasestruktur

være av interesse. Basert på et utleveringspålegg fra domstolen kan Politiet be om å få utlevert de relevante loggdata som tidligere beskrevet.

Denne løsningen vil sørge for en balanse mellom lagring av data på grunn av lovbestemmelser og beskyttelse av personvernet til brukerne. Dette systemet kan som alle andre bli misbrukt, men et system basert på separering av aktivitet og kundeinformasjon, samt sikker kommunikasjon mellom aktørene, hever terskelen for misbruk og feil betraktelig. I tillegg reduserer det skaden om en av databasene hos tjenestetilbyderne skulle bli utsatt for innbrudd, da man trenger begge for å få en fullstendig oversikt.

Relevant arbeid

Sentralt i modellen som er presentert er samvirket mellom tjenestetilbydernes databaser og den sentrale databasen, noe som kan sees på som en distribuert database. Det er mange hensyn som må tas dersom man skal koble sammen ulike databasesystemer, utfordringene rundt dette er undersøkt i [80]. De fleste utfordringene er relevante, for eksempel samvirke mellom databasesystemer fra ulike leverandører, design med mer. Noen utfordringer er langt mindre relevante, for eksempel ytelsesproblemer da databasesystemene hos tjenestetilbyderne kun skal skrive til det sentrale lageret og ikke lese. Skrivingen skal også skje med uker eller måneders mellomrom som er en vesentlig forskjell fra konvensjonelle databasesystemer.

I [78] presenteres prinsippene for distribuerte systemer for innbruddsovervåkning i nettverk. Likhetene mellom modellen og distribuerte innbruddsover-

våkningssystemer er at begge er basert i nettverk og er koblet til heterogene innsamlingspunkter. Forskjellene er at innbruddsovervåkningssystemet reagerer på kjente mønster som indikerer et angrep mot nettverket i sanntid, mens datalagringsmodellen lagrer trafikkdata og har de tilgjengelige i tilfelle de trengs.

Det forskes på systemer for trafikkovervåkning på veier som har noen likhetstrekk med modellen som er presentert, men det er mange vesentlige forskjeller som gjør at det ikke er overførbart til problemstillingen rundt sentralisering av datalagring. [10]

3.8 Oppsummering

Dette kapittelet har tatt for seg endringene ved å implementere DLD i de ulike aksessteknologiene og tjenestene, samt et forslag til hvordan en sentralisert lagring kan realiseres. Innholdet i hele kapittelet er basert på informasjon gitt i EU-direktivet, informasjon gitt av kilder i tillegg til eget arbeid. Et viktig forbehold for innføringen av løsningen, er implementeringen av direktivet i norsk lov og tilhørende forskrifter. Det er disse som vil gi tjenestetilbyderne et konkret grunnlag for å utvikle og beregne kostnader for systemer for datalagring. Lagringstid, -type og detaljnivå på data er vesentlige forutsetninger som må på plass før en nøyaktig kostnad kan anslås.

Innsamlingen av data skjer i veldig stor grad i dag som en del av faktureringsrutinene, og er derfor kjente og innarbeidede prosedyrer. Dette skjer med en kortere lagringstid enn det direktivet vil pålegge, men denne endring vil være forholdsvis udramatisk. Lagringen for de tjenestene der man ikke har gjort datalagring før, primært e-post, vil ikke være teknisk vanskelig. Det vil riktignok være en en del betenkeligheter knyttet til reell anvendbarhet i henhold til direktivets intensjon. Andre betenkeligheter er personvernmessige hensyn og hvorvidt man skal lagre trafikkdata som blir generert ved sending av søppelpost.

Det er flere hyllevaresystemer som er beregnet på å tilfresstille det stadig økende antallet lover som pålegger lagring av ulike typer trafikkdata. Disse vil nok øke i antall, spesielt med tanke på at hele Europa skal inn under samme lovverk, og flere andre nasjoner utenfor EU har egne lover som pålegger en form for datalagring.

Et viktig poeng er at utviklingen og konvergeringen av teknologi kan endre forutsetningene for hvordan kommunikasjonstjenester leveres. Det er en trend mot at teknologi konvergerer og at man får tjenester som før hadde ulike nettverk inn på samme nettverk. Et godt eksempel på dette er IP-telefoni som har flyttet mye av telefontjenesten fra det opprinnelige telefonnettet over på et IP-basert nett. Det gjenstår å se hvordan utviklingen vil fortsette og om substituttjester som Skype vil ta deler av telefonmarkedet fra IP-

telefontjenesten. Årsaken til at dette er relevant er at DLD foretar lagring av kommunikasjonen mellom parter, og i mange scenarioer vil tjenestetilbyderen være den mottakene part. Det gjør at man vil ha et ledd mellom sender og mottaker av kommunikasjonen som ikke vil være underlagt direktivet. I kapittel 4 vil denne problemstillingen bli nærmere forklart og undersøkt.

4 Bruk av trafikkdata i etterforskning

Bakgrunnen for innføringen av DLD var å bekjempe alvorlig kriminalitet og harmonisere lovgivningen mellom EU-landene. Dette kapittelet vil se på hvordan etterforskning ved hjelp av trafikkdata kan foregå, og sette dette i sammenheng med kriminaltekniske undersøkelser av elektroniske spor. Det vil bli presentert en del case studies som praktiske eksempler på saker som har brukt denne typen trafikkdata.

4.1 Kriminalteknisk bruk av elektroniske spor

Elektroniske spor er blitt stadig mer vanlige på grunn av endringen i måten vi kommuniserer og handler på. De aller fleste systemer for kommunikasjon, samhandling og betaling baserer seg på elektroniske systemer med ulike grad av logging. Dette kan bidra til etterforskningen og oppklaringen av kriminalitet. DLD har som intensjon å harmonisere og standardisere denne typen lovgivning innen EU og EØS.

For å kunne dra nytte av digitale spor, forutsettes det at handlinger dokumenteres og at man kan ha tillit til det som dokumenteres. Loggføring av aktiviteten i elektroniske systemer er ikke noe som begrenser seg til å kunne dokumentere kriminalitet eller uønskede handlinger. Logging er et viktig verktøy for å kunne feilsøke, dimensjonere og drifte systemer, i tillegg til å dokumentere hva som foregår i systemene. Graden av detaljer i loggene varierer fra system til system og hvilket formål en logg har. Feilretting og etterforskning av kriminalitet har to grunnleggende forskjellige formål og har derfor behov for ulike typer informasjon.

Et viktig prinsipp for å kunne ha tillit til logger er at systemene implementerer prinsipper som sørger for integritet i data, det vil si at endringer og forfalskninger ikke er mulig uten synlige spor. Et av disse prinsippene er at når en logg føres, skal den delen av systemet som skriver loggen ha tilgang til å skrive til logger de selv ikke har tilgang til å lese. Samtidig skal samme del av systemet kunne lese logger den ikke har tilgang til å skrive. Dette prinsippet heter write up / read down og er den type prinsipper man må se etter i system dersom man ønsker å bruke informasjonen som bevis, da det betraktelig minsker muligheten til å endre logger. Et eksempel på et system som har lagt opp til at bevis skal kunne hentes ut på en måte som er hensiktsmessig, er UMTS som har "Lawful Interception" som en del av spesifikasjonen. [61]

Elektroniske spor kan dokumentere aktivitet som uttak i minibank eller telefonsamtaler, men kan ikke bevise hvem som gjennomførte uttaket eller hvem som brukte telefonen. En rekke eksempler på denne problemstillingen

finnes i kapittel 4.3, som tar for seg en rekke case studies. Et av problemene ved interenettrafikk er at direktivet og dagens praksis for logging baserer seg på IP-logger, noe som gir en veldig god indikasjon på hvilken juridisk bruker som har aktivitet knyttet til sitt abonnement, men lite annen informasjon. Dette er fordi at de fleste abonnementer har en IP-adresse til sitt bredbåndmodem og flere brukere på samme IP-adresse. For å la flere brukere, tjenester og nettverksutstyr bruke samme IP-adresse, brukes Network Adress Translation (NAT) og IP-porter. Det fører til at man utelukkende kan bruke tjenesteleverandørens logger til å påvise at aktiviteten kan knyttes til en spesifikt endepunkt, men ikke til en spesifikk datamaskin eller brukerkonto. Problemet forsterkes av at mange brukere benytter trådløse aksesspunkt hvor mange av disse igjen ikke har noen form for adgangskontroll. I ytterste konsekvens kan det føre til at man har en logg hos tjenesteleverandørene påviser aktivitet hos en kunde, men aktiviteten stammer fra en inntrenger på kundens usikrede trådløse nettverk.

Et tiltak for å dokumentere hvem som bruker en tjeneste eller et gitt brukerutstyr er innlogging. Bruk av innlogging er mest relevant for tjenester, og ikke for generelt bruk av Internett eller telefon. Innlogging ved hjelp av biometriske data, for eksempel fingeravtrykk, irismønster og tilsvarende kan bidra til å låse opp og igjen terminaler, og kan bidra til å motvirke misbruk av egne tjenester og kontoer. Bruk av innlogging, uavhengig av om det er passord eller biometriske data, er avhengig av et godt designet system som bidrar til å sikre at tjenester kan knyttes til en bruker med høy grad av sannsynlighet. Dette hensynet er dog i sterk kontrast til personvernhensynene, som på den ene siden ønsker å beskytte brukeren mot misbruk ved hjelp av sikkerhetsmekanismer, men som på samme måte vil beskytte brukeren mot unødvendig overvåkning.

4.2 Bruk og verdien av trafikkdata

Trafikkdata som samles inn når man bruker en tjeneste eller aksessteknologi, kan være av nytte i etterforskning av kriminalitet. For å få tak i disse data, må politiet ha et utleveringspålegg fra en domstol som pålegger tjenesteleverandøren å utlevere data. Utlevering av trafikkdata er noe annet enn kommunikasjonskontroll beskrevet under kapittel 2.3, hvor Politiet har tilgang til innholdet i kommunikasjonen og har anledning til å høre på denne i sanntid.

Verdien av trafikkdata varierer sterkt, noe en rekke eksempler viser i kapittel 4.3. Data kan bidra både til å sjekke mistenkte ut av saker, bekrefte påståtte forhold og bidra som en kritisk del av bevisførselen. I en høringsuttalelse fra datatilsynet om forebygging av internettrelaterte overgrep mot barn, kommer tilsynet med en rekke synspunkter på hvordan politiet må tillegges ansvaret for å forhindre denne typen overgrep og at virkemidler må tas i bruk i takt med den teknologiske utviklingen. Tilsynet poengterer at dette må sees i sammenheng med personvern. Trafikkdata vil uten tvil være en viktig forutsetning for denne typen arbeid, og høringsuttalelsen står i kontrast til de andre uttalelsene datatilsynet kommer med angående direktivet.

Datatilsynet har tidligere pålagt flere operatører å slette aktivitetslogger for internettrafikk etter syv dager. [6] Pålegget ble senere trukket og omgjort til 30 dager etter press og innsigelser fra operatørene selv og Politiet. IP-logger er den røde tråden som gjør det mulig å etterforske internettkriminalitet og derfor er det er derfor en viktig debatt hvor lenge slike logger skal beholdes. Debatten kan bli irrelevant om direktivet innføres, i og med at dette setter rammer for lagringstiden, men det er liten tvil om at syv dager er utilstrekkelig for å kunne bidra til en etterforskning.

4.3 Case studies

En motvekt til argumentene om personvern som brukes i debatten rundt all form for lagring og registrering av informasjon rundt borgere i et land, finner vi i de sakene som løses helt eller delvis på grunnlag av trafikkdata. Det finnes en rekke eksempler på dette som illustrer viktigheten av denne typen informasjon i etterforskninger.

Baneheia

I mai 2000 ble to jenter på åtte og ti år funnet voldtatt og drept etter å ha vært savnet i et døgn. To menn ble pågrepet, siktet og dømt for gjerningene. En av de tiltalte nektet straffeskyld, og deler av bevisene mot ham var trafikkdata som dokumenterte bruken av mobiltelefon i området hvor drapene ble begått i det aktuelle tidsrommet.

Grunnlaget for det som ble kjent som mobilbeviset, var at det rundt tidspunktene for drapene ble sendt og mottatt tekstmeldinger på telefonen til den ene tiltale via en basestasjon i nærheten av åstedet. Dette er nettopp denne typen informasjon som er tenkt lagret i henhold til DLD.

Mobiltelefoner vil hele tiden motta et kontrollsignal som forteller de hvilke basestasjoner som er tilgjengelige, en basestasjon er stasjonær og kan bestå av flere antenner som utgjør egne celler. Man er normalt tilkoblet den med sterkest signal med mindre denne ikke har kapasitet. Basestasjoner har et globalt unikt idnummer som kalles Cell ID. [31] Det at alle basestasjoner og telefoner har unike idnummer gjør at samtaler kan switches mellom alle brukere av GSM. En annen konsekvens av denne unike identifiseringen av endepunktene er at de må være del av trafikkdata for å kunne switche samtalen riktig og når denne informasjonen lagres så har man i realiteten lokasjonsdata.

Lokasjonsdata skal lagres i forbindelse med trafikk. Dermed er det den eller de basestasjonene man er koblet til i løpet av en samtale som registreres

i henhold til direktivet. Det er ikke pålagt å registrere alle basestasjoner en telefon er koblet til når den ikke er del av en samtale. Dette på tross av at man i henhold til GSM standarden hele tiden oppdaterer et sentralt register med hvilken basestasjon man er tilkoblet til enhver tid.

Dette er et svært relevant case, da det ikke bare illustrerer bruken av trafikkdata i rettssaker, men også hvordan dette ikke nødvendigvis er ubestridelige bevis. Det ble prosedert og ført flere ekspertvitner i retten som var uenige om det var dekning på åstedet fra den aktuelle basestasjonen. Dette ble også satt i sammenheng med at en telefon kan knyttes opp til andre basestasjoner enn den nærmeste på grunn av kapasitet og trafikkavvikling. Mobilbeviset ble forsøkt understøttet ved hjelp av målinger, rekonstruksjon og matematiske modeller. Mobiltrafikken ble også sannsynliggjort i retten ved at mobiltelefonen ikke nødvendigvis trengte å være på selve åstedet, men i sykkelvesken til den tiltalte ved drapstidspunktet, og at den tiltalte hadde tid til å begå drap og voldtekt mellom de tekstmeldingene som ble sendt over basestasjonen.

Baneheiasaken er et godt eksempel på at trafikk- og lokasjonsdata kan bidra til å plassere mistenkte i nærheten av kriminelle handlinger uten å ha behov for innholdet i kommunikasjonen. Det er også et godt eksempel på bruk av trafikkdata som samsvarer med hensikten bak direktivet.[88, 94, 89, 91, 95]

Knutby

Knutby-saken er nesten like omtalt i norsk presse som Baneheia-drapene. Bakgrunnen er drapet på Alexandra Fossmo og drapsforsøket på Daniel Linde. Sara Svensson var barnepiken for familien Fossmos barn. Alexandra Fossmos ektemann ble dømt for drapet og drapsforsøket. Blant de tekniske bevisene var tekstmeldinger som var sendt av Helge Fossmo til Sara Svensson. Disse inneholdt kommunikasjon som skulle manipulere Sara Svensson til å ta livet av Helge Fossmos kone. Tekstmeldingene ble gjenopprettet fra Sara Svenssons telefon og brukt av aktoratet som del av bevisførselen. Tekstmeldingene ble beskrevet som "helt avgjørende" i bevisførselen mot Helge

Fossmo.

Denne saken viser at trafikkdata i seg selv ikke trenger å gi gode bevis. Sara Svensson og Helge Fossmo ble dømt for drapet og drapsforsøket. De hadde de to siste månedene før handlingene sendt 1200 tekstmeldinger til hverandre og pratet i 13 timer på telefonen sammen. Når Helge Fossmo ble spurt om tekstmeldingene, forklarte han de som helt normal dagligdags kontakt. Rekonstruksjonen av selve innholdet i kommunikasjonen var i dette tilfellet kritisk. Sett i sammenheng med DLD, vil ikke direktivet lagre innholdet i tekstmeldinger. Det ville derfor ikke vært til særlig nytte i lignende saker, siden selve innholdet i kommunikasjonen er av interesse. [87, 90, 93, 92]

Trafikkdata som beskriver kommunikasjon mellom personer som kjenner hverandre godt vil sannsynligvis bidra med lite informasjon i en etterforskning. Trafikkdata vil være nyttige om de kan bekrefte eller avkrefte handlinger eller lokasjon i tilknytning til den kriminelle handlingen. I knutbysaken var ikke dette tilfellet og politiet kunne bare stille spørsmål angående mengden kommunikasjon som var oppsiktsvekkende stor. Dette er et tilfelle hvor trafikkdata ikke hjalp etterforskningen i noen særlig grad men hvor innholdet var det avgjørende beviset.

K.U. v. Finland

K.U. v. Finland er et søksmål som ble anlagt av K.U. mot staten Finnland på grunnlag av brudd på artikkel 8 og 13 i EMK. Bakgrunnen for søksmålet er at K.U. ble trakassert på en internettbasert datingside i mars 1999, da han var 12 år gammel. Dette forholdet ble anmeldt av K.U., men på grunn av Finsk personvernlovgivning kunne hverken politi eller finske domstoler pålegge tjenesteleverandøren å utlevere opplysninger om hvem som stod bak trakasseringen av K.U. Trakasseringen bestod av et falskt profil av K.U., med en rekke opplysninger som førte til at en eldre mann tok forbindelse og ønsket et møte med K.U. Menneskerettighetsdomstolen kom fram til at Finland hadde brutt artikkel 8 i EMK, og tilkjente K.U. 3000 euro i erstatning. [32]

Denne saken viser at ulike former for personvernforhold kan komme i direkte konflikt med hverandre. Et sentralt tema er i hvilken grad man skal beskytte en potensiell forbryter sitt personvern, eller den som blir utsatt for forbrytelsen. I denne sammenhengen kan man også diskutere hva som skal kunne kalles ytringsfrihet og hva som er kriminell adferd.

Eksempler fra Økokrim

I artikkelen "Fra Økokrim: Lagringsplikt for trafikkdata" skriver økokrim-sjef Einar Høgetveit om datalagringsdirektivet, hva direktivet vil bety i praksis og noen eksempler på saker som har vært løst ved hjelp av den typen informasjon som direktivet skal pålegge å lagre:

Under "Operasjon Kola" ble en belgisk mann i arrestert for seksuelt misbruk av sine døtre. Opprullingen av saken førte etter hvert til 2500 mistenkte, en million mediefiler, 50 000 e-poster og lokaliseringen av 30 barn. Saken ble løst ved hjelp av trafikkdata, og selve etterforskningen involverte Interpol, Europol og politi i 28 forskjellige land.

"Operasjon Sledgehammer" prøvde å identifisere de 150 000 forskjellige IP-adressene som var inne på en kroatisk nettside med bilder av seksuelle overgrep. IP-adressene ble logget over en periode på 72 timer og hadde opphav fra 170 ulike land. Når adressene ble levert til norsk politi var informasjonen verdiløs, da tjenesteleverandørene hadde slettet loggene for de aktuelle datoene.

Høgetveit fastslår at det er få saker av alvorlig art som ikke involverer elektroniske spor i etterforskningen. Han fremhever også muligheten til å benytte elektroniske logger til å fastslå den reelle verdien av for eksempel fremsatte trusler over Internett, hvor man raskt kan identifisere kilden. Videre uttrykker han en bekymring over etterforskning av nettbedragerier. Typiske trekk for bedragerier over Internett eller e-post, er at de går over landegrenser og dermed blir vanskeligere å etterforske. Å lette etterforskningsarbeidet i disse typer saker er et argument som kan forsvare EUs hensikt

bak å harmonisere lovgivning av data- og trafikklagring.

Misbruk av trådløst lokalnett

Et eksempel på konsekvensene av misbruk av trådløse hjemmenett er omtalt i en artikkel i [59]; En familiefar fikk datautstyr beslaglagt etter at noen hadde brukt hans trådløse nett til å laste ned barnepornografi. Det viste seg i etterkant at det var familiens leietaker som var gjerningsmannen. Dette er et godt eksempel på at bruk av IP-logger og andre tekniske hjelpemidler kan brukes effektivt, men også at de har sine begrensninger. Dette spesielt med tanke på at trådløse nettverk med kobling til Internett ofte kan være enkle å misbruke.

Oppsummering av case studies

Casene som er dekket i dette kapittelet er tatt med for å sette den teoretiske bruken av elektroniske spor og trafikkdata i sammenheng med saker hvor dette faktisk har blitt brukt. Det som ikke er belyst i disse casene, er hvordan de samme data kan brukes til å ekskludere mistenkte. Det er tydelig at trafikkdata kan bevise bruken av en gitt abonnent til en gitt tid og sted, men dette alene er ikke nok. Det må også bevises at en person brukte dette utstyret med det abonnementet på det aktuelle tidspunktet og stedet. Trafikkdata sier ingenting om en mobiltelefon er stjålet eller ikke, men gir Politiet et gripbart bevis som kan bidra til oppklaring. Spesielt Baneheia- og Knutbysakene viser både mulighetene og begrensningene ved bruk av trafikkdata og hvordan data kan utnyttes for å bidra til en etterforskning.

4.4 Forfalskning av trafikkdata

Forfalskning eller endring av trafikkdata er en trussel som må tas med når man skal vurdere hvor stor tillit man har til at data som lagres av datalagringsdirektivet er riktige. I et eksempel i [12] analyseres metoden man må bruke for å etterforske og avsløre forfalskede e-postdata. Dette er det mest relevante eksempelet, da e-post er den tjenesten og teknologien hvor brukeren har størst adgang til å endre de data som beskriver kommunikasjonen. I de andre teknologiene skjer registreringen av trafikkdata som en del av nettverkskommunikasjonen under sending av data. Eksempelet gir en god forklaring på hvorfor det i de fleste tilfeller vil være enkelt å oppklare denne typen forfalskning. Hvis man forfalsker en e-post etter innføringen av datalagringsdirektivet, vil faktisk data som er lagret være en tredjeparts dokumentasjon på handlingene og fungere etter hensikten. På tross av dette vil det være en langt større utfordring å oppdage eller å få mistanke om forfalskning enn å etterforske den.

5 Omgåelse av datalagring

Datalagringsdirektivet har som intensjon å bidra til etterforskningen av alvorlig kriminalitet. I kapittel fire ble det gått gjennom en rekke case studies for å gi noen eksempler på dette. Det finnes derimot en rekke teknikker for å unngå registrering gjennom DLD og disse vil bli undersøkt i dette kapittelet. Et argument mot direktivet er at disse teknikkene vil gjøre direktivet lite hensiktsmessig som et etterforskningsverktøy og vil bidra mer til et storebrorsamfunn som tillater overvåkning som en del av hverdagen. Dette argumentet må settes i et perspektiv. Man kan unngå å legge igjen fingeravtrykk ved å bruke hansker, men like fullt dømmes kriminelle på bakgrunn av jevnlig. Teknikkene som gjennomgås i dette kapittelet skal illustrere hvilke utfordringer som kan hindre effektiviteten til DLD. De fleste teknikkene har en teknologisk terskel som forutsetter at de, som bruker de må ha litt større kunnskaper enn hvordan man tar på seg en hanske.

5.1 Proxy

Proxy er en betegnelse på en maskin eller et program som opptrer som et mellomledd mellom to parter. Det finnes en rekke bruksområder for proxyer, men det er to hovedårsaker til å benytte seg av en proxy. Den første er anonymitet, som blir fokuset i dette kapittelet, og den andre er hurtig tilgang til ressurser. Det klassiske eksemplet på lagring av ressurser i en proxy for hurtig tilgang, er nyhetssider som hentes av mange. Det blir lite hensiktsmessig å hente den samme nyhetssiden fra opphavsstedet hver gang den skal aksesseres, noe som gjør at proxyen øker hastighet og minsker ekstern båndbredderbruk. I tillegg til dette kan proxyer brukes til å filtrere innhold, eksempelvis skoler som vil ekskludere nettsider med et gitt innhold. Man kan også sette opp en proxy til å avlytte kommunikasjonen mellom parter, noe som kvalifiserer som ondsinnet bruk og kalles "man in the middle"-angrep.

Fordelene med denne teknologien er en reduksjon i trafikkmengden når den brukes til å forhåndslagre nettsider. Anonymitet og frihet er et av de store poengene bak Internett, men dette er også en av bakdelene når det misbrukes. Anonymitet har mange bruksområder - i tillegg til rene personvernhensyn og beskyttelse mot identitetstyveri eller svindel, er anonymitet viktig i de deler av verden der man kan risikere forfølgelse og undertrykkelse som følge av internettbruk. Et eksempel på dette er Kina hvor proxyer brukes til å filtrere innholdet kinesere får tilgang til, noe som kan omgås ved hjelp av proxyer. Da Kina blokkerte Google, ble tjenesten elgooG satt opp som et mottrekk for å gi tilgang på tross av innholdsfiltreringen som var satt opp. [46]

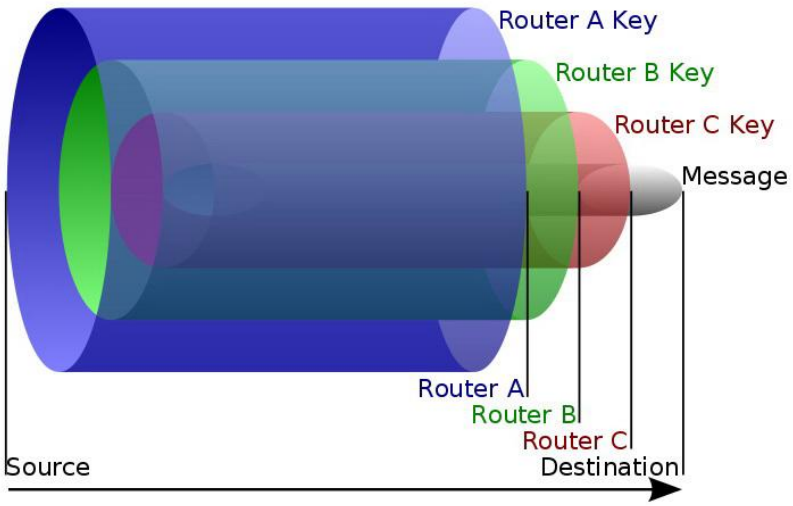
Bakdelene med proxytjenester er at de er gode verktøy for å omgå regler - alt fra en forholdsvis harmløs omgåelse av adgangsregler som bare tillater å gi tjenester til brukere fra enkelte land, til svært alvorlige kriminelle eller terrorhandlinger. De fleste kriminelle kan ha en viss nytte av anonymitet, for eksempel terrorister, økonomisk kriminalitet og personer involvert i ulovlig pornografi.

Proxyer kan bli fremstilt som de kriminelles hellige gral i søken på anonymitet, men i praksis er dette en del mer nyansert. Å sette opp og drifte en proxy

har en teknologisk terskel som ligger utover det den jevne bruker har. Man er også avhengig av at proxytjenesten fungerer mens den brukes. I tillegg må man ha tiltro til at proxyen gjør det man tror den gjør, og samtidig være trygg på at personene som er ansvarlig for tjenesten ikke samarbeider med politi eller myndigheter.

5.2 Onion routing

Onion routing eller løkrouting er en teknikk som bruker et nettverk av mellomledd for å maskere hvor trafikken kommer fra og hvor den skal. Denne lagvise teknikken har blitt sammenlignet med en løk, derav navnet. Teknikken har fellestrekk med konvensjonell bruk av proxy, men er mye mer komplekst, da det er snakk om et nettverk og ikke ett enkelt ledd mellom partene. Et annet særtrekk ved løkrouting er at meldingene krypteres lagvis mellom de ulike nodene i nettet før det sendes ut av nettet og mot endelig mottaker. Et annet prinsipp innen løkrouting er at meldingene skal sendes innad i nettverket på en nettverkssti som er uforutsigbar. Dette kombinert med kryptering gjør at en node kan være fiendtlig uten at dette kompromitterer sikkerheten til informasjonen som blir sendt via den.



Figur 8: Illustrasjon av løkrouting[98]

TOR

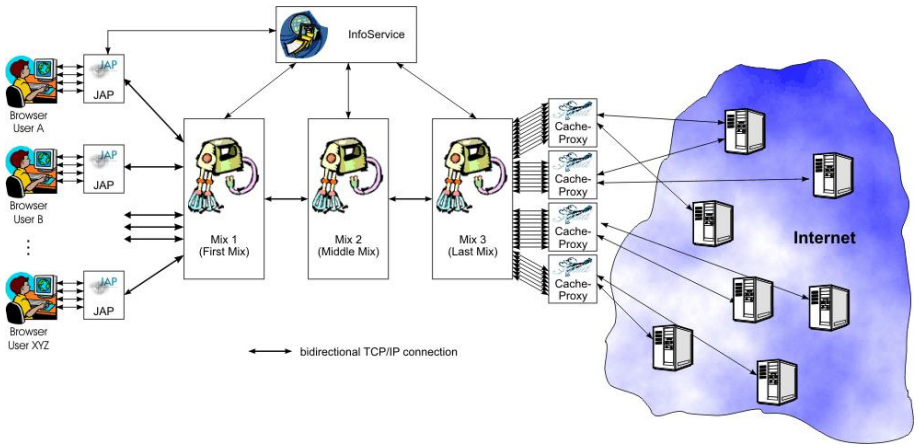
TOR (The onion router), er implementeringen av forskningen på løkrouting. Systemet er fritt tilgjengelig og kjører i dag som en tjeneste på Internett. Målene for tjenesten er enkelhet og plattformuavhengighet, noe som gjør at brukerterskelen er lav og det kan installeres de fleste typer operativsystemer. I [30] beskrives problemstillingen bak TOR, som er metoder for å unngå trafikkanalyse og bevare anonymitet. Artikkelen gir også en oversikt over trusselbildet mot TOR, som inkluderer bruk av TOR til å anonymisere kriminell aktivitet og TOR-noder som tilhører noen som ønsker å få tilgang til informasjonen i datastrømmene som går i nettverket.

I [38] beskrives det hvordan e-post kan sendes anonymt gjennom et TOR-nettverk. Det er viktig å bemerke at oppkobling gjennom en tjenesteleverandør underlagt DLD vil medføre anonymitet for internettkoblinger, men e-post vil fortsatt lagres hos tjenesteleverandøren. Dette kan omgås ved å bruke en e-posttjenesteleverandør som ikke er underlagt direktivet.

Tjenester som TOR er på ingen måte en totalløsning som løser alle utfordringer knyttet til anonymitet og sikkerhet. Dette ble gjort svært klart av en hendelse i slutten av 2007. En svensk sikkerhetskonsulent utnyttet en svakhet og fikk tak blant annet passord til mer enn 1000 e-postkontoer. En god del av disse var e-postkontoer tilhørende ambassader og industrikonserner. Denne informasjonen hadde ikke vært mulig å få tak i om brukerne av TOR hadde kombinert konfidensialiteten av sender og mottaker som TOR nettverket tilbyr med integriteten og konfidensialiteten av innhold som SSL tilbyr. [74] Bruk av SSL er anbefalt på TORs sider for å få gjennomgående sikkerhet.

5.3 JonDonym/AN.ON

JonDonym/AN.ON[45] tjenesten er også en lagvis tjeneste som TOR, men har en noe annen struktur. I stedet for en sti som bygges gjennom et nettverk på en uforutsigbar måte, sendes trafikken i JonDonym gjennom egne såkalte Mix-servere som blander trafikken før den sendes ut av nettverket. Denne tjenesten benytter seg også av kryptering mellom partene som tar del i nettverket.



Figur 9: Arkitekturen for JonDonym/AN.ON[43]

Noe som skiller TOR og JonDonym, sett bort fra strukturen, er at JonDonym er underlagt den tyske implementeringen av datalagringsdirektivet og logger trafikkdata i henhold til dette. Informasjonen som logges er IP-adressen på innkommende tilkobling til første Mix-server og deretter kanalnummeret på mellomliggende og utgående Mix-servere. I tillegg logges portnummeret og tidspunkter for utgående tilkoblinger.[44] Dette forteller en hel del om kommunikasjonen som foregår over dette nettverket. Det logges derimot ikke hvilke nettsider eller IP-adresser man kobler seg til. Dette betyr i realiteten at man har en tilsvarende mulighet til å dokumentere aktiviteten over JonDonym nettverket som man har når man går via en kommersiell tjenesteleverandør for internettjenester. Konsekvensen av dette er at bruksområdet for JonDonym begrenses til å anonymisere sin nettaktivitet ovenfor

andre enn myndighetene. Dette er en fordel med tanke på arbeidet mot kriminalitet, men er dertil betenkelig når et system laget med det eneste formål å tilby anonymitet blir pålagt å logge informasjonen som gjør det mulig å identifisere den parten som kommuniserer ut via tjenesten og trafikkmønsteret denne har.

5.4 Tjenester

En rekke tjenester kan brukes for å omgå DLD. Felles for de fleste av tjenestene som er beskrevet i dette kapittelet er at de er programmer som ligger oppå operativsystemer, altså høynivå, i motsetning til Virtual Private Network (VPN) som er den eneste lavnivåtjenesten som ligger maskinnært.

VPN er en teknologi som tilbys kommersielt og som kan benyttes privat eller i jobben. Poenget med tjenesten er å gi ekstern tilgang til et nettverk. Måten dette løses på er at man sender setter opp en tilkobling mellom brukerutstyret som har internettilgang og en maskin i det interne nettverket som også har internettilgang. Trafikken over denne tilkoblingen loggføres som trafikk mellom disse to partene, men inneholder trafikk mellom brukerutstyret på den ene siden, og den brukeren kommuniserer med inne i det interne nettverket på den andre. Dette er en effektiv maskering av hvem man rellt kommuniserer med. Loggene som internettilbyderen sitter igjen med viser tilkoblingen mellom brukeren og en maskin som befinner seg i det interne nettverket, som i realiteten kan ha fungert kun som et bindeledd til det interne nettverket. Det er en rekke måter å realisere VPN på og mange av disse brukes for å realisere intranett for bedrifter over Internett og lignende og man kan benytte seg av en rekke sikkerhetsmekanismer for å beskytte innholdet i kommunikasjonen. Det finnes mye litteratur om denne teknologien - et sammendrag og lenker til mer spesialisert litteratur finnes i [100].

Microsoft Messenger (MSN) er ett av flere lynmeldingsprogrammer og egner seg godt som eksempel på denne typen tjeneste. MSN er basert på en proprietær Microsoft-protokoll som har blitt gransket grundig av grupper innen åpen kildekodemiljøet, og resultatet er tredjepartsklienter basert på åpen kildekode som er kompatible med protokollen. Dette har ført til at man har fått kartlagt måten kommunikasjonen i MSN foregår på, og en vanlig samtale mellom to eller flere parter skjer ved at innleggene i samtalen sendes til en server som tilhører Microsoft og videreformidles deretter til den eller de andre parten(e) i samtalen. Unntaket er om man overfører en fil som del av samtalen, noe som vil opprette en direktekobling mellom partene.

Årsaken til at denne tjenesten er interessant, er ikke bare fordi at det er en offentlig form for kommunikasjon som ikke er underlagt DLD, men også fordi bruk av tjeneste ikke direkte kobler samtalepartnere med hverandre i IP-logger. Tjenesten er også en potensiell substituttjeneste for telefon, sms og e-post som er underlagt DLD. MSN er også standard programvare som del av Windows operativsystem, noe som gjør tjenesten tilgjengelig på majoriteten av datamaskiner. I tillegg er MSN tilgjengelig som en tjeneste via nettleser.[29, 54, 55]

Webmail er et alternativ til å bruke en klient på datamaskinen for å jobbe med e-post. Dette omgår ikke direktivet om man bruker webmailen som tjenesteleverandøren tilbyr, da det er bare en alternativ måte å aksessere tjenesten på. Det finnes i hovedsak to smutthull, og det første er å bruke en tilbyder som ikke er underlagt europeisk lov og sende fra denne adressen. Den andre metoden er å la sender og mottaker benytte samme e-postkonto, noe som Al-Qaida brukt som taktikk i forkant av terrorbombingen i Madrid. Når gruppen skulle kommunisere, gikk de inn og skrev en e-post som ble lagret som et utkast. En annen del av organisasjonen gikk inn på kontoen etterpå, leste utkastet, slettet det og eventuelt svarte ved å lagre et nytt utkast. Dette er et godt eksempel på en type bruk som ikke ville blitt fanget opp av direktivet.[85]

Internet Relay Chat (IRC) er en meldingstjeneste som ligner mye på MSN, men som har noen vesentlige forskjeller. Den første er at kontaktene man kommuniserer med i MSN må legges til i en kontaktliste som inneholder e-postadresser hos brukeren. Ved bruk av IRC eksisterer ikke dette, og man har mindre informasjon å gå etter dersom man vil finne ut hvem som har kommunisert med hvem. I motsetning til MSN, er IRC basert på en åpen protokoll, noe som gjør at servere kan settes opp av hvem som helst. Det blir dermed problematisk å kunne pålegge logging av disse tjenestene. Det finnes per i dag ingen lov eller forskrift som pålegger logging av denne type tjeneste og i tillegg kan en server stå et vilkårlig sted i verden. IRC er beskrevet i RFC 1459.

Skype [76] er en IP-telefontjeneste som ikke leveres av et telekomselskap,

men av en programvare som utvikles av programvareselskapet Skype Technologies S.A., eid av Ebay. Det spesielle med Skype er at det i motsetning til vanlig IP-telefoni, som kjøpes av andre kommersielle aktører, er at det er gratis og distribuert system. For å ringe med tjenesten, legger man inn andre brukere i en kontaktliste på samme måte som for MSN. Når de er tilgjengelige i listen, kan man ringe direkte til alle. Skype tilbyr også ringing til fasttelefoner, noe som gjøres gjennom en Skype-sentral. Protokollen som ligger til grunn for tjenesten er undersøkt i [9]. Protokollen er lukket og derfor er resultatene i artikkelen basert på observasjoner, ikke dokumentasjon. Artikkelen slår fast at innlogging skjer mot en Skype-server og at søk etter brukeren man skal kommunisere med skjer distribuert. Det at brukerlokasjonen er distribuert på denne måten, får det til å se ut som at Skype må endre systemene mot sin opprinnelige hensikt for å tilfredsstille datalagringsdirektivet for de samtalene dette gjelder. Hvilke samtaler som eventuelt kommer inn under direktivet er uklart da tjenesten foregår helt eller delvis over Internett. Det er naturlig å tro at samtaler mellom Skype-klienter og det offentlige telefonnettet **kan** bli underlagt direktivet, men dette er en juridisk vurdering som ikke er del av denne oppgaven. Artikkelen slår fast at oppkoblingen til samtalen skjer ved hjelp av TCP-protokollen, mens selve samtalen går over UDP-protokollen. Det betyr at innledningen av samtalen er basert på en protokoll som er egnet for å logging om denne typen bruk faller inn under direktivet.

5.5 Andre omgåelser

Det finnes flere omgåelser som ikke ligger på siden av det som er gått gjennom allerede. Disse er i varierende grad relevante og bør derfor undersøkes på lik linje med de foregående teknikkene.

En enkel metode som er gjør det vanskelig å spore gjerningsmannen er hvis man stjeler brukerutstyr. Mottiltakene mot dette er bruken av PIN-koder og passord. På samme måte som bankkort, kan telefoner sperres av operatøren, noe som også sperrer den misbrukte brukerkontoen. Dette gjør at tyveri av brukerutstyr kun er et problem så lenge man ikke har sperret kontoen, noe som vil kunne gjøres raskt for de fleste typer brukerutstyr.

Et alternativ til å stjele brukerutstyret er å kapre termineringsadressen, noe som kan sammenlignes med å stjele identiteten til brukerutstyret. Dette kan ha en svært varierende nytteverdi for angriperen. Årsaken til at det kan være svært lite effektivt, er at man ikke kan bruke to identiske termineringsadresser samtidig. Det vil oppstå en konflikt om man prøver på dette, så dette angrepet vil kun være effektivt om man utfører det når den legitime brukeren ikke bruker termineringsadressen. Et eksempel på dette er hvis man kopierer termineringsadressen til en bruker i et hjemmenett og bruker denne når den legitime brukeren er på jobb.

Kryptering av trafikk er ikke et ulovlig mottiltak og er heller ikke treffende i forhold til direktivet, men må nevnes for å danne et helhetsbilde. Kryptering av mottaker og avsenderadresse fungerer bare om de som skal være mellompunkter i transaksjonen kan dekode og se adressen til enten sluttmottaker eller neste ledd i kjeden. Dette er på mange måter synonymt med løk-routing og kan også kombineres med løk-routing, som er anbefalt av TOR. Denne teknikken kunne avverget tappingen av brukernavn og passord av e-postkontoer diskutert under TOR. Kryptering er mest hensiktsmessig i forhold til innholdet i kommunikasjon, og er i så måte helt irrelevant i forhold til DLD som bare ser på trafikkdata.

Man kan sende en mengde tom trafikk til mange mottakere for å maskere

hvilken trafikk som inneholder reell kommunikasjon. Denne teknikken kan være hensiktsmessig mot for eksempel industrispionasje og er svært relevant innen militær kommunikasjon, men som et mottiltak mot DLD er den lite effektiv. Teknikken vil være lite effektiv fordi at man ved etterforskning av kriminalitet normalt sett vil vite enten mottaker eller tidsrom som er aktuelt, og dermed kunne sortere ut uinteressant trafikk. Teknikken ligner på padding, som er noe man gjør for å gi all trafikk samme lengde eller størrelse. Dette er noe mer effektivt, da en rekke typer trafikk har svært karateristiske størrelser, men igjen er dette mer hensiktsmessig innen beskyttelse mot kriminelle enn mot registreringen som skjer i henhold til datalagringsdirektivet.

5.6 Oppsummering

Kapittelet har gått gjennom en rekke type omgåelser som kan ha ulik betydning for effektiviteten til DLD. Felles for alle omgåelsene, er at de uansett legger igjen et elektronisk avtrykk som kan etterforskes. De teknikkene som ser ut til å ha størst betydning for direktivet er de som ikke er tilsiktet, altså en migrering av brukere over til tjenester som MSN og Skype, hvor man i stor grad vil kunne se trafikken mellom brukere og servere, men ikke mellom ulike brukere. De tilsiktede tjenestene som TOR og JonDonym legger igjen et elektronisk avtrykk, men vil være effektive til å beskytte innholdet hvis de blir brukt korrekt. Det er derimot betydelig at JonDonym som er en anonymiseringstjeneste er tatt inn under det tyske datalagringsdirektivet og pålagt logging på sine servere. Det er i den sammenheng viktig å påpeke at JonDonym er en kommersiell tjeneste, mens TOR er et åpen kildekodeprosjekt. De mest effektive omgåelsene er kapring av termineringsadresse eller innbrudd i et nettverk og tyveri av brukerutstyr. De er riktignok effektive for å unngå identifikasjon i henhold til DLD, men de er dertil egnet for konvensjonell etterforskning.

6 Konklusjon

Oppgaven har undersøkt bakgrunnen og hensikten for Datalagringsdirektivet og hvilke og hvor store tekniske konsekvenser dette vil ha. Kontroversen rundt direktivet og en gjennomgang av relevante nasjonale og internasjonale lover har også blitt tatt med som bakgrunnsstoff. Flere gråsoner har blitt belyst med tanke på hvorvidt man har anledning til å logge trafikkdata for enkelte tjenester, og om dette er hensiktsmessig, mulig eller kontraproduktivt. Bruken av trafikkdata både med og uten suksess har blitt illustrert, samt at trafikkdata kun utgjør en brøkdel av en helhetlig etterforskning av kriminelle handlinger. Det fins en rekke måter å omgå registrering på, alt fra enkle ikke-tekniske metoder til hele nettverk som har som sin eneste oppgave å motsette seg trafikkanalyse, noe som er hele poenget med datalagringsdirektivet.

6.1 Funn

Direktivet føyer seg inn i en ny trend av lovverk som i stadig større grad lagrer de elektroniske sporene vi legger igjen. Tidligere har denne typen logging vært motivert av dokumentasjon i forbindelse med fakturering, pålitelighets- og ytelsesmessige forhold.

Det har vist seg at endringene fra systemene i dag er liten for noen aksessteknologier eller tjenester og stor for andre. I forbindelse med de klassiske telefontjenestene har alltid trafikkdata blitt lagret på grunn av fakturering eller driftsformål. E-post er den tjenesten som i aller størst grad vil bli endret, hvor man går fra ingen lagring av trafikkdata, til lagring av trafikkdata for alle e-poster som sendes. Det er også denne tjenesten hvor personvernet i størst grad vil bli utfordret. Det er ikke stor forskjell i informasjonen man finner i de data man samler inn, men det er en vesensforskjell i at adresseinformasjonen står i klartekst og derfor er det prinsipielt mye enklere å utvinne informasjon fra. Dette henger sammen med potensialet for misbruk, hvor pseudonymisering er en teknikk brukt i forslaget til sentralisert lagring i kapittel 3 som kan heve personvernet betraktelig. Pseudonymisering av e-post vil i så fall ikke bare kreve pseudonymisering av brukeren som er juridisk eier av e-postkontoen, men også selve adressen om denne inneholder personidentifiserbar informasjon. Dette er teknisk mulig, men mer omfattende enn fjerningen av koblingen mellom bruker og trafikk.

Bruken av denne type trafikkdata er kritisk for etterforskning, noe som ble presentert i en rekke case studies i kapittel 4. Det er et mål med direktivet at lovverkene på dette området skal harmoniseres gjennom hele EU-området. Dette er en fornuftig hensikt sett fra ordensmaktens synspunkt, men på grensen til et overgrep ifølge personvernforkjempere. Debatten har oversett at majoriteten av informasjonen lagres allerede i dag, og den har i liten grad erkjent at trafikkdata har bidratt til å løse kriminelle handlinger som det offentlige stiller store krav til at Politiet skal oppklare. Konkrete eksempler er gått gjennom i kapittel 4 og Baneheia- og Knutbysakene er gode eksempler på hver sin måte. Trafikkdata og elektroniske spor gir konkret dokumentasjon

fra en tredjepart om hva slags kommunikasjonstrafikk som har forekommet når og mellom hvem. Dette kan bidra med informasjon som kan avkrefte eller bekrefte annen informasjon som kommer fram under en etterforskning. Disse systemene er i stor grad bygd for å ha en høy integritet, opprinnelig fordi de dannet grunnlaget for fakturering og leveransen av kvalitetsmessig gode tjenester. Det er nettopp dette, kombinert med teknikker for å hindre forfalskning eller endring av informasjonen i denne typen systemer, som gjør at de egner som dokumentasjon og bevis.

En rekke teknikker kan brukes for å omgå registreringsplikten som følger av direktivet. Det mest kjente er bruk av proxy, som er et anonymiserende mellomledd for senderen av trafikken, og dette er en kjent teknikk blant både lovbrytere og etterforskere. Det finnes derimot en rekke mer sofistikerte teknikker som utvikler hele nettverk for å sikre anonymitet, men det er vist at alle disse teknikkene ikke er helhetlige eller ufeilbarlige. Bruken av denne typen teknikker er også i varierende grad begrenset, grunnet en brukerterskel som ligger godt over gjennomsnittet. Man må dessuten ha en tjeneste som fungerer hele tiden om man skal få garantert anonymitet. Alt dette tatt i betraktning er det mulig å omgå direktivet, men man vil alltid legge igjen et elektronisk avtrykk som kan etterforskes og potensielt lede fram til en ansvarlig person. Når enkelte anonymiseringstjenester er pålagt logging i henhold til implementeringen av datalagringsdirektivet i landet de holder til, vil det å bruke en slik tjeneste til kriminelle formål vil være å gi Politiet dokumentasjon på sine handlinger. Den største trusselen mot å gjøre datalagringsdirektivet lite effektivt ligger i at det er svært teknologispesifikt og derfor må derfor endres om det skal dekke den migreringen av brukere mellom gamle og nye tjenester. Et godt eksempel på dette er substituttjenestene Skype og MSN, hvor Skype muligens kan være underlagt direktivet i noen tilfeller, mens MSN er helt uregulert. Dette på tross av at de, fra brukerens ståsted, leverer samme type tjenester gjennom lynmeldinger, lyd- og videotelefoni. Denne brukermigreringen er ikke en tilsiktet handling fra brukeren i den hensikt å unngå datalagring, men motivert av at denne typen tjenester er gratis.

Anonymitet er ikke bare et verktøy for kriminelle, men også en nødvendighet for brukere med legitime formål. Varslere og folk som lever i samfunn uten informasjonsfrihet trenger anonymitet og metoder for å omgå sperrer som enten regulerer eller identifiserer informasjonen, senderen og mottakeren. Dette vil bli vesentlig vanskeligere ved en innføring av datalagringsdirektivet. Problemstillingen er i mindre grad relevant for Norge i og med at vi har varslerparagrafer i Arbeidsmiljøloven og ytringsfrihet, men det er viktig å poengtere at man ved en implementering av DLD innfører et system som kan misbrukes for å innhente informasjon og bryte disse rettighetene. En eventuell implementering av DLD i norsk lov bør vurderes utvidet til også å ta for seg private og offentlige organisasjoners adgang til datalagring, hvor misbruket nok vil være mer relevant enn for de data som blir samlet inn av tjenesteleverandører av offentlige kommunikasjonstjenester. Hvis en innføring av DLD skal få troverdighet og støtte, er det viktig at både den juridiske og tekniske implementasjonen gir forbrukere tillit til at trafikkdata er vanskelige å misbruke, og at de innsamlede data som blir pålagt utlevert bidrar til etterforskningen av alvorlig kriminalitet i henhold til den opprinnelige hensikten.

Misbruk av trafikkdata er noe som skjer allerede i dag og vil skje i framtiden uavhengig av om man innfører DLD. Det er uvisst hva slags misbruk man vil se. En mulig problemstilling er tjenesteleverandører som ikke sikrer trafikkdata på en tilfredsstillende måte og dermed blir utsatt for datatyveri eller utro tjenere som misbruker innsamlede data. Det er allerede gitt eksempler på begge deler i oppgaven. Mye av potensialet for misbruk vil forsvinne om man innfører den sentraliserte lagringen. Dette vil også tjene det formålet at man har en organisasjon som har som eneste formål å motta, lagre og sikre data samt å overlevere data til politiet etter pålegg.

6.2 Fremtidig arbeid

Det viktigste arbeidet i forbindelse med direktivet, er å få en avklaring om det skal innføres eller stoppes ved hjelp av et veto. Dette vil tvinge seg fram når regjeringen må ta stilling til direktivet som EØS-medlem, men kan ta tid dersom en Norsk Offentlig Utredning (NOU) skal gjennomføres.

Personvernnemda etterlyser en tydeligere framstilling av behovet og nytteverdien av direktivet fra Politiet, og dette kan være et svært konstruktivt bidrag til debatten som viser nytteverdien av trafikkdata for å oppklare kriminalitet. Kapittel 4 inneholder en rekke case studies som er gode eksempler, men en kvantitativ analyse av bidraget trafikkdata gjør i dag, og kan gjøre etter en innføring, satt i sammenheng med andre etterforskningsverktøy vil illustrere at dette er et viktig verktøy for Politiet.

Kostnadene vil bli enklere å kartlegge når et regelverk som fastlegger detaljene foreligger. Dette fører til at graden av konkurransevridning kan kartlegges, og det vil bli enklere for politikere å vurdere hvorvidt det offentlige vil ta kostnaden av innføringen og driftingen av løsningene som må på plass for å tilfredsstille direktivet.

Undersøkelser og avklaringer rundt mulighetene for en sentralisert lagringsløsning basert på politiske synspunkter og synspunktene til tjenesteleverandørene, vil kunne komme etter en vurdering av kostnadene basert på regelverket som skal ligge til grunn for innføringen av direktivet.

Referanser

[1] ACLU. Federal Court Strikes Down National Security Letter Provision of Patriot Act. http://www.aclu.org/safefree/nationalsecurityletters/31580prs20070906.html. [Online; aksessert feb 2009].

[2] ACLU. Section 215. http://action.aclu.org/reformthepatriotact/215.html. [Online; aksessert feb 2009].

[3] ACLU. USA PATRIOT Act. http://www.aclu.org/safefree/resources/17343res20031114.html. [Online; aksessert feb 2009].

[4] Advokatsamfundet. Delningssynpunkter på lagrådsremissen En anpassad försvarsunderrättelseverksamhet. http://www.advokatsamfundet.se/Documents/Advokatsamfundet_sv/Nyheter/Yttranden.pdf. [Online; aksessert feb 2009].

[5] Advokatsamfundet. Synpunkter på utkast till lagrådsremiss En anpassad försvarsunderrättelseverksamhet. http://www.advokatsamfundet.se/Documents/Advokatsamfundet_sv/Nyheter/JU%20synpunkter.pdf. [Online; aksessert feb 2009].

[6] Aftenposten. Datatilsynet gir etter for nettpoliti. http://www.aftenposten.no/forbruker/digital/nyheter/internett/article2943630.ece. [Online; aksessert mars 2009].

[7] Georg Apenes. Totalitært svermeri. http://www.dagbladet.no/kultur/2006/12/17/486293.html. [Online; aksessert feb 2009].

[8] AutoPASS. AutoPASS tjenester. http://www.autopass.no/Bruk+av+autopass/AutoPASS+tjenester. [Online; aksessert feb 2009].

[9] Shulzrinne Baset. An analysis of the Skype Peer-to-Peer Telephony Protocal. http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf. [Online; aksessert april 2009].

[10] De Moor Bellemans, De Schutter. Data Aqustition, interfacing and pre-processing of highway traffic data. .

[11] bt.no. EU vil saumfare flypassasjerene. http://www.bt.no/utenriks/article436388.ece. [Online; aksessert feb 2009].

[12] Eoghan Casey. Digital Evidence and Computer Crime 2nd edition. .

[13] Electronic Privacy Information Center. Data Retention. http://epic.org/privacy/intl/data_retention.html. [Online; aksessert feb 2009].

[14] Computerworld. EU-direktiv vil gi økte telepriser. http://www.idg.no/bransje/bransjenyheter/article9007.ece. [Online; aksessert jan 2009].

[15] Computerworld. Flere fødselsnumre stjålet. http://www.idg.no/bransje/bransjenyheter/article63081.ece. [Online; aksessert mars 2009].

[16] Computerworld. Henlegger sak mot Tele 2. http://www.idg.no/bransje/bransjenyheter/article85302.ece. [Online; aksessert mars 2009].

[17] Computerworld. Irer kan knekke snokeloven. http://www.idg.no/computerworld/article89048.ece. [Online; aksessert jan 2009].

[18] Computerworld. Norge kan unngå snokeloven. http://www.idg.no/computerworld/article89143.ece. [Online; aksessert jan 2009].

[19] Computerworld. Tele2-skandalen: - Ikke datainnbrudd. http://www.idg.no/bransje/bransjenyheter/article64758.ece. [Online; aksessert mars 2009].

[20] Comuterworld. Tvinges til politiarbeid. http://www.idg.no/computerworld/cwtv/article91168.ece. [Online; aksessert feb 2009].

[21] datalagringsdirektivet.no. Netcom om Datalagringsdirektivet. http://www.datalagringsdirektivet.no/node/26. [Online; aksessert feb 2009].

[22] datalagringsdirektivet.no. Telenor om Datalagringsdirektivet. http://www.datalagringsdirektivet.no/node/30. [Online; aksessert feb 2009].

[23] Datatilsynet. Datalagringsdirektivet. http://www.datatilsynet.no/templates/article____2156.aspx. [Online; aksessert feb 2009].

[24] Datatilsynet. Datatilsynet. http://www.datatilsynet.no/. [Online; aksessert jan 2009].

[25] Datatilsynet. Den svenske signalspaningsloven. http://www.datatilsynet.no/templates/Page____2338.aspx. [Online; aksessert feb 2009].

[26] Datatilsynet. Dom frå EU om Datalagringsdirektivet. http://www.datatilsynet.no/templates/Page____2600.aspx. [Online; aksessert feb 2009].

[27] Datatilsynet. FRA-loven - Virkning for personvernet. http://www.datatilsynet.no/upload/Dokumenter/saker/2008/08-01404-3%20Utredning%20442416.pdf. [Online; aksessert feb 2009].

[28] Datatilsynet. Støtteerklæring til menneskerettsdomstol-sak om FRA-loven. http://www.datatilsynet.no/templates/Page____2602.aspx. [Online; aksessert feb 2009].

[29] Sugano Day, Rosenberg. A Model for Presence and Instant Messaging. http://www.ietf.org/rfc/rfc2778.txt. [Online; aksessert april 2009].

[30] Syverson Dingledine, Mathewson. Tor: The Second-Generation Onion Router. http://www.torproject.org/tor-design.pdf. [Online; aksessert april 2009].

[31] Bettstetter Ebenspächer, Vögel. GSM - Switching, services and protocols. .

[32] Studie en Informatiecentrum Mensenrechten (SIM). EHCR: K.U. v. Finland. http://sim.law.uu.nl/SIM/CaseLaw/hof.nsf/233813e697620022c1256864005232b7/435050a4e6f14497c125751200463aae?OpenDocument. [Online; aksessert mars 2009].

[33] ESTA. Electronic System for Travel Authorization. https://esta.cbp.dhs.gov/esta/WebHelp/ESTA_Screen-Level_Online_Help_1.htm#Is%20there%20a%20fee%20for%20a%20travel%20authorization? [Online; aksessert feb 2009].

[34] Haber et al). Efficient signature schemes supporting redaction, pseudonymization, and data deidentification.

[35] EU. Directive 2006/24/EC . http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf. [Online; aksessert jan 2009].

[36] Jarle Lindseth Eystein Leren. Common Criteria-sertifisering i den norske karftforsyningen, 2008.

[37] Forbrukerombudet. Datalagringsdirektivet truer personvernet. http://forbrukerportalen.no/Artikler/2008/1201264304.64. [Online; aksessert feb 2009].

[38] Syverson Goldschlag, Reed. Privacy on the Internett. http://www.onion-router.net/Publications/INET-1997.html. [Online; aksessert april 2009].

[39] Messaging Anti-Abuse Working Group. Email Metrics Program: The Network Operators Perspective Report 6 - Second Quarter 2007. http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf. [Online; aksessert april 2009].

[40] HP. HP Data Retention and Guardian Online (HP DRAGON). http://h20208.www2.hp.com/cms/solutions/ci-b/dragon/index.jsp?jumpid=ex_r2140_w1/en/large/tsg/go_dragon. [Online; aksessert mai 2009].

[41] HP. News advisory - HP Extends Leadership in Telecom Data Retention Market. http://h71028.www7.hp.com/enterprise/downloads/HP_dragonupdate_April9.pdf. [Online; aksessert mai 2009].

[42] Høyre. Høyre sterkt kritiske til EUs datalagringsdirektiv. http://www.hoyre.no/artikler/2008/1/1200656969.03. [Online; aksessert feb 2009].

[43] JAP. Description of the system and communication protocol. http://anon.inf.tu-dresden.de/develop/doc/mix_short/. [Online; aksessert april 2009].

[44] JAP. Implementation of data retention according to the German Telecommunications Act. http://anon.inf.tu-dresden.de/dataretention_en.html. [Online; aksessert april 2009].

[45] JAP. Project: AN.ON - Anonymity.Online. http://anon.inf.tu-dresden.de/index_en.html. [Online; aksessert april 2009].

[46] Will Knight. Google mirror beats Great Firewall of China. http://www.newscientist.com/article/dn2768. [Online; aksessert april 2009].

[47] Økokrim. Økokrim. http://www.okokrim.no/. [Online; aksessert jan 2009].

[48] Liberaleren. KrF mot datalagringsdirektivet. http://www.liberaleren.no/2008/03/06/krf-mot-datalagringsdirektivet/. [Online; aksessert feb 2009].

[49] Liberaleren. Kun Venstre og SV vil programfeste nei til DLD. http://www.liberaleren.no/2009/02/16/kun-venstre-og-sv-vil-programfeste-nei-til-dld/. [Online; aksessert feb 2009].

[50] Liberaleren. Legg ned veto mot datalagringsdirektivet! http://www.liberaleren.no/2008/01/13/kampanje-legg-ned-veto-mot-datalagringsdirektivet/. [Online; aksessert feb 2009].

[51] Incisive Media Investments Ltd. How data rules will burden business. http://www.computing.co.uk/articles/print/2165870. [Online; aksessert mars 2009].

[52] Ungdom mot EU. Alle ungdomspartia mot direktivet. http://umeu.no/umeu/nyheter/2008/01/alle_ungdomspartiene_mot_overvakingsdirektivet/. [Online; aksessert feb 2009].

[53] N/A. Kvalitativ Metode på Wikipedia. http://no.wikipedia.org/wiki/Kvalitativ_metode. [Online; aksessert 12. desember 2008].

[54] N/A. MSN Messenger Protocol. http://www.hypothetic.org/docs/msn/. [Online; aksessert april 2009].

[55] N/A. MSNPiki Unofficial MSN Protocol Documentation. http://msnpiki.msnfanatic.com/index.php/Main_Page. [Online; aksessert april 2009].

[56] N/A, 2001. forelesningsfoil fra høgskolen i Agder, basert på Steinar Kvale: Det kvalitative forksningsintervju.

[57] NA24. E-postjakt på Se og Hør-spion. http://arkiv.na24.no/Nyhet/226850/E-postjakt+p%C3%A5+Se+og+H%C3%B8r-spion.html. [Online; aksessert mars 2009].

[58] Liv Signe Navarsete. Skriftlig spørsmål fra Beate Heieren Hundhammeren til samferdsleministeren. http://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=42215. [Online; aksessert jan 2009].

[59] Nettavisen. Slakter sikkerhet i trådløse nett. http://pub.tv2.no/nettavisen/it/article298557.ece. [Online; aksessert mars 2009].

[60] CBS News. Rebel Librarians Go On A Tear. http://www.cbsnews.com/stories/2003/05/28/national/main555885.shtml. [Online; aksessert feb 2009].

[61] Nyberg Niemi. UMTS Security, kapittel 2.3.7 Lawful interception. .

[62] HOD (Helse og omsorgsdepartementet). Lov om helsepersonell m.v. (helsepersonelloven). http://www.lovdata.no/all/nl-19990702-064.html. [Online; aksessert jan 2009].

[63] HOD (Helse og omsorgsdepartementet). Lov om helseregistre og behandling av helseopplysninger (helseregisterloven). http://www.lovdata.no/all/nl-20010518-024.html. [Online; aksessert jan 2009].

[64] HOD (Helse og omsorgsdepartementet). Lov om medisinsk og helsefaglig forskning (helseforskningsloven). http://www.lovdata.no/all/hl-20080620-044.html. [Online; aksessert jan 2009].

[65] JD (Justis og politidepartementet). Kommunikasjonskontrollforskriften . http://www.lovdata.no/for/sf/jd/xd-19950331-0281.html. [Online; aksessert jan 2009].

[66] JD (Justis og politidepartementet). Lov om behandling av personopplysninger (personopplysningsloven). http://www.lovdata.no/all/nl-20000414-031.html. [Online; aksessert jan 2009].

[67] Post og teletilsynet. Notat om "FRA-loven" og routing av elektronisk kommunikasjon via Sverige. http://www.datatilsynet.no/upload/Dokumenter/saker/2008/FRA-notat-npt_08122008.pdf. [Online; aksessert feb 2009].

[68] Post og teletilsynet. Post- og teletilsynet. http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME?menuid=11672. [Online; aksessert jan 2009].

[69] Times Online. Spy cameras to spot drivers' every move. http://www.timesonline.co.uk/tol/news/article589690.ece. [Online; aksessert feb 2009].

[70] OPSI. Part 11 Retention of Communications Data. http://www.opsi.gov.uk/acts/acts2001/ukpga_20010024_en_11#pt11. [Online; aksessert feb 2009].

[71] Personvernkommisjonen. NOU 2009: 1 Individ og integritet. http://www.regjeringen.no/nb/dep/fad/dok/NOUer/2009/nou-2009-1.html?id=542049. [Online; aksessert feb 2009].

[72] Politiet. Kripos. http://www.politi.no/. [Online; aksessert jan 2009].

[73] Washington Post. Local Officials Rise Up to Defy The Patriot Act. http://www.washingtonpost.com/wp-dyn/content/article/2005/11/04/AR2005110401088.html. [Online; aksessert feb 2009].

[74] The Register. Tor at heart of embassy passwords leak. http://www.theregister.co.uk/2007/09/10/misuse_of_tor_led_to_embassy_password_breach/. [Online; aksessert april 2009].

[75] SD (Samferdlselsdepartementet). Ekomloven. http://www.lovdata.no/all/hl-20030704-083.html. [Online; aksessert mars 2009].

[76] Skype. Skype - snakk sammen. http://www.skype.com/intl/no/. [Online; aksessert mai 2009].

[77] SÄPO. Synspunkter på delningen den 22 december 2006 av lagrådsremissen En anpassad försvarunderrättelsesverksamhet. http://www.sakerhetspolisen.se/download/18.7671d7bb110e3dcb1fd80008986/remissvar070104.pdf. [Online; aksessert feb 2009].

[78] Stallings. Cryptography and network security 4.th edition. .

[79] Sun. Challenges of Data Retention Compliance. http://www.sun.com/storage/white-papers/compliance_paper.pdf. [Online; aksessert mai 2009].

[80] Valduriez Tamer Özsu. Principles of distributed database systems 2.nd edition. .

[81] Teknofil.no. Norske turister i Danmark overvåkes. http://teknofil.no/wip4/print_article.epl?id=19055. [Online; aksessert feb 2009].

[82] Teknologirådet. Saken forklart Datalagringsdirektivet. http://www.teknologiradet.no/dm_documents/SF_Datalagringsdirektivet_for_web_6CUnh.pdf. [Online; aksessert mars 2009].

[83] Tews. Practical attacks against WEP and WPA. http://dl.aircrack-ng.org/breakingwepandwpa.pdf. [Online; aksessert mai 2009].

[84] Pyshkin Tews, Weinmann. Breaking 104 bit WEP in less than 60 seconds. http://eprint.iacr.org/2007/120.pdf. [Online; aksessert mai 2009].

[85] NY Times. Unsent E-Mail Helped Plotters Coordinate Madrid Bombings. http://www.nytimes.com/2006/04/30/world/europe/30spain.html?_r=1&scp=3&sq=madrid%20bombing%20mail&st=cse. [Online; aksessert april 2009].

[86] tu.no. Sverige kan sniklese SMS-ene våre. http://www.tu.no/it/article172585.ece. [Online; aksessert feb 2009].

[87] VG. Avviser draps-kontakt med Sara. http://www.vg.no/nyheter/utenriks/artikkel.php?artid=228290. [Online; aksessert mars 2009].

[88] VG. Full krig om mobilgåten. http://www.vg.no/pub/skrivervennlig.hbs?artid=2446724. [Online; aksessert mars 2009].

[89] VG. Kan ha brukt mobil like ved åstedet. http://www.vg.no/pub/skrivervennlig.hbs?artid=6336300. [Online; aksessert mars 2009].

[90] VG. Leter etter flere drapsmeldinger. http://www.vg.no/nyheter/innenriks/artikkel.php?artid=228060. [Online; aksessert mars 2009].

[91] VG. Mobilen gir ikke Viggo alibi. http://www.vg.no/pub/skrivervennlig.hbs?artid=8092116. [Online; aksessert mars 2009].

[92] VG. Pastoren ga drapsordre på SMS. http://www.vg.no/nyheter/utenriks/artikkel.php?artid=224840. [Online; aksessert mars 2009].

[93] VG. Pastorens sms-meldinger til barnepiken. http://www.vg.no/nyheter/utenriks/artikkel.php?artid=227422. [Online; aksessert mars 2009].

[94] VG. Tre ukjente tekstmeldinger granskes. http://www.vg.no/pub/skrivervennlig.hbs?artid=4470273. [Online; aksessert mars 2009].

[95] VG. Usikkert om mobildekningen drapsdagen. http://www.vg.no/pub/skrivervennlig.hbs?artid=8103170. [Online; aksessert mars 2009].

[96] Wikipedia. Community network. http://en.wikipedia.org/wiki/Community_network. [Online; aksessert mars 2009].

[97] Wikipedia. FRA-lagen. http://sv.wikipedia.org/wiki/FRA-lagen. [Online; aksessert feb 2009].

[98] Wikipedia. Onion diagram. http://en.wikipedia.org/wiki/File:Onion_diagram.svg. [Online; aksessert mai 2009].

[99] Wikipedia. USA PATRIOT Act. http://en.wikipedia.org/wiki/USA_PATRIOT_Act. [Online; aksessert feb 2009].

[100] Wikipedia. Virtual private network. http://en.wikipedia.org/wiki/Virtual_private_network. [Online; aksessert april 2009].

[101] Svein Willassen. Å lagre eller å ikke lagre. http://www.willassen.no/svein/pub/lagrellerikke.pdf. [Online; aksessert mars 2009].

[102] www.neitileu.no. Norge må avvise EUs datalagringsdirektiv - om nødvendig må veto tas i bruk. http://www.neitileu.no/organisasjon/politikk/uttalelser/norge_maa_avvise_eus_datalagringsdirektiv_om_noedvendig_maa_veto_tas_i_bruk. [Online; aksessert feb 2009].

[103] www.neitileu.no. SP - Nei til datalagringsdirektivet. http://www.neitileu.no/nyhetsklipp/forsvar_og_sikkerhet/sp_nei_til_datalagringsdirektivet. [Online; aksessert feb 2009].

A Directive 2006/24/EC

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 15 March 2006

on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [4] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

(3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

---

[1] Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

[2] Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

[3] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

[4] OJ L 201, 31.7.2002, p. 37.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, *inter alia*, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

(12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.

(13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.

(15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.

(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

(18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [1] provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.

(19) The right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC to receive compensation, which derives from Article 23 of that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

[1] OJ L 69, 16.3.2005, p. 67.

(20) The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.

(23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.

(24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making [1], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.

(25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2], and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

[1] OJ C 321, 31.12.2003, p. 1.

[2] OJ L 108, 24.4.2002, p. 33.

(b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

  (1) concerning fixed network telephony and mobile telephony:

    (i) the calling telephone number;

    (ii) the name and address of the subscriber or registered user;

  (2) concerning Internet access, Internet e-mail and Internet telephony:

    (i) the user ID(s) allocated;

    (ii) the user ID and telephone number allocated to any communication entering the public telephone network;

    (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

  (1) concerning fixed network telephony and mobile telephony:

    (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

    (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

— the cases in which information was provided to the competent authorities in accordance with applicable national law,

— the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

— the cases where requests for data could not be met.

2. Such statistics shall not contain personal data.

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

'1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (*) to be retained for the purposes referred to in Article 1(1) of that Directive.

(*) OJ L 105, 13.4.2006, p. 54.'

Aricle 12

Future measures

1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the *Official Journal of the European Union*.

Article 16

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 17

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

For the European Parliament	*For the Council*
The President	*The President*
J. BORRELL FONTELLES	H. WINKLER

Declaration by the Netherlands

pursuant to Article 15(3) of Directive 2006/24/EC

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC, the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

Declaration by Austria

pursuant to Article 15(3) of Directive 2006/24/EC

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

Declaration by Estonia

pursuant to Article 15(3) of Directive 2006/24/EC

In accordance with Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

Declaration by the United Kingdom

pursuant to Article 15(3) of Directive 2006/24/EC

The United Kingdom declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Cyprus

pursuant to Article 15(3) of Directive 2006/24/EC

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

Declaration by the Hellenic Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

Declaration by the Grand Duchy of Luxembourg

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Slovenia

pursuant to Article 15(3) of Directive 2006/24/EC

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

Declaration by Sweden

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Lithuania

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the draft Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (hereafter the 'Directive'), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

Declaration by the Republic of Latvia

pursuant to Article 15(3) of Directive 2006/24/EC

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Declaration by the Czech Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Declaration by Belgium

pursuant to Article 15(3) of Directive 2006/24/EC

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Poland

pursuant to Article 15(3) of Directive 2006/24/EC

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

Declaration by Finland

pursuant to Article 15(3) of Directive 2006/24/EC

Finland declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Germany

pursuant to Article 15(3) of Directive 2006/24/EC

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).