

Kapittel 6

Datalagringsdirektivet

– er dets krav om lagring av trafikkdata forenlig med Den europeiske menneskerettighetskonvensjonen?

Jon Wessel-Aas

Jon Wessel-Aas, B.Sc. International Relations, London School of Economics & Political Science 1988, cand.jur., Universitetet i Oslo 1995. Arbeider som advokat i Norsk rikskringkasting. Styremedlem i Den internasjonale jurist-kommisjon, norsk avdeling.

1 Innledning – problemstilling og avgrensninger

Tema for denne artikkelen er EUs datalagringsdirektiv (DLD).³⁹⁰ Artikkelenes hovedproblemstilling er hvorvidt DLDs krav til nasjonal lovgivning om tvungen lagring av trafikkdata fra alle borgeres bruk av tele- og internettbaserte kommunikasjons tjenester er forenlig med Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8 og 10 om henholdsvis beskyttelse av retten til privatliv og privat kommunikasjon og om beskyttelse av ytrings- og informasjonsfriheten.³⁹¹

390. Direktiv 2006/24/EF om lagring av data fremkommet ved bruk av elektronisk kommunikasjon, med endring av direktiv 2002/58/EC.

DLD ble vedtatt i 2006, og var direkte foranlediget av terrorbombene i henholdsvis London og Madrid, noe som også fremgår direkte av direktivets fortale. Direktivets angitte formål er imidlertid delt: Det skal sikre myndighetene historiske spor og/eller bevis for å kunne avverge, etterforske og iredteføre «serious crime», ved å innføre plikt for tilbydere av telekommunikasjons-/internettjenester til å registrere og lagre kundenes/brukernes trafikkdata. Det skal også harmonisere kravene til lagring hos aktørene i tele-/internettsektoren, for å gi mest mulig like markedsvilkår på tvers av landegrensene. Det tiltales likevel forskjell i lagringstid på opptil 18 måneder; lagringsplikten skal gjelde i minimum 6 og maksimum 24 måneder.

Direktivet overlater for øvrig til statene å regulere når og på hvilke vilkår den enkelte stats myndigheter kan få tilgang til enkeltindividers trafikkdata. Direktivet definerer ikke nærmere hva som omfattes av begrepet «serious crime». Rent formelt krever selve direktivet heller ikke at nasjonal rett gir adgang til utlevering av de lagrede data til politi eller andre myndigheter. Det er formelt sett bare lagringsplikten som er direktivets gjenstand.

Det ligger implisitt i direktivet at EU har forutsatt at denne formen for tvungen masselagring av personopplysninger i seg selv er forenlig både med EUs eget charter om fundamentale rettigheter og med EMK. EU antar dermed at så lenge behandlingen av de lagrede data og vilkårene for eventuell utlevering av dem til politi eller andre myndigheter tilfredsstiller de krav til rettssikkerhet og proporsjonalitet som EMK oppstiller, vil forholdet til menneskerettighetene være ivaretatt.

Spørsmålet er imidlertid etter min mening nettopp om slik tvangsregistrering og -lagring er forenlig med EMKs krav til respekt for særlig personvernet / retten til privat kommunikasjon, jf. EMK artikkel 8.

At identifiserbare individers trafikkdata omfattes av den typen personopplysninger som er beskyttet av EMK artikkel 8, er sikker rett. Det ble slått fast allerede i 1984 i Den europeiske menneskerettsdomstols (EMD) avgjørelse i saken *Malone mot Storbritannia*.³⁹² Dette er bekreftet i en rekke senere avgjørelser.

Videre er det slått fast av EMD at *selve lagringen* av slike opplysninger utgjør et inngrep i artikkel 8 når den skjer uten borgernes samtykke, *uavhengig* av om og på hvilke vilkår staten senere kan få tilgang til / bruke de lagrede opplysningene, jf. for eksempel EMDs avgjørelser i sakene *Leander mot Sverige* og *Amann mot Sveits*.³⁹³

391. Begrepet «trafikkdata» brukes her som samlebetegnelse på de data om kommunikasjonen som skal lagres i henhold til DLD (se nærmere om dette i pkt. 2 nedenfor). Dermed omfattes også blant annet såkalte lokasjonsdata – informasjon om hvor den enkelte befant seg da kommunikasjonen fant sted.

392. *Malone mot Storbritannia* (dom 2.8.1984).

Ettersom den lagringen som DLD forutsetter, utvilsomt utgjør et inngrep i artikkel 8 første ledd, er spørsmålet om inngrepsvilkårene i artikkel 8 annet ledd er oppfylt.

For at inngrep skal kunne aksepteres, kreves 1) at inngrepet er hjemlet i nasjonal lovgivning på en tilstrekkelig klar måte, 2) at inngrepet er begrunnet i visse samfunnsmessige hensyn – i dette tilfellet typisk nasjonal sikkerhet, forebygging av kriminalitet og/eller beskyttelse av andres rettigheter – og 3) at inngrepet er nødvendig i et demokratisk samfunn for å ivareta de anførte hensynene.

Ettersom DLD ikke er implementert i norsk rett, kan ikke lovskravet vurderes ennå. Kravet om at inngrepet må kunne henføres under ett eller flere av de legitime formål, vil – som ellers – ikke volde problemer. Det er således nødvendighetsvilkåret som er interessant å vurdere i denne artikkelen. Innholdet i dette utdypes nedenfor.

EMDs praksis og rettskildene for øvrig viser etter min mening klart at det i DLDs tilfelle først og fremst er *selve registreringen og lagringen* av alles trafikkdata som er inngrepet som må kunne forsvares som nødvendig i et demokratisk samfunn – *uavhengig* av de nærmere vilkår for myndighetenes tilgang.³⁹⁴ Dette innebærer ikke at reglene for tilgang til og videre bruk av dataene er irrelevant. Poenget er at dette spørsmålet er subsidiært og forutsetter at selve lagringen i utgangspunktet kan forsvares som nødvendig i et demokratisk samfunn.³⁹⁵

Det vil også være slik at jo mer liberale de nasjonale reglene er – materielt og prosessuelt – med hensyn til politiets eller andre myndigheters tilgang til de lagrede opplysningene, jo mer inngripende vil EMD anse lagringen som. Man kan for eksempel i Norge anta at Politiets sikkerhetstjenestes (PST) fullmakter etter straffeprosessloven § 216 b bokstav d, jf. politiloven § 17 d, til å få utlevert blant annet historiske trafikkdata i rent forebyggende øyemed,

393. Leander mot Sverige (dom 6.3.1987) og Amann mot Sveits (dom 16.2.2000).

394. Dette er også lagt til grunn av Romanias forfatningsdomstol, som i 2009 prøvet implementering av DLD i rumensk rett, mot egen grunnlov og EMK (avgjørelse nr. 1258 av 8. oktober 2009), ifølge uautorisert engelsk oversettelse av rettens bemerkninger, funnet her <http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html> (sist lastet ned 20.4.2010). Dommen er analysert i neste kapittel av denne boken. Se også Patrick Dreyer, «Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Data Retention with the ECHR», *European Law Journal* 2005, s. 365–375, som konkluderer tilsvarende.

395. Her synes Ingvild Bruce å være av en annen oppfatning, jf. hennes artikkel «Datalagringsdirektivet – en menneskerettskrenkelse eller -forpliktelse», *Lov og Rett* 2010, s. 6, motsatt Jon Wessel-Aas, «Datalagringsdirektivet og EMK – kommentarer til Ingvild Bruce», *Lov og Rett* 2010, s. 154.

uten krav til mistanke og – i hastesaker – uten forutgående kjennelse fra retten, står uendret. Da vil inngrepets effekt fremstå som ganske lite forutberegnelig, og derfor desto mer alvorlig for den enkelte borger. Men dette settes altså først på spissen dersom lagringen som sådan anses som akseptabel. Og i denne artikkelen behandles utelukkende dette spørsmålet.

Jeg vil nedenfor i punkt 2 kort beskrive nærmere hvilke data som kreves lagret. Deretter vil jeg i punkt 3 redegjøre for hvilke hovedprinsipper som har vært gjeldende hittil i europeisk rett (utenom EMK) når det gjelder innsamling og lagring av personopplysninger generelt og trafikkdata spesielt. I punkt 4 vil jeg så se nærmere på hva som kan utledes av EMDs relevante praksis på området, med fokus på nødvendighetsvilkåret. En oppsummering og avsluttende refleksjoner gis i punkt 5.

Jeg vil konsentrere behandlingen om forholdet til EMK artikkel 8 om retten til respekt for privatlivet og fortrolig kommunikasjon. DLD har imidlertid også en klar side til ytringsfriheten, jf. EMK artikkel 10. Inngrepet i den private kommunikasjonsfriheten støter an mot pressens kildevern, som etter sikker rett er beskyttet av artikkel 10.³⁹⁶ At statlige inngrep i kommunikasjon mellom potensielle kilder for pressen og pressen anses som inngrep både i artikkel 8 og 10, bekreftes i *Weber og Saravia mot Tyskland*.³⁹⁷ I denne artikkelen avgrenser jeg mot utdypning av denne problemstillingen ettersom hovedinngrepet skjer i artikkel 8.

2 Kort om hva som kreves lagret

«Trafikkdata» omfatter ikke selve innholdet i kommunikasjonen, men stort sett alle andre opplysninger om kommunikasjonen inngår i begrepet. Hva som skal tvangslagres, fremgår av direktivets artikkel 5. Grovt oppsummert skal følgende opplysninger registreres og lagres:

For telefoni (både tale- og tekstkommunikasjon):

- Når du kommuniserer og hvor lenge.
- Hvem du kommuniserer med.
- Hvor du befinner deg når du kommuniserer.
- Opplysninger som identifiserer telefonen og hva slags utstyr som brukes.

For e-post og Internett:

396. Jf. Goodwin mot Storbritannia (dom 27.3.1996), og Financial Times mfl. mot Storbritannia (dom 15.12.2009).

397. Weber og Saravia mot Tyskland (dom 29.6.2008).

- Når du sender e-post.
- Hvem som mottar e-posten.
- Når du går på nettet.
- IP-adressen din.
- Hvor lenge du er på nettet.
- Opplysninger om utstyr du bruker ved oppkobling.

3 Hovedprinsipper om lagring av personopplysninger i europeisk rett – særlig om trafikkdata

En vesentlig bakgrunn for å forstå hvordan innsamling, registrering og lagring av personopplysninger vurderes etter EMK, er utformingen av de øvrige felles-europeiske konvensjoner og direktiver som hittil har regulert spørsmålene.

De viktigste av disse er:

- Europarådets konvensjon av 20. januar 1981 nr. 108 om personvern i forbindelse med elektronisk behandling av personopplysninger (persondatakonvensjonen)
- EU-direktiv 1995/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger (personopplysningsdirektivet)
- EU-direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (kommunikasjonsdirektivet)

Innenfor Europarådet er persondatakonvensjonen senere fulgt opp med en særlig anbefaling fra ministerkomiteen om bruk av persondata i politisektoren.³⁹⁸

Anbefalingen inneholder detaljerte prinsipper om vilkår for innsamling, lagring, sikring samt bruk av personopplysninger for kriminalitetsbekjempelse, og ikke minst sletting av slike personopplysninger. Det går tydelig frem av disse at man har hatt for øye det alminnelige etterforskningsprinsipp: at det skal foreligge en konkret etterforskning og en relevant og forholdsmessig begrunnelse for registrering av den enkelte personopplysning, og videre at opplysninger skal slettes så snart disse vilkårene ikke er til stede.

398. Recommendation No R (87) 15 – Regulating the use of personal data in the police sector, som er forankret i både persondatakonvensjonen og EMK artikkel 8, lister opp en rekke prinsipper for innsamling, lagring og håndtering av personopplysninger for politiformål.

EMD refererer selv regelmessig til så vel persondatakonvensjonen som til ministerkomiteens anbefaling i saker som angår statenes håndtering av persondata.³⁹⁹

Grunnprinsippene i de nevnte EU-direktivene er de samme som i konvensjonen, selv om de er utpenslet i større detalj i direktivet, særlig når det gjelder persondata fra elektroniske kommunikasjonssystemer (naturlig nok, da direktivet er vedtatt langt senere).

Felles for disse internasjonale regelsettene er imidlertid at de alle – blant annet under henvisning til EMK – bygger på utgangspunktet om vern av personopplysninger og av privatlivets fred, herunder kommunikasjonsfortroligheten.

Videre forutsetter de at selve registreringen og lagringen av personopplysninger – selv når det skjer i henhold til avtale mellom vedkommende person og for eksempel tilbyder av teletjenester – skal begrenses i omfang og tid til det som er strengt nødvendig for gjennomføring av tjenesten og administrasjon av kundeforholdet. Deretter skal opplysningene slettes. For trafikkdata går dette uttrykkelig frem av kommunikasjonsdirektivet artikkel 6. I direktivets fortale (avsnitt 30) understrekes dessuten generelt at «[s]ystemer til levering af elektroniske kommunikationsnet og kommunikationstjenester bør konstrueres, så de begrænser mængden af nødvendige personopplysninger til et absolut minimum».

Etter kommunikasjonsdirektivet og de øvrige direktiver og konvensjoner nevnt ovenfor er altså registrering og lagring av personopplysninger et eventuelt nødvendig onde som bør begrenses i størst mulig grad. Ministerkomiteens anbefaling angående innsamling mv. av personopplysninger til politiformål presiserer disse prinsippenes anvendelse i kriminalitetsbekjempelsen.

Kommunikasjonsdirektivets artikkel 15 nr. 1 sier at selv om dets regler om blant annet trafikkdata ikke er til hinder for bruk av lagrede opplysninger til kriminalitetsbekjempelse, skal slik bruk være «nødvendig, passende og forholdsmæssig i et demokratisk samfund». Det er et poeng å fremheve at det da siktes til politiets bruk av data som fortsatt finnes lovlig lagret i henhold til kommunikasjonsdirektivets artikkel 6.

At EU selv erkjenner at den tvangsmessige masselagring av trafikkdata til politiformål som DLD krever, innebærer et brudd med disse grunnprinsippene, fremgår av DLDs egne bestemmelser: DLD artikkel 3 nr. 1 fraviker uttrykkelig kommunikasjonsdirektivets regler om lagring og sletting av blant annet trafikkdata, jf. kommunikasjonsdirektivet artikkel 6. Og DLD artikkel 11 innfører et nytt ledd 1 a til kommunikasjonsdirektivets artikkel 15, hvor det sies at artikkel 15 nr. 1 (jf. ovenfor) ikke gjelder for data som lagres i hen-

399. Se eksempelvis S. og Marper mot Storbritannia (dom 4.12.2008).

hold til DLD. Ingen av disse bestemmelsene hadde vært nødvendige dersom DLD hadde kunnet vedtas innenfor rammen av kommunikasjonsdirektivet.

Til slutt i dette punktet skal jeg vise hvordan Europarådet og norsk lovgiver i nyere tid løste balansen mellom behovet for ytterligere sikring av trafikkdata i kriminalitetsbekjempelsen på den ene side og respekt for personvern og kommunikasjonsfrihet på den annen side.

Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (Datakriminalitetskonvensjonen), ble utarbeidet og vedtatt nettopp med henblikk på å effektivisere kriminalitetsbekjempelsen i forhold til utviklingen av elektroniske kommunikasjonsmedier.

Datakriminalitetskonvensjonen pålegger konvensjonsstatene å innføre en rekke strafferettslige og straffeprosessuelle tiltak for bedre å kunne bekjempe alvorlig kriminalitet som enten skjer ved bruk av elektronisk kommunikasjon eller slik at elektroniske spor er viktige for etterforskningen av forholdene. Konvensjonens artikkel 16 pålegger statene å ha regler som muliggjør *midlertidig sikring av blant annet trafikkdata* som antas å kunne ha betydning som bevis i en konkret straffesak.

Det er altså ikke snakk om generell plikt til lagring trafikkdata, men om målrettet bevissikring som tvangsmiddel under etterforskning. Konvensjonsforpliktelsen ble i norsk rett gjennomført ved vedtagelsen av straffeprosessloven § 215 a. Paragraf 215 a første ledd bestemmer at påtalemyndigheten som ledd i etterforskning kan «gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis».

Av forarbeidene til § 215 a fremgår at det var diskusjon om det burde stilles strengere vilkår for et slikt sikringspålegg, for eksempel krav om skjellig grunn til mistanke.⁴⁰⁰ Under henvisning til at sikringspålegg ikke innebar at politiet fikk tilgang til de sikrede data, og at politiet burde ha mulighet til å sikre lagring av data på et så tidlig stadium av etterforskningen som mulig, valgte departementet den vedtatte løsningen. Det ble i den forbindelse vist til at de personvern- og rettssikkerhetsmessige betenkeligheter forbundet med å tillate en så vid ramme for sikringspålegg til en viss grad ville kunne reduseres av forholdsmessighetsvilkåret i straffeprosessloven § 170 a.

Denne gjennomgangen av grunnprinsippene i europeisk personvernrett frem til DLD viser to vesentlige poenger:

- 1) At selve innsamlingen og lagringen av personopplysninger, herunder trafikkdata, regnes som et selvstendig inngrep som må kunne forsvares som

400. Ot.prp. nr. 40 (2004–2005) kapittel 4.2.

- nødvendig og forholdsmessig, uavhengig av vilkårene for myndighetenes eventuelle tilgang til opplysningene.
- 2) At Europarådet og senere norsk lovgiver så sent som i 2005 mente at den midlertidige tvangslagring av trafikkdata hjemlet i straffeprosessloven § 215 a var så langt det var nødvendig og forholdsmessig å gjøre inngrep i personvernet.

4 EMDs praksis – nødvendighetsvurderingen og dens gjenstand

Nødvendighetskravet er av EMD blitt presisert slik at det fra statens side må godtgjøres at det foreligger et *presserende samfunnsmessig behov* («pressing social need») for inngrepet. Det er ikke tilstrekkelig at inngrepet er nyttig eller hensiktsmessig – det skal være nødvendig. Det må påvises at inngrepet er egnet til å ivareta de hensyn som begrunner det, at de samme hensyn ikke kan ivaretas på alternative, mindre inngripende måter, og at det alt i alt er proporsjonalitet mellom «mål og middel».

En svakhet ved en slik generell og abstrakt vurdering av lagringsplikten som jeg vil foreta her, er at en eventuell prøving for EMD jo formelt vil dreie seg om inngrep i én eller flere konkrete klager(e)s rettigheter – og ikke om en prøving av den generelle lagringsplikten som sådan.

Man kan for eksempel tenke seg at inngrepet vil vurderes som relativt sett mer inngripende dersom klageren er en psykiatrisk pasient som hevder at tvangslagring av trafikkdata kan avsløre at denne kommuniserer jevnlig med en psykiater, sammenlignet med for eksempel lagring av trafikkdata som viser at det foregår alminnelig kommunikasjon mellom en arbeidstager og dennes arbeidsgiver. Samtidig illustrerer dette noe av det grunnleggende problemet med et slikt lagringskrav som DLD foreskriver – jf. lagringens «blanket and indiscriminate nature», for å bruke EMDs terminologi fra saken *S. og Marper mot Storbritannia*.⁴⁰¹ Av den grunn mener jeg at det likevel, med disse forbehold, er for- svarlig å vurdere lagringskravet mer generelt i en fremstilling som denne.

Det har i debatten hittil også blitt pekt på at DLDs lagringsregime inneholder mange «hull» med hensyn til former for elektronisk kommunikasjon som faller utenfor, samt andre tekniske omgåelsesmetoder for kriminelle som ønsker å kommunisere uregistrert. På dette punkt kan det åpenbart reises spørsmål om inngrepets egnethet. Jeg velger likevel i det videre å fokusere på proporsjonalitetskravet.

401. *S. og Marper mot Storbritannia* (dom 4.12.2008).

I et tilfelle som DLD synes også dette å ville være det vesentligste ved en eventuell prøving i EMD. Tilsvarende betraktninger gjør at jeg også har valgt å avgrense mot de spørsmål den løpende utviklingen av teknologi (jf. smart-telefoner mv.) reiser. Denne utviklingen gjør det åpenbart vanskeligere å overskue hvilken samling av opplysninger om den enkeltes kommunikasjons- og bevegelsesmønstre som egentlig vil bli kartlagt. Og dette er et relevant moment, både i nødvendighetsvurderingen og som ledd i forutberegnelighetsvurderingen i lovskravet.

EMD har ikke hatt til prøving et inngrep i EMK artikkel 8 som er fullt ut parallelt med den typen tvangslagring som DLD krever. Det er kanskje heller ikke så merkelig. Som gjennomgangen i punkt 3 ovenfor viser, ville den type registrering og lagring som DLD krever, ikke lovlig kunne ha blitt gjennomført i stater som var bundet av blant annet EUs kommunikasjonsdirektiv, som igjen bygger på hevdvunne prinsipper forankret både i Europarådets persondatakonvensjon og EUs eget personopplysningsdirektiv.

All praksis som angår inngrep i personvernet, er selvfølgelig relevant – ikke minst praksis som gjelder registrering, lagring og videre bruk av personopplysninger. Problemet er at foreliggende praksis fra EMD om de rettssikkerhetskrav som må stilles for å unngå misbruk av personopplysninger, ikke direkte angår den grunnproblemstillingen DLD reiser.

DLD innebærer en permanent, automatisk, systematisk og unntaksfri registrering og lagring (i minst seks måneder) av alle borgeres personopplysninger. Mer konkret: trafikkdata som dokumenterer den enkeltes private kommunikasjonsmønstre og -nettverk – helt uavhengig av og løsrevet fra noen individuell vurdering av relevansen av registreringen og lagringen for den enkelte som rammes av inngrepet.

I de EMD-sakene som angår innsamling, lagring og/eller bruk av personopplysninger til politiformål, har det hovedsakelig dreid seg nettopp om enkeltindivider hvis personopplysninger var blitt registrert, lagret og eventuelt brukt som ledd i mer eller mindre *målrettede* tiltak. Enten for å oppklare konkrete straffesaker under etterforskning, eller for å forebygge terrorisme eller annen alvorlig kriminalitet som truer nasjonal sikkerhet.

EMD har for eksempel tatt stilling til flere tilfeller av bruk av straffeprosessuell kommunikasjonskontroll, noe som prinsipielt er godtatt som virkemiddel i kriminalitetsbekjempelse når kontrollen skjer som ledd i etterforskning av konkrete saker og de nødvendige rettssikkerhetsgarantiene er på plass, både med hensyn til forutberegnelighet og proporsjonalitet.

Enten EMD har vurdert slike inngrep i forhold til lovskravet eller nødvendighetskravet, har hovedelementene i vurderingen vært å unngå at inngre-

pene baserer seg på vilkårlighet eller er uproporsjonale overfor *det individ som rammes av inngrepet*.

Det kreves at vedkommende enten hører til en kategori personer eller har utøvet eller deltatt i en bestemt form for aktivitet som begrunner at myndighetene kan tvangsregistrere og lagre dennes personopplysninger til politiformål. Se blant annet Kjølbro's sammenfatning på s. 575–576 i hans kommentar til EMK, med videre henvisninger til praksis.⁴⁰² Der skriver han også følgende særskilt om registrering og lagring av personopplysninger til politiformål:

«Der foretages en forholdsvis indgående prøvelse af, om begrundelsen for at foretage og opretholde en registrering af oplysninger er relevant og tilstrækkelig, og der lægges bl.a. vægt på oplysningernes karakter, formål og alder.»⁴⁰³

Anvendt på DLD vil registreringen og lagringen av hver enkelt borgers trafikkdata i seg selv være fullstendig vilkårlig, uten noe som helst konkret etterforsknings- eller etterretningsformål. Og konservativt anslått vil lagringen helt frem til den opphører, ha vært fullstendig unødvendig for noe som helst formål for 95 prosent av de rammede. DLD nyanserer heller ikke mellom de forskjellige typer trafikkdata som kreves lagret, med hensyn til deres nødvendighet. Det er meget vanskelig å se forholdsmessigheten i et slikt inngrep, basert på de ovennevnte kriteriene.

EMD har riktignok i sakene *Weber og Saravia mot Tyskland* (dom 29. juni 2008) og *Liberty mfl. mot Storbritannia* (dom 1. juli 2009) prinsipielt akseptert tilsynelatende vidtgående strategisk overvåkning av kommunikasjon så fremt systemene er underlagt tilstrekkelig kontroll.

Ingen av de to sakene kan imidlertid etter min mening sammenlignes med DLDs krav om registrering og lagring av alle borgeres trafikkdata. Begge sakene dreide seg om vedkommende stats systemer for såkalt strategisk overvåkning av telekommunikasjonsaktivitet inn og ut av landet, noe som i utgangspunktet bærer preg av relativt sett mindre målrettethet enn mer alminnelig kommunikasjonskontroll rettet mot konkrete personer.

I ingen av tilfellene ble imidlertid all kommunikasjon som foregikk, registrert og lagret. Systemene baserte seg på automatiserte søk etter bestemte tekniske og/eller innholdsbaserte søkekriterier, hvis formål nettopp var å sile ut for nærmere analyse den kommunikasjonen som kunne antas å være relevant for å avdekke trusler mot nasjonal sikkerhet eller annen alvorlig organisert kriminalitet.

402. Jon Fridrik Kjølbro, *Den Europæiske Menneskerettighedskonvention*, København 2007.

403. Op.cit. s. 576, hvor han også henviser til saken *Segerstedt-Wiberg mfl. mot Sverige* (dom 6.6.2006).

Da EMD aksepterte tiltaket i Tysklands tilfelle, ble det nettopp lagt vekt på at de enkelte søkene var basert på spesielle tillatelser, hvor både søkets mål og de anvendte søkekriteriene var godkjent som relevante ut fra de lovfestede kriminelle aktiviteter som skulle forebygges/avverges.

I den britiske saken ble det konstatert krenkelse – i prinsippet overfor enhver borger – fordi myndighetene hadde for vid skjønnsadgang med hensyn til utforming av søkekriterier og til hvilken aktivitet som kunne begrunne registrering, avlytting mv.

I begge sakene stilte EMD for øvrig krav til rettssikre ordninger for sletting av opplysninger i materiale som i utgangspunktet ble «silt ut», men som ikke hadde relevans for det aktuelle formålet.

Disse sakene bekrefter at EMD stiller krav om konkret begrunnelse under nødvendighetsvurderingen for registrering og lagring av hver enkelt personopplysning for hvert enkelt individ, og til sletting av det som eventuelt har vært lagret, så snart en slik begrunnelse ikke foreligger. Dette er helt i samsvar med de prinsippene som har vært grunnpilarer i europeisk personvernrett frem til DLD.

Etter min vurdering er saken *S. og Marper mot Storbritannia* det nærmeste man kommer de problemstillinger som DLD reiser.⁴⁰⁴ Det er – så vidt jeg kan se – den eneste avgjørelsen som gjelder tvungen registrering og masselagring av personopplysninger om lovlydige borgere, uten annet formål enn eventuell bruk i fremtidige straffesaker.

Saken gjaldt registrering og lagring av fingeravtrykk, DNA og celleprøver av alle borgere som hadde vært mistenkt for straffbare forhold, uavhengig av om den enkelte senere ble funnet skyldig. Klagerne var ikke funnet skyldige i noe straffbart forhold. EMD dømte Storbritannia for krenkelse av klagernes rettigheter etter EMK artikkel 8.

EMDs dom i saken passer godt inn i det mønster som gjennomgangen hitil har tegnet. EMD viser i domspremissene dessuten uttrykkelig til prinsippene i persondatakonvensjonen og til ministerkomiteens anbefaling, jf. behandlingen ovenfor under punkt 3.

Det sentrale i dommen er etter min mening nettopp at EMD reagerte på lagringens «blanket and indiscriminate nature» (avsnitt 119), at den var uten annet formål enn potensiell bruk i etterforskning av fremtidige straffesaker. Dette gjelder i høyeste grad også DLD, hvor registreringen og lagringen rammer absolutt alle, og – i motsetning til *S. og Marper*-saken – uavhengig av om personene noensinne har vært i politiets søkelys.

Statens anførsel om at lagringen ikke ville ha noen nevneverdig effekt for borgeren fordi opplysningene bare ville brukes dersom de ved en senere

404. *S. og Marper mot Storbritannia* (dom 4.12.08).

anledning kunne knytte borgeren til kriminelle handlinger, ble av EMD besvart på følgende treffende måte:

«The Court is unable to accept this argument and reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.» (avsnitt 121)

EMD la også vekt på uskyldspresumsjonen ved å vise til at lagringen av ikke-dømte personers opplysninger stilte dem i kategori med straffedømte, i motsetning til den øvrige befolkningen. Dette kan rimeligvis ikke forstås slik at lagringen hadde vært konvensjonsmessig dersom den gjaldt hele befolkningen. Det bør derimot forstås som et naturlig tilleggsmoment i det konkrete tilfellet. Og det fremgår av premissene på dette punkt at poenget var å likestille de ikke-dømte med borgere for øvrig, ettersom slik registrering og lagring ikke lovlig kunne skje overfor borgerne generelt, uten den enkeltes samtykke.

Det kan også være verd å merke seg at EMD i *S. og Marper* ikke interesserte seg for garantiene eller manglende sådanne mot misbruk av de lagrede opplysningene, selv om retten streifer dette under drøftelsen av lovskravet (avsnitt 95–99). Dette bekrefter etter min vurdering hva jeg har sagt under punkt 1 ovenfor, at i et tilfelle som DLD er det grunnleggende problemet selve lagringen. Dersom denne i seg selv ikke kan forsvares som forholdsmessig, kan dette ikke «repareres» ved å vise til at reglene for tilgang til og bruk av opplysningene eventuelt er strenge.

Jeg never avslutningsvis at det ikke finnes grunnlag for – som enkelte i debatten har antydnet – å hevde at det skulle foreligge en *positiv forpliktelse* etter EMK til å innføre DLD for å beskytte potensielle ofre for kriminalitet. Dommen som det har vært henvist til i den sammenheng, er *K.U. mot Finland* (dom 2. desember 2008).

Den slår imidlertid bare fast at en absolutt taushetsplikt for internettleverandører i finsk rett, som hindret politiet i å få oppgitt identiteten til den som sto bak en åpenbart straffbar personvernkrenkende annonse på nettet, var en krenkelse av fornærmedes rettigheter etter artikkel 8. Begrunnelsen var at en slik rettsstilstand ikke åpnet for en interesseavveining mellom hensynet til offerets og den mistenktes personvern.

At man av dette ikke kan utlede noen positiv forpliktelse til masselagring av trafikkdata, slik DLD krever, synes ganske opplagt.⁴⁰⁵

405. Jf. også Bruce op.cit., og Wessel-Aas op.cit.

5 Oppsummering – avsluttende refleksjoner

Basert på gjennomgangen ovenfor anser jeg det som usannsynlig at den lagringen som DLD forutsetter, skal kunne passere en prøving etter EMK artikkel 8 (eller 10) etter *normale* standarder.

Selv om EU gjennom derogasjonsbestemmelsene i DLD i realiteten effektivt har opphevet de personvernprinsippene som inntil da gjaldt i EUs kommunikasjonsdirektiv, og formelt har kompetanse til det EU-rettslig, kan ikke EU uten videre og ensidig endre rettstilstanden etter EMK.

En kompliserende faktor i praksis er at spørsmålet om DLDs forhold til EMK mest sannsynlig kommer (indirekte) opp for EU-domstolen før EMD får en klagesak til behandling. Det verserer allerede to tyske saker for EU-domstolen, der spørsmålet om DLD er forenlig med EUs eget charter om grunnleggende rettigheter, sannsynligvis vil besvares.⁴⁰⁶

Disse rettighetene forutsettes å gi tilsvarende beskyttelse som EMK, og EU-domstolen legger i praksis stor vekt på EMK og EMDs praksis. Dersom EU-domstolen skulle komme til at DLD er akseptabelt etter EUs charter om grunnleggende rettigheter, vil en senere prøving av DLD (det vil si dets implementering i nasjonal rett) i en individuell klage til EMD langt på vei innebære at EMD blir bedt om å overprøve EU-domstolen.

Dette vil skape et klart spenningsforhold, som vil kunne prege EMDs vurdering. EMD har tidligere uttalt at der hvor et inngrep i konvensjonsrettighetene skjer som ledd i vedkommende stats oppfyllelse av forpliktelser etter EU-lovgivning som av EU-domstolen er funnet å være forenlig med grunnleggende rettigheter, vil EMD presumere at heller ikke EMK er krenket.⁴⁰⁷ Forutsetningen for en slik presumsjon er blant annet at beskyttelsen av rettigheter i den konkrete sak ikke var «manifestly deficient».

I lys av DLDs klare avvik fra hva som har vært normale standarder for beskyttelse av privatliv og kommunikasjonsfrihet, jf. ovenfor, mener jeg at denne forutsetningen vil settes alvorlig på prøve i et slikt scenario.

Lignende konflikter oppstår i forhold til FNs sikkerhetsrådsresolusjoner om terrorbekjempelse, som alle stater er forpliktet til å følge, endog med forrang foran andre forpliktelser. Disse setter også flere grunnleggende rettigheter etter EMK på prøve. I en rapport utarbeidet for Europarådet konkluderer Iain Cameron med at EMD kan og bør håndheve kjernen i de grunnleggende rettighetene etter EMK også i slike tilfeller.⁴⁰⁸

406. Forente saker C-92/09 og C-93/09.

407. Bosphorus mot Irland (dom 30. 6.2005), se særlig avsn. 155–157.

408. Iain Cameron, *The European Convention on Human Rights, Due Process and United Nations Security Council Counter-Terrorism Sanctions*, Report 6. Februar 2006 Council of Europe (kan leses her: http://www.coe.int/t/e/legal_affairs/legal_co-operation/public_international_law/Texts_& Documents/Docs%202006/I.%20Cameron%20Report%202006.pdf (sist lastet ned 14.4.2010)).

At EU etter vedtagelsen av Lisboa-traktaten, hvoretter EU selv ser ut til å ville bli direkte part til EMK, og slik at EMD kan prøve EU-domstolens avgjørelser direkte, som øverste og siste instans i menneskerettsspørsmål, kan muligvis også bidra til en modifisering av Bosphorus-doktrinen.

Spørsmålet da er etter min mening egentlig om EMD ved en eventuell prøving vil fastholde de prinsippene som har vært gjeldende hittil, eller om EMD vil akseptere at «present day conditions» er så dramatisk annerledes enn for få år siden at det er akseptabelt å snu opp ned på tradisjonelle personvern- og rettsstatsprinsipper i den preaktive kriminalitetsbekjempelsens navn.

I lys av hvor lite villig EMD hittil har vært til å akseptere at truslene fra terror og annen organisert kriminalitet skal kunne begrunne fravikelse av normale standarder etter EMK, tror jeg at EMD vil være tilbakeholdne med hensyn til å fire på kravene i DLDs tilfelle.⁴⁰⁹

409. Se blant annet EMDs ferske dom i Gillian og Quinton mot Storbritannia (12. januar 2010), som er nærmere kommentert på min nettside: Uhuru: <http://www.uhuru.biz/?p=38>.