DATALAGRING OG MENNESKERETTIGHETENE

- Utredning til Justisdepartementet og Samferdselsdepartementet

Professor Hans Petter Graver, Institutt for privatrett, UiO
Advokat Henning Harborg, Advokatfirmaet Thommessen AS

Sekretær: Advokatfullmektig Espen Ostling, Advokatfirmaet Thommessen AS

Oslo, 1. oktober 2015

INNHOLD

1 INNLEDNING

1.1 Temaet, mandatet og utgangspunkter for denne utredningen

Datalagringsdirektivet (DLD) ble gjennomført i norsk rett ved lov 11. april 2011 nr. 11 (lagringsloven). Lagringsloven pålegger ekomtilbydere å lagre data for de fem tjenestekategoriene som fremgikk av DLD artikkel 5, det vil si fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni. I Justisdepartementets forslag til ny lov (Prop. 49 L for 2010-11) ble lagringstiden satt til ett år, men Stortinget reduserte den til 6 måneder.

EU-domstolen konkluderte i dom av 8. april 2014 (DLD-dommen) med at direktivet er ugyldig. Direktivet ble funnet å være i strid med EU-charteret artikkel 7 og 8 om retten til privatliv og retten til personvern, og gikk lenger enn unntaksadgangen i artikkel 52 åpner for. Det betyr i korte trekk at DLD ble funnet å være mer inngripende i retten til privatliv og personvern enn det som ble ansett nødvendig for å ivareta allmenne interesser eller andres rettigheter. I tillegg til dommen i EU-domstolen er den nasjonale lovgivningen som gjennomførte datalagringsplikten underkjent av domstoler i Storbritannia, Tyskland, Nederland, Østerrike, Belgia, Tsjekkia, Slovakia, Slovenia, Bulgaria, Romania og Kypros.

Loven har – blant annet som følge av DLD-dommen – aldri blitt satt i kraft, og det er i kjølvannet av dommen reist spørsmål ved om loven kan settes i kraft uten man krenker grunnleggende rettigheter, eventuelt om det kan gjøres tilpasninger til loven som gjør at den kan settes i kraft uten å krenke de grunnleggende rettighetene. Det er disse spørsmålene som er tema i denne utredningen. Oppdraget er i mandatet beskrevet slik:

> *Justis- og beredskapsdepartementet og Samferdselsdepartementet ønsker å få utredet hvilke konkrete tilpasninger i den norske lagringsloven med tilhørende forskrifter som eventuelt er nødvendig for at loven skal kunne settes i kraft uten at Norge krenker retten til personvern etter Grunnloven § 102 samt våre menneskerettslige forpliktelser slik disse må forstås i lys av EU-domstolens dom av 8. april 2014 om datalagringsdirektivet. Det må også påses at den løsningen som foreslås er forenlig med kommunikasjonsverndirektivet 2002/58 EF.*
>
> *I tilbørlig utstrekning skal det ses hen til de vurderinger som er foretatt i andre nordiske land.*
>
> *Oppdraget innebærer primært å undergi de ulike elementene i lagringsplikten (lagringspliktens omfang) en grundig vurdering av om de tilfredsstiller vilkårene for inngrep i personvernet. I den forbindelse må det tas hensyn til den teknologiske utviklingen.*
>
> *Siden EU-dommen kan anses å kaste et generelt nytt lys over forståelsen av forholdsmessighetsvurderingen, bør også øvrige sider ved lagringsloven undergis en fornyet vurdering – primært i den grad det foreslås endringer i lagringspliktens omfang.*

Utredningen skal kunne brukes som grunnlag for en høring av eventuelle forslag til lovendringer. Det må derfor redegjøres grundig for så vel konkrete lovendringsforslag som de vurderinger som fører til at det ikke foreslås lovendringer.

Som allerede nevnt, vurderte EU-domstolen forholdet mellom DLD og nærmere angitte grunnleggende rettigheter, slik de er beskyttet i EU-charteret. Ettersom DLD ikke skal anvendes direkte i Norge og Norge ikke er bundet av EU-charteret, vil adgangen til å sette den norske lagringsloven til side bero på en annen rettslig avveining enn den EU-domstolen sto overfor.

Mandatet ber oss om å vurdere spørsmålet både etter Grunnloven, de internasjonale menneskerettigheter og direktiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon). Vi har valgt å konsentrere våre analyser og vurderinger om EMK og praksis i EMD.

Etter vårt syn er det vanskelig å ha noen begrunnet oppfatning om rekkevidden av Grunnloven § 102 for datalagring uavhengig av de internasjonale kildene. Bestemmelsen er ny, og det nasjonale kildematerialet sparsomt. Vi tar derfor ikke stilling til innholdet av § 102, og heller ikke om det må anses sammenfallende med innholdet av de internasjonale menneskerettighetene. Vi tar dermed ikke stilling til om de skrankene som vi mener må oppstilles på grunnlag av menneskerettighetene må anses å ha grunnlovs rang i norsk rett.

Når det gjelder de internasjonale menneskerettighetene, er det språklige innholdet av FN-konvensjonen om de sivile og politiske rettigheter og EMK langt på vei sammenfallende. Samtidig er det en omfattende praksis fra EMD som er relevant for vårt spørsmål. Vi har derfor valgt ikke å gi noen særskilt vurdering av datalagring etter andre menneskerettighetsinstrumenter enn EMK.

Direktivet om personvern og elektronisk kommunikasjon er en del av EØS-avtalen og dermed bindende for Norge. Artikkel 5 inneholder krav om at nasjonal lovgivning forbyr enhver annen person enn brukerne, uten samtykke fra vedkommende bruker, å avlytte, oppfange, lagre eller på andre måter overvåke kommunikasjonen og tilhørende trafikkopplysninger. Det kan imidlertid etter artikkel 15 nr. 1 gjøres unntak fra dette dersom det er nødvendig, egnet og rimelig i et demokratisk samfunn av hensyn til nasjonal sikkerhet (det vil si statens sikkerhet), forsvar, offentlig sikkerhet og forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger eller ulovlig bruk av det elektroniske kommunikasjonssystemet. Ut fra måten denne bestemmelsen er formulert på, antar vi at den ikke setter snevrere grenser for lagring enn EMK. Vi foretar derfor ikke noen selvstendig vurdering av unntaksbestemmelsen i direktivet.

Spørsmålet om krenkelse kan komme opp på forskjellige måter. Normalt vil eventuelle krenkelser være utslag av konkret anvendelse av loven. For datalagring vil det i så fall være spørsmål om bruken av lagrede opplysninger i et enkelttilfelle. For datalagring kan

imidlertid spørsmålet komme opp også i helt generell form. Sakene for EU-domstolen var foreleggelser fra nasjonale domstoler (en irsk og en østerriksk) i saker som gjaldt krav fra eller på vegne av borgere om at deres rettigheter var krenket i kraft av selve lagringen av data. Synspunktet var altså i korte trekk at lagringen av data for de formål DLD skal ivareta i seg selv representerer et brudd på borgernes grunnleggende rettigheter, og at direktivet som fastsetter plikten til å foreta slik lagring derfor måtte være ugyldig. I lys av blant annet bestemmelsen i EMK artikkel 13, kan vi vanskelig skjønne annet enn at en tilsvarende sak, det vil si en sak om datalagringen som sådan er i strid med EMK og/eller Grunnloven, måtte vært tillatt fremmet i Norge. Vår vurdering handler i stor grad om å spå utfallet av en slik sak. En sak kan også komme opp som spørsmål om krenkelse av kommunikasjonsverndirektivet. Siden dette er del av EØS-regelverket, vil det kunne bli forelagt EFTA-domstolen. Vi går ikke nærmere inn på dette.

Det er bred enighet om at den lagringen loven skal sikre, i seg selv er et inngrep i borgernes grunnleggende rettigheter, først og fremst vernet om privatliv og korrespondanse. Det store spørsmålet er derfor om inngrepet som lagringen representerer, kan forsvares (rettferdiggjøres) eller om det vil utgjøre en krenkelse. Etter praksis fra EMD er dette for det første spørsmål om den loven som gir hjemmel for lagring er presis nok med hensyn til de formål som dataene kan brukes til og med hensyn til garantier for at det ikke skjer misbruk. For det andre er det spørsmål om de hensyn som begrunner lagringen er godt nok begrunnet og tunge nok til å begrunne det inngrepet i rettigheter som lagringen innebærer. Som vi skal komme tilbake til, vil spørsmålet koke ned til en forholdsmessighetsvurdering. Det avgjørende er derfor hva domstolene, derunder EMD, må forventes å mene om forholdsmessigheten av datalagring på bestemte vilkår. For lovgiver er derved utfordringen å utforme plikten til datalagring på en slik måte at domstolene vil anse det som et forholdsmessig inngrep i borgernes rettigheter.

Datalagring har vært behandlet av EU-domstolen og av nasjonale domstoler i en rekke land. I de fleste av sakene har datalagringsregler som bygger på DLD blitt underkjent. Disse avgjørelsene sier imidlertid ikke noe direkte om hvordan regler om datalagring må utformes for ikke å komme i konflikt med personvernet eller om betingelser som må oppfylles for at datalagring i det hele tatt skal være forenlig med disse rettighetene. Det foreligger ingen autoritative avgjørelser om dette etter EMK eller andre internasjonale menneskerettighetsinstrumenter. Rettsavgjørelsene fra EU bygger i hovedsak på EUs egne regler i charteret for grunnleggende rettigheter. Disse forholdene gjør at en utredning om de spørsmål som vårt mandat reiser er beheftet med en viss usikkerhet. Vi tror imidlertid at på bakgrunn av de reaksjoner som DLD er blitt møtt med av EU-domstolen, og av domstolene i en rekke av EUs medlemsland, vil utgangspunktet for en vurdering etter EMK være at generell lagring av kommunikasjonsdata representerer et betydelig inngrep i personvernet som, hvis overhodet, bare kan skje innenfor meget snevre rammer. Det er neppe sannsynlig at en domstol som EMD i denne forbindelse vil innrømme videre rammer for datalagring enn EU-domstolen. Det er grunn til å tro at

skepsis til slike inngrep i personvernet er større blant dommere fra en rekke av Europarådets medlemsland enn den tradisjonelt har vært hos oss.[1]

1.2 Arbeidet med utredningen

Vi ble opprinnelig gitt en frist med utredningen til 1. juni 2015. På grunn av andre oppgaver ble det vanskelig å holde denne fristen, og vi ba 30. april om en ny frist. Ny frist ble satt til 1. oktober. Vi har avholdt møte med Justisdepartementet og Samferdselsdepartementet underveis 1. juli og 24. september. Vi har ikke holdt møte med andre i forbindelse med arbeidet. Den 15. mai fikk vi et innspill fra Norsk journalistlag om journalisters kildevern. Innspillet er av journalistlaget lagt ut på nett. Vi har ikke mottatt andre innspill til arbeidet. Advokatfullmektig Espen Ostling har fungert som sekretær for utrederne.

1.3 Viktige utviklingstrekk av betydning for ønsket om datalagring

De senere år har det vokst frem former for kriminalitet som i seg selv er egnet til å true stabiliteten i samfunnet. Terrorisme er straffbare handlinger som har som formål nettopp å skape frykt og undergrave stabiliteten i samfunnet og grunnlaget for den demokratiske rettsstaten. Også enkelte andre kriminalitetsformer er i seg selv egnet til å svekke stabiliteten i samfunnet, som for eksempel alvorlig og omfattende korrupsjon.

Med den elektroniske hverdagen har det oppstått nye muligheter, både til å samle opplysninger om borgernes atferd som grunnlag for å oppklare straffesaker og til å krenke borgernes grunnleggende interesser i å beskytte sin personlige integritet. Det er i dette krysspresset spørsmålet om lagring av kommunikasjonsdata og om politiets tilgang til disse data oppstår. Opplysning om personers kommunikasjon som kan gi tidspunkt, varighet og sted for elektronisk kommunikasjon kan gi informasjon som er helt nødvendig for å oppklare visse former for forbrytelser, og som kan gi vesentlig tilleggsinformasjon for etterforskning og oppklaring av andre forbrytelser.

Kriminalitetens art og omfang utgjør en viktig faktor i vurderingen av politiets behov for etterforskningsmetoder. Nye metoder bør ikke åpnes for og eksisterende ikke utvides uten et konkret behov. På den annen side må de hjemler som står til politiets disposisjon være tilstrekkelig til å bekjempe alvorlig kriminalitet.

En viktig endring i kriminalitetsutviklingen er økningen av den såkalte ”offerløse» kriminalitet. Offeret i straffbare handlinger ønsker normalt både å anmelde og medvirke til oppklaring av den straffbare handling. For de straffbare handlinger som har hatt en økning i de senere årene er det i mindre grad noe ”offer» som bidrar til oppklaring ved å anmelde eller gi annen informasjon i saken. I narkotikasaker vil ”kjøperen» av narkotikaen se seg tjent med å holde forholdet skjult ettersom ervervet er straffbart. Antallet anmeldte narkotikaforbrytelser er nesten utelukkende et resultat av at politiet og andre kontrollmyndigheter selv avdekker og anmelder forhold. Det samme gjelder en del former for økonomisk kriminalitet og kriminalitet knyttet til IKT (informasjons- og kommunikasjonsteknologi). Den teknologiske utviklingen har forandret metodene som

[1] Se https://www.nj.no/filestore/Hringsnotatkildevernlagringsloven.pdf.

brukes både ved terror og andre former for kriminalitet, noe som også skaper et behov for nye metoder ved etterforskning og bekjempelse av kriminalitet.

En annen endring er den økte oppmerksomheten på organisert kriminalitet. Omfanget av organisert kriminalitet er vanskelig å fastslå, og politiet har derfor ingen oversikt over hvor omfattende denne kriminaliteten er. Omfanget av organisert kriminalitet i vid forstand er likevel antatt å være økende i Norge. Utviklingen internasjonalt tilsier at organisert kriminalitet vil være tiltagende de kommende år. Samtidig er det en økt internasjonalisering av kriminaliteten i takt med internasjonaliseringen av samfunnet for øvrig. Grov internasjonal kriminalitet skjer i større grad i ly av forretningsvirksomhet som gir seg ut for å være lovlig, og under dekke av tilsynelatende regulær handel over landegrenser. Likeledes blir det stadig enklere for personer som begår kriminelle handlinger, som det blir for lovlig virksomhet, å overføre penger og investere internasjonalt. Politiet må i et økende antall saker forholde seg til multinasjonale selskaper som med- eller motaktører. Det pengesterke norske markedet er i økende grad gjenstand for oppmerksomheten til personer med kriminelle tilbøyeligheter og nettverk i utlandet. Ventelig vil det komme et økende tilbud av illegale varer og tjenester, bedragerikonsepter og lignende rettet mot Norge. Likeledes ser politiet nå flere eksempler på at utenlandske personer oppretter kontakt og samarbeid med nordmenn for derved mer effektivt å kunne begå kriminalitet i Norge med hovedbase i utlandet.

1.4 Grunnleggende hensyn

Lagring og tilgjengeliggjøring av kommunikasjonsdata til overvåknings- og etterforskningsformål er kontroversielt og vanskelig. Mens politiet og påtalemyndigheten understreker nødvendigheten av tilgang til slike data, ser talspersoner for personvernet lagringen som et uønsket og farlig tiltak. Vurderingen av tiltakets karakter er avhengig av ståsted. Fra politiets side kan tilgang til og analyse av trafikkdata fremstå som lite inngripende overfor den enkelte. Trafikkdata kan underbygge en mistanke som kan gi grunnlag for å sette i verk mer inngripende etterforskningsskritt som ransaking, beslag eller aktiv overvåkning av bestemte personer. De kan også kvittere ut personer som er utenfor mistanke, uten at personene noensinne behøver å vite at de har figurert som mistenkte. Kostnadene er lave, slik at analyser kan iverksettes uten alt for stor ressursbruk. Risikoen for at de som er under etterforskning oppdager dette og dermed innretter seg for å vanskeliggjøre etterforskningen er lav. Fra politiets side kan dermed lagring og tilgang til kommunikasjonsdata fremstå som et effektivt og lite kostnadskrevende tiltak, som i liten grad griper inn i den enkeltes interessesfære og som derfor fremstår som lite inngripende sammenliknet med mange av politiets klassiske tvangsmidler.

Fra borgernes side kan dette fortone seg annerledes. Lagring av kommunikasjonsdata retter seg mot alle personer som gjør bruk av elektroniske kommunikasjonstjenester uten hensyn til om de gjør noe ulovlig eller ikke og berører således så godt som hele befolkningen. Selv om lagringen skjer ut fra det formål å bekjempe straffbare handlinger innebærer det et inngrep ikke bare overfor dem som har noe å skjule for politiet. Dette har Høyesterett lagt til grunn i flere saker, blant annet i forbindelse med overvåkning i arbeidslivet. I Rt. 2013 s. 143 sier førstvoterende:

Som lagmannsretten understreker, vil kontrolltiltak ikke bare kunne være en ulempe for den som har noe å skjule, men også for den som ikke har noe å skjule. At generell overvåkning i arbeidslivet vil være en belastning, understrekes i NOU 2009:1 Individ og integritet side 22, hvor det heter:

"Personvernkommisjonen mener at det å bli overvåket i sitt daglige virke vil oppfattes som en belastning av de fleste. Dersom opplysningene som innhentes ved slik overvåkning i tillegg blir brukt til andre formål enn de opprinnelig var beregnet for, og andre formål enn dem man har fått informasjon om, øker dette belastningen og følelsen av overtramp mot den personlige integritet."

Dette kan jeg på generelt grunnlag slutte meg til.

Lagringen gjelder ikke bare opplysninger om blant annet om hvem man har kommunisert med, med hvilke midler og når, men også hvor man har befunnet seg på forskjellige tidspunkt. Ved lagringen skilles heller ikke ut opplysninger om personer med hvem kommunikasjonen bør nyte særlig beskyttelse som leger, journalister og advokater. Selv om innholdet av kommunikasjonen ikke lagres, gir opplysningene grunnlag for å samle opplysninger om forhold om enkeltpersoner som mange vil holde for seg selv, som hvem de kommuniserer med, hvor de til enhver tid befinner seg og hva slags aktivitet de utøver på internett.

Når slike data lagres må man også ta i betraktning mulighetene for at opplysningene kan bli tilgjengelig for andre gjennom straffbare handlinger. Uansett sikkerhetssystemer vil data ikke kunne sikres fullstendig mot at uvedkommende trenger seg inn og får tak i opplysninger.

2 EU-DOMSTOLENS AVGJØRELSE

EU-domstolen vurderte i de forenede saker C-293/12 og C-594/12 gyldigheten av DLD ut fra EU-rettens grunnleggende rettigheter. Domstolen kom i dom avsagt 8. april 2014 til at direktivet er ugyldig og at *"EU-lovgiver ved vedtagelsen af direktiv 2006/24 har overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til chartrets artikel 7, 8 og 52, stk. 1"*. Bakgrunnen for saken var foreleggelser fra High Court i Irland og Verfassungsgerichtshof i Østerrike. Domstolen innledet sin vurdering med å gi en sammenfatning av hvilke data direktivet gir grunnlag for innsamling av (avsnitt 26). Domstolen slo deretter fast at disse formene for informasjon, sett under ett, vil kunne gi svært detaljert informasjon om individers privatliv (avsnitt 27). Etter domstolens oppfatning vil dette potensielt påvirke personers bruk av elektronisk kommunikasjon, og derfor også deres utøvelse av ytringsfriheten, som er sikret gjennom artikkel 11 i EU-charteret (avsnitt 28).

Videre slo domstolen fast at direktivet utvilsomt innvirker på retten til privatliv og personvern, som er sikret gjennom henholdsvis artikkel 7 og 8 i charteret (avsnitt 29). Domstolen konkluderte deretter med at innsamling og lagring av informasjon knyttet til en persons privatliv, utvilsomt medfører en krenkelse av rettighetene nedfelt i artikkel 7 (avsnitt 33-34). Tilsvarende ble nasjonale myndigheters tilgang til slik informasjon funnet å konstituere et brudd på artikkel 8 om personvern (avsnitt 35-36). På grunn av direktivets vide nedslagsområde, ble krenkelsene i tillegg funnet å være *"meget vidtrækkende og må anses for at være af særligt alvorligt karakter"* (avsnitt 37). Som et tileggsargument ble det vist til at lagringen og bruken av data uten formidling av dette til eksponentene er egnet til å gi de aktuelle personene følelsen av at deres privatliv overvåkes.

Domstolen gikk deretter over til å vurdere om direktivet likevel var i overensstemmelse med EU-charteret, som åpner for unntak på visse vilkår, jf. EU-charteret artikkel 52 (avsnitt 38). Domstolen viste til at unntaksadgangen må være nedfelt i lov og respektere "the essence» i en rettighet. Unntakene må videre være forholdsmessige, og kun foretas om de er nødvendige og tjener formål som er anerkjent av EU eller for å beskytte andres rettigheter eller friheter. Det springende punktet for domstolen ble etter dette om DLD tilfredsstilte unntaksadgangen i artikkel 52.

Domstolen slo for det første fast at DLD tilfredsstiller vilkåret i artikkel 52 om mål om allmenn interesse (avsnitt 44). Selv om det i dag er mulig å benytte andre kommunikasjonsformer som ikke er lagringspliktige, betyr det ikke at tiltaket ikke er formålstjenlig. Formålet om å bekjempe kriminalitet er reelt. Retten pekte særlig på behovet for å bekjempe organisert kriminalitet og terrorisme. Retten viste også til artikkel 6 i EU-charteret hvor det fremgår klart at den enkelte ikke bare har rett til frihet, men også sikkerhet, herunder rett til å bli beskyttet mot alvorlig kriminalitet (avsnitt 42).

Domstolen vurderte deretter om kravet til forholdsmessighet var oppfylt. I tråd med domstolens praksis må direktivet være egnet til å oppnå de legitime formålene det søker å oppnå, og det må ikke overskride grensen for hva som er nødvendig for å oppnå disse formålene (avsnitt 46).

Før domstolen foretok den konkrete prøvingen av om direktivet oppfylte kravet til forholdsmessighet, minnet den om at prøvingsintensiteten vil avhenge av hvilke rettigheter som krenkes, krenkelsens karakter og alvorlighetsgrad, samt formålet som søkes oppnådd ved krenkelsen (avsnitt 47). I lys av at retten til privatliv er en fundamental rettighet, samt at direktivet medførte en alvorlig krenkelse av denne rettigheten, konkluderte domstolen med at lovgivers skjønnsmargin var begrenset, og at domstolens prøving av denne skjønnsmarginen var streng (avsnitt 48).

I den konkrete vurderingen fant domstolen at datalagring var et egnet virkemiddel i kampen mot alvorlig kriminalitet (avsnitt 49).

Domstolen konkluderte derimot med at virkemidlet oversteg grensen for hva som kunne anses nødvendig (avsnitt 69). Det ble i den forbindelse for det første minnet om at det for personvern kun er strengt nødvendige krenkelser som aksepteres. Dette innebærer at EU-retten på dette området må bestå av klare og presise bestemmelser, samt sikkerhetstiltak som gir en effektiv beskyttelse mot misbruk og ulovlig tilegnelse av data (avsnitt 54). Dette gjelder særlig når personlige data blir underlagt automatisk behandling, og når det er en betydelig risiko for misbruk (avsnitt 55).

I den konkrete vurderingen av om direktivet medførte et brudd på EU-charterets artikkel 7 og 8 viste retten til en rekke forhold.

Retten vektla for det første at direktivet medførte innsamling av samtlige data fra alle former for elektronisk kommunikasjon. Videre ville samtlige brukere av elektronisk kommunikasjon bli berørt. Direktivet har altså ingen former for begrensninger i hva slags informasjon som skal innsamles, eller fra hvem. Direktivet ville derfor medført et inngrep i rettighetene til nærmest hele den europeiske befolkning, og uten hensyntagen til om informasjonen som innsamles omfattes av ulike former for lovbestemt taushetsplikt. Til tross for at formålet med direktivet var begrensning av alvorlig kriminalitet, stiller direktivet verken krav til at de som berøres skal være mistenkt for alvorlig kriminell virksomhet, eller at de har noen form for befatning med slik virksomhet (avsnitt 56-58).

Domstolen vektla videre at direktivet ikke oppstiller noen krav til at informasjonen som innsamles er relevant med hensyn til offentlig sikkerhet. I den forbindelse ble det lagt særlig vekt på at informasjonsinnsamlingen ikke har begrensninger med hensyn til tid, sted, eller hvem som rammes (avsnitt 59).

Domstolen la også vekt på at direktivet verken oppstiller materielle eller prosessuelle vilkår med hensyn til nasjonale myndigheters tilgang og bruk av dataene som innsamles. Direktivets artikkel 4, som regulerer slike spørsmål, sier ikke eksplisitt at tilgang og bruk er begrenset til tilfeller hvor formålet er å forhindre, oppdage eller straffeforfølge nærmere avgrensede alvorlige kriminelle handlinger. Tvert imot følger det av artikkel 4 at medlemslandene selv skal bestemme vilkårene og prosedyrene for tilgang og bruk, men da i overensstemmelse med krav om nødvendighet og forholdsmessighet (avsnitt 61). Det ble i den forbindelse særlig poengtert at direktivet ikke krever at tilgang og bruk skal være begrenset til det som er strengt nødvendig i lys av formålet som søkes oppnådd, og at det ikke stilles krav om at tilgang og bruk skal være begrenset til den

informasjonen som en domstol eller annet uavhengig offentlig organ har vurdert som nødvendig i et konkret tilfelle (avsnitt 62).

Domstolen vektla også at direktivets artikkel 6 krever at lagringsperioden skal være minimum seks måneder for all innsamlet informasjon, uavhengig av sannsynligheten for at informasjonen er nyttig for å oppnå direktivets formål (avsnitt 63). I videreføringen av dette ble det også vist til at direktivet ikke oppstiller objektive vilkår som sikrer at lengden på lagringstiden, mellom 6 og 24 måneder, blir begrenset til det som er strengt nødvendig (avsnitt 64).

På grunnlag av de nevnte forhold konkluderte domstolen med at direktivet ikke oppstiller tilstrekkelig klare og presise regler for rekkevidden av krenkelsene av artikkel 7 og 8 i EU-charteret. Direktivet sikret derfor ikke at disse krenkelsene begrenses til det strengt nødvendige (avsnitt 65).

Domstolen konkluderte også med at direktivet ikke oppstiller sikkerhetstiltak som gir en effektiv beskyttelse mot misbruk og ulovlig tilegnelse av data. Det ble blant annet vist til at direktivet ikke legger konkrete føringer for hvilke sikkerhetstiltak tjenesteleverandørene må innføre, at økonomiske hensyn tillates vektlagt ved vurderingen av dette, og at direktivet ikke krever irreversibel destruering av innsamlet materiale ved endt lagringstid (avsnitt 66-67).

Avslutningsvis ble det også understreket at direktivet ikke setter krav til at den innsamlede informasjon må holdes innenfor EUs grenser. Dette reiser tvil om hvorvidt et uavhengig organ kan sikre etterlevelse av rettighetene om personvern, i tråd med i artikkel 8 nr. 3 i charteret.

Som det fremgår av gjennomgangen ovenfor, pekte domstolen på en rekke forhold før de konkluderte med at direktivet var strid med de grunnleggende rettighetene i artikkel 7 og 8 i EU-charteret. Ettersom domstolens konklusjon baserer seg på en helhetlig vurdering av disse forholdene, er det vanskelig å trekke sikre slutninger om hva som var utslagsgivende for domstolen. Dette medfører at det er uklart hvilke konkrete justeringer direktivet måtte vært underlagt for at kravet til proporsjonalitet skulle blitt ansett oppfylt. Et sentralt punkt i EU-domstolens vurdering var at direktivet verken gir prosessuelle eller materielle regler om tilgang til og bruk av data. Ei heller oppstiller direktivet objektive vilkår for å sikre at tilgang og bruk skjer i tråd med prinsippene om nødvendighet og forholdsmessighet. Denne oppgaven overlates til nasjonale myndigheter. Dermed oppstår spørsmålet om de nasjonale datalagringslovgivningene kan utformes på en måte som medfører at unntaksvilkårene i EU-charteret artikkel 7 og 8 blir oppfylt. I en rekke land har den nasjonale lovgivningen som gjennomførte direktivet blitt underkjent. Sverige og Danmark utgjør, som vi skal komme tilbake til, unntak fra denne tendensen. Foreløpig har ikke EU-domstolen tatt stilling til om noen av de nasjonale lovgivningene medfører brudd på artikkel 7 eller 8.

Etter vår oppfatning er det høyst uklart om nasjonale myndigheter ved implementering av direktivet kan reparere samtlige av de forhold domstolen vektla. I avsnitt 59 i dommen kritiseres direktivet for ikke å oppstille noen krav til at informasjonen som

innsamles er relevant med hensyn til offentlig sikkerhet. Domstolen viste i den forbindelse spesifikt til at informasjonsinnsamlingen ikke har begrensninger med hensyn til tid, sted, eller hvem som rammes. Det kan argumenteres for at domstolen undergraver selve kjernen i direktivet, når de i dette avsnittet vektlegger at direktivet ikke begrenser datainnsamlingen til å skje fra *"persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."* Om EU-domstolen mente at dette forholdet i seg selv medfører at grensen i proporsjonalitetsvurderingen var overskredet, er vanskelig å vite. Domstolen sa samtidig i avsnitt 44 at lagring av data med sikte på å gi de kompetente myndigheter tilgang til dem forfølger et mål med allmenn interesse. Ut fra dette kan det synes som om domstolen ikke mente at datalagring som sådan stred mot charteret, men at datalagring kan forsvares hvis det ledsages av nasjonale regler som på en forsvarlig måte angir og begrenser myndighetenes tilgang til de lagrede data. Denne tolkningen av dommen er lagt til grunn både av svenske og tyske myndigheter i sine vurderinger, og av engelske High Court of Justice i saken Davis med flere mot The Secretary of State for the Home Department. Men det er ut fra de kravene som domstolen oppstiller vanskelig å se at selv svært klare og presist avgrensede regler om tilgang til og bruk av data, vil være tilstrekkelig for å unngå en krenkelse av charterets artikkel 7 og 8.

Det store, prinsipielle spørsmålet om hvorvidt datalagring som sådan er i strid med charteret er altså etter vår oppfatning ikke løst i dommen. Det er for oss uklart om domstolens uttalelser i avsnitt 59 (sitert ovenfor) i realiteten slår bena under allmenn datalagring eller om slik lagring kan rettferdiggjøres med tilstrekkelig presisjon i kriteriene for bruk og nødvendige rettssikkerhetsmekanismer. Det er imidlertid grunn til å tro at EU-domstolen vil uttale seg om det prinsipielle spørsmålet i sak C-203/15 som ligger til behanding. Saken gjelder en foreleggelse datert 4. mai 2015 fra Kammarrätten i Stockholm i en sak mellom Tele2 Sverige AB og Post- och telestyrelsen. Kammarrätten har forelagt følgende spørsmål for EU-domstolen:

> *Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime (as described [below under points 1-6]) compatible with Article 15(1) of Directive 2002/58/EC, 1 taking account of Articles 7, 8 and 15(1) of the Charter?*
>
> *If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:*
>
> - *access by the national authorities to the retained data is determined as [described below under paragraphs 7-24], and*
> - *security requirements are regulated as [described below under paragraphs 26-31], and*

- *all relevant data are to be retained for six months, calculated as from the day the communication is ended, and subsequently deleted as [described below under paragraphs 25]?*

Slik det ser ut for oss, foranlediger det første spørsmålet stillingtaken til det vi ovenfor har kalt det prinsipielle spørsmålet. Det er ikke dermed sagt at spørsmålet er endelig løst for Norges del. EU-charteret er som kjent kke bindende for Norge. Rettighetene som er knesatt i charterets artikkel 7 og 8 er imidlertid – i alle fall hovedsak – også å finne i en rekke andre kilder som Norge er bundet av, herunder EMK. Dersom DLD implementeres i norsk rett, må det forventes at norske domstoler vil måtte vurdere om reglene er i strid med rettighetsbestemmelser Norge er bundet av. EU-domstolen konkluderte med at lovgivers skjønnsmargin er begrenset på dette området som følge av de berørte rettighetenes karakter og graden av krenkelsen. Det må, som vi skal komme tilbake til, forventes at også norske domstoler vil foreta en intens prøving av reglenes gyldighet.

3 OVERORDNEDE REGLER OM BESKYTTELSE AV PRIVATLIVET

3.1 Norsk rett

3.1.1 Grunnloven

Grunnlovens § 102 beskytter privatlivet og borgernes kommunikasjon. I annet ledd pålegger bestemmelsen statens myndigheter å sikre et vern om den personlige integritet. Bestemmelsen utgjør en generell bestemmelse om respekt for privatlivets fred, personvern og personopplysningsvern. Teksten i Grunnloven § 102 er modernisert sammenlignet med EMK fra 1950 og SP fra 1966 idet den – i likhet med EU-charteret artikkel 8 – uttrykkelig nevner kommunikasjon, og ikke bare korrespondanse.

Lønning-utvalget viste til at en beskyttelse av privatlivets fred, personvern og personopplysningsvern har fått økt aktualitet både som følge av den tekniske utvikling og den rettslige utvikling. Med "personvern" forstod Lønning-utvalget ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse, noe som også innbefattet det for norsk rett tradisjonelle begrepet "privatlivets fred". Begrepet "personopplysningsvern" forstod utvalget som et nyere begrep som har sammenheng med økt innsamling, bruk og lagring av personopplysninger i samfunnet. Utvalget forstod personopplysningsvern som vern av den enkeltes rett til innflytelse på bruk og spredning av informasjon om seg selv.

Den teknologiske utviklingen var også en viktig del av begrunnelsen til Lønning-utvalget for å grunnlovsfeste personopplysningsvernet:

> *Grunnlovsfesting av retten til privatlivets fred, personvern og personopplysningsvern kan i tillegg vise seg å bli et viktig rettslig verktøy i møte med fremtidens teknologiske utvikling og utfordringer. Lovregulering på enkeltområder vil i noen grad måtte ligge i etterkant av den teknologiske utvikling, nettopp fordi fremtidens konkrete problemstillinger kan være vanskelige å forutsi. Dermed oppstår behovet for det generelle og overordnede vern, der prinsippet om privatlivets fred, personvern og personopplysningsvern er nedfelt i den høyeste rettskilde. Det kan ikke utelukkes at den teknologiske utvikling gjør at en slik grunnlovsbestemmelse vil vise seg å bli sentral i de kommende tiår.*[2]

Utvalget peker med dette på at bestemmelsen skal ha selvstendig betydning på et dynamisk område hvor lovgivningen ikke alltid rekker å følge med utviklingen.

Lønning-utvalget foreslo grunnlovsfestet en regel om at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare skulle kunne finne sted i henhold til lov. Utvalget presiserte i denne forbindelse at lovhjemmel ikke er et tilstrekkelig vilkår for systematisk innhenting, oppbevaring og bruk av personopplysninger, men at det måtte innfortolkes et forsvarlighetskrav ved siden av kravet til lovhjemmel. Denne forsvarlighetsvurderingen skulle det imidlertid være

[2] Dok.nr.16 (2011-2012) s. 175-176.

lovgiver som måtte foreta, slik at domstolene etter utvalgets oppfatning bare skulle kunne overprøve denne vurderingen der lovgiver ikke oppfyller sin plikt til å sikre personopplysninger tilstrekkelig.

Bestemmelsen om lovgivning ble ikke fulgt opp av konstitusjonskomiteens flertall. De ville ha en bestemmelse om myndighetenes plikt til å sikre personvernet mer som en "politisk retningslinje", selv om også denne vil innebære en "ytterste skranke for lovgiver".[3] Komiteen ga imidlertid samtidig uttrykk for at § 102 "skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede".

Flertallet i kontroll- og konstitusjonskomiteen uttalte som begrunnelse for det forslaget som de stilte seg bak og som ble vedtatt:

> *Det alternativ flertallet stiller seg bak, gjør retten til privatliv mv. i første ledd til en rettighet for den enkelte. Når retten er til 'respekt for' privatlivet, er det likevel for å synliggjøre at lovlig etterretning ikke er utelukket, som diskutert av Menneskerettsutvalget.*
>
> *Av de grunner som fremhevet av utvalget, er annet ledd utformet mer som en politisk retningslinje, som imidlertid innebærer en ytterste skranke også for lovgiver.*
>
> *Samme presisering som her er foreslått, er gjennomført i samtlige menneskerettighetskonvensjoner og i EUs Charter of fundamental Rights.*

To ulike mindretall hadde formulert alternative forslag. Felles for disse var at de i tillegg omtaler særskilt beskyttelse av personopplysninger.

Flertallsforslaget vitner om en oppfatning av at retten til personvern i EMK artikkel 8 nr. 1 og i EU-charteret artikkel 7 og 8 nr. 1 er relativt sammenfallende. Grunnlovsbestemmelsen favner begge. Forslagene fra mindretallet om å gå lenger og også uttrykkelig verne personopplysninger, ble avvist.

Med dette kan det se ut som om komiteen ønsket å dempe domstolskontrollen med lovgivningen i enda større grad enn Lønning-utvalgets forslag tilsa. I samme retning trekker flertallets kommentar om at "[n]år retten er til "respekt for" privatlivet, er det likevel for å synliggjøre at lovlig etterretning ikke er utelukket, som også diskutert av Menneskerettighetsutvalget."

Bestemmelsen var gjenstand for behandling i Høyesterett allerede i november 2014, se Rt. 2014 s. 1105. Et spørsmål her var om det kan stilles særlige kvalitative krav til den lovbestemmelsen som hjemler inngrep i personvernet, og hvilken betydning det

[3] Innst.186 S (2013-2014) s. 27.

eventuelt skal ha for domstolsprøvingen. Saken gjaldt bruk av overskuddsinformasjon fra kommunikasjonskontroll som ledd i etterforskningen av en sak om innsidehandel og manipulasjon av aksjekurser. I innledningen av etterforskningen ble saken etterforsket som en sak om organisert kriminalitet, og mistanken om dette ga grunnlag for å gjennomføre kommunikasjonskontroll av de mistenktes telefoner og datautstyr. Påtalemyndigheten frafalt imidlertid siktelsen som gikk ut på at de straffbare handlingene var foregått på en organisert måte. Det materialet som påtalemyndigheten hadde fått, fikk derfor status som overskuddsmateriale for siktelsene om innsidehandel og kursmanipulasjon. Spørsmålet for Høyesterett var om dette innebar at de opplysningene som var innhentet om de siktede gjennom kommunikasjonskontrollen måtte legges bort.

Førstvoterende tok i dommen utgangspunkt i at kommunikasjonskontroll er et integritetsinngrep "*som bare er tillatt dersom, og utelukkende i den utstrekning, dette har hjemmel i lov, direkte eller ved forskrift med hjemmel i lov. Dette følger allerede av det alminnelige legalitetsprinsippet som er etablert ved konstitusjonell sedvanerett, og som nå kommer til uttrykk i § 113*".[4] På denne bakgrunn slo han fast at oppbevaring av materiale som er innhentet ved kommunikasjonskontroll bare kan skje i den utstrekning det er hjemmel for dette i lov eller i forskrift gitt med hjemmel i lov. Han tok også som utgangspunkt at en lov som tillater kommunikasjonskontroll må tilfredsstille visse kvalitetskrav: den må være tilgjengelig og så presis som forholdene tillater og gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for innsyn, sikkerhet og sletting. Et mindretall på to dommere mente at det ikke kunne stilles andre krar til lovens klarhet når det gjelder kommunikasjonskontroll en det som ellers gjelder for regler som gir adgang til inngrep overfor enkeltpersoner.

Førstvoterende trekker blant annet frem at loven må gi rimelige garantier for å sikre personvernet. Flertallets tilnærming innebærer at § 113 er mer enn en politisk retningslinje og en "ytterste skranke", og at domstolene bør gå ganske langt inn i vurderingen av hvilken etterretning som kan tillates innen de rammer privatlivets fred setter, også når etterretningen bygger på lov. Selv om man kan diskutere dommens prejudikatsverdi for forståelse av grunnloven og det norske legalitetsprinsippet, gir den uttrykk for en oppfatning som ikke er særlig kontroversiell når det gjelder tolkningen av EMK. I *S. and Marper v. UK* uttalte EMD i avsnitt 95:

> *The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion*

[4] Rt. 2014 s. 1105 avsnitt 24.

conferred on the competent authorities and the manner of its exercise (see Malone v. the United Kingdom, 2 August 1984, §§ 66-68, Series A no. 82; Rotaru v. Romania [GC], no. 28341/95, § 55, ECHR 2000-V; and Amann, cited above, § 56).

3.1.2 Personopplysningsloven og beskyttelse av personopplysninger

Personopplysningsloven er den generelle loven for behandling av personopplysninger i Norge. Loven trådte i kraft den 1. januar 2001 og erstattet personregisterloven fra 1978. Personregisterloven kom til anvendelse på opprettelsen av personregistre, det vil si registre eller fortegnelser der personopplysninger ble lagret systematisk. Den teknologiske utviklingen åpnet imidlertid for stadig nye muligheter til å behandle personopplysninger uten at det ble opprettet et register, og det var nødvendig med et nytt regelverk som var tilpasset dagens situasjon. Målet var å lage en teknologiuavhengig lov. Samtidig var Norge, gjennom EØS-avtalen, forpliktet til å implementere EUs personverndirektiv (direktiv 95/46/EF).

Personopplysningsloven bygger på visse kjerneverdier som er felles for nasjonal lovgivning som bygger på internasjonale konvensjoner og standarder.[5] Det overordnede synspunktet er at personlige data skal være gjenstand for en fair og lovlig behandling. Dette innebærer for det første et krav om proporsjonalitet med de tre kravene til at innsamling og behandling av persondata skal være egnet og relevant for formålet, at det skal være nødvendig og at inngrepet i personvernet ikke må veie tyngre enn fordelen av det. Det er en økende tendens til at internasjonale og nasjonale domstoler legger begrensninger på behandlingen av persondata ut fra en selvstendig vurdering av proporsjonaliteten. I norsk sammenheng er Rt. 2014 s. 1105 uttrykk for denne tendensen også på det straffeprosessuelle området.

For det andre innebærer det overordnede utgangspunktet at mengden av persondata som samles inn skal være så liten som mulig og begrenset til det som er nødvendig for det formålet som dataene samles inn for. I slekt med dette er prinsippet om at formålet med datainnsamling og databehandling skal være klart angitt og at data ikke må brukes til andre formål. Dette prinsippet ble understreket av Høyesterett i Rt. 2013 s. 234.

I denne saken hadde et avfallsselskap sammenlignet de ansattes timelister med logger fra GPS-systemer som viste når bilene hadde vært i aktivitet og hvilke søppeldunker som var håndtert når. Førstvoterende uttalte blant annet at:

> *… innsamling av opplysninger skal skje til uttrykkelig angitte og saklige formål, og at senere behandling ikke må være uforenlig med disse formål. Dette prinsippet, som er nedfelt i artikkel 6 første ledd bokstav b i nevnte direktiv 95/46/EF, regnes internasjonalt som et fundamentalt og viktig prinsipp på personopplysningsrettens område.*

[5] Se nærmere Lee A. Bygrave, Data Privacy Law An International Perspective, Oxford University Press Oxford 2014 s. 145-167.

De andre viktige kjerneverdiene for lovgivningen om persondata er retten til innflytelse på behandlingen av data som gjelder en selv, kravet til kvaliteten av de data som behandles, datasikkerhet og egen beskyttelse av særlig sensitive data. Lagring av kommunikasjonsdata utfordrer flere av disse. Retten til innflytelse utfordres ved at den enkelte ikke får bestemme over bruken av opplysninger som genereres gjennom at man bruker kommunikasjonstjenester, selve mengden av data som lagres utfordrer datasikkerheten og særlig sensitive data kan miste sin beskyttelse hvis lagringen omfatter kommunikasjonen også til for eksempel helsepersonell og sjelesørgere. Også kravet til datakvalitet utfordres gjennom at kommunikasjonsdata bare indirekte sier noe om kommunikasjon som har funnet sted, slik at de kan gi opphav til feilslutninger om konkrete personers tilknytning til straffbare handlinger.

Politiets behandling av personopplysninger er regulert i en rekke lover, forskrifter og instrukser. Generelt kan man si at også behandling av personopplysninger der politiet er ansvarlig, reguleres av personopplysningsloven. En viktig begrensning følger imidlertid av personopplysningsforskriftens § 1-3, som gir unntak fra personopplysningslovens virkeområde for saker som behandles eller avgjøres i medhold av rettspleielovene, herunder straffeprosessloven. Det er imidlertid ikke gitt at denne begrensningen gjelder behandling av opplysninger utenfor den konkrete straffesak, for eksempel nedtegnelse av opplysninger i sentrale og lokale registre som brukes i politiets saksbehandling. Dette vil bero på en konkret vurdering. Personopplysningslovens anvendelsesområde vil også innskrenkes i den grad særlov regulerer behandlingsmåte, jf. personopplysningsloven § 5.

3.2 Internasjonale menneskerettigheter

Retten til privatliv og personvern er en grunnleggende del av det internasjonale menneskerettighetsvernet. Som mange av de andre grunnleggende rettighetene sprang det ut av erfaringene fra diktatur og undertrykkelse og begivenhetene rundt andre verdenskrig. Retten til privatliv er viktig fordi en privat sfære muliggjør utfoldelse for individet. Uten privatliv er det vanskelig å realisere og opprettholde en personlig identitet, verdighet, autonomi, fantasi og kreativitet. Privatlivet muliggjør det å tenke og skape i frihet og å knytte bånd til medmennesker i fortrolighet. Privatliv muliggjør også å bygge forhold basert på tillit, vennskap og intimitet, noe som er av avgjørende betydning for å utvikle sosiale relasjoner og et sivilt samfunn. Mangel på privatliv vil føre til at den enkelte trekker seg inn i seg selv og til at individene isoleres. Slik er privatliv også nødvendig for å sikre oppnåelsen av andre menneskerettigheter som ytringsfrihet og andre politiske friheter samt retten til en rettferdig rettergang. Beskyttelse av privatlivet er avgjørende for at kritiske røster skal kunne tørre å varsle om kritikkverdige forhold og for pressens mulighet til å fylle sin samfunnsoppgave. Beskyttelse av privatlivet er endelig viktig i beskyttelsen av den enkelte mot statsmakt og andre mektige institusjoner. Der staten kan overvåke kommunikasjon, gir det staten mulighet til kontroll og manipulasjon gjennom for eksempel å diskreditere borgere gjennom offentliggjøring av ufordelaktig informasjon om dem, å forutsi og gripe inn overfor opplevde trusler mot den politiske makten og å kartlegge og profilere ulike grupper av minoriteter på grunnlag av for eksempel etnisitet eller politisk holdning.

De aller fleste traktater om sivile og politiske menneskerettigheter inneholder bestemmelser som anerkjenner personvern som grunnleggende rettighet. Dette kommer først og fremst til uttrykk i bestemmelser om retten til privatliv ("privacy" eller "private life"). Slike bestemmelser finner vi blant annet i konvensjoner vedtatt av De Forente Nasjoner (FN) og Europarådet. Bestemmelsene bygger på FNs Verdenserklæring om menneskerettighetene av 1948 artikkel 12 som lyder som følger:

> *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 (forkortet "SP") ble vedtatt 16. desember 1966 og trådte i kraft 23. mars 1976. Den inneholder en bestemmelse (artikkel 17) som lyder omtrent det samme som artikkel 12 i Verdenserklæringen:

> *1) Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.*
>
> *2) Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.*

FNs Menneskerettighetskomité har uttalt i General Comment nr. 16 av 23. mars 1988 at SP artikkel 17 krever at personopplysninger innen både offentlig og privat sektor blir behandlet i samsvar med grunnleggende prinsipper for personopplysningsvern.

I sin rapport om "The Right to Privacy in the Digital Age" fra 30. juni 2014 stiller FNs høykommissær for menneskerettigheter opp følgende betingelser for at et inngrep i retten til privatliv etter FN-konvensjonen artikkel 17 skal være lovlig, se avsnitt 23:

> *These authoritative sources point to the overarching principles of legality, necessity and proportionality, the importance of which also was highlighted in many of the contributions received. To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet*

these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

Ethvert inngrep må således ifølge høykommissæren ha hjemmel i lov, og loven må være tilstrekkelig tilgjengelig, klar og presis til at den enkelte ut fra loven kan fastslå hvem som er autorisert til å foreta overvåkning av data, og på hvilke betingelser. Inngrepet må videre være nødvendig å oppnå et formål, forholdsmessig til dette formålet og det minst inngripende middel for å nå det, og det må kunne påvises at det er en mulighet for at målet vil bli realisert gjennom inngrepet. Det er myndighetene som ønsker inngrepet som må vise at inngrepet har sammenheng med et legitimt mål. Inngrepet må til slutt ikke gjøre kjernen i retten til privatliv meningsløs, og inngrepet må være i samsvar med andre rettigheter, slik som retten til ikke å bli diskriminert.

Den europeiske menneskerettskonvensjonen 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 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.

Artikkel 8 (1) verner om fire rettigheter: privatlivet, familielivet, hjemmet og korrespondansen. EMD har i liten grad skilt de ulike rettighetene fra hverandre, og langt på vei vil retten til privatliv og retten til korrespondanse gli over i hverandre. Tilsvarende vil vernet om privatlivet og om det private hjem i mange tilfeller være vanskelig å holde helt atskilt. Samlet sett er det imidlertid tale om et vern om den private sfære.

Bestemmelsen pålegger en stat å ha lover som verner privatlivets fred og som verner den enkelte mot å få sin integritet og ære krenket – både av offentlige myndigheter og private aktører. Plikten omfatter også at det må finnes lover som regulerer innsamling, forvaltning og spredning av personopplysninger

Inngrepsadgangen i EMK artikkel 8 (2) setter altså krav til at inngrepet har hjemmel i lov og oppfyller et legitimt formål. For øvrig må det være nødvendig i et demokratisk samfunn for å oppnå formålet om å bekjempe kriminalitet og vareta den nasjonale sikkerheten. Inngrepet bør ikke gå lenger enn det som er nødvendig for å oppnå nevnte formål, det vil si at det stilles krav til forholdsmessighet.

Den europeiske menneskerettighetsdomstolen har definert privatliv (”private life”) relativt bredt. Domstolen fastslår at begrepet omfatter visse aktiviteter som utføres i den offentlige sfære (jf. for eksempel *Niemietz v. Germany*, dom av 16. desember 1992, og og *Peck v. UK*, dom av 28. januar 2003). Domstolen har også pekt på at selv offentlige

handlinger kan være omfattet av privatlivet dersom det foreligger en systematisk eller permanent lagret fortegnelse over dem, se P.G. and J.H. v UK. Dette er en videreføring av at registrering og videre behandling av personopplysninger, uten at den registrerte har gitt sitt samtykke til eller fått kunnskap om behandlingen, i seg selv vil være et inngrep etter artikkel 8(1) (jf. eksempelvis Leander-saken). For det tredje, når domstolen vurderer hvorvidt en handling utgjør et inngrep i privatliv mv., legges det blant annet vekt på folks rimelige forventninger om hva som er privat. Et fjerde moment er at registrering og lagring av personopplysninger – uten at disse brukes videre – i seg selv kan være nok til å utgjøre et inngrep i henhold til artikkel 8(1), jf. *Amann v. Switzerland, dom av 16. februar 200*0. Det siste momentet er at også private aktørers behandling av personopplysninger kan rammes av EMK artikkel 8, jf. for eksempel *von Hannover v. Germany*, dom av 7. februar 2010.

EMD har i flere avgjørelser vurdert lovligheten av kommunikasjonskontroll og overvåkning av datatrafikk mot beskyttelsen av privatlivet i EMK artikkel 8. Allerede i *Malone v. UK* fra 2. august 1984 slo EMD fast at trafikkdata, liste over telefonnumre som det var ringt fra på en bestemt telefon, er omfattet av retten til uhindret kommunikasjon etter EMK artikkel 8, se avsnitt 84. I saken P.G. and J.H. v UK slo domstolen fast at telekommunikasjonsselskapenes registrering av slike data for faktureringsformål ikke er en krenkelse og må avgrenses mot ”the interception of communications which may be undesirable and illegitimate in a democratic society unless justified”. EMD har også, blant annet i *Weber and Saravia v. Germany*, avgjørelse av 29. juni 2000, slått fast at selve det forhold at det finnes lovgivning som gir anledning til hemmelig overvåkning av kommunikasjon i seg selv er et inngrep overfor kommunikasjonsfriheten til den som kan bli gjenstand for overvåkning. Det er således ikke avgjørende om hjemlene faktisk blir brukt eller om myndighetene får kjennskap til og nyttiggjør seg informasjonen.

I *Weber and Saravia v. Germany* dreide det seg om strategisk overvåkning av blant annet kommunikasjonen med utlandet med sikte på å avdekke trusler mot rikets sikkerhet. Domstolen aksepterte tiltakene da den fant at de var tilstrekkelig avgrenset både med hensyn til hvilken kommunikasjon som kunne overvåkes og i de situasjoner som dette kunne skje. I en senere tilsvarende sak, *Liberty and others v. UK*, ble overvåkningsregimet underkjent av EMD. I denne saken hadde myndighetene tilgang til kommunikasjonen til "any person who sent or received any form of telecommunication outside the British Islands during the period in question”, uten at utvalget av den kommunikasjonen som skulle overvåkes var nærmere begrenset i offentlig tilgjengelig lovgivning. Domstolen har også hatt en rekke saker som gjelder kontroll med kommunikasjonen til individualiserte personer, senest *Kennedy v. UK*. Slik overvåkning er blitt godtatt når loven klart angir hva slags forhold og situasjoner som kan gi grunn til tiltaket, og beslutningen om iverksetting konkret angir hvem som kan overvåkes.

EMD har således hatt en rekke andre saker som gjelder myndighetenes *tilgang* til kommunikasjonsdata og også deres tilgang til å overvåke pågående kommunikasjon både ved å avlytte bestemte personer og ved mer generell, strategisk overvåkning av kommunikasjon. Foreløpig har den ikke hatt til behandling spørsmålet om hvorvidt *lagring* av kommunikasjonsdata med det formål senere å gjøre opplysninger tilgjengelig

for politiets arbeid lar seg forene med EMK. Dette reiser helt andre spørsmål enn de som har vært oppe i domstolens tidligere saker. På den ene side er det snakk om data som er mindre sensitive enn det som har vært tilfelle i noen av de tidligere sakene siden det ikke dreier seg om innholdet av den kommunikasjonen som skjer. På den annen side er utvalget av de data som skal lagres verken avgrenset til bestemte situasjoner eller kretser av personer. Det ligger en sak til behandling i EMD som gjelder konvensjonsmessigheten av politiets tilgang til kommunikasjonsdata som telekommunikasjonsoperatørene lagrer for sine egne formål, se *Hannes Trettes and Others v. Austria*[6]. Men i et slikt tilfelle er ikke selve lagringen av data en krenkelse, se P.G. and J.H. v UK, da registreringen teleselskapet gjør for sine faktureringsformål ut fra sin "very nature" må avgrenses mot registrering som skjer for overvåkningsformål. Avgjørelsen i den saken vil derfor neppe løse spørsmålet om hvorvidt og hvordan datalagring lar seg forene med EMK.

Kravet til at loven må gi den som kan bli gjenstand for overvåkning mulighet til å fastslå når overvåkning vil kunne skje, innebærer ikke at den enkelte må få beskjed i hvert tilfelle slik at man kan innrette seg etter at man er under overvåkning. Kommunikasjonskontrollen kan med andre ord holdes hemmelig overfor den som er under kontroll. Men loven må presist angi betingelsene for å foreta en slik kontroll, hva slags typer av handlinger som kan gi grunnlag for kontroll, avgrensning av kretsen av personer som det kan foretas kontroll overfor, begrensning av tiden som kontrollen kan skje, prosedyrene for undersøkelse, bruk og lagring av data, forsiktighetstiltak ved deling av dataene med andre og omstendighetene under hvilke de registrerte data kan eller må slettes, se *Weber and Savaria v. Germany* avsnitt 95.

Kravet til proporsjonalitet kan innebære begrensninger i adgangen til lagring av data overhodet. I *S and Marper v. UK* fra 4. desember 2008 var spørsmålet om det var adgang til å lagre vevsprøver, DNA-profiler og fingeravtrykk fra personer som hadde vært under etterforskning for straffbare handlinger, men hvor tiltale ikke var tatt ut og etterforskningen avsluttet. UK argumenterte med at de registre som ble bygget opp gjennom lagring av slike data var av uvurderlig betydning for etterforskning og oppklaring av straffbare handlinger. EMD kom likevel til at slik lagring av data fra personer som ikke var dømt for straffbare handlinger var uproporsjonal. Selv om utviklingen av moderne teknologi innebærer at mulighetene til å oppklare straffbare handlinger blir mer effektiv, kan ikke myndighetenes adgang til å utnytte slik teknologi være ubegrenset. I den forbindelse uttalte EMD i avsnitt 112 at

> *... the Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.*

[6] Application no. 3599/10

En avgjørende faktor i denne saken var at Storbritannia var alene om å tillate en slik ubegrenset lagring av data om personer. Storbritannias argumentasjon for at dette skyldtes at Storbritannia var særlig avanserte i bruk av ny teknologi i etterforskningen, hadde ikke overbevisende vekt for EMD.

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.*

Som vi ser går charteret i artikkel 8 en del lengre enn de andre bestemmelsene i å spesifisere hva som ligger i personopplysningsvernet ved at det gir regler om behandlingen av opplysninger, rett til innsyn for den opplysningene angår og krav om kontroll med behandlingen av opplysninger. Disse mer presise kravene er en sentral bakgrunn for EU-domstolens behandling av DLD og for de vilkårene som domstolen satte for at datalagring skal kunne være i samsvar med charteret. Siden charteret ikke direkte er bindende for Norge, vil det være et sentralt punkt om tilsvarende krav kan utledes av de internasjonale menneskerettighetsreglene og grunnloven, eller eventuelt av EØS-avtalen.

3.3 EØS

Etter endringen i Lisboa sier artikkel 6 i Unionstraktaten at "Unionen anerkjenner de rettigheter, friheter og prinsipper som er fastsatt i Den europeiske unions pakt av 7. desember 2000 om de grunnleggende rettigheter, tilpasset i Strasbourg 12. desember 2007, som skal være likeverdig med traktatene." EU-charterets artikkel 7 og 8, samt artikkel 52 om unntaksadgangen, er innholdsmessig relativt lik EMK artikkel 8. Likheten mellom EMK og EU-charteret kommer også frem i charteret artikkel 52 nr. 3 som sier at "I det omfang dette Charter inneholder rettigheter som tilsvarer de som er sikret ved den europeiske konvensjon om vern menneskerettigheter og grunnleggende friheter, har de samme betydning og omfang som i konvensjonen. Denne bestemmelse er ikke til hinder

for at EU-retten kan yde en mere omfattende beskyttelse". I tillegg til å sikre minst det samme beskyttelsesnivå i EUs domstoler som under EMK, krever bestemmelsen også at EU-domstolen fortolker charteret på nytt dersom EMD styrker beskyttelsen av en rettighet hjemlet i EMK eller beslutter å utvide konvensjonsbestemmelsens anvendelsesområde.[7]

Et av formålene med artikkel 6 er å beskytte medlemsstater fra å bli underlagt forskjellige menneskerettighetsstandarder når de implementerer EU-retten. Dette skulle tilsi at en restriksjon på en rettighet som er del av EMK, bare kan forsvares dersom begrensningen også ville være tillatt etter konvensjonen.[8] På den annen side er det påpekt at det er "lite sannsynlig at EU-domstolen vil tillate medlemsstatene å bruke charteret til å rettferdiggjøre unntak fra traktatfestede forpliktelser."[9] I sin uttalelse 2/13 om EUs tiltredelse til EMD, ordlegger EU-domstolen seg om påvirkningen av EMK på EU-retten på en noe svakere måte enn charterets Artikkel 52 (3). Domstolen uttalte at den "lar seg inspirere (…) av retningslinjene i de internasjonale instrumentene om beskyttelse av menneskerettighetene", og at "EMK er av særlig betydning". Videre understreker domstolen at grunnleggende rettigheter må "tolkes og anvendes innenfor EU i samsvar med det forfatningsmessige rammeverket" i EU (avsnitt 177) der implementeringen av prosessen med integrering og oppnåelse av EUs mål, inkludert bevegelsesfriheten, "er Unionens *raison d'être*" (avsnitt 172).

Det følger av EU-domstolens uttalelse 2/13 at dens tilnærming til tolkningen av grunnleggende rettigheter innen EU i sin natur er forskjellig fra EMDs tilnærming til menneskerettighetene i EMK. EU-domstolen understreker i sin uttalelse at grunnleggende rettigheter i EU-retten må "tolkes og anvendes innen EU i samsvar med EUs konstitusjonelle rammeverk."[10] Dette konstitusjonelle rammeverket inkluderer de spesifikke særtrekkene ved EUs rettsorden og dens autonomi, prosessen med å skape en stadig tettere union mellom medlemsstatene, EUs formål, slik disse er nedfelt i Unionstraktatens Artikkel 3, og beskyttelsen av grunnleggende rettigheter som stipulert i charteret. EMDs tilnærming er tuftet på en dynamisk oppfatning, basert på formålet og hensikten med beskyttelsen av menneskerettighetene slik disse er definert i EMD og omfatter ikke EUs mål om markedsintegrering og bevaringen av EU-rettens spesifikke særtrekk. Siden dette er EU-domstolens eksplisitte mål også når den etablerer og tolker grunnleggende rettigheter, ligger det i sakens natur og er uunngåelig at det vil være forskjeller i resultatene de to domstolene kommer frem til. Av dette følger at resultatene fra EU-domstolen ikke alltid vil være veldig relevante for EMDs tolkning av EMK.

EU-charteret er ikke bindende for Norge. Det kan imidlertid indirekte få betydning fordi det er henvist til det i rettsakter som er bindende for Norge, eller i relevant rettspraksis fra EU-domstolen eller EFTA-domstolen. Vilkårene i EU-charteret artikkel 52 er dessuten

---

[7] Se Koen Lenaerts, The Court of Justice of the European Union and the Protection of Fundamental Rights, *Polish Yearbook of International Law*, nummer 31 / 2011, side 79-106, lagt ut på www.ceeol.com s. 98.

[8] Se Tobias Lock, The ECJ and the ECtHR: The Future Relationship between the Two European Courts, *The Law and Practice of International Courts and Tribunals* 8 (2009) 375-398 s. 382.

[9] Dorota Lecykiewicz, "Effective Judicial protection" of Human Rights after Lisbon: Should National Courts be Empowered to Review EU Secondary Law, *E.L. Rev* 2010, 35(3), 326-348 s. 332.

[10] Uttalelse 2/13 avsnitt 177.

relativt like bestemmelser om adgangen til unntak fra sletteplikten i personverndirektivet 1995/46/EF og kommunikasjonsverndirektivet 2002/58 EF. Begge disse direktivene er innlemmet i EØS-avtalen og således bindende for Norge. De er i hovedsak implementert i henholdsvis *personopplysningsloven* og *ekomloven*.

4 VURDERINGER OG RETTSAVGJØRELSER I ANDRE LAND

4.1 Sverige

DLD ble implementert i svensk rett gjennom lov- og forskriftsendringer som trådte i kraft 1. mai 2012. Bestemmelsene om lagring finnes i *lag om elektronisk kommunikation* (2003:389) (forkortet "LEK") kapittel 6 § 16 a-f. Nærmere bestemmelser er gitt i *forordning om elektronisk kommunikation* §§ 37-46.[11]

Den svenske implementeringen samsvarer i all hovedsak med minimumskravene oppstilt i direktivet. Et eksempel på dette er at lagringstiden er 6 måneder, se LEK kap. 6 § 16 d. Samtidig er den svenske reguleringen noe mer detaljert enn i direktivet. Dette følger naturlig av at direktivet overlater til nasjonale myndigheter å ta stilling til hvordan en rekke forhold nærmere skal reguleres. På to punkter går den svenske reguleringen lengre enn hva som kreves etter direktivet, se LEK kapittel 6 § 16 a. For det første omfatter lagringsplikten også data som er nødvendig for å lokalisere mobilt kommunikasjonsutstyr ved kommunikasjonens slutt. For det andre omfatter lagringsplikten data som genereres ved mislykket oppringning.[12]

I kjølvannet av EU-domstolens avgjørelse av 8. april 2014 ble det på oppdrag fra det svenske Justisdepartementet foretatt en utredning med mandat å analysere de svenske datalagringsreglene, vurdert opp mot EU-retten. Utredningen (Ds 2014:23), konkluderte med at de svenske reglene ikke er i strid med EU-retten.[13] Leverandører som etter EU-domstolens dom hadde gitt uttrykk for at de ikke ville følge datalagringsreglene ble, som følge av utredningens konklusjon, pålagt av det svenske post- og teletilsynet (forkortet "PTS") å gjenoppta lagringsaktivitetene.

To tjenesteleverandører påklaget vedtakene fra PTS til forvaltningsdomstolen i Stockholm. Retten konkluderte med at reglene ikke var i strid med svensk Grunnlov (*Regeringsformen*), Europakonvensjonen eller EU-charteret. Det ble fastslått at reglene utgjorde et inngrep i retten til privatliv og personvernet, men inngrepet ble funnet å oppfylle unntaksvilkårene, herunder kravet til proporsjonalitet, som følger av charteret. Klagen ble derfor avslått.[14] Avgjørelsen er anket, og kammarrätten i Stockholm ba i april 2015 EU-domstolen om en forhåndsavgjørelse.[15] Domstolen har foreløpig ikke avgitt sin forhåndsavgjørelse. En annen tjenesteleverandør har gjort gjeldende overfor Europakommisjonen at Sverige bryter charterets artikkel 7 og 8 ved å håndheve bestemmelsene om datalagring.[16]

Per i dag har det altså verken blitt foretatt endringer i de svenske reglene om datalagring eller i håndhevelsen av disse reglene.

---

[11] SOU 2015:31 *Datalagring och integritet*, s. 110
[12] Op.cit. s. 111
[13] Op.cit. s. 117
[14] Op.cit. s. 139
[15] EU-domstolens sak C/203/2015) i saken Tele2 Sverige AB, http://www.kammarrattenistockholm.domstol.se/Om-kammarratten-/Nyheter-och-pressmeddelanden/Forhandsavgorande-om-den-svenska-datalagringen-begars-fran-EU-domstolen/
[16] SOU 2015:31 *Datalagring och integritet*, s. 139

4.2 Danmark

Datalagringsdirektivet ble implementert i dansk rett gjennom den såkalte *logningsbekendtgørelsen* (*Bekendtgørelse nr. 988 af 28/09/2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik*). Bekendtgørelsen trådte i kraft 15. september 2007.[17] Også i Danmark går den nasjonale lovgivningen lengre enn hva som kreves etter direktivet. Blant annet er lagringsplikten for tjenesteleverandørene ett år, se bekendtgørelsen § 9. Reglene om politiets adgang til å hente og benytte data er gitt i *retsplejeloven* kapittel 71. For en nærmere redegjørelse av de danske reglene, se Prop. 49 L (2010-2011) kapittel 4.1.

Etter EU-domstolens avgjørelse 8. april 2014 foretok Danmarks justitieministerium en utredning av de danske datalagringsreglene. Ministeriet publiserte en rapport med sine vurderinger og konklusjon den 2. juni 2014.[18] I likhet med rapporten om de svenske reglene konkluderte ministeriets rapport med at de danske datalagringsreglene ikke var i strid med EU-charterets artikkel 7 eller 8. Dette ble blant annet begrunnet med at de danske reglene er klare og presise, og at reglene gir en effektiv beskyttelse mot misbruk og ulovlig tilgang.[19] Det ble også vist til at dansk rett, i motsetning til direktivet, inneholder flere materielle og prosessuelle bestemmelser som regulerer adgangen til data.

4.3 Storbritannia

Storbritannia implementerte datalagringsdirektivet i april 2009 gjennom *The Data Retention (EC Directive) Regulations 2009*. Etter EU-domstolens avgjørelse i 2014 ble de nasjonale reglene endret, og et nytt regelverk ble introdusert gjennom *The Data Retention and Investigatory Powers Act 2014* ("DRIPA") som etter hastebehandling i parlamentet trådte i kraft 17. juli 2014.

I en avgjørelse avsagt 17. juli 2015 konkluderte the English High Court med at også DRIPA-regelverket er i strid med EU-charterets artikkel 7 og 8.[20] Domstolen avgrenset sin prøving av den britiske loven til om den var "incompatible with the requirements of EU law as interpreted by the CJEU in Digital Rights Ireland". Retten tok det utgangspunktet at EU-domstolens dom ikke innebærer at datalagring som sådan er i strid med EU-retten, men at dette er avhengig av de reglene som gir tilgang til de lagrede dataene er tilstrekkelig presise og begrunnet og omkranset av tilstrekkelige garantier. Domstolen fant at det britiske regelverket ikke oppstiller klare og presise regler som sikrer at tilgang til og bruk av data blir begrenset til det som er strengt nødvendig for å oppnå formålet om å avverge, oppdage eller straffeforfølge nærmere definerte alvorlige kriminelle handlinger. Videre vektla retten at reglene ikke setter som vilkår at tilgang til og bruk av data skal være begrenset til den informasjonen som en domstol eller annet uavhengig offentlig organ har vurdert som nødvendig i et konkret

[17] Prop. 49 L (2010-2011) s. 32
[18] SOU 2015:31 *Datalagring och integritet*, s. 143
[19] Op.cit. s. 145
[20] Avgjørelse [2015] EWHC 2092

tilfelle. Ved vurderingen ble sentrale avsnitt fra EU-domstolens avgjørelse sitert og tillagt stor vekt.

Det er foreløpig ikke avklart om britiske myndigheter vil anke avgjørelsen.

4.4 Tyskland

I Tyskland blir databeskyttelse sett som en av rettsstatens grunnpilarer. Dette må forstås på bakgrunn av erfaringene med to diktaturer i landets nære fortid.[21] Et av kjennemerkene til DDR-regimet var nettopp innsamling av personlige data gjennom uoffisielle medarbeidere. Disse opplysningene ble systematisk brukt til å rive opp familiebånd og legge personlige skjebner i grus. Resultatet er at det i dag knapt finnes noe annet land hvor personlige data har samme rettsbeskyttelse.

Den 20. mars 2010 avsa den tyske forfatningsdomstolen dom i en sak om foreneligheten av den tyske loven som gjennomførte DLD med grunnloven. Dommen reiser spørsmål i to retninger. For det første om DLD i seg selv strider mot grunnleggende rettigheter i EU-retten eller menneskerettighetene. Dernest om de tyske reglene som gjennomfører direktivet strider mot slike rettigheter. Den tyske forfatningsdomstolen kom til at direktivet som sådan ikke stred mot den tyske grunnloven. Den uttalte at lagring av kommunikasjonsdata ikke under enhver omstendighet er uforenelig med grunnloven. Retten la til grunn at direktivet ga nasjonale myndigheter et stort nasjonalt handlingsrom blant annet ved at det ikke påla nasjonale myndigheter å bruke slike lagrede data i kriminalitetsbekjempelse eller beskyttelse av nasjonale sikkerhetsinteresser. På grunn av dette handlingsrommet må domstolene prøve om den gjennomføringen som myndighetene har valgt er i overensstemmelse med grunnloven.

Begrunnelsen for at direktivet i seg selv ikke stred mot den tyske grunnloven var at etter direktivet skal de angjeldende data lagres av private, og ikke av de statlige myndighetene. Retten bygget her på den såkalte rettsstatlige asymmetrien som er grunnleggende i tysk rett: Mens private i utgangspunktet har frihet og ikke behøver å gi noen begrunnelse for eller rettferdiggjøre sine handlinger, er utgangspunktet for myndighetene motsatt: alt myndighetene gjør, må de kunne rettferdiggjøre under henvisning til et rettslig akseptabelt grunnlag. Det er derfor en grunnleggende forskjell mellom private og offentlige handlinger. Det er derfor først når de lagrede data blir gjort tilgjengelig for myndighetene at det oppstår behov for å rettferdiggjøre dette mot grunnrettighetene i den tyske grunnloven.

Forfatningsdomstolen tok utgangspunkt i at en slik datalagring bare kan være i overensstemmelse med grunnlovens beskyttelse av privatlivet og kommunikasjonsfriheten dersom de generelle kravene til proporsjonalitet oppfylles. Med dette overordnede utgangspunktet utledet retten en rekke helt bestemte betingelser som må oppfylles.

[21] Se Johannes Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305.

For det første må lovgiveren gi regler som sikrer at det ikke er opp til den enkelte teleoperatør å bestemme i hvilket omfang og på hvilken måte de lagrede data skal beskyttes mot misbruk. Mengden og arten av data tilsier at det settes strenge krav som sikrer mot at data kommer på avveie eller misbrukes. Slike regler må i det minste angi at de data som lagres må adskilles fra de øvrige dataene i virksomheten, tilgangen må være låst på tilfredsstillende måte og når det gis tilgang må det skje ut fra en sikker protokoll som sikrer direkte kontakt mellom den som oppbevarer dataene og den som gis tilgang, samt sporbarhet av kontakt og datautlevering.

Dernest må reglene sikre at de lagrede dataene bare kan brukes til formål hvor en slik tilgang er av overordentlig viktighet for å beskytte tungtveiende rettsgoder. Bruk av data til etterforskning og forfølgelse av straffbare handlinger kan bare skje i individuelle tilfeller hvor det er begrunnet mistanke om overtredelse av en alvorlig straffbar handling. Lovgiveren må på forhånd angi hvilke straffebud som skal kunne komme i betraktning som grunnlag for å kunne kreve data utlevert.

Skal det være tilgang til data for å avverge farer og for alminnelige etterretningsformål, må det foreligge en konkret trussel mot liv, legeme eller personlig frihet eller mot den nasjonale sikkerhet. Dataene kan således ikke være generelt tilgjengelige for sikkerhets- eller etterretningstjenesten.

Kommunikasjonen til personer hvor det er behov for særlig fortrolighet kan i utgangspunktet ikke være tilgjengelig for myndighetene. Dette dreier seg blant annet om kommunikasjonen til psykologer og sjelesørgere (det sosiale og kirkelige område – kontakten til leger, advokater og skatterådgivere er ikke omfattet av unntaket til domstolen). Lovgiveren må sørge for at det i utgangspunktet og som hovedregel er offentlighet om at myndighetene gis tilgang til data og at skjult anvendelse av dem reserveres for ekstreme tilfeller hvor undersøkelsens formål blir forfeilet om vedkommende som undersøkes gjøres kjent med det. Endelig er det et krav at det må foreligge en rettslig beslutning om overlevering og bruk av data.

Dersom det dreier seg om å gi tilgang til opplysninger om bestemte personers kommunikasjon eller om bestemte IP-adresser er kravene mindre strenge fordi det bare dreier seg om et mindre utsnitt av de lagrede dataene og fordi myndighetene selv i slike tilfeller ikke gis direkte tilgang til de lagrede data.

Flere kommentatorer har pekt på at de kravene retten oppstiller i praksis ikke lar seg oppfylle, og at de dermed gjøre det umulig å lagre og gi tilgang til trafikkdata uten å komme i konflikt med grunnloven. Blant annet er det ikke mulig i praksis for telekommunikasjonsselskaper å filtrere ut kommunikasjonen til og fra personer som skal særlig beskyttes så som leger, psykologer og sjelesørgere.[22]

Enkelte kommentarer er kritiske og problematiserer rettens karakteristikk av lagring av kommunikasjonsdata som "et særlig tungt inngrep" i grunnlovfestede rettigheter. Retten

[22] Se Björn Gercke, Ausgestaltung der Vorratsdataenspeicherung und Verwendung gespeicherten Datsn, StV (Strafverteidiger) 2010 Heft 6 - 282.

forklarer ikke hvordan en lagring av data som kommunikasjonsleverandørene allerede i dag foretar frivillig for å vareta egne behov blant annet i forbindelse med fakturering kan bli særlig tungtveiende inngrep når lagringen skjer på grunnlag av en offentligrettslig plikt.[23] Hvordan borgernes følelse av å bli overvåket forandrer seg med det rettslige grunnlaget for lagringen blir heller ikke forklart i dommen. Karakteristikken av lagringen som et særlig tungt inngrep har betydning for den slutningen retten trekker om de vilkårene som må oppstilles for å gi myndighetene tilgang til de lagrede dataene. Svikter denne, svikter dermed en viktig premiss for rettens videre vurderinger.

To dommere dissenterte. Dommer Eichenberger viste til at lagrede data ikke vil omfatte innholdet av kommunikasjonen og at dataene lagres desentralt hos de enkelte kommunikasjonsleverandører, hvilket medfører at lagringsplikten i seg selv ikke kan anses som det store inngrepet i rettigheter som flertallet mener det er. Den største faren ligger ikke i selve lagringen, men i sikkerhetsproblemene og misbrukspotensialet som denne store mengden lagrede data utgjør, både fra tjenestetilbyderen selv, fra uvedkommende som måtte få tilgang og fra uhjemlet bruk av dataene til offentlige formål.

4.5 Rettslig prøving i andre land

Som nevnt i avsnitt 1.1 har den nasjonale lovgivningen som gjennomførte lagringsplikten etter DLD vært gjenstand for prøving i en rekke europeiske land.

4.5.1 Østerrike

Den østerrikske forfatningsdomstolen avsa 27. juni 2014 en avgjørelse hvor store deler av den implementerte datalagringslovgivningen ble satt til side.[24] Domstolen konkluderte med at reglene var i strid med EMK artikkel 8 og konstitusjonsfestede regler om personvern. Avgjørelsen ble begrunnet i at datalagringsreglene ikke oppstilte tilstrekkelig klare og presise regler om lagring av, tilgang til og sletting av data.

4.5.2 Belgia

Forfatningsdomstolen i Belgia underkjente den nasjonale datalagringslovgivningen i en avgjørelse 11. juni 2015.[25] Den nasjonale lovgivningen ble funnet å være i strid med artikkel 7, 8 og 52 i EU-charteret.

4.5.3 Nederland

I en avgjørelse fra 11. mars 2015 konkluderte en nederlandsk underrettsdomstol med at den nasjonale datalagringslovgivningen medførte et brudd på charterets artikkel 7 og 8 og 52.[26] Konkret ble det vist til at det ikke forelå adekvate garantier for effektivt å begrense informasjonstilgangen til bruk for bekjempelse av alvorlig kriminalitet, og til det strengt nødvendige i den forbindelse. Domstolen så også prinsipielle problemer med selve lagringsplikten. Den viste til at lagringen ikke skiller mellom nyttig og unyttig informasjon, ei heller mellom hvilke personer som rammes. Retten la også vekt på at

[23] Se Markus Mösti, Vorratsdatenspeicherung - wie geht es weiter? ZRP 2011, 225.
[24] Avgjørelse G 47/2012, 59/2012 G, G 62/2012, 70/2012 G, G 71/2012
[25] Avgjørelse 84/2015.
[26] Avgjørelse C/09/480009 / KG ZA 14/1575

lovgivningen ikke oppstiller objektive kriterier for å begrense lagringstiden til det strengt nødvendige. Regelverket som ble vurdert var allerede under endring som følge av EU-domstolens avgjørelse, men det hadde ikke trådt i kraft. Det gjenstår å se hvilken betydning endringen av regelverket får.

4.5.4 Tsjekkia

Den tsjekkiske forfatningsdomstolen underkjente store deler av den implementerte datalagringslovgivningen gjennom to avgjørelser i 2011. [27] Domstolen konkluderte med at lovgivningen ikke oppstilte tilstrekkelig klare, presise og detaljerte regler, at det ikke forelå tilstrekkelige mekanismer for å sikre at innhentende data kun ble brukt til forebyggelse og oppklaring av alvorlig kriminalitet, og at grunnleggende krav om nødvendighet ikke var møtt. Som ledd i vurderingen viste domstolen til praksis fra EMD, samt avgjørelser fra andre europeiske forfatningsdomstoler. Etter avgjørelsene ble den tsjekkiske lovgivningen undergitt vesentlige endringer, og den nye lovgivningen har foreløpig ikke blitt angrepet rettslig.

4.5.5 Bulgaria

I en avgjørelse fra Bulgarias forfatningsdomstol avsagt 12. mars 2015 ble den nasjonale datalagringslovgivningen funnet å være i strid med EU-charteret og den bulgarske grunnloven.[28]

4.5.6 Romania

De rumenske datalagringsreglene ble underkjent av landets forfatningsdomstol allerede i 2009.[29] Lovgivningen ble deretter endret, men ved avgjørelse avsagt 8. juli 2014 ble også den nye lovgivningen funnet å være grunnlovsstridig. [30] Avgjørelsen følger EU-domstolens avgjørelse tett, og det ble særlig vektlagt at inngrepene ikke oppfylte krav til forholdsmessighet, og at det ikke forelå et adekvat vern mot misbruk.

4.5.7 Slovakia

Etter EU-domstolens dom besluttet den slovakiske forfatningsdomstolen å sette deler av datalagringslovgivningen ut av kraft i påvente av behandling av en klage over lovgivningens gyldighet. Klagen ble avgjort 29. april 2015, og forfatningsdomstolen konkluderte med at lovgivningen var grunnlovsstridig. [31] Reglene ble funnet å ha et for vidt nedslagsområde, og det ble også påpekt mangler ved mekanismene som skal verne mot misbruk.

4.5.8 Slovenia

Forfatningsdomstolen i Slovenia avgjorde den 3. juli 2014 at den implementerte datalagringsretten er ugyldig.[32] Domstolen fant at krenkelsen av borgernes grunnleggende rettigheter var uforholdsmessig, og la blant annet vekt på den betydelige

[27] Avgjørelse Pl. ÚS 24/10 (22. mars 2011) og avgjørelse Pl. ÚS 24/11 (22. desember 2011)
[28] http://sofiaglobe.com/2015/03/12/bulgarias-constitutional-court-scraps-data-retention-provisions/
[29] Avgjørelse 1258/2009
[30] Avgjørelse 82/2012
[31] Avgjørelse PL. ÚS 10/201478
[32] Avgjørelse U-I-65/13-19

og uselektive lagringen av data, at de valgte lagringsvarigheter ikke var tilstrekkelig begrunnet (8 måneder for internettdata, 14 måneder for telefondata) og at bruken av innhentede data ikke var begrenset til saker om alvorlig kriminalitet.

4.5.9 Kypros

I februar 2011 avgjorde kypriotisk høyesterett at deler av den nasjonale datalagringslovgivningen var grunnlovsstridig.[33] Sammenliknet med de øvrige europeiske avgjørelsene på dette området er den kypriotiske avgjørelsen langt mindre vidtrekkende. Domstolen avgjorde kun at visse konkrete bestemmelser om tilgang til og bruk av lagret informasjon var grunnlovsstridige. Selv om bestemmelsene kom inn ved implementeringen av datalagringsdirektivet, hadde de dessuten ingen klar forankring i direktivet.

[33] Avgjørelse 65/2009, 78/2009, 82/2009 og 15/2010-22/2010

5 UTREDNINGER OM AVVEININGEN AV PERSONVERNET MOT KRIMINALITETSBEKJEMPELSE

5.1 Generelt om avveiningen

Utgangspunktet i norsk straffeprosess er at politiet under etterforskning har krav på tilgang til alt som kan ha betydning som bevis i en straffesak og at lovbestemte taushetspliktregler bare kan påberopes i begrenset utstrekning. Det betyr at også data som er samlet inn som ledd i nye elektroniske kommunikasjonstjenester i prinsippet er tilgjengelig for politiet. I praksis vil det ofte by på problemer for politi og påtalemyndighet å få tilgang til slike data, enten fordi de ikke er oppbevart, eller fordi de disponeres av foretak som ikke står under norsk jurisdiksjon. En tysk dommer som ville ha tilgang til data fra Facebook ble henvist til Facebooks europeiske datterselskap i Irland hvor han fikk opplyst at de data han etterspurte lå lagret på firmaets server i USA.[34]

Det er med den bakgrunnen politiet ønsker at det skal gis regler om oppbevaring og lagring av trafikkdata. Det kan likevel være grunn til å spørre om det straffeprosessuelle utgangspunktet lar seg opprettholde i lys av den kommunikasjonstekniske utviklingen. Som følge av at stadig mer av sosiale, økonomiske og kommersielle relasjoner skjer elektronisk, genereres det data om forhold som det tidligere ikke var tenkelig at myndighetene skulle få tilgang til. Fra slike data kan man i dag vite hvor en person han har vært, hvem han har vært i forbindelse med, hvordan disse relasjonene har vært, hvilke interesser og preferanser han har, hva han har kjøpt, hvordan hans økonomiske status er og så videre. Mengden av data og de mulighetene de gir for innblikk i personers mest private og intime liv gir grunnlag for å revurdere det straffeprosessuelle utgangspunktet om at påtalemyndigheten har krav på tilgang til alt som kan ha betydning som bevis i en straffesak på nytt. Dette er blant annet understreket av EMD i *S. and Marper v. the United Kingdom*, 04.12.2008 (Grand Chamber) hvor den uttaler i avsnitt 112:

> *The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.*

På den annen side er det ikke bare mengden av potensielle data og opplysninger som lar seg samle inn om en person som har endret seg med moderne kommunikasjonsteknologi. Den har også skapt helt andre muligheter enn tidligere til å planlegge og koordinere handlinger, også kriminelle handlinger. I tillegg utgjør kommunikasjonsteknologien en arena for nye typer av samfunnsskadelige handlinger. Med kommunikasjonsteknologien endres med andre ord både bredden og dybden av de opplysningene som myndighetene kan få om personer i samfunnet og personers muligheter til effektivt å kunne foreta samfunnsskadelige handlinger.

[34] Se Masing ved note 31.

Avveiningen av hensynet til personvernet og hensynet til forebygging og etterforskning av kriminelle handlinger, har vært gjenstand for en rekke tidligere utredninger.

5.2 Politiets metodeutvalg – NOU 2004:6

I NOU 2004:6 avga politiets metodeutvalg innstilling om politiets bruk av metoder i forebyggende øyemed. Utvalget vurderte blant annet politiets bruk av "observerende og manipulerende metoder". De observerende metoder er metoder som overvåking, spaning og sporing. Når det gjelder spørsmålet om å gi en klar lovhjemmel for bruken av slike metoder peker utvalget på som motargument mot lovregulering av politimetoder at det kan blottlegge metoder på en uheldig måte. Politiet må etter utvalgets oppfatning kunne holde skjult de begrensinger i metodebruken som gir mulighet for personer som begår straffbare handlinger til å innrette sine disposisjoner på en måte som vil avsløre politiet. Når metoden som sådan og hovedvilkårene for at politiet kan gripe inn er lovregulert, mener utvalget at detaljer må kunne holdes hemmelig av taktiske grunner.[35]

Utvalget vurderte særskilt om det burde åpnes for blant annet bruk av kommunikasjonskontroll i forebyggende øyemed. Dette burde etter utvalgets oppfatning ikke avvises på prinsipielt grunnlag. Utvalget mente at dette måtte bero på en avveining som til syvende og sist vil bero på den enkeltes verdivalg. Utvalget fremhever at om det skal åpnes for de mest integritetskrenkende metoder, må det foreligge et dokumentert behov, og behovet må bygge på eksistensen av trussel om alvorlig kriminalitet. Videre må det godtgjøres at en metode kan gi et vesentlig bidrag til å motvirke trusselen. For de mest inngripende metoder må det kreves at metoden vil kunne gi et vesentlig bidrag til å løse politiets oppgaver, eller med andre ord forebygge straffbare handlinger. Bruk av tvangsmidler er integritetskrenkende, og kan føre til at uskyldige personer blir krenket. Slike kontrollskader må ikke bli så store eller så omfattende at den effekt som oppnås ved metodebruken, ikke kan forsvares.

Utvalgets flertall foreslo en regel om lagring og utlevering av kommunikasjonsdata (§ 8-17). I henhold til denne bestemmelsen skulle tilbyder av tilgang til offentlig telenett og offentlig teletjeneste oppbevare registrerte opplysninger om teletrafikk i 1 år til bruk for politiet. Retten skulle kunne treffe beslutning om tillatelse for politiet til å innhente trafikkdata og posisjonsdata knyttet til kommunikasjonsanlegg personen besitter, eller knyttet til en bestemt basestasjon, når "*det er god grunn til å tro at en person forbereder en alvorlig straffbar handling*". Tillatelsen skulle kunne omfatte både historiske data og fremtidige data. Rettens tillatelse skulle bare kunne gis når opplysningen ville være av vesentlig betydning for å forebygge den straffbare handling, og bare når mindre inngripende metoder ikke ville være anvendelige.

Den foreslåtte bestemmelsen var mindre omfattende enn reglene i datalagringsdirektivet da politiets adgang til kommunikasjonskontroll var avgrenset til situasjoner hvor det var grunn til å mistenke en bestemt person i å forberede straffbare handlinger og til denne personens kommunikasjonsutstyr eller til en bestemt basestasjon. Det var således ikke tale om en hjemmel til å innhente data om en ubestemt krets av personer eller utstyr.

[35] NOU 2004:6 s. 175.

Enhver som hadde vært gjenstand blant annet for kommunikasjonskontroll skulle ha krav på etter begjæring å få opplysning om dette når det var gått ett år fra metodebruken mot vedkommende var avsluttet. Retten til innsyn skulle likevel ikke gjelde saker som behandles av PST, da det for disse sakene gjør seg gjeldende særlige hensyn. Retten til underretning skulle kunne utsettes eller helt avskjæres etter beslutning av en domstol "*dersom det vil være til skade for politiets arbeid med saken at underretning gis eller andre forhold taler for at underretning bør unnlates eller utsettes*".

5.3 Metodekontrollutvalget – NOU 2009:15

Metodekontrollutvalget hadde til mandat blant annet å vurdere politiets bruk av skjulte tvangsmidler og politiets adgang til "å ta i bruk dataavlesning som metode i etterforskningen". Utvalget avga sin rapport som NOU 2009:15. Utvalget anga kjernen i personvernet som "*vernet mot å bli observert eller overvåket i den innerste personlige sfæren, og herunder en rett til å ha kontroll over opplysninger om en selv, særlig opplysninger som oppleves som personlige.*"[36] Utvalget tok som utgangspunkt at retten til personvern og rettsikkerhet er grunnleggende rettigheter samtidig som bekjempelse av kriminalitet kan være et legitimt behov som kan rettferdiggjøre inngrep i disse rettighetene. På den annen side vil vurderingen av hvor stort et inngrep er, avhenge blant annet av hva informasjonen brukes til. De fleste vil oppleve det ekstra inngripende at informasjon om dem blir behandlet av politiet. På grunnlag av en avveining av forholdet mellom personvern og rettssikkerhet på den ene side og hensynet til bekjempelse av kriminalitet på den andre side la utvalget til grunn som utgangpunkt for sine vurderinger "*at skjulte tvangsmidler bare bør kunne brukes i etterforskingen av alvorlige forbrytelser. Dreier det seg om forbrytelser hvor alvorlighetsgraden ikke i seg selv kan rettferdiggjøre skjult tvangsmiddelbruk, bør slike metoder bare kunne brukes der særlige behov tilsier det. Behovet kan for det første oppstå ved kriminalitet uten noe offer som kan forventes å bidra til oppklaring, eller i etterforsking av kriminalitet som begås i lukkede miljøer som politiet av ulike grunner ikke kan forventes å få eller kunne innhente informasjon fra. Dette vil kunne gjelde profesjonelle kriminelle miljøer eller miljøer med sterk indre justis. Slikt behov vil også kunne oppstå i etterforsking av internasjonal eller grenseoverskridende kriminell virksomhet*."[37]

Utvalget la til grunn et nødvendighetsprinsipp som grunnlag for politiets informasjonsinnhenting.[38] I dette ligger for det første at det ikke åpnes for større tilgang til bruk av skjulte etterforskningsmetoder enn det som er nødvendig ut fra formålet. Men prinsippet innebærer også begrensninger i andre retninger. Innsamling av bruk av informasjon må være mest mulig målrettet og i minst mulig grad omfatte informasjon som ikke er relevant, den må ramme færrest mulig personer som ikke er mistenkt for straffbare handlinger og informasjonen bør ikke videreformidles til flere personer enn det som er nødvendig ut fra formålet.

[36] NOU 2009:15 s. 21.
[37] NOU 2009:15 s. 22.
[38] NOU 2009:15 s. 55.

6 LOV AV 15. APRIL 2011 OM ENDRINGER I EKOMLOVEN OG STRAFFEPROSESSLOVEN MV. (GJENNOMFØRING AV EUs DATALAGRINGSDIREKTIV I NORSK RETT)

6.1 Lovarbeidet

DLD er foreslått innlemmet i norsk rett gjennom endringer i ekomloven og straffeprosessloven mv. Lovvedtak ble fattet i Stortinget 15. april 2011 nr. 11, men er ikke satt i kraft. Lovarbeidet ble startet ved at Samferdselsdepartementet, Justisdepartementet og Fornyingsdepartementet 8. januar 2010 sendte på høring et forslag til hvordan datalagringsdirektivet kan gjennomføres i norsk rett. Høringsfristen var 12. april 2010. Over 130 skriftlige innspill kom inn, i tillegg til flere innlegg på Samferdselsdepartementets blogg. Det ble også arrangert høringsmøter om saken.

I høringen ga blant annet representanter for politi og påtalemyndighet uttrykk for at datalagringsdirektivet var helt nødvendig for å kunne bekjempe alvorlig kriminalitet. Mange andre høringsinstanser pekte imidlertid på at det var betydelige personvernutfordringer knyttet til lagring av store mengder kommunikasjonsdata for hele befolkningen. Prop. 49 L (2010-2011) inneholder en oversikt over høringsinstansene og deres hovedsynspunkter.

Lovforslaget ble lagt frem av Regjeringen Stoltenberg ved Prop. 49 L (2010-2011), og vedtatt i Stortinget med visse endringer og med støtte fra Høyre, se Innst.275 L (2010-2011). Øvrige partier var mot lovforslaget. Frp, SV, SP og Krf gikk inn for å utsette en eventuell implementering i påvente av en revidering fra EU. De fire partiene trakk frem personvernhensyn og rettsstatsprinsipper blant begrunnelsene for å gå imot DLD. De viste også til at det er "fullt mulig å sette store spørsmålstegn ved hvorvidt direktivet faktisk betyr økt nytte for politiet". Det ble fremsatt flere mindretallsforslag, men ingen av dem gikk ut på å vedta strengere regler om utlevering uten tilhørende lagringsplikt.

Loven ble vedtatt på et tidspunkt da Norge ikke var bundet av DLD. Siktemålet var ikrafttredelse så snart det var praktisk mulig – ikke at dette skulle utstå til DLD ble innlemmet i EØS-avtalen. Samtidig ble loven utformet slik at den tilfredsstilte de krav til lovendringer som ble ansett nødvendige for at Stortinget skulle kunne samtykke til innlemmelse av DLD i EØS-avtalen, jf. Prop. 50 S (2010-2011) punkt 1 side 1.

6.2 Lovvedtakets innhold

6.2.1 Oversikt

Lovvedtaket inneholder to hovedelementer, en plikt for ekomtilbydere til å lagre abonnements-, trafikk-, og lokaliseringsdata i 6 måneder, og rett til utlevering på visse vilkår. Lagringsplikten er oppstilt i ekomloven kapittel 2 mens bestemmelsene om utlevering er inntatt i straffeprosessloven §§ 210 b-d. Samlet omtales endringene i de to lovene noen steder som lagringsloven. Det gjøres også enkelte steder i denne utredningen.

6.2.2 Lagringsplikten

De sentrale bestemmelser i ekomloven er §§ 2-7 og 2-7a og to nye ledd i § 2-9:

> *§ 2-7. Kommunikasjonsvern m.v. Plikt til å slette data*
>
> *§ 2-7 annet ledd skal lyde:*
>
> *Trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren skal slettes eller anonymiseres så snart de ikke lenger er nødvendig*
>
> 1. *til kommunikasjons- eller faktureringsformål,*
> 2. *for å oppfylle plikten etter § 2-7 a til å lagre data eller*
> 3. *for å oppfylle andre krav fastsatt i medhold av lov.*
>
> *Annen behandling av slike data krever samtykke fra bruker.*
>
> *Ny § 2-7a skal lyde:*
>
> *§ 2-7 a. Plikt til lagring av data*
>
> *Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i 6 måneder til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefon, mobiltelefon, internettelefoni, internettaksess og e-post.*
>
> *Myndigheten kan gi forskrift, treffe enkeltvedtak eller inngå avtale om plikten til å lagre data, herunder om tiltak for å ivareta dataenes konfidensialitet, integritet og tilgjengelighet. Myndigheten kan gi forskift om at tilbyder kan kreve fremlagt politiattest fra personer som skal behandle lagringspliktige data på tilbyderens vegne. Myndigheten kan ved forskrift eller enkeltvedtak helt eller delvis frita fra plikten til å lagre data etter første ledd eller helt eller delvis pålegge andre enn de som omfattes av første ledd, plikt til å lagre data dersom dette må til for å oppnå formålet med bestemmelsen.*
>
> *§ 2-9 tredje ledd skal lyde:*
>
> *Taushetsplikten er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Det samme gjelder ved vitnemål for retten. Taushetsplikten er heller ikke til hinder for at opplysninger som nevnt i første punktum gis til annen myndighet i medhold av lov.*

§ 2-9 nytt femte ledd skal lyde:

Taushetsplikten er heller ikke til hinder for at andre data enn de som er nevnt i tredje ledd, kan utleveres til politi og påtalemyndighet i medhold av straffeprosessloven §§ 210 b, 210 c, 216 b eller 222 d, eller til Politiets sikkerhetstjeneste i medhold av politiloven § 17 d, eller til Finanstilsynet i medhold av verdipapirhandelloven § 15-3 annet ledd nr. 3.

Ekomtilbydernes lagringsplikt er nærmere regulert i datalagringsforskriften (14. mai 2013 nr. 484). Forskriftens ikrafttredelse beror på loven.

I forbindelse med Stortingets behandling av loven ble det vedtatt ulike sikringstiltak for ivaretakelse av personvernet. Tiltakene er nærmere regulert i personopplysningsforskriften § 7-1. Nytt her er at Datatilsynet ved utferdigelse av konsesjon skal vurdere om det skal stilles krav om kryptering av lagringspliktig data samt pålegge nødvendige vilkår for å sikre lukket lagring. Brudd på vilkårene er straffesanksjonert. Forskriftsendringen skal tre i kraft samtidig med loven.

Ved vurdering av om kryptering skal pålegges og eventuelt omfang av plikten, forutsettes Datatilsynet å foreta en interesseavveining mellom alle parter ut fra personvernhensyn. Vurderingene vil kunne falle ulikt ut for forskjellige lagringspliktige tilbydere og for forskjellige lagringspliktige data. Ved pålegg om lukket lagring gir bestemmelsen en oppramsing av minstekrav som må stilles for å sikre lukket lagring. Dette er krav om identitetskontroll, tilgangskontroll, fysisk og elektronisk sikring av lagringsmediet og omgivelsene rundt, begrensninger i muligheten for å hente ut data online, samt krypteringskrav ved forsendelse av data over landegrensene.

6.2.3 Utleveringen av data – i hvilke tilfeller

Vilkårene for politiet og påtalemyndighetens tilgang til trafikk- og lokasjonsdata i etterforskningsøyemed er nedfelt i straffeprosessloven §§ 210 b og 210 c. Straffeprosessloven §§ 210 b og 210 c gjelder henholdsvis utlevering av trafikkdata og basestasjonsdata. Basestasjonsdata regnes som spesielt inngripende overfor personvernet på grunn av den store mengde overskuddsinformasjon som omfattes. Bestemmelsene er likelydende med unntak av at strafferammen for å få tilgang til basestasjonsdata er fem år, mens den for trafikkdata er fire år. Loven fremstår med dette som både strengere og mer presis enn datalagringsdirektivet hva gjelder politiets tilgang til opplysningene. Det er ikke er fullt sammenfall mellom hvilke straffbare handlinger som kan gi grunnlag for utlevering av henholdsvis trafikkdata (§ 210 a) og basestasjonsdata (§ 210 b). I tillegg til de forhold som kan gi adgang til tilgang til basestasjonsdata, kan det gis tilgang til trafikkdata blant annet til etterforskning av dokumentfalsk og det å søke å få tilgang til seksuelle handlinger med barn og ungdom. Strafferammene er dessuten forskjellige, da den for å gi tilgang til basestasjonsdata må være på minst fem år, mens den for å gi tilgang til trafikkdata må være på minst fire år. Disse forskjellene illustrerer at bestemmelsene er utformet etter en konkret vurdering av behovet for data i forbindelse med etterforskningen av hver enkelt straffbar handling.

Bestemmelsene sier at:

[Ny] § 210 b skal lyde:

Retten kan ved kjennelse pålegge utlevering for et bestemt tidsrom av trafikkdata, og lokaliseringsdata som ikke omfattes av § 210 c, og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som etter loven kan medføre straff av fengsel i 4 år eller mer, eller som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, 145 annet ledd, 145 a, 145 b, 162, 162 b, 162 c, 190 a, 201 a, 203, 204 a, 270 første ledd nr. 2, 317, jf. § 162, eller § 390 a, eller av utlendingsloven § 108 fjerde ledd.

Forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning.

Utlevering etter paragrafen her kan bare pålegges dersom det må antas at opplysningene vil være av vesentlig betydning for etterforskningen.

Utenfor domstolens ordinære kontortid fremsettes begjæring om utlevering for Oslo tingrett etter nærmere bestemmelser gitt av departementet.

§ 210 annet og fjerde ledd gjelder tilsvarende.

[Ny] § 210 c skal lyde:

Retten kan ved kjennelse pålegge utlevering for et begrenset tidsrom av opplysninger om hvilke telefoner eller annet kommunikasjonsutstyr som innenfor et nærmere bestemt geografisk område har vært satt i forbindelse med bestemte telefoner eller kommunikasjonsutstyr og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som etter loven kan medføre straff av fengsel i 5 år eller mer, eller som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, § 162, 162 b, 162 c, eller § 317, jf. § 162, eller av utlendingsloven § 108 fjerde ledd.

§ 210 b annet til femte ledd gjelder tilsvarende.

Krav på utlevering forutsetter altså bare at det er skjellig grunn til mistanke om at det er begått bestemte forbrytelser. I det ligger etter rettspraksis krav om sannsynlighetsovervekt om at samtlige straffbarhetsvilkår er oppfylt. Straffbarhetsvilkårene trenger imidlertid ikke knyttes til en bestemt person. I høringsbrevet foreslo departementet at politiet måtte godtgjøre at "noen med skjellig grunn mistenkes". Departementet vurderte som et alternativ å lovfeste kravet til skjellig grunn uten krav om mistanke til en konkret person, men forkastet det på grunn av de personvernmessige konsekvensene. Departementet uttalte at "Lagringsplikten innebærer at tilfanget av data øker både i omfang og tid. Åpnes det dessuten for at politiet skal få utlevert data uten å måtte knytte mistanken til en konkret person, vil samtidig politiets tilgang til overskuddsinformasjon øke tilsvarende." I høringen gikk samtlige instanser innenfor politi- og påtalemyndighet sterkt imot forslaget om å innføre et krav om at mistanken skulle knyttes til en bestemt person, og departementet viderefører derfor ikke forslaget med den knappe begrunnelsen at det "vil innebære en for stram begrensning på bruken av data".

Utlevering skal for det første kunne skje til etterforskning av forbrytelser med en nærmere angitt strafferamme. For personspesifikke trafikk- og lokaliseringsdata må strafferammen være på minst fire år for at utlevering skal kunne skje, for basestasjonssøk må strafferammen være minst fem år. Bakgrunnen for forskjellen var at basestasjonssøk anses "mer inngripende i forhold til personvernet, blant annet fordi man da får med seg mye overskuddsinformasjon". Om valget av minimum strafferammer på henholdsvis fire og fem år sies det lite i forarbeidene. De inneholder ingen redegjørelse for hva virkningen av forskjellen er, og heller ikke en åpen vurdering av hvorfor det er riktig at akkurat de minimumsnivåene settes.

Utlevering skal for det andre kunne skje til en del andre spesifikt angitte forbrytelser med lavere strafferammer enn fire år. De særlige forbrytelsene som er ramset opp i både § 210 b og § 210 c er ulovlig etterretningsvirksomhet (forbrytelser mot statens selvstendighet og mot Norges statsforfatning), narkotikaforbrytelser (derunder doping), hvitvasking av utbytte av narkotikaforbrytelser og menneskesmugling. Ved skjellig grunn til mistanke om slike forbrytelser kan altså både personspesifikke trafikkdata og basestasjonssøk kreves utlevert. Etter § 210 b kan personspefikke trafikkdata i tillegg kreves utlevert ved skjellig grunn til mistanke om dokumentfalsk, grooming, seksuelle overgrep mot barn, barneporno, datakriminalitet og forstyrrelse av privatlivet. I Prop. 49 L (2010-2011) heter det at "Felles for disse bestemmelsene er at de gjelder forhold som vil kunne være særlig vanskelige å etterforske uten tilgang til data". En mer utførlig begrunnelse gis egentlig ikke.

6.2.4 Utleveringen av data – til hvilket formål

Det som reguleres direkte i §§ 210 b og 210 c er utlevering til politi og påtalemyndighet i etterforskningsøyemed, det vil si i saker det er skjellig grunn til mistanke om at det er begått en straffbar handling. Gjennom plasseringen av utleveringsbestemmelsene i straffeprosessloven kapittel 16 åpnes det også for utlevering av data i *avvergende* øyemed, jf. straffeprosessloven § 222 d. Adgangen er begrenset til de forbrytelser som er oppregnet i bestemmelsens første og annet ledd. Det dreier seg i korte trekk om

bestemte former for organisert og annen alvorlig kriminalitet. Bruk av tvangsmidler i avvergende øyemed krever kjennelse fra retten og forutsetter at bruken vil skje som ledd i etterforskning og det er "rimelig grunn til å undersøke" om det foreligger en handling som rammes av et av de aktuelle straffebudene.

Det er imidlertid ikke foreslått at de nye særlige reglene i §§ 210 b og 210 c skal kunne benyttes i *forebyggende* øyemed, men gjennom bestemmelsen i politiloven § 17 d kan utlevering av data også være aktuelt i slikt øyemed. Etter politiloven § 217 d kan PST som ledd i sin forebyggende virksomhet nytte bestemte tvangsmidler, blant annet straffeprosessloven § 216 b som i annet ledd bokstav d åpner for utlevering av bestemte data. Med forebyggende øyemed sikter man til handlinger som ligger lenger frem i tid enn i tilfeller hvor det er spørsmål om tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d. Adgangen er begrenset til de forbrytelser som er oppregnet i § 17 d første ledd, hvilket gjelder terrorhandlinger, ulovlig etterretningsvirksomhet og en del grove frihets- og legemskrenkelser Bruk av tvangsmidler i forebyggende øyemed krever kjennelse fra retten og forutsetter at "det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen, at forebygging ellers i vesentlig grad vil bli vanskeliggjort og inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig".

6.2.5 Utleveringen av data – til hvilke aktører

Ved vurdering av de personvernmessige betenkeligheter ved datalagring, derunder faren for misbruk eller at data skal komme på avveie, vil det i praksis ha betydning hvem som kan gis tilgang til de lagrede data. Bestemmelsene i §§ 210 b og 210 c er utformet som tvangsmidler i straffeprosessloven kapittel 16 om beslag og utleveringspålegg. Det innebærer at tilgang til data er forbeholdt politi og påtalemyndighet. Lovvedtaket fra 2011 åpner imidlertid også en begrenset adgang for Finanstilsynet til lagrede data etter verdipapirhandelloven. § 15-3 annet ledd nr. 3. Tilgangen bygger på to EU-direktiv som legger opp til at tilsynet selv skal forfølge og iretteføre brudd på direktivbestemmelsene[1]. Under behandlingen av lagringsloven ble det vurdert om også tilsynets tilgang burde gå via politiet. Så lenge det var domstolskontroll med tilsynets tilgang, fant imidlertid ikke departementet at dette ville bidra til ytterligere styrking av personvernet.

Etter lovvedtaket skal ingen andre myndigheter ha tilgang til data, og det skal heller ikke være tilgang til data for private i sivile saker. Det ble under lovarbeidene diskutert om det burde være en adgang for andre myndigheter til lagrede data, slik det tidligere i noen grad var etter tolloven § 12-4 første ledd, merverdiavgiftsloven § 16-3 og ligningsloven § 6-13a, som alle åpnet for at kontrollmyndighetene på bestemte vilkår kunne pålegge teleoperatørene å gi opplysninger om navn og adresse til en abonnent som ikke har offentlig telefonnummer eller telefaksnummer. Departementet fastholdt imidlertid at tilgang burde være forbeholdt politi og påtalemyndighet, med det særskilt begrunnede unntaket som gjelder Finanstilsynet. Tilsvarende ble det konkludert med at det ikke skulle være adgang til å kreve utlevert lagrede data til bruk som bevis i sivile saker.

Rettslig er adgangen til data regulert gjennom taushetspliktsbestemmelsen i ekomloven § 2-9. Bestemmelsen pålegger tilbyder og installatør plikt til "å bevare taushet om

innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter". De samme subjektene pålegges "å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder får anledning til selv å skaffe seg kjennskap til slike opplysninger". For politi og påtalemyndighetens tilgang til data etter de nye bestemmelsene i §§ 210 b og 210 c er det oppstilt et særskilt unntak fra taushetsplikten i ekomloven § 2-9 femte ledd. For å hindre utlevering av lagrede data til bruk som bevis i sivile saker, er det videre inntatt en ny bestemmelse i tvisteloven § 22-3 som skal hindre retten i å gi fritak fra taushetsplikten slik den kan i andre tilfeller av lovbestemt taushetsplikt.

En problemstilling som verken er berørt i proposisjonen eller noen annen fremstilling vi har sett, gjelder siktede og deres forsvareres tilgang til etterforskningsmateriale. Hvis lagrede data skal benyttes som bevis i straffesaken, vil både tiltalte, eventuelle medtiltalte, forsvarere og domstolen få tilgang til det materialet som er plukket ut fra aktoratets side. Med mindre særlige begrensninger skulle få anvendelse, vil beviset også måtte føres i åpen rett – slik at allmennheten også får tilgang. Allerede denne anvendelsen av beviset kan ha en personvernmessig slagside som ikke er tatt opp i proposisjonen. Ganske særlig må det gjelde der dataene ikke bare gjelder tiltalte selv, men også samtalepartnere eller andre som ikke er parter i saken. Denne problemstillingen strekker seg imidlertid lenger enn til bare det bevismaterialet påtalemyndigheten har plukket ut til bruk i saken. Forsvarerne har i utgangspunktet krav på innsyn i alle dokumentene i saken, derunder hele det elektroniske beslaget. Dette kan særlig ha betydning ved basestasjonssøk. Vi kan ta som eksempel at påtalemyndigheten med hjemmel i § 210 c har krevd utlevert opplysninger om alle telefoner som har vært benyttet på et bestemt sted på et gitt tidspunkt, og at påtalemyndigheten har lagt frem det som bevis det som er nødvendig for å underbygge at den tiltalte var på dette stedet til angitt tidspunkt. Forsvarerne og tiltalte kan imidlertid ha et ønske om tilgang til det øvrige materialet, for eksempel for å føre bevis for alternative gjerningsmenn. Vi kan vanskelig å se at det innenfor rammen av straffeprosesslovens regler om rett til sakens dokumenter og EMKs alminnelige krav til "equality of arms" er anledning til å nekte forsvarerne og tiltalte tilgang til dette materialet. Vilkårene for tilbakehold i straffeprosessloven § 242 a kan i bestemte tilfeller være oppfylt, men det beror i så fall på tilfeldigheter. Hovedregelen må være at tiltalte og dennes forsvarer har krav på innsyn. Det samme må etter omstendighetene gjelde fornærmede og dennes eventuelle bistandsadvokat.

6.2.6 Hvor lenge data kan lagres

Lagringsplikten etter ekomloven er begrenset til seks måneder. Departementet foreslo en lagringstid på 12 måneder. Det skulle ikke skilles mellom teknologier, slik at lagringstiden ble lik for de ulike tjenestene og ulike typer data. I avtalen mellom Arbeiderpartiet og Høyre ble tiden begrenset til seks måneder fordi "hensynet til personvern tilsier at de relevante data ikke skal lagres lengre enn hva som er strengt nødvendig av hensyn til kriminalitetsbekjempelse." Lagringstiden var et av forholdene som etter avtalen skulle være gjenstand for en senere evaluering.

Lagringsplikten avløses av en sletteplikt, slik at data som ikke er utlevert skal slettes etter utløpet av seks måneder. Data som utleveres til politiet avgrenses i tid ved kjennelsen om utlevering. Kjennelsen må fastsette hvilket tidsrom data kan hentes fra og også hvilke data som skal utleveres. Tidsrommet kan ikke være lenger enn det som implisitt følger av kravet i tredje ledd om at dataene må være av vesentlig betydning for etterforskningen. Kravet om vesentlig betydning gjelder også for hvilke data som kan utleveres.

Data som er utlevert til politiet, skal behandles i henhold til politiregisterloven. Det gjelder også håndtering av overskuddsinformasjon hos politi og påtalemyndighet. Loven bestemmer i § 4 at opplysninger kan behandles til det formålet de er innhentet for og til andre politimessige formål, med mindre det er bestemt i lov eller i medhold av lov at retten til behandling er begrenset, eller at opplysninger kan behandles til andre formål enn de politimessige. Tjenestemenn i politiet og påtalemyndigheten kan etter § 21 gis tilgang til opplysninger gjennom direkte søk, eller opplysninger kan gjøres tilgjengelig for dem på annen måte i den utstrekning det er et tjenestemessig behov, og det er til formål som omfattes av loven. Opplysninger som etter sin art er sensitive, eller som er gitt av noen med særskilt beskyttelsesbehov, eller som er ikke-verifiserte, bør underlegges særskilt tilgangsbegrensning. Det er verken i loven eller i forskrifter tatt stilling til hvorvidt utleverte kommunikasjonsdata er sensitive i lovens forstand. I § 15 stiller loven krav til planlagte og systematiske tiltak for å sørge for tilfredsstillende informasjonssikkerhet

6.2.7 Lagringsløsning og datasikkerhet

Når det gjaldt lagringsløsning og datasikkerhet, gikk departementet inn for at det skal være opp til den enkelte tilbyder å velge lagringsløsning og at det er tilbyderne som med utgangspunkt i personopplysningsloven med forskrifter, må foreta en trusselvurdering for å fastslå hvilke sikringstiltak som er nødvendige, og iverksette sikringstiltak i samsvar med konklusjonene fra en slik risikovurdering. Loven selv inneholder derfor ikke konkrete regler om lagring og datasikkerhet, men ekomloven § 2-7 a gir myndighetene hjemmel til å gi forskrift om tiltak for å ivareta dataenes konfidensialitet, integritet og tilgjengelighet. Det er heller ikke noe krav om at dataene skal lagres i Norge eller innenfor EØS-området.

Forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse dataene (datalagringsforskriften) er fastsatt av Post- og teletilsynet den 14. mai 2013. Kapittel 2 fastlegger omfanget av lagringsplikten, kapittel 3 krav til lagringen mv. og kapittel 4 krav til behandling og tilrettelegging av lagringspliktige data. Sentrale krav til lagringen er regler som skal sikre dataintegritet og sporbarhet, og krav om sletting minst én gang daglig av data som er seks måneder gamle. Behandling av lagrede data kan bare skje for utlevering til den registrerte, for retting etter personopplysningsloven, for tilgjengeliggjøring for myndighetene etter samtykke og for utlevering etter pålegg fra retten. I tillegg kan utføres nødvendig vedlikehold av databasen.

Post- og teletilsynet fører tilsyn med bestemmelsene i forskriften. Datatilsynet har til oppgave å kontrollere at lover og forskrifter som gjelder for behandling av

personopplysninger blir fulgt, jf. personopplysningsloven § 42. Datatilsynets tilsynsansvar gjelder både data lagret i medhold av ekomloven og data lagret i medhold av konsesjoner gitt av Datatilsynet med hjemmel i personopplysningsloven. Det vil i noen grad være overlappende tilsynskompetanse mellom Post- og teletilsynet og Datatilsynet på dette området. Det foreligger en avtale mellom Post- og teletilsynet og Datatilsynet om utøvelse av tilsyn.

6.2.8 Underretning og rettslig prøving

Etter de vanlige reglene i straffeprosessloven skal det gis underretning til den mistenkte og til den som rammes av et utleveringspålegg, men retten kan beslutte at slik underretning kan utsettes "*dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis*". I lagringsloven er inntatt samme regel. Departementet begrunner det med at "*slik utsatt underretning kan være særlig aktuelt i de tilfellene hvor dataene søkes innhentet i en tidlig fase av etterforskningen og før det er foretatt noen pågripelse. Blir den som i slike tilfeller rammes, klar over utleveringspålegget, kan det ofte miste mye av sin effekt. Videre etterforskning, eksempelvis ransaking og beslag, kan dessuten bli vanskeliggjort*", se proposisjonen s. 106-107.

Etter straffeprosessloven § 100a skal retten oppnevne advokat for den mistenkte som ikke varsles. Forsvareren kan påanke rettens kjennelse. Forsvareren kan også begjære at det gis underretning til mistenkte om bruken av tvangsmiddelet, men han har taushetsplikt om saken overfor mistenkte og andre utenforstående. Den som rammes av et utleveringspålegg uten å være mistenkt eller siktet har ikke krav på å få oppnevnt advokat. Oppnevning av advokat skal også skje når tvangsmidler anvendes i forebyggende øyemed.

Advokatens oppgaver er begrenset til å vareta mistenktes interesser. Det er således ingen formell ordning som varetar interessene til andre berørte. Datalagringsloven gjør ingen endring i dette.

6.3 Vurderingen av forholdet til menneskerettighetene i lovforslaget

I forberedelse av datalagringsloven vurderte departementene også forholdet til menneskerettighetene, både personvernet i EMK artikkel 8, ytringsfriheten i artikkel 10 og uskyldspresumsjonen i artikkel 6. Det var strid om disse vurderingene under høringen og i den øvrige debatten rundt direktivet og loven.

Departementets utgangspunkt var at både datalagringsdirektivets krav til lagring, og til utlevering, kunne innebære et inngrep i retten til privatliv, herunder korrespondanse, se Prop. 49 L (2010-2011) s. 25. Begge deler måtte derfor ha hjemmel i lov, ha et lovlig formål, og ikke være mer omfattende enn nødvendig ("nødvendig i et demokratisk samfunn").

Departementet tolket lovkravet som både et krav om hjemmel i lov, og også et krav til tilgjengelighet, klarhet og presisjon i utforming av loven. Det kan imidlertid, som vi skal komme tilbake til, særlig på bakgrunn av EU-domstolens dom, stilles spørsmål ved om ikke de materielle kravene til loven er mer omfattende og også omfatter krav til at loven inneholder tilstrekkelige rettssikkerhetsgarantier og garantier mot misbruk. Dette

spørsmålet er ikke reist i proposisjonen, og dermed ikke vurdert som ledd i forberedelsen av den norske loven.

Kravet til lovlig formål antok departementet var oppfylt uten nærmere begrunnelse og uttalte at "formålene om å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter, er legitime formål etter EMK artikkel 8 nr. 2", se s. 26.

De mest omfattende vurderingene i proposisjonen knyttet seg til spørsmålet om hvorvidt inngrepet er nødvendig i et demokratisk samfunn. Med henvisning til saken Olsson mot Sverige[39] la departementet til grunn at vilkåret byr på en toleddet vurdering; først en vurdering av om det foreligger "a pressing social need", dernest en konkret forholdsmessighetsvurdering av inngrepet og de legitime hensynene det skal vareta.

Departementet la uten videre til grunn at "det er på det rene at det foreligger et presserende samfunnsmessig behov for å bekjempe alvorlig kriminalitet. Departementet anser at tilgang til data kan være av avgjørende betydning for at en rekke straffbare og ulovlige handlinger oppklares", se Prop. 49 L s. 26. Det er imidlertid ingen drøftelse av hva som utgjør "alvorlig kriminalitet", og proposisjonen inneholder heller ikke senere en omfattende drøftelse av hvilke forbrytelser som skal omfattes av de norske reglene.

Derfra gikk departementet inn i den konkrete forholdsmessighetsvurderingen. Departementet uttalte innledningsvis at "Vurderingen av hva som er nødvendig i et demokratisk samfunn for å vareta ett eller flere legitime formål, er videre skjønnsmessig og beror på en konkret avveining av en rekke ulike hensyn", og departementet tok som utgangspunkt at statene må ha en forholdsvis stor skjønnsmargin ved vurderingen av hvilke tiltak det er nødvendig å iverksette for å bekjempe alvorlig kriminalitet og ivareta den nasjonale sikkerheten og andres rettigheter. Det heter deretter at det avgjørende er en konkret avveining av inngrepets styrke for de som rammes og de hensynene som tilsier inngrep. Departementets avveining var deretter denne:

> *EMD har ikke tidligere tatt stilling til om og under hvilke omstendigheter en generell myndighetspålagt lagringsplikt av data er nødvendig i et demokratisk samfunn for å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter. Departementet kan imidlertid ikke se at det skal være avgjørende for om den pålagte lagringsplikten er forholdsmessig. For det første må behovet for en slik generell myndighetspålagt lagringsplikt ses i lys av de gjeldende samfunnsforholdene. Her er det på det rene at stadig mer av den mellommenneskelige kommunikasjonen foregår ved bruk av ulike digitale og elektroniske virkemidler. Samtidig vil behovet for tilgang til data for å oppklare kriminalitet, øke. For det andre er det ingen av de generelle momentene som EMD har oppstilt som tilsier at en slik generell myndighetspålagt lagringsplikt som sådan vil være uforholdsmessig. EMD understreker derimot at det må foretas en*

[39] Sak nr. 10465/83, dom av 24. mars 1988

konkret avveining av inngrepets styrke vurdert opp mot de hensynene som tilsier inngrep. I vurderingen av inngrepets styrke, kan det imidlertid være av betydning at det foreligger en generell myndighetspålagt lagringsplikt. Det må også være av vesentlig betydning om det foreligger tilfredsstillende rettssikkerhetsgarantier som kan forhindre vilkårlig tilgang til opplysningene. Dette er det samme utgangspunktet for forholdsmessighetsvurderingen som EU har kommet frem til, jf. datalagringsdirektivet artikkel 4 og fortalen kapittel 9 og 25. Også den tyske forfatningsdomstolen har lagt til grunn at den myndighetspålagte lagringsplikten som sådan ikke er i strid med den tyske forfatningen, såfremt særlig reglene om lagring og tilgang til opplysningene er tilfredsstilende, se dom avsagt av den tyske forfatningsdomstolen (første senat), 2. mars 2010 i sakene 1 BvR 256/08, 1 BvR 263/08 og 1 BvR 586/08, avsnitt 219. Departementet kan heller ikke se at EMDs dom S og Marper mot Storbritannia (storkammer), 4. desember 2008, nr. 30562/04 og 30566/04 (EMD-2004-30562 *), tilsier at det må fastsettes et annet utgangspunkt for forholdsmessighetsvurderingen.*

Både høringen og EUs lovgivningsprosess har vist at det kan være delte meninger om hvor inngripende den myndighetspålagte lagringen av data er for privatlivet. Det er redegjort nærmere for departementets syn på dette spørsmålet i kapittel 6 om personvern. Lagringstiden foreslås satt til 12 måneder, jf. kapittel 9. Politiet og påtalemyndighetens tilgang til opplysningene er foreslått begrenset til alvorlig kriminalitet samt enkelte nærmere bestemte lovbrudd som anses som særlig vanskelig å etterforske uten tilgang på data. Basestasjonssøk er særlig inngripende i personvernet og strafferammekravet er således foreslått satt høyere her enn ved utlevering av personspesifikk data. I begge tilfeller er utlevering underlagt domstolskontroll, jf. kapittel 12. Domstolen skal treffe beslutning ved kjennelse som innebærer en plikt til å begrunne beslutningen. Mistenkte skal underrettes om utleveringspålegg. Ved utsatt underretning skal det oppnevnes en offentlig advokat for å ivareta vedkommendes rettssikkerhet. Overskuddsinformasjon hos politi og påtalemyndighet skal håndteres i samsvar med reglene i lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven). Loven har ikke trådt i kraft. Muligheten for å omgå disse vilkårene ved vitneforklaring i straffesaker eller begjæring om bevisfremleggelse i sivile søksmål, foreslås dessuten stengt.

Den konkrete forholdsmessighetsvurderingen inneholder altså lite annet enn påpekning av at muligheten for å bekjempe alvorlig kriminalitet i samfunnet vil svekkes dersom politi og påtalemyndighet ikke sikres tilgang til data, samt et referat av det forslaget som skulle fremmes. Det siste ble formodentlig ansett relevant ut fra departementets syn om

at det i vurderingen må være av betydning at det foreligger en generell myndighetspålagt lagringsplikt.

Forholdsmessighetsvurderingen inneholder imidlertid ikke en egentlig vurdering av inngrepets styrke, det vil si hva det innebærer for borgerne. Departementet gikk heller ikke inn i noen konkret vurdering av betydningen av å beskytte mot de enkelte handlingene som skulle gi hjemmel for politiets tilgang til de lagrede opplysningene. Noen slik vurdering foretok departementet heller ikke i forbindelse med vurderingen av reglenes nødvendighet. I nødvendighetsvurderingen pekte departementet på at det vil være av vesentlig betydning om det foreligger tilfredsstillende rettssikkerhetsgarantier som kan forhindre vilkårlig tilgang til opplysningene. Etter forslag fra flere høringsinstanser, herunder Riksadvokaten, kom det inn et vilkår om at utlevering av data skulle være betinget av at dataene måtte være av vesentlig betydning for etterforskningen.

Departementet la til grunn at hensynet til rettssikkerheten var oppfylt gjennom vilkårene i lovforslaget, det vil si vilkårene om at:

- politiet og påtalemyndighetens tilgang til opplysningene skulle være begrenset til alvorlig kriminalitet samt enkelte nærmere bestemte lovbrudd som anses som særlig vanskelig å etterforske uten tilgang på data,
- domstolen skal treffe beslutning ved kjennelse som innebærer en plikt til å begrunne beslutningen,
- mistenkte skal underrettes om utleveringspålegg, og at det ved utsatt underretning skal oppnevnes en offentlig advokat for å ivareta vedkommendes rettssikkerhet, og
- overskuddsinformasjon hos politi og påtalemyndighet skal håndteres i samsvar med reglene i lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

Departementet foretok imidlertid ikke noen utdypning av hvilke rettssikkerhetskrav som må være tilfredsstilt for at ordningen skulle være i samsvar med konvensjonens krav. Som vi ser, behandlet departementet bare kravet til tilgjengelighet, klarhet og presisjon i utforming av loven i forbindelse med lovskravet. I behandlingen av forholdsmessigheten var det behovet for å avverge og oppklare kriminelle handlinger som sto i sentrum for vurderingen. Dermed inneholder ikke proposisjonen noen vurdering av hvilke rettssikkerhetsmessige krav som må være oppfylt for at lagringsplikten skal tilfredsstille kravet til lov. Her skiller således departementets utredning seg fra tilnærmingen til EU-domstolen og den tyske forfatningsdomstolen. Det er ikke grunnlag for å hevde at disse kravene inngår i statenes skjønnsmargin.

Når det gjelder forholdet til pressens kildevern, tok departementet utgangspunkt i at DLD ikke inneholder regler som gjør inngrep i pressens rett til å forholde seg taus om sine kilders identitet, men at DLD i praksis kan oppfattes som en utfordring for kildevernet

idet det foreskriver en systematisk lagring av all data, se Prop. 49 L s. 19. Departementet så forholdet til pressens kildevern i lys av de generelle reglene i straffeprosessloven § 170a, og pekte egentlig ikke på særlige spørsmål knyttet til datalagring.

Et problem med departementets utredning her er at den ikke tydelig får frem den faktiske situasjonen som oppstår når all kommunikasjon med pressen er registrert, lagret og tilgjengelig for politiet. Dette er en situasjon som er vesentlig forskjellig fra den ordinære etterforskningssituasjonen. Det er også utfordringer her knyttet til den tradisjonelle garantien i slike tilfeller med å begrense adgangen til å bruke slik informasjon som bevis. En viktig side ved tilgangen til kommunikasjonsdata er den betydning det har for etterforskningen, og skadevirkningene for den frie presse kan bli like store selv om opplysningene ikke kan brukes som bevis. Departementet foretar heller ikke noen nærmere vurderinger av de utfordringene som knytter seg til bruken av slike opplysninger i politiets etterretningsvirksomhet og arbeid for å forhindre lovbrudd. Her kan man for eksempel tenke seg at bruk av opplysninger om kontaktene til en journalist som arbeider med en reportasje om ekstreme eller kriminelle miljøer kan være nyttige for politiet, men ødeleggende for pressens arbeid.

Proposisjonen inneholder også en kort vurdering av uskyldspresumsjonen, og det konkluderes med at den ikke medfører særlige utfordringer for datalagring. Men her foretas ingen vurdering av betydningen av at de lagrede dataene også vil omfatte kontakt mellom advokater og klienter. I forbindelse med utarbeidelsen av forslaget til lov ble også forholdet til menneskerettighetene vurdert.

6.4 Departementets redegjørelse for hva som vil oppnås ved gjennomføring av loven

Departementet ga en utredning om betydningen for politiets etterforskning å gi tilgang til kommunikasjonsdata. Det er en utbredt oppfatning hos politi og påtalemyndighet at elektroniske data har nytteverdi i kriminalitetsbekjempelsen, se Prop. 49 L (2010-2011) s. 36. Departementet anfører at elektroniske data normalt veier tungt som bevis, siden de er objektivt konstaterbare. Slike bevis bidrar til å rekonstruere et hendelsesforløp gjennom å se på hvilket kommunikasjonsmønster eller bevegelsesmønster mistenkte har. Elektroniske data kan ha stor betydning som innledende bevis ved at de kan identifisere mistenkte og gi grunnlag for annen bevissikring, som innhenting av DNA-prøve, ransaking og avhør. Departementet peker videre på at nytten av elektroniske data som bevis ikke nødvendigvis kommer til syne i domsgrunnene. Mistenktes visshet om at politiet har hentet ut elektroniske data, eller motstrid som påvises mellom mistenktes første forklaring og uthentede data, kan bane veien for at han avgir en ny forklaring som senere utgjør hovedbeviset i saken.

Et viktig moment i departementets vurdering var at norske politimyndigheter skulle være i stand til å yte nødvendig hjelp når andre land ber om dette i etterforskningen av sine alvorligste straffesaker og saker om terror fordi de mangler data.

I diskusjonen om loven ble det anført at kriminelle har lett for å omgå dataspor, slik at datalagring ikke blir så effektivt som ønskelig i kriminalitetsforebyggelsen og

etterforskningen. Til dette pekte departementet på at mulighetene til å omgå lagring ikke var noe nytt, samtidig som norsk politis erfaring med bruk av data gjennom mange år har bidratt til oppklaring av mange saker. En sak som ble nevnt som et illustrerende eksempel var Nokas-saken, se Prop. 49 L s. 45:

> *Kripos viser til at man ikke kjenner noen straffesak hvor de involverte var mer bevisst på ikke å etterlate seg elektroniske spor, enn i Nokas-saken. Til tingretten forklarte de domfelte at de stadig ble instruert om ikke å bringe med egen mobiltelefon til ransområdet under planleggingen av ranet. Under ranet ble det brukt egne "ranstelefoner" som de domfelte kvittet seg med etterpå. Enkelte av de involverte hadde stor teknisk kunnskap om politiets metoder, herunder forholdet til basestasjoner og basestasjonssøk, og det ble også beslaglagt avansert teknisk utstyr for å blokkere kommunikasjon ("jammer"). Likevel ble gjerningspersonene innhentet av politiets systematiske metoder. Under en bag i en bil som de senere domfelte hadde senket i Drammensfjorden, fant politiet et SIM-kort som kunne knyttes til én av gjerningspersonene. Hovedmannen ble pågrepet som følge av at etterforskerne i samarbeid med spansk politi kunne identifisere IP-adresse fra e-poster han hadde sendt fra Spania. I tingrettens dom avslørte retten stadig motstrid i de siktedes forklaringer om hvor de hadde oppholdt seg, på grunn av lokaliseringsdata som indikerte at de hadde vært i nærheten av lovbruddet. I dommen beskrives kontaktmønsteret mellom de siktede ut fra trafikkdata som etterforskerne fikk innhentet. Tingretten merket seg også at en av ranernes "omgåelsesmetoder" også ble en iøynefallende fellesnevner for de involverte: Alle deres personlige mobiltelefoner hadde ingen inn- eller utgående telefontrafikk den aktuelle helgen, sammenlignet med dagene like før og etterpå.*

Departementet pekte på at ved gjennomføring av direktivet ville lagringstiden bli forlenget, noe som ga grunn til å tro at flere saker kan oppklares. Når det gjelder terrorhandlinger, har det i de senere år vært en tendens til at små grupperinger og personer som samarbeider med terrornettverk i utlandet, opptrer mindre "gjennomtenkt" under planleggingen, og er lette å avsløre. Samtidig er det svært viktig at slike terrorhandlinger avsløres, siden handlingene er potensielt svært farlige. Departementet viste også til at datalagring som metode er mindre sårbar for kriminelle omgåelsesmetoder enn sikringspålegg og kommunikasjonskontroll.

Siden det hittil ikke har vært lagret data ut over den tiden tilbyderne av kommunikasjonstjenester lagrer for sine egne formål, finnes naturlig nok ikke tall eller annen dokumentasjon for hva slik lagring vil bety av fordeler for etterforskningen. Departementet gjengir en spørreundersøkelse Kripos utførte i 2010 om bruk av historiske trafikkdata i etterforskningen. Denne gir indirekte noe informasjon om betydningen av datalagring. Respondentene ble spurt om de hadde innhentet historiske data til bruk i etterforskning. Dette var blitt gjort i 51,9 % av sakene. I de sakene hvor historiske data

ikke ble innhentet, var hovedårsaken at det ikke ble ansett nødvendig av hensyn til etterforskningen. I 2,6 % av sakene var årsaken at de data som kunne vært interessante var slettet på grunn av for kort lagringstid.

På spørsmål om det hadde vært relevant å innhente historiske data lengre tilbake i tid i saker hvor trafikkdata ble innhentet, svarte ca 60 % at de var helt enig eller litt enig i dette for så vidt gjaldt mobil- og fasttelefoni, mens ca 25 % var litt uenig eller uenig.

Departementet nevner også to eksempler på saker hvor fellende dommer er bygget på blant annet data som er mottatt fra politiet i land med lagringsplikt, men hvor de norske dataene ikke var tilgjengelige for politiet fordi de var slettet av telekommunikasjonsleverandørene. De to sakene var narkotikasaker hvor politiet hadde mottatt opplysninger henholdsvis fra Nederland og Sverige.

7 VURDERING AV MULIG OMFANG OG INNHOLD AV REGLER OM LAGRING AV KOMMUNIKASJONSDATA

7.1 Innledning

Den klareste og umiddelbare konsekvensen av EU-domstolens avgjørelse er at det ikke lenger består noen EØS-rettslig plikt til å innta direktivet i avtalen og å gjennomføre det i nasjonal rett. Det enkelte land står dermed fritt til å bestemme at det ikke vil innføre regler om plikt til å lagre kommunikasjonsdata. Også EU-kommisjonen har i en uttalelse nylig gjort det klart at datalagring nå er et nasjonalt anliggende:

> ***European Commission statement on national data retention laws***
>
> *We have seen press reports suggesting that the European Commission is "threatening to take Germany to court" over concerns regarding its national data retention law.*
>
> *As the European Commission has repeatedly said since the European Court of Justice annulled the EU Data Retention Directive: the decision of whether or not to introduce national data retention laws is a national decision. The European Commission has no intention to go back on this statement or reopen old discussions.*
>
> *We are aware that data retention is often the subject of a very sensitive, ideological debate and that sometimes there can be a temptation to draw the European Commission into these debates. The European Commission is not ready to play this game.*
>
> *We have been very clear that the Commission is not coming forward with any new initiatives on Data Retention. In the absence of EU rules, Member States are free to maintain their current data retention systems or set up new ones, providing of course they comply with basic principles under EU law, such as those contained in the ePrivacy Directive.*
>
> *We are therefore neither opposing, nor advocating the introduction of national data retention laws.*
>
> *This is why suggestions that the Commission is considering court action against the German draft data retention law are misleading. The College of Commissioners is not contemplating such action.*[40]

DLDL-dommen innebærer på den annen side ikke at enhver lagring og utlevering av kommunikasjonsdata er i strid med menneskerettighetene eller EUs charter, hvilket Kommisjonens uttalelse understreker at heller ikke den mener. For Norges del er det avgjørende spørsmålet som nevnt innledningsvis om Grunnloven § 92 eller EMK er til hinder for at datalagring pålegges tilbyderne ved lov, eventuelt på hvilke vilkår og til

[40] Uttalelse av 16. september 2015: http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm

hvilket bruk. Vi vil som nevnt i innledningen konsentrere våre vurderinger om forholdet til EMK.

I EMK er artikkel 8 om privatliv og vern om korrespondanse den helt sentrale bestemmelsen, men lagringen kan også reise spørsmål under artikkel 10 om ytringsfrihet. Vi vil nedenfor i hovedsak behandle artikkel 8.

Det synes å være bred enighet om at den rene lagring av data utgjør et inngrep i retten til privatliv og korrespondanse i EMK artikkel 8 (1). Det er lagt til grunn av departementet i Prop. 49 L (2010-2011) og av de fleste andre som har uttalt seg om spørsmålet, deriblant Høyesterett i Rt. 2014 s. 1105:

> *Også EMK artikkel 8 og FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17 forstås slik at kommunikasjonskontroll i etterforskingsøyemed er en innblanding i privat- og familielivet og i den personlige integritet som bare kan foretas så langt den er "in accordance with the law" og forholdsmessig. Dette gjelder også den rene lagring av materiale innhentet ved slik kontroll, uavhengig av den senere bruken, jf. dommer av Den europeiske menneskerettsdomstolen (EMD) i Leander mot Sverige (26. mars 1987) avsnitt 48 [EMD-1981-9248], Amann mot Sveits (16. februar 2000) avsnitt 69 [EMD-1995-27798] og S. og Marper mot Storbritannia (4. desember 2008) avsnitt 67 [EMD-2004-30562]. Jeg viser også til Prop. 147 L (2012-2013) side 95, hvor departementet på tilsvarende måte legger til grunn at "selve oppbevaringen innebærer en behandling av personopplysninger og utgjør et inngrep i personvernet". (avsnitt 29 – vår understrekning).*

Vi er enige i at den rene lagringen av data innebærer et inngrep i rettighetene beskyttet av EMK artikkel 8 (1), og ser ikke grunn til å problematisere det spørsmålet nærmere. Det avgjørende for konvensjonsmessigheten av en lagringsplikt som den foreslått ved lagringsloven er derfor om den kan rettferdiggjøres etter artikkel 8 annet ledd:

> *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.*

Inngrep kan altså etter bestemmelsen rettferdiggjøres der tre vilkår er oppfylt: inngrepet må (i) ha hjemmel i lov, (ii) ivareta nærmere angitte formål og (iii) være nødvendig i et demokratisk samfunn. I lys av EMDs praksis vil det første og det tredje vilkåret kunne komme på spissen i spørsmålet om datalagring etter lagringsloven kan rettferdiggjøres. Det er neppe uenighet om at det andre vilkåret om at lagringsloven må tilgodese relevante formål er oppfylt. Lagringsplikten kan ses som et tiltak både i) av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, ii) for å forebygge uorden eller kriminalitet, og iii) for å beskytte andres rettigheter og friheter.

Lagringsplikten vil, om lagringsloven settes i kraft, materielt sett ha hjemmel i lov. Når vi likevel sier at lovskravet kan komme på spissen i en sak om lagringsloven, er bakgrunnen at EMD ikke bare stiller krav om at et inngrep materielt sett har hjemmel i lov, men også kvalitative krav til lovhjemmelen for at den skal kunne hjemle et inngrep i artikkel 8. I *S. and Marper v. UK* avsnitt 95 uttalte for eksempel domstolen:

> *The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise (see Malone v. the United Kingdom, 2 August 1984, §§ 66-68, Series A no. 82; Rotaru v. Romania [GC], no. 28341/95, § 55, ECHR 2000-V; and Amann, cited above, § 56).*

I senere saker bruker domstolen formuleringen "*the expression "in accordance with the law" under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him,*" se for eksempel *Liberty v. UK* avsnitt 59. Vi skal gå nærmere inn på lovskravets innholdet i saker om kommunikasjonskontroll i avsnitt 7.2.

Det tredje vilkåret om at inngrepet må være nødvendig i et demokratisk samfunn byr på, som vi har vært inne på blant annet i avsnitt 6.3, en konkret forholdsmessighetsvurdering av inngrepet og de formål det skal ivareta. Det kvalitative kravet til lovhjemmel og vurderingen av proporsjonalitet kan i saker om kommunikasjonskontroll og andre overvåkningstiltak lett gli over i hverandre. Ikke minst gjelder det fordi det stilles krav til "adequate legal protection against arbitrariness". Det kravet går blant annet på hvilke rettssikkerhetsgarantier og andre sikkerhetsgarantier som tiltaket er omkranset av. Kravet til "adequate legal protection against arbitrariness" regnes av EMD blant de kvalitative kravene til lovhjemmel, men de nevnte forhold vil også ha betydning for vurderingen av hvor stort inngrep tiltaket anses å være, og dermed også i vurderingen av inngrepets proporsjonalitet. Det kan være et hensiktsmessighetsspørsmål om man henfører vurderingen av de nevnte forhold under lovskravet eller nødvendighetskriteriet.[41] Når vi i avsnittene 7.4 flg. gjennomgår de forskjellige momentene som etter vår oppfatning vil ha betydning for om datalagring etter lagringsloven vil være i overensstemmelse med artikkel 8, vil de fleste av disse

[41] Se D. Wright, P. De Hert (eds.), Privacy Impact Assessment, Springer 2012 s. 46-47

kunne henføres både under lovskravet og under forholdsmessighetsvurderingen. Vi ser ingen grunn til å sondre skarpt mellom de to kriteriene. Samlet sett dreier det seg om en vurdering av om lagringsloven møter de kriterier som EMD og har trukket opp.

I praksis innebærer vår tilnærming at det avgjørende for lagringslovens skjebne er den vurderingen av lovens konvensjonsmessighet som vil bli foretatt i domstolene – først i de nasjonale domstoler og deretter, dersom de nasjonale domstoler finner at loven er i overensstemmelse med EMK, i EMD. Vurderingen vil innebære en avveining av de kryssende hensyn, og et helt sentralt spørsmål er hvilken prøvingsintensitet domstolene vil legge til grunn. Dette er altså et spørsmål om hvilken skjønnsmargin den norske lovgiveren har. Vi vil se nærmere på hvilken prøvingsintensitet som kan forventes i avsnitt 7.3.

I fremstillingen ligger også vårt syn på departementets forholdsmessighetsvurdering. I mandatet for denne utredningen skriver departementet at:

> *Det var på det rene at lagringsplikten innebar et inngrep i personvernet. Inngrepet måtte derfor rettferdiggjøres etter EMK artikkel 8 nr. 2, noe som innebar at inngrepet måtte ha hjemmel i lov, oppfylle et legitimt formål, og være nødvendig i et demokratisk samfunn. Direktivet ivaretok et presserende samfunnsmessig behov for å bekjempe alvorlig kriminalitet. Hva som skulle lagres fulgte direkte av direktivet og ble ikke undergitt en konkret vurdering. Inngrepet ble derfor søkt rettferdiggjort i form av konkrete vilkår og begrensinger i retten til tilgang og bruk av data. Etter departementets syn gav dette gode garantier mot vilkårlighet og maktmisbruk.*
>
> *Lagringslovens regler om utlevering av data bygger følgelig på en meget grundig og konkret forholdsmessighetsvurdering.*

Som det vil fremgå av det følgende, er vi ikke enig i at loven bygger på en meget grundig vurdering av forholdsmessigheten av datalagring.

7.2 EMDs praksis i saker om telefonavlytting og –kontroll

EMD har ikke hatt til behandling spørsmålet om konvensjonsmessigheten av innhenting og lagring av kommunikasjonsdata utelukkende til det formål å forebygge eller oppklare straffbare handlinger uten at tiltakene er begrunnet i et aktuelt behov på gjennomføringstidspunktet og uten noen form for rettsordre. EMD har imidlertid gjennom årene avsagt avgjørelser i flere saker om telefonavlytting eller annen kontroll med bruk av telefoner. Verken telefonavlytting eller annen kontroll med telefonbruk er som sådan i strid med EMK. Tvert imot kan det være et spørsmål om statene i noen grad må åpne for slike etterforskningstiltak for å oppklare bestemte former for kriminalitet, se nærmere under avsnitt 7.5.

De fleste av avgjørelsene fra EMD om telefonavlytting og –kontroll omhandler individuell overvåkning. Individuell overvåkning kjennetegnes av at den er rettet mot en bestemt person, gruppe eller lokale(r). Dette er den tradisjonelle formen for overvåkning, som i

de fleste tilfeller forutsetter en konkret mistanke rettet mot et begrenset antall individer. Det foreligger imidlertid også noen avgjørelser som vurderer lovligheten av såkalt "strategisk overvåkning". Strategisk overvåkning kjennetegnes av at den *ikke* er rettet mot et begrenset antall individer, men tvert imot omfatter et stort antall telefonlinjer, mobiltelefoner etc. som på forhånd ikke er konkretisert. Overvåkningen skjer altså overfor et større antall brukere som på tidspunktet for overvåkningen ikke er kjent, med det formål å fange opp kommunikasjon som inneholder visse på forhånd definerte ord eller setninger.

Det er avgjørelser om strategisk overvåkning som har flest likhetstrekk med datalagring i tråd med direktivet, ettersom også den strategiske overvåkningen gjelder et større antall individer som på overvåkningstidspunktet ikke er mistenkt for en kriminell handling. Men også EMDs avgjørelser om individuell overvåkning kan gi veiledning ved spørsmålet om hvordan EMD vil vurdere en potensiell klage på nasjonal lovgivning som gjennomfører direktivet.

EMDs praksis fastslår at både individuell og strategisk overvåkning medfører et inngrep i artikkel 8 nr. 1. Like klart er det imidlertid at lovgivning som åpner for kommunikasjonskontroll *kan* være akseptabelt dersom lovgivningen møter de kravene som EMD har oppstilt etter artikkel 8 annet ledd. At slik lovgivning kan være akseptabel, ga EMD klart uttrykk for i *Klass and others v. Germany*, dom av 6. september 1978:

> *As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. (avsnitt 48)*

For at inngrepene skal aksepteres under konvensjonen, må de som nevnt oppfylle unntaksvilkårene oppstilt i artikkel 8 nr. 2, og i sakene om telefonavlytting er det særlig lovskravet og nødvendighetsvilkåret som har kommet på spissen. Vilkåret om at telefonavlytting må være i samsvar med loven inndeles av EMD i tre elementer. For det første må overvåkningen ha hjemmel i lov[42]. For det andre må loven være "accessible", hvilket innebærer at loven må være offentlig tilgjengelig.[43] For det tredje må loven gi

[42] I tråd med EMDs forståelse av begrepet "law" er det en materiell fremfor en formell vurdering som er avgjørende, jf. Kruslin v France.
[43] Se Liberty v, UK og Weber and Saravia v. Germany, som er omtalt nedenfor.

borgerne mulighet til å forutse og forstå under hvilke omstendigheter overvåkning kan skje (kravet til "foreseeability")[44], det vil i korthet si at reglene som åpner for overvåkning må være tilstrekkelig klare og presist utformet. Domstolen har gjennom en rekke saker utpenslet "foreseeability"-kriteriet ganske detaljert for saker om kommunikasjonskontroll. Domstolens praksis ble oppsummert i *Weber and Saravia v. Germany*, avgjørelse av 29. juni 2006:

> *93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, inter alia, Leander, cited above, p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, Malone, cited above, p. 32, § 67; Huvig, cited above, pp. 54-55, § 29; and Rotaru, cited above, § 55). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see Kopp v. Switzerland, judgment of 25 March 1998, Reports 1998-II, pp. 542-43, § 72, and Valenzuela Contreras v. Spain, judgment of 30 July 1998, Reports 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see Malone, ibid.; Kopp, cited above, p. 541, § 64; Huvig, cited above, pp. 54-55, § 29; and Valenzuela Contreras, ibid.).*
>
> *94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, Malone, cited above, pp. 32-33, § 68; Leander, cited above, p. 23, § 51; and Huvig, cited above, pp. 54-55, § 29).*
>
> *95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences*

[44] Dette kravet behandles undertiden som ledd i vurderingen av om inngrepet er nødvendig i et demokratisk samfunn, se for eksempel Kennedy v. UK, som omtales nedenfor.

> *which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, Huvig, cited above, p. 56, § 34; Amann, cited above, § 76; Valenzuela Contreras, cited above, pp. 1924-25, § 46; and Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003).*

I *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, dom av 28. juni 2007, ble det lagt til:

> *In addition, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection against arbitrary interference with Article 8 rights (see Klass and Others, cited above, pp. 25-26, §§ 54-56; mutatis mutandis, Leander v. Sweden, judgment of 26 March 1987, Series A no. 116, pp. 25-27, §§ 60-67; Halford, cited above, p. 1017, § 49; Kopp, cited above, p. 541, § 64; and Weber and Saravia, cited above, § 94). The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see Klass and Others, cited above, p. 23, § 50).*

Kriteriene som ble oppsummert i *Weber and Saravia v. Germany* er senere fulgt opp og sitert i senere avgjørelser, blant annet i *Liberty v. UK*, dom av 1. juli 2008, og *Kennedy v. UK,* dom av 18. mai 2010. EMDs praksis er også oppsummert av Høyesteretts flertall i Rt. 2014 s. 1105:

> *Oppbevaring av materiale som er innhentet ved kommunikasjonskontroll, kan altså, i henhold til Grunnloven og det internasjonale menneskerettighetsvernet, bare skje i den utstrekning det er hjemmel for dette i lov eller i forskrift gitt med hjemmel i lov. For å gi en slik hjemmel som Grunnloven og menneskerettskonvensjonene krever, holder det ikke at loven er formelt sett i orden, og at den etter alminnelige tolkningsprinsipper gir grunnlag for lagringen. Det gjelder også kvalitative krav: Loven må være tilgjengelig og så presis som forholdene tillater. Den må dessuten - i lys av den forhøyede risikoen for misbruk og vilkårlighet som erfaringsmessig kan foreligge når myndigheter tillates å operere i hemmelighet - gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for innsyn, sikkerhet og sletting. For så vidt gjelder*

> *tolkningen av EMK artikkel 8 på dette punktet, viser jeg til EMDs dommer i Malone mot Storbritannia (2. august 1984) avsnitt 66 [EMD-1979-8691], Kopp mot Sveits (25. mars 1998) avsnitt 72 [EMD-1994-23224], Amann mot Sveits (16. februar 2000) avsnitt 56 [EMD-1995-27798], S. og Marper mot Storbritannia (4. desember 2008) avsnitt 99 [EMD-2004-30562] og Kennedy mot Storbritannia (18. mai 2010) avsnitt 152 [EMD-2005-26839].*

De to nevnte britiske sakene, *Liberty* og *Kennedy,* gir god innføring i den praktiske anvendelsen av de siterte retningslinjene. I begge sakene prøvde EMD britisk lovgivning som åpnet for kommunikasjonskontroll av hensyn til blant annet forebygging og oppklaring av alvorlige straffbare handlinger ("serious crime"). Prøvingen besto i begge saker av en detaljert gjennomgang (subsumsjon) av lovgivningen under de kriterier EMD har oppstilt – med forskjellig resultat.

Liberty gjaldt "the Interception of Communications Act 1985" som åpnet for blant annet kontroll gjennom et kommunikasjonsanlegg Storbritannia hadde opprettet på 1990-tallet. Anlegget kunne fange opp kommunikasjon fra 10 000 telefonlinjer samtidig. Informasjonen som ble fanget opp var både fra telefoner, e-post og fax, med det fellestrekk at enten avsenderen eller mottakeren befant seg utenfor Storbritannia. Overvåkningen ble begrunnet i formål som nasjonal sikkerhet og forebyggelse og avdekking av grov kriminalitet.

Det kan argumenteres for det er denne EMD-avgjørelsen som har størst overføringsverdi, i hvert fall flest likhetstrekk, med en eventuell sak om lagring i tråd med DLD. For å innhente informasjon måtte det foreligge en rettsordre, men disse kunne være svært vidt formulert. Rettsordrene var ikke rettet mot bestemte personer som var mistenkt for grov kriminalitet, men omfattet isteden spesifikke undersjøiske telefonkabler (ikke linjer), hvor det var mistanke om at relevant informasjon kunne bli delt. Informasjon fra samtlige telefonlinjer som benyttet seg av de overvåkede kablene, ble derfor innhentet. Enhver som var avsender eller mottaker av elektronisk kommunikasjon som gikk mellom Storbritannia og et annet land, risikerte således å bli rammet av overvåkningen.

EMD konkluderte med at overvåkningen medførte et brudd på artikkel 8:

> *In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law.* (avsnitt 69)

Kennedy gjaldt "the Regulation of Investigatory Powers Act 2000" som åpnet for kontroll med innenlands kommunikasjon og da kun overfor enkeltpersoner eller klart identifiserte lokaler ("single set of premises") på grunnlag av nærmere spesifiserte kriterier hvorav ett var "the purpose of preventing or detecting serious crime". EMD konkluderte i den saken med at det ikke forelå et brudd på artikkel 8, og viste særlig til at vilkårene for å foreta hemmelig overvåkning var klare og presise, at det var klare regler om sletting av innhentet materiale, samt at det var gode rutiner for å avverge misbruk av innhentet informasjon.

Av interesse er også *Iordachi v. Moldova*, dom av 10. februar 2009, om kommunikasjonskontroll mot enkeltpersoner blant annet av hensyn til etterforskning av alvorlige kriminelle handlinger. Også der siterte EMD kriteriene domstolen hadde oppsummert i *Weber and Saravia v. Germany* (sitert ovenfor) og vurderte om den omtvistede lovgivningen møtte de kriteriene. EMD fant at loven ikke var tilstrekkelig klar og presis, og at den ikke ga et adekvat vern mot misbruk. Det ble vist til at de handlinger som kunne lede til kommunikasjonskontroll ikke var tilstrekkelig konkretisert, og at det heller ikke var tilstrekkelig klart hvilke personer som kunne bli utsatt for slike tiltak. Videre ble det lagt vekt på at domstolskontrollen var av nærmest formell karakter, derunder at statistikk underbygget at en høy andel av rettsanmodningene om å foreta overvåkning ble godkjent. Det ble også pekt på at lagring og sletting av innhentet informasjon ikke var underlagt klare rutiner.

En del av EU-domstolens argumenter mot at direktivet oppfylte unntaksvilkårene i charterets artikkel 7 gikk nettopp på manglende klarhet og presisjon. Gjennomgangen av EMDs utlegning av "foreseeability"-elementet i lovskravet i saker om kommunikasjonskontroll, viser etter vår oppfatning at samme type betraktninger kan ha betydning for vurderingen av om EMK artikkel 8 er oppfylt.

7.3 Hvilken skjønnsmargin har nasjonal lovgiver?

Justisdepartementet mente i høringsbrevet at nasjonalstatene må ha en stor skjønnsmargin i spørsmålet om lagringsplikten er nødvendig:

> *Ved vurderingen av hvilke tiltak det er nødvendig å iverksette for å vareta den nasjonale sikkerheten og bekjempe kriminalitet, må statene ha en stor skjønnsmargin. Hvor inngripende tiltaket er, vil også ha konkret betydning for vurderingen av om inngrepet er nødvendig.*

Flere av høringsinstansene argumenterte for en snevrere skjønnsmargin. For eksempel fremholdt Advokatforeningen at *"EMD antageligvis vil føle seg særlig kallet til å sette opp strenge kriterier for å tillate generell overvåkning av befolkningen …"*, og konkluderte med at skjønnsmarginen må antas å være vesentlig snevrere enn det som ble lagt til grunn i høringsnotatet.[45] Disse innspillene ble ikke undergitt nærmere drøftelse i proposisjonen[46], og departementet la i punkt 3.3.5.2 til grunn at "*statene som utgangspunkt må ha en forholdsvis stor skjønnsmargin ved vurderingen av hvilke tiltak*

[45] Prop. 49 L (2010-2011) s. 17
[46] Prop. 49 L (2010-2011)

det er nødvendig å iverksette for å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter."

EU-domstolen tok en ganske annen tilnærming til spørsmålet enn departementet. Mens departementets vurdering tok utgangspunkt i det legitime formål direktivet tar sikte på å oppnå, tok EU-domstolens vurdering utgangspunkt i de rettighetene som krenkes ved direktivet, og graden av krenkelsen. I lys av at retten til privatliv er en fundamental rettighet, samt at direktivet medførte en alvorlig krenkelse av denne rettigheten, konkluderte domstolen med at lovgivers skjønnsmargin var begrenset, og at domstolens prøving av denne skjønnsmarginen var streng:

> *In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict. (avsnitt 48)*

EU-domstolens avgjørelse gjelder EU-lovgiverens skjønnsmargin, mens temaet for oss er den nasjonale lovgiverens skjønnsfrihet overfor nasjonale domstoler og EMD. Avveiningene er ikke nødvendigvis de samme. Den skjønnsmarginen som nasjonalstatene har etter EMD begrunnes blant annet i at det kan være særlige lokale eller nasjonale forhold som best avveies i nasjonalstaten selv. Slike betraktninger gjør seg ikke gjeldende for EU-domstolens prøving av EU-lovgivning. Den skjønnsmarginen som er begrunnet i at en del avveininger best gjøres nasjonalt, kan også tilsi at det vil være forskjeller i Høyesteretts og EMDs prøving av norsk lovgivnings konvensjonsmessighet. Den skjønnsmargin som EMD overlater til nasjonalstatene, er ikke nødvendigvis en skjønnsmargin for nasjonal lovgiver. Tvert imot vil man i et rettighetsperspektiv kunne mene at lav prøvingsintensitet i EMD fordi den mener at avveiningen best gjøres nasjonalt, tilsier at det er enda viktigere at de nasjonale domstoler prøver avveiningen.

Skjønnsmarginen kan altså være forskjellig for forskjellige domstoler og etter forskjellige instrumenter. Vi tror likevel ikke forskjellene skal overdrives i denne saken. Det er felleseuropeisk lovgivning som ligger til grunn for lagringsloven, og det er vanskelig å se særlige lokale forhold som kan tilsi forskjeller fra land til land. Det dreier seg om avveining av grunnleggende hensyn – personvernet mot muligheter for kriminalitetsbekjempelse – som må forventes å ha betydelig vekt i alle jurisdiksjoner, og som egner seg for felleseuropeiske løsninger.

EMD har som nevnt i avsnitt 7.2 ikke tatt stilling til spørsmål som er direkte sammenliknbare med dem datalagringsdirektivet reiser, men det foreligger altså flere avgjørelser om andre straffeprosessuelle etterforskningstiltak og tvangsmidler som kan gi grunnlag for visse slutninger. Det gjelder både DNA-registre og forskjellige former for kommunikasjonskontroll. EMD har i slike saker gitt grundige redegjørelser for hvilken skjønnsmargin EMD vil tillate.

I de tidligere sakene om forskjellige former for kommunikasjonskontroll la EMD til grunn at statene har en viss skjønnsmargin i spørsmålet om adgang til kommunikasjonskontroll for å ivareta nasjonal sikkerhet og bekjempelse av alvorlig kriminalitet. I *Klass and others v. Germany*, dom av 6. september 1978, uttalte EMD:

> *As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (cf., mutatis mutandis, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 45-46, para. 93, and the Golder judgment of 21 February 1975, Series A no. 18, pp. 21-22, para. 45; cf., for Article 10 para. 2, the Engel and others judgment of 8 June 1976, Series A no. 22, pp. 41-42, para. 100, and the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, para. 48). Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. (avsnitt 49)*

I *Weber and Saravia v. Germany* (29. juni 2006) om strategisk overvåkning av elektronisk kommunikasjon uttalte EMD at:

> *The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (see,* inter alia*,* Klass and Others*, cited above, p. 23, § 49;* Leander*, cited above, p. 25, § 59; and* Malone*, cited above, pp. 36-37, § 81). Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see* Klass and Others*, cited above, pp. 23-24, §§ 49-50;* Leander*, cited above, p. 25, § 60;* Camenzind v. Switzerland*, judgment of 16 December 1997,* Reports *1997-VIII, pp. 2893-94, § 45; and* Lambert*, cited above, p. 2240, § 31). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and*

> *the kind of remedy provided by the national law (see* Klass and Others*, cited above, pp. 23-24, § 50). (avsnitt 106)*

Under henvisning til den oppstilte skjønnsmargin, samt at det forelå et adekvat og effektivt vern mot misbruk av overvåkningen, konkluderte EMD med at det ikke forelå brudd på artikkel 8.

I *Kennedy v. UK* (18. mai 2010) anførte Storbritannia at lovgiver har "*a fairly wide margin of appreciation*" på området for bekjempelse av alvorlig kriminalitet (avsnitt 148), under blant annet henvisning til *Weber and Saravia v. Germany*. EMD tok ikke konkret stilling til anførselen, men retningslinjene for vurderingen av om inngrepet var "*necessary in a democratic society*" kan tilsi at EMD gikk tett på forholdsmessighetsvurderingen:

> *As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see Klass and Others, cited above, §§ 49 to 50; and Weber and Saravia, cited above, § 106).* (avsnitt 153)

Om statens skjønnsmargin ble det ikke uttalt noe spesifikt for dette området, og EMD viste isteden til sin mer generelle rettssetning for denne vurderingen:

> *The Court has acknowledged that the Contracting States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded (see Kvasnica v. Slovakia, no. 72094/01, § 80, 9 June 2009).* (avsnitt 154)

I *Liberty and others v. UK* (1. juli 2008), der EMD som nevnt i avsnitt 7.2 kom til motsatt konklusjon i spørsmålet om den omtvistede lovgivningen ga den nødvendige *foreseeability*, uttalte EMD seg ikke eksplisitt om Storbritannias skjønnsmargin, formodentlig fordi hoveddelen av rettens begrunnelse gjaldt lovskravet og ikke tiltakets nødvendighet. Domstolen sammenliknet imidlertid overvåkningen med den som ble vurdert i *Weber and Saravia v. Germany*, og viste derunder til at Tyskland hadde regler om overvåkning som tilfredsstilte kravene i forholdsmessighetsvurderingen.

Tilnærmingen vitner etter vår oppfatning om at EMD i slike saker ikke vil anerkjenne en betydelig skjønnsmargin for statene.

Avgjørelsen i *S. and Marper v. UK* (4. desember 2008) trekker i samme retning. Den gjaldt ikke kommunikasjonskontroll, men om det medførte et brudd på retten til privatliv at politiet nektet å destruere fingeravtrykk og DNA-prøver tilhørende to personer som hadde vært siktet for kriminelle handlinger, men som ikke ble dømt. Ved vurderingen av hvilken skjønnsmargin Storbritannia skulle tillates, uttalte retten at

> *The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see Connors v. the United Kingdom, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see Evans v. the United Kingdom [GC], no. 6339/05, § 77, ECHR 2007-...). Where, however, there is no consensus within the Member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see Dickson v. the United Kingdom [GC], no. 44362/04, § 78, ECHR 2007-...).* (avsnitt 102)

Domstolen fant at England, Wales og Nord-Irland virket å være de eneste jurisdiksjonene i Europarådet som tillot oppbevaring av fingeravtrykk og DNA-materiale på ubestemt tid fra enhver person i enhver alder mistenkt for en hvilken som helst straffbar handling. Som følge av europeisk konsensus på området konkluderte EMD med at skjønnsmarginen var snever:

> *The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.* (avsnitt 112)

EMD konkluderte med at det forelå et brudd på artikkel 8:

> *In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.* (avsnitt 125).

De gjennomgåtte avgjørelsene tilsier etter vår oppfatning at EMD neppe vil innrømme nasjonalstatene "en forholdsvis stor skjønnsmargin", slik departementet la til grunn. Foreløpig er det ingen klar europeisk konsensus om hvorvidt man gjennom detaljregulering og justeringer av direktivet kan unngå å komme i strid på artikkel 8, men bakgrunnen for problemstillingen er en (langt på vei) felleseuropeisk løsning fra EUs side. Datalagringen innebærer uansett en avveining av grunnleggende verdier og rettigheter som vi tror EMD neppe vil mene egner seg for forskjellige løsninger i forskjellige jurisdiksjoner. Den foreløpige utviklingen viser også at et betydelig antall nasjonale domstoler har konkludert med at den implementerte retten bryter med fundamentale menneskerettigheter.

7.4 De grunnleggende hensyn i avveiningen og det spesielle ved den foreslåtte datalagringen – betydningen av overvåkningselementet

Hensynet til en effektiv forfølgelse av straffbare handlinger er sentralt i vårt rettssamfunn. Det er også et viktig hensyn at strafferettspleien skjer på grunnlag av et så fullstendig faktisk grunnlag som mulig, og at det faktiske grunnlaget for rettsavgjørelser i straffesaker er korrekt. Bevisvurderingen i straffesaker bør ligge så nær sannheten som mulig. I tillegg er det et selvstendig hensyn at alvorlige lovbrudd blir oppklart. At saker blir værende uoppklarte er i seg selv smertelig for samfunnet.

Straffbare handlinger er ikke bare skadelige for enkeltinteresser, men kan også virke destabiliserende på samfunnet generelt. Opplever borgerne at trusselen om kriminalitet blir for stor, vil dette kunne skape en utrygghetsfølelse som igjen vil kunne true samfunnssikkerheten ved at borgerne tar oppgaven med å beskytte seg og sine i egne hender. En slik utrygghetsfølelse vil også kunne svekke borgernes tillit til staten, en tillit som er en forutsetning for vår samfunnsorden og vårt demokrati. Derfor utgjør kriminalitet en trussel mot stabiliteten i og kvaliteten på det samfunnet vi lever i. Uten at vi foreløpig tar stilling til om fordelene ved datalagring er tilstrekkelig godt begrunnet, er det neppe tvil eller uenighet om at opplysninger om tidspunkt, varighet og sted for elektronisk kommunikasjon kan være verdifulle for å oppklare visse former for

forbrytelser, og som kan gi vesentlig tilleggsinformasjon for etterforskning og oppklaring av andre.

Mot dette står hensynet til beskyttelsen av individets rettigheter og integritet mer allment og personvernet mer spesielt. Søken etter opplysninger i strafferettspleien er begrenset av regler som skal sikre enkeltindividet mot overgrep. Dette er en velkjent problemstilling i straffeprosessen, og ligger under blant annet begrensninger i vitneplikten og i politiets og påtalemyndighetens adgang til å anvende tvangsmidler.

Så langt skiller ikke datalagring etter lagringsloven seg fra tilfeller av kommunikasjons-kontroll rettet mot enkeltpersoner eller grupper på bakgrunn av mistanker om straffbare forhold, eventuelt konkret begrunnede ønsker om å forebygge straffbare handlinger. Så langt skiller datalagring etter lagringsloven seg heller ikke fra spørsmål om utlevering til politiet av data som teletilbydere eller andre har lagret av andre grunner (for eksempel egen fakturering) til etterforskning av mistenkte straffbare handlinger. Også i slike tilfeller tilsier beskyttelsen av privatlivet en avveining av hensynet til kriminalitetsbekjempelse og hensynet til personvernet. Like fullt er det etter vår mening viktige prinsipielle forskjeller. Lagringslovens regler om lagringsplikt innebærer oppbevaring av data utelukkende fordi de vil kunne ha betydning for etterforskning eller forebyggelse av straffbare handlinger. Det er altså snakk om lagring som går ut over det som er nødvendig av tekniske og økonomiske grunner knyttet til tilbud og drift av kommunikasjonstjenestene.

Det er etter vår oppfatning stor prinsipiell forskjell på regler som gir politiet og påtalemyndigheten tilgang til opplysninger som av andre grunner allerede finnes, og regler, som ut fra hensynet til oppklaring av *mulige* straffesaker, pålegger lagring av data som ellers ikke ville blitt lagret.

Når data lagres utelukkende ut fra det formålet å bekjempe og oppklare mulige straffbare handlinger, dreier det seg i realiteten om en form for overvåkning. Det er vanskelig å se prinsipielle forskjeller på datalagring utelukkende myntet på bruk i etterforskning av mulige straffbare handlinger og kameraovervåkning med lagring av billedmaterialet. Det dreier seg i begge tilfeller om innsamling av informasjon om personer uten at de er mistenkt eller gjenstand for særlig oppmerksomhet fra myndighetene på det tidspunkt som registreringen av opplysningene skjer.

Selv om ikke innholdet i kommunikasjon lagres, er det snakk om systematisk innsamling av opplysninger som er egnet til å kartlegge enkeltindividers kommunikasjon og bevegelser. Det er data som kan fortelle om private forbindelser, preferanser, vaner, sympatier, antipatier og en rekke andre forhold av strengt privat karakter. Dataene kan i tillegg gi informasjon om profesjonelle forbindelser, forretningsstrategier, og andre tilsvarende forhold av faglig eller yrkesmessig karakter. Selv om slike forhold ikke kan defineres som en del av privatlivet i snever forstand, nyter de åpenbart vern etter EMK artikkel 8.

Som gjennomgangen i avsnitt 7.2 viser, har EMD hittil ikke tatt stilling til konvensjonsmessigheten av slike rene overvåkningstiltak. De saker som er behandlet har alle handlet om mer begrensete former for overvåkning som enten er basert på konkrete mistanker eller i alle fall har tilknytning til konkrete saker. Vår oppfatning er at man ikke kan se bort fra at de prinsipielle forskjeller som er påpekt her, kan medføre at EMD vil gripe forholdsmessighetsvurderingen annerledes an i en sak om datalagring etter lagringsloven (eller tilsvarende lovgivning basert på DLD i andre land) enn det som var tilfellet i de sakene om kommunikasjonskontroll som er behandlet. Man har ingen garanti for at EMD også i en sak om DLD-inspirert datalagring vil ta det utgangspunkt at slik innsamling i utgangspunktet er tillatelig så lenge lovgivningen er tilstrekkelig klar og tilgjengelig, skaper den nødvendige forutsigbarhet, og ivaretar grunnleggende rettsikkerhetsgarantier, derunder oppstiller de nødvendige rettssikkerhetsgarantier*. Det kan etter vår oppfatning ikke utelukkes at de personvernmessige betenkelighetene ved overvåkningselementet er så fremtredende og tungtveiende at man simpelthen ikke kan anse datalagring nødvendig i et demokratisk samfunn.*

Dersom EMD skulle ta samme innfallsvinkel til de rene lagringssaker som de har gjort i de tidligere sakene om forskjellige former for kommunikasjonskontroll, synes det i alle fall klart at lagring og bruk av slike opplysninger vil være underlagt en grundig forholdsmessighetsvurdering. Vi skal i de følgende avsnitt gå gjennom de vesentlige momenter i den vurderingen.

Vårt syn er at dersom slik lagring skal kunne aksepteres, må det påvises at lagring utover det som er kommersielt og teknisk nødvendig faktisk har påviselig effekt i form av bedrete muligheter til etterforskning og oppklaring av forbrytelser, og da en så betydelig effekt at nytten oppveier det omfattende inngrepet som lagringen representerer i personvernet og andre rettigheter. Vi tror videre at en forutsetning må være at det etableres et strengt regime både med hensyn til de rettslige rammene som dette kan skje innenfor og med hensyn til kontroll med bruken. Det siste følger blant annet av de kravene til lovens kvalitet som EMD har oppstilt, og særlig "foreseeability"-elementet og kravet til effektive rettsmidler, se for eksempel *Kruslin v. France*, dom av 24. april 1990, om telefonavlytting der EMD, etter å ha uttrykt bekymring om de tilgjengelige rettsmidler la til:

> *Above all, the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has*

been discharged by an investigating judge or acquitted by a court. The information provided by the Government on these various points shows at best the existence of a practice, but a practice lacking the necessary regulatory control in the absence of legislation or case-law.

In short, French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. (avsnitt 35 og 36)

7.5 Kan statene ha en menneskerettslig plikt til å foreta datalagring?

Det følger av EMK artikkel 2 at statene har en positiv plikt til å beskytte borgernes liv mot alle former for trusler, herunder livstruende kriminelle handlinger. Statenes positive plikter omfatter også å sikre de enkelte rettighetene i EMK, selv om disse i konvensjonen er formulert som forpliktelser til ikke å gjøre inngrep i rettighetene. En slik plikt er utviklet gjennom rettspraksis med det formålet å sikre en effektiv beskyttelse av rettighetene, ikke bare mot inngrep fra staten, men også fra private. En tilsvarende plikt kan også følge av Grunnloven § 92 sitt krav om staten skal "respektere og sikre" menneskerettighetene.

Plikten for staten til å sikre menneskerettighetene innebærer blant annet en plikt til effektiv forebyggelse og forfølgelse av handlinger som innebærer krenkelser av menneskerettighetene gjennom å gjøre slike krenkelser straffbare og gjennom å sikre en effektiv strafferettslig forfølgelse av dem. Dette stiller krav både til de materielle og prosessuelle reglene, og til etterforskningen og påtalemessig oppfølgning. I praksis fra EMD er likevel disse forpliktelsene utviklet på ad hoc basis, slik at det er vanskelig å si noe sikkert og endelig på generelt grunnlag om innhold og omfang av dem.[47]

På den annen side bør det fastholdes at det internasjonale menneskerettighetsvernets kjerne først og fremst retter seg mot å beskytte borgerne fra misbruk fra myndighetenes side. Myndighetenes plikt til å beskytte rettighetene også mot inngrep fra private er et supplement til, og en utfylling av, den beskyttelse rettighetene gir mot statens maktutøvelse. Beskyttelse mot staten og beskyttelse mot andre er derfor ikke to sider av samme sak som kan avveies fritt mot hverandre uten at man risikerer å uthule det vernet som rettighetene skal gi mot statlig maktutøvelse.

Forpliktelsene til å treffe nødvendige tiltak for å forebygge og oppklare organisert kriminalitet, menneskehandel og korrupsjon er således begrenset til det som ikke er i strid med de grunnleggende prinsippene i en statsparts nasjonale rettsorden. Det betyr at Grunnloven og internasjonale menneskerettighetskonvensjoner som Norge er forpliktet av og har gjennomført i norsk rett setter rammene for forpliktelsene etter konvensjonen. Uttalelsene til Europarådet til korrupsjonskonvensjonen viser dessuten at kommunikasjonskontroll ligger i grenselandet for hva som er tillatelige etterforskingsskritt selv når det er snakk om alvorlige forbrytelser.

[47] Se Trine Baumbach, Strafferet og menneskeret, Karnov Group, København 2014 s. 355.

Etter EMDs praksis har statene en forpliktelse til å kriminalisere og straffe krenkelser av fundamentale verdier og aspekter ved menneskeverdet. Dette innebærer også en plikt til effektivt å etterforske mulige krenkelser av menneskerettighetene.[48] Det stilles med andre ord kvalitative krav til etterforskningen i form av at politiet arbeider hurtig og effektivt og foretar de relevante etterforskingsskritt som saken gir anledning til.[49] Dette kan også etter omstendighetene innebære et krav om at staten innretter sin lovgivning slik at den gir politiet de nødvendige hjemler for å kunne utføre en effektiv etterforskning.

I saken *K.U. v. Finland*, dom av 2. desember 2008, hadde noen plassert en kontaktannonse på internett i navnet til en tolvårig gutt, hvor han angivelig søkte etter jevnaldrende gutter til seksuell kontakt. Da gutten og hans foreldre oppdaget det, anmeldte de forholdet til politiet. Politiet søkte kommunikasjonsleverandøren om IP-adressen til den som hadde lastet opp annonsen, men fikk avslag. Politiets begjæring om rettslig utleveringspålegg førte ikke frem, da svikaktig bruk av andres navn på internett ikke hørte til de lovbrudd som ga hjemmel for utlevering av kommunikasjonsopplysninger. EMD kom til at staten hadde brutt sin forpliktelse til å gi en effektiv beskyttelse av retten til privatliv etter artikkel 8 ved ikke å gi hjemmel for utlevering av opplysninger som var nødvendige for etterforskning og oppklaring av saken. Domstolen uttalte blant annet i avsnitt 49:

> *The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.*

Dommen viser med andre ord at menneskerettighetene kan inneholde en plikt for statene til å sikre politiet tilgang til kommunikasjonsdata til det formål å oppklare straffbare handlinger som innebærer krenkelser av personers rettigheter, dersom dette er nødvendig for oppklaring av forbrytelsen. Sentralt i begrunnelsen er det at garantien for personvernet på internett og i bruken av kommunikasjonstjenester ikke kan være absolutt. Dette kan også brukes som argument for at statene i visse tilfeller også må sørge for at data om slik bruk er tilgjengelig ut over det som telekommunikasjons-selskapene finner nødvendig å oppbevare ut fra sine formål. Selv om det ikke foreligger noen EØS-rettslig plikt til å innføre regler om lagring av kommunikasjonsdata, kan en slik

[48] Se Linda Gröning, Erling Johannes Husabø og Jørn Jacobsen, Frihet, forbrytelse og straff – En systematisk fremstilling av norsk strafferett, Fagbokforlaget Bergen 2015 s. 110-111.
[49] Se Baumbach s. 413.

plikt dermed foreligge etter EMK. I så fall må lagring og tilgang til kommunikasjonsdata utformes og praktiseres i skjæringsfeltet mellom grunnleggende rettigheter; på den ene siden retten til en effektiv beskyttelse for rettigheter individene har mot krenkelser, og på den annen side personvernet og ytringsfriheten som krenkes av inngrep i kommunikasjonsfriheten.

Også gjennom ulike internasjonale konvensjoner har Norge forpliktet seg til å bekjempe særskilte former for kriminalitet på ulike måter. De fleste av konvensjonene medfører forpliktelser til kriminalisering av særlige straffbare handlinger, men enkelte inneholder også forpliktelser av straffeprosessuell karakter. Dersom pliktene etter konvensjonene strekker seg så langt at de påfører statene en plikt til å lagre data for å kunne oppklare eller avverge bestemte former for kriminalitet, vil det kunne ha betydning i den forholdsmessighetsvurderingen som må gjøres etter EMK.

En sentral konvensjon er FNs konvensjon 15. november 2000 om grenseoverskridende organisert kriminalitet og dens protokoller om henholdsvis menneskehandel, menneskesmugling og ulovlig produksjon av og handel med skytevåpen. Konvensjonen inneholder omfattende forpliktelser til å kriminalisere handlinger begått som ledd i organisert kriminalitet, hvitvasking og korrupsjon, andre tiltak for å bekjempe hvitvasking og korrupsjon, samt regulering av internasjonalt samarbeid i slike saker. Konvensjonen og protokollen om menneskehandel ble gjennomført i norsk rett ved lov 4. juli 2003 nr. 78.

Konvensjonens artikkel 20 nr. 1 lyder i norsk oversettelse slik:

> *Dersom det ikke er i strid med de grunnleggende prinsippene i en statsparts nasjonale rettsorden, skal statsparten, innenfor rammen av sine muligheter og slik bestemmelsene i den nasjonale lovgivningen foreskriver, treffe de nødvendige tiltak for å gi sine vedkommende myndigheter tillatelse til hensiktsmessig bruk av kontrollert levering og, dersom den anser det hensiktsmessig, bruk av andre særlige etterforskningsteknikker, for eksempel elektronisk eller andre former for overvåking og spaningsoperasjoner, på sitt territorium med sikte på effektiv bekjemping av organisert kriminalitet.*

Bestemmelsen nevner ikke datalagring uttrykkelig, men siden den nøyer seg med å ramse opp eksempler på de etterforskingsskritt som er ansett nødvendig kan den også gi argumenter for at landene må tillate lagring av kommunikasjonsdata i bekjempelsen av menneskehandel.

Etter Europarådets strafferettskonvensjon mot korrupsjon artikkel 23 nr. 1 plikter konvensjonsstatene å vedta lovgivning som åpner for å bruke "spesielle etterforskningsteknikker" ("special investigative techniques") for å lette innsamling av bevismateriale i tilknytning til korrupsjonshandlinger, samt for å identifisere, oppspore, fryse og beslaglegge midler til og utbytte fra korrupsjon. Artikkel 23 (1) har følgende ordlyd:

> *Each Party shall adopt such legislative and other measures as may be necessary, including those permitting the use of special investigative techniques, in accordance with national law, to enable it to facilitate the gathering of evidence related to criminal offences established in accordance with Article 2 to 14 of this Convention and to identify, trace, freeze and seize instrumentalities and proceeds of corruption, or property the value of which corresponds to such proceeds, liable to measures set out in accordance with paragraph 3 of Article 19 of this Convention.*

Bestemmelsen er nettopp begrunnet i de særlige vanskelighetene som oppdagelse og etterforskning av korrupsjon er forbundet med. I Explanatory Report til konvensjonen uttales det at selv om bestemmelsen ikke lister opp forskjellige etterforskningsmetoder, referer bestemmelsen i særdeleshet til "*the use of under-cover agents, wire-tapping, bugging, interception of telecommunications, access to computer systems and so on*".[50] Samtidig erkjennes det at "*most of these techniques are highly intrusive and may give rise to constitutional difficulties as regards their compatibility with fundamental rights and freedoms. Therefore, the Parties are free to decide that some of these techniques will not be admitted in their domestic legal system*". Norske myndigheter la til grunn at norsk straffeprosess tilfredsstilte kravene i artikkel 23 da konvensjonen ble gjennomført med endring i straffeloven i 2003, se Ot.prp. 78 (2002-2003) s. 26.

Som vi ser, går ikke forpliktelsene i disse konvensjonene lengre enn det som kan anses som akseptable etterforskningsmetoder etter internasjonale menneskerettigheter og nasjonale forfatninger. Det kan neppe heller være grunnlag for å strekke plikten til å sikre menneskerettighetene etter EMK lengre enn dette. Man vil i dermed ikke kunne utlede noen plikt til datalagring ut fra statens plikt til å sikre menneskerettighetene. Statens plikt går ikke lengre enn til å sikre dem med de midler som er tillatelige ut fra blant annet beskyttelsen av privatlivet. Sagt på en annen måte kan man si at plikten til å sikre menneskerettighetene kan utgjøre et lovlig formål for inngrep i rettigheter, men den kan ikke erstatte de andre elementene i vurderingen av inngrepets lovlighet og proporsjonalitet.

7.6 Er de kriminalitetsbekjempende fordelene ved datalagring tilstrekkelig dokumentert?

En viktig del av forholdsmessighetsvurderingen er bedømmelsen av om et inngrep i en rettighet er egnet og relevant for formålet og at inngrepet er nødvendig. Kravet til at et inngrep er nødvendig betyr ikke at det må være uunnværlig, men det innebærer på den annen side mer enn at det er nyttig eller ønskelig, se *Handyside v. UK* avsnitt 48. Den begrunnelsen som myndighetene gir for et inngrep må etter EMDs praksis være "relevant and sufficient", se *S. and Marper v. UK* avsnitt 101. I vurderingen av om det er nødvendig inngår at det samme formålet ikke kan nås med et tiltak som er mindre inngripende. Når man skal bedømme om lagring av kommunikasjonsdata er i overensstemmelse med menneskerettighetene, er ikke spørsmålet om bruk av

[50] Se http://conventions.coe.int/Treaty/EN/Reports/Html/173.htm

kommunikasjonsdata som sådan er egnet og nødvendig for politiets arbeid. Allerede i dag har politiet tilgang til store mengder av slike data, både data som kommunikasjonsleverandører lagrer til egne formål, og data som fremkommer gjennom iverksettelse av etterforskingsskritt eller preventive tiltak i form av overvåkning og kommunikasjonskontroll. Det avgjørende for vurderingen av datalagringens forholdsmessighet er mernytten som politiet har av at kommunikasjonsdata blir lagret, ut over den lagringen som skjer av tekniske og kommersielle grunner eller på grunnlag av særlige vedtak etter prosess- og politilovgivningen i tilfeller der politiet har et konkret behov.

De uttalelsene som er gitt til Justisdepartementet av politiet og påtalemyndigheten etter dommen i EU-domstolen går entydig i den retningen at lagring av kommunikasjonsdata er nødvendig for oppklaring av mange straffesaker. I mange saker er det vanskelig for politiet å få tak i vitner. Tendensen er særlig tydelig innen organisert kriminalitet og i saker om offerløs kriminalitet. I slike saker kan trafikkdata og elektroniske spor være svært sentrale bevis. Informasjonen er på mange måter et taust vitne og representerer i mange saker en tråd som lar seg følge. Riksadvokaten skriver 26. mai 2014 at "*manglende mulighet til å bruke historiske trafikkdata vil kort og godt avskjære politiet fra å gjennomføre en adekvat etterforskning ved mange straffbare handlinger hvor oppklaring er sterkt ønskelig i et vidt samfunnsmessig perspektiv*". Kripos peker i sin uttalelse 23. mai 2014 på at utviklingen går i retning av at stadig mindre data lagres av tilbyderne av kommersielle og tekniske grunner, og at politiets tilgang til denne typen bevis forsvinner. Videre uttaler de at "*Trafikkdata er og vil være et avgjørende verktøy for politiet i bekjempelse av alvorlig kriminalitet. Det finnes ikke alternative virkemidler som kan erstatte verdien av denne typen objektiv informasjon i straffesaker*".

I hvilken grad lagring av trafikkdata kan gi informasjon som kan være til nytte for etterforskning og avverging av straffbare handlinger, er omstridt. Den tekniske utviklingen går i retning av muligheter for å kommunisere som ikke etterlater seg kommunikasjonsdata. Etter hvert som kriminelle har blitt mer bevisste tar de i økende grad i bruk slike kommunikasjonsformer. Til dette blir det innvendt fra politihold at de som planlegger straffbare handlinger blir mer sikkerhetsbevisste etter hvert som tidspunktet for utførelsen nærmer seg. Dette er en av grunnene til at det er nødvendig med tilgang til eldre data. Det er også slik at det ofte er personer som ikke er så innvevd i kriminelle miljøer som først blir tatt, og at man fra dem kan rulle opp mer sentrale deler av et kriminelt nettverk. Siden det derfor kan ta tid å identifisere de mer sentrale aktørene, kan tilgang til eldre data være nødvendig. Politiet har også pekt på at fingeravtrykk fortsatt har vært viktig som bevis i mange saker, selv om kriminelle vet at de med lette midler kan sikre seg mot å sette slike spor. At en etterforskningsmetode er lett å omgå betyr derfor ikke uten videre at den ikke er effektiv i mange saker.

Vi har ikke forutsetninger for å foreta en faglig vurdering av effektiviteten av datalagring som middel i etterforskning eller avverging av forbrytelser. Dette krever inngående innsikt både i teknologiske og politifaglige spørsmål. I lys av det inngrepet i personvernet som datalagring innebærer, kan det imidlertid legges til grunn at nytten og nødvendigheten av lagring av kommunikasjonsdata må kunne underbygges på en

overbevisende måte for at et slikt tiltak kan anses forholdsmessig. Som nevnt ovenfor ble inngrepet som datalagring innebærer av EU-domstolen karakterisert som vidtrekkende og av særlig alvorlig karakter.

Hvilke krav som skal stilles til dokumentasjon er uklart. I saker om vidtgående inngrep stiller EMD gjerne krav til at staten bygger sine tiltak på inngående analyser og studier som sikter til å finne den beste balansen mellom de hensyn som skal ivaretas gjennom inngrepet og rettighetene til dem som blir berørt.[51] I *S. and Marper v. UK* gikk domstolen utenom problemet. Først uttalte den at "*neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position"*. Dette trekker i retning av at den ikke mente at UK hadde oppfylt kravet til å vise at lagringen av DNA og fingeravtrykk, som denne saken dreide seg om, var oppfylt. Så sa domstolen imidlertid at den "*accepts that the extension of the database has nonetheless contributed to the detection and prevention of crime*". Saken ble imidlertid løst på et annet grunnlag idet domstolen fant at den britiske ordningen "*fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard*". Dette må i alle fall tas til uttrykk for at domstolen ikke var overbevist om nødvendigheten av tiltaket ut fra det materialet som ble presentert, vurdert opp mot styrken av det inngrepet som det var tale om. I denne saken var det spørsmål om lovligheten av en ordning som tillot politiet å oppbevare vevsprøver, DNA-profiler og fingeravtrykk tatt fra personer som hadde vært mistenkt i en straffesak, men hvor saken senere var henlagt eller hvor vedkommende var frifunnet. Storbritannia var alene om å ha så vidtgående regler om lagring av slikt materiale fra personer som ikke var dømt i en straffesak.

Heller ikke EU-domstolen er klar på hvilken dokumentasjon som kreves. I avsnitt 49 aksepterer domstolen på generelt grunnlag at kommunikasjonsdata gir muligheter til å oppklare kriminalitet og derfor må anses som et brukbart redskap i etterforskning av straffesaker. Lagring av slike data er derfor egnet til å gjennomføre de mål som ligger til grunn for DLD. I avsnitt 51 spør domstolen så om den datalagringen som er foreskrevet i direktivet er nødvendig. Den peker på at målet om å bekjempe alvorlig kriminalitet er viktig og kan være avhengig av moderne etterforskningsteknikker. Men så uttaler domstolen videre at "*et sådant mål af almen interesse kan imidlertid, hvor grundlæggende det end er, ikke i sig selv begrunde, at en foranstaltning med henblik på datalagring som den, der er indført med direktiv 2006/24, anses for nødvendig af hensyn til bekæmpelsen af grov kriminalitet*". Ut over dette gir ikke domstolen angivelse på hvilke krav til dokumentasjon som må oppfylles.

Det som i alle fall kan trekkes ut av disse dommene er at kravet til dokumentasjon av nødvendigheten av et tiltak må vurderes opp mot arten og styrken av inngrepet som det er tale om. Siden det er på det rene at datalagring representerer et inngrep av

[51] Se D. Wright, P. De Hert (eds.), Privacy Impact Assessment, Springer 2012 s, 54-58.

vidtrekkende og alvorlig karakter, vil kravet til dokumentasjon av nødvendigheten måtte settes høyt. Det er videre på det rene at det forholdet at datalagring skal oppfylle et legitimt og viktig behov, og at trafikkdata ofte er av vesentlig betydning for å oppklare straffesaker og avverge lovbrudd, ikke i seg selv er tilstrekkelig til at forholdsmessighetskravet er oppfylt. Det er mernytten av den generelle lagringen av kommunikasjonsdata som må påvises. Selv om det er lett å vise at kommunikasjonsdata som sådan ofte er viktig i etterforskningen, har det vist seg vanskelig å gi noen dokumentasjon for at lagring av trafikkdata faktisk fører til bedre oppklaring i betydelig målestokk. Redegjørelsen for behovet for datalagring i proposisjonen til lagringsloven er generell og basert på risiko- og sannsynlighetsbetraktninger. Kripos' undersøkelse som er gjengitt i proposisjonen til lagringsloven tyder ikke på at etterforskerne mener at de har gått glipp av viktige bevis i mange saker, og det er nevnt bare to saker i Justisdepartementets redegjørelse hvor samarbeid med utenlandsk politi som har tilgang til lagrede trafikkdata har hatt betydning for domfellelse, se ovenfor avsnitt 6.4. Senere uttalelser fra norske rettshåndhevende myndigheter er også hypotetiske idet det ikke finnes erfaringer med etterforskning ut fra data som er lagret.

Det forhold at politiet har vært avskåret fra tilgang til trafikkdata og IP-adresser betyr ikke uten videre at flere saker ville blitt oppklart om slike data hadde vært lagret. Det som i høyden kan sies er at dette ville medført en høyere sannsynlighet for oppklaring uten at det er lett å tallfeste denne sannsynligheten. Data som er samlet inn i EU om forholdet mellom innføring av lagringsplikt og endring i oppklaringsfrekvenser gir ikke noen klar støtte for at flere saker oppklares når datalagring innføres. En undersøkelse gjort av forskningsavdelingen til den tyske forbundsdagen ga ikke grunnlag for å påvise signifikante endringer i oppklaring som følge av innføring av datalagring i perioden 2005-2010.[52]

På den annen side kan det være at det tar lengre tid før effektene av et slikt tiltak viser seg i oppklarte straffesaker. I en sammenstilling gjort av EU-kommisjonen i 2013 fremholdes det at det foreløpig har gått for kort tid til at man kan trekke noen statistisk holdbare slutninger av bruk eller fravær av kommunikasjonsdata, og at hvorvidt en etterforskning lykkes eller mislykkes er resultat av en mengde samvirkende faktorer.[53] Sammenstillingen fremholder imidlertid at tilgang til lagrede trafikkdata ofte er av avgjørende betydning, særlig i saker om terrorisme og organisert kriminalitet, alvorlige seksualforbrytelser, etablering av forsett til å begå forbrytelser og store grenseoverskridende saker. Dette underbygges gjennom eksempler fra en rekke forskjellige land, og fra enkelte land som Tyskland og Tsjekkia rapporteres det om dramatiske konsekvenser for etterforskning at domstolene har underkjent regler om datalagring. På den annen side lar slike dramatiske konsekvenser seg ikke avlese i endringer i oppklaringsprosenten i straffesaker i Tyskland. Sammenstillingen redegjør også for de statistiske opplysningene som medlemslandene har rapportert inn i medhold av rapporteringsplikten i DLD artikkel 10. Det foreligger statistikk fra 23 medlemsland

[52] Wissenschaftlicher Dienst des Deutschen Bundestages, Sachstandsbericht v. 18.03.2011, WD 73000036/11.

[53] Evidence for necessity of data retention in the EU, DG Home, European Commission March 2013 s. 8, http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

siden 2008. Statistikken viser at krav om tilgang til lagrede data var fremsatt meget hyppig, i alt over to millioner ganger per år, noe som tilsvarer elleve forespørsler per 100 saker som ble etterforsket. Forespørslene fordelte seg ulikt på sakene, slik at det i enkelte saker ble fremsatt svært mange forespørsler om tilgang til lagrede data. I 67 % av tilfellene dreide det seg om data yngre enn tre måneder, og i 89 % av sakene dreide det seg om data som var seks måneder gamle eller yngre. I 11 % av sakene var dataene seks til tolv måneder gamle.

Det svenske forslaget til nye lagringsregler bygger på at tilgang til trafikkopplysninger ofte er av avgjørende betydning for oppklaringen av straffesaker. Utredningen har innhentet opplysninger om politiets praksis, og konstaterer at de fleste av de opplysningene som politiet innhenter er yngre enn en måned. Ca 20-25 % er eldre enn tre måneder, mens 10 % av den totale mengden er eldre enn fem måneder. Det er særlig ved tidkrevende undersøkelser av alvorlige straffbare handlinger at det er behov for opplysninger som skriver seg lengre tilbake i tid.[54] På denne bakgrunn konkluderer utredningen med at en kortere lagringstid enn seks måneder vil føre til at formålet med lagringen ikke oppfylles.

Denne vurderingen står i kontrast til vurderingen til den tyske regjeringen, som er kommet til at lagring kan pålegges for trafikkdata i ti uker, men for lokaliseringsdata bare i fire uker. Differensieringen bygger på at inngrepsintensiteten er forskjellig for de forskjellige typer av data og at dette må gjenspeiles i lagringstiden for at inngrepet skal være forholdsmessig. De fastsatte lagringstidene anses å være tilstrekkelige for at de nødvendige data skal være tilgjengelige i et overveiende antall av tilfeller, se kommentaren til avsnitt 1 i forslaget til § 113b i telekommunikasjonsloven.

Ulikhetene i vurderingene i det svenske og tyske forslaget understreker den usikkerheten som vurderingene av behovet for og nytten av datalagringen er forbundet med, samt vurderingenes hypotetiske karakter. I samme retning trekker det at en rekke land som er medlem av Europarådet klarer seg uten regler om lagring av trafikkdata. Mangelen på en enhetlig tilnærming i lovgivning og praksis øker risikoen for at en domstolsprøving av lagringsregler vil konkludere med at lagring krenker personvernet og andre rettigheter. Det vil lett kunne fremstå som at man setter hele befolkningen under systematisk overvåkning fordi dette vil kunne føre til en lettere oppklaring av et antall straffesaker, hvis mengde eller karakter ikke lar seg nærmere fastslå annet enn ved generelle hypoteser. Uten en bedre og mer konkret dokumentasjon av nytten av datalagring enn den som hittil har vært presentert, antar vi at en plikt for telekommunikasjonsleverandørene til å lagre trafikkdata vil bli ansett som et uforholdsmessig inngrep i personvernet.

[54] Se Ds 2014:23 s. 86.

7.7 Hvilken betydning spiller lagringstiden og utvalget av forbrytelser data kan benyttes til etterforskning av?

7.7.1 Begrensninger fastsatt i EMDs praksis

Som vist i avsnitt 7.2, har EMD både i saker om individuell og strategisk telefonavlytting utlagt foreseeability-kriteriet slik at loven må klargjøre i hvilke tilfeller og under hvilke vilkår kommunikasjonskontroll kan finne sted ("the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"). Dette er videre presisert dit hen at loven må inneholde en rekke sikkerhetsmekanismer som skal verne mot misbruk:

> *[T]he Court has developed following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.*

Blant de sentrale mekanismene er altså at loven må presisere hvilke kriminelle handlinger som kan gi grunnlag for overvåkningen, hvilke kategorier av personer som kan bli rammet og legge begrensninger på varigheten av kontrollen. Av disse tre begrensningene er det utelukkende begrensningene på lengden på kontrolltiltaket som kan overføres direkte til datalagring. Den første av de tre nevnte begrensningene går på i hvilke tilfeller kontrolltiltaket kan gjennomføres. For datalagring er det en ikke-problemstilling: Kontrolltiltaket – selve innsamlingen av informasjon – knyttes ikke til bestemte handlinger, men skal gjennomføres overfor enhver til enhver tid. Derfor er heller ikke den andre begrensningen aktuell for datalagring. Slik datalagring foreslås gjennomført, kan det ikke gjøres noen begrensning til kategorier av personer som kan bli underlagt kontrollen. Poenget er tvert imot at man skal samle inn informasjon om enhver, slik at man har dette tilgjengelig for det tilfellet at det skulle bli behov for det i oppklaring eller forebygging av straffbare handlinger.

Det faktum at EMD så langt har ansett det nødvendig å begrense kontrolltiltakene til (forholdsvis) klart definerte tilfeller av straffbare handlinger og klart definerte kategorier av personer, etterlater tvil om hvorvidt EMD i det hele tatt vil tillate at datalagring kan skje på nærmere bestemte vilkår. Det forutsetter i så fall at EMD forlater sin praksis for så vidt gjelder de to nevnte kriterier, og i stedet utvikler nye kriterier for datalagring. For det tilfellet at EMD skulle akseptere at DLD-inspirert datalagring mot enhver kan tillates, er det etter vår oppfatning enhver grunn til å tro at EMD vil stille krav til hjemmelsloven som er minst like strenge som dem som gjelder for kommunikasjonskontroll mot enkeltpersoner basert på konkrete mistanker. Når tiltaket ikke kan begrenses til bestemte handlinger eller personkategorier, er det grunn til å forvente at EMD i alle fall nedfeller tilsvarende begrensninger til uthentingen av lagret informasjon, det vil si at denne knyttes til konkretiserte straffbare handlinger og – om mulig – kategorier av

personer. Vi skal se nærmere på hvordan begge typer av begrensninger er gjennomført i lagringsloven, og om de imøtekommer de kriterier EMD har oppstilt for kommunikasjonskontroll.

7.7.2 Begrensningen av de handlinger som kan gi grunnlag for tiltak

Lagringsloven bestemmer som påpekt i avsnitt 6.2.3 at informasjon skal kunne hentes til etterforskning eller avverging av straffbare handlinger med en minste strafferamme på henholdsvis fire år for trafikkdata og fem år for basestasjonssøk, samt for enkelte andre nærmere oppregnede straffbare handlinger med lavere strafferamme. Det er neppe tvil om at de særskilt oppregnede handlinger tilfredsstiller EMDs krav om foreseeability. Spørsmålet er imidlertid om spesifikasjon gjennom anvisning på en minste strafferamme skaper den nødvendige forutsigbarhet.

To avgjørelser fra EMD er i den sammenheng av særlig interesse. Den første er *Iordachi v. Moldova*, dom av 10. februar 2009. Den gjaldt en moldovsk lov som åpnet for "*operational investigative measures*" blant annet til "*the prevention of serious, very serious and exceptionally serious offences*". Etter § 16 i den moldovske straffeloven var "serious offences … considered to be those offences which are punishable with imprisonment of up to fifteen years; very serious offences are intentional offences punishable with imprisonment of over fifteen years; and exceptionally serious offences are those intentional offences punishable with life imprisonment". Det ble opplyst at ca 59 % av alle straffbare handlinger regulert i straffeloven falt innenfor disse kategoriene. Om dette uttalte EMD:

> *[T]he nature of the offences which may give rise to the issue of an interception warrant is not, in the Court's opinion, sufficiently clearly defined in the impugned legislation. In particular, the Court notes that more than one half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants. (avsnitt 44)*

Den andre sentrale avgjørelsen er *Kennedy v. UK*, dom av 18. mai 2010. Som forklart i avsnitt 7.2, gjaldt den the Regulation of Investigatory Powers Act 2000 som i artikkel 5 åpnet for telefonavlytting der hvor det er nødvendig "in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom". EMD uttalte seg om hvorvidt de to første alternativene – "national security" og "serious crime" – var tilstrekkelig klare. Uttrykket "serious crime" var i samme lovs artikkel 8 definert til å gjelde straffbare handlinger som enten handlinger "for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more" eller handlinger som "involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose".

Om holdbarheten av disse kriteriene uttalte EMD:

As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, section 5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom (see paragraphs 31 to 32 above). The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance (Al-Nashif, cited above, § 121). Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means (see paragraph 33 above). As for "serious crime", this is defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime is also explained in the Act (see paragraphs 34 to 35 above). The Court is of the view that the reference to serious crime, together with the interpretative clarifications in the Act, gives citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures. The Court therefore considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to an interception order is sufficiently clear (compare and contrast Iordachi and Others, cited above, § 46).

De to avgjørelsene er ikke uten videre enkle å harmonere. Forskjellen på de to regelsettene som var til bedømmelse var at det moldovske benyttet strafferammen som avgrensningskriterium, mens det britiske benyttet den sannsynlige straffen for en førstegangsovertreder av en viss alder, alternativt bestemte karakteristika ved handlingen eller dens resultat (bruk av vold, betydelig økonomisk gevinst eller at det har preg av å være organisert). Så vidt vi kan forstå, burde bruken av strafferamme skape større forutsigbarhet enn antakelser om hvilken straff som kan være aktuell. I det lyset

er det overraskende at EMD aksepterte den britiske loven, men ikke den moldovske. Vi antar at den avgjørende forskjellen i praksis var opplysningen om hvor stor andel av straffbare handlinger som falt innenfor de kategorier som loven tillot avlytting for. Tilsvarende tall er imidlertid ikke gitt for den britiske loven.

Vi har ikke gjennomgått den norske straffeloven for å anslå hvor stor andel av straffebudene som har en strafferamme på minst fire år, men med mindre det er en vesentlig andel, burde den norske loven anses å skape den nødvendige forutsigbarhet dersom EMD underkastes den samme prøve som den som ble benyttet i *Kennedy v. UK*. Vi minner imidlertid om at det etter vår oppfatning er såpass store forskjell på rettede kontrolltiltak og systematiske overvåkningstiltak at man ikke kan se bort fra at EMD vil skjerpe kravene til forutsigbarhet for når lagrede kan benyttes.

For å bedre muligheten for at en lagringslov skal overleve EMDs prøving, vil vi anbefale at man presiserer de straffbare handlinger nærmere. Det bør gjøres en nærmere gjennomgang av for hvilke forbrytelser lagrede data skal kunne innhentes til etterforskning av, og de forbrytelsene bør listes opp spesifikt. En slik gjennomgang er fordelaktig ikke bare av hensyn til forutsigbarhet, men også av hensyn til å dokumentere nødvendigheten av datalagring. Det er i den sammenheng grunn til å minne om avsnitt 60 i EU-domstolens dom om DLD der betydningen av konkret rettferdiggjøring poengteres:

> *Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.*

Vi ser det ikke som vår oppgave å definere hvilke straffbare handlinger det bør kunne hentes ut lagrede data for. Det krever politifaglige analyser og avveininger som vi ikke er de rette til å foreta. Vi vil imidlertid påpeke at terrorhandlinger og andre angrep på den nasjonale sikkerheten i alle fall historisk har stått i en særstilling. Uten at det har belegg i EMD-praksis fra de senere år, vil vi tro at det vil være tyngre for EMD å sette til side tiltak som er begrenset til slike handlinger. En avgrensning som den gjort i politiloven § 17 d vil antakelig bedre mulighetene for at datalagring anses konvensjonsmessig. Bestemmelsen åpner for bruk av bestemte tvangsmidler i forebyggende øyemed, men kun for PST og kun dersom det er grunn til å undersøke om noen forbereder brudd på a) straffeloven § 147a, b) straffeloven §§ 90, 91 og 91a, eller c) straffeloven §§ 222, 223, 227, 229, 231 eller 233.

Kravet til proporsjonalitet tilsier uansett at det bør være et kriterium at den mistenkte handlingen er av alvorlig karakter i seg selv, det vil si at det ikke dreier seg om en mindre alvorlig krenkelse av det aktuelle straffebudet. Dette bør komme klart til uttrykk som et vurderingstema i loven. Vi mener også at man bør opprettholde kriteriet om at de innhentede opplysningene må være av vesentlig betydning for etterforskningen. Det bidrar kanskje ikke til økt forutsigbarhet, men er en vesentlig materiell sikkerhetsmekanisme.

7.7.3 Begrensningen av hvilke kategorier av personer tiltak kan gjennomføres overfor

Nært forbundet med begrensningen til bestemte straffbare handlinger er begrensningen om at loven må presisere hvilke grupper av personer telefonavlytting kan skje mot som ledd i en etterforskning eller for å forebygge kriminalitet. Denne begrensningen er slått fast av EMD i flere saker. Det at telefonavlytting må begrenses til bestemte straffbare handlinger, innebærer selvfølgelig også en begrensning av hvilke personer som det kan gjennomføres tiltak mot. Kravet om "a definition of the categories of people liable to have their telephones tapped" går imidlertid lenger enn dette. Nøyaktig hva som ligger i kravet er imidlertid ikke helt klart. Avgjørelsen i *Iordachi v. Moldova* tilsier at kravet innebærer at det må følge av loven hvilken tilknytning en person må ha til en (mistenkt) straffbar handling for at tiltak skal kunne benyttes overfor vedkommende, det vil si om tiltak kan benyttes mot mistenkte, tiltalte eller også andre personer. I avgjørelsen fant EMD at en ordlyd som innebar at "suspects, defendants or other persons involved in a crime" ikke var tilstrekkelig til å oppfylle kravet til foreseeability, fordi lovgivningen ikke definerte uttrykket "other persons involved in a crime" nærmere.

I *Weber and Saravia v. Germany,* avgjørelse av 29. juni 2006, synes imidlertid EMD å akseptere at de relevante kategorier av personer også kan defineres på annet vis. Saken gjaldt strategisk overvåkning av trådløs telefonkommunikasjon, typisk mobiltelefoner. Overvåkningen var ikke rettet mot konkrete individer, men derimot mot internasjonale samtaler hvor konkrete, utvalgte ord ble benyttet for å fange opp samtalene. I sin oppsummering av tidligere rettspraksis viste EMD i avsnitt 95 (sitert i avsnitt 7.2) at det var et krav at loven måtte inneholde "a definition of the categories of people liable to have their telephones tapped", og uttalte deretter i avsnitt 97 konkret om denne overvåkningen:

> *The Court further observes that the conditions for strategic monitoring, as laid down in section 3(1) and (2) of the amended G 10 Act, in particular, indicated which categories of persons were liable to have their telephone tapped: the persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links (or also via fixed telephone lines in the case of monitoring to avert an armed attack on Germany, in accordance with section 3(1), point 1). In addition, the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers listed in section 3(1), points 1-6, or had be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers (section 3(2)).*

Vi kan vanskelig skjønne annet enn at EMD i den saken aksepterte videre definisjoner av de aktuelle personer enn det som var tilfellet i den senere moldovske saken.

Slik vi ser det, vil et vilkår om en definisjon av aktuelle personer langt på vei utelukke systemer for datalagring i tråd med DLD dersom det oppstilles for selve lagringen som tiltak. Lagringen skal nettopp gjelde enhver. Dersom vilkåret derimot knyttes til utleveringen av data, vil man for trafikkdata kunne innta de nødvendige avgrensninger i loven. For basestasjonssøk vil det imidlertid være mer utfordrende. Basestasjonssøk kan innebære innhenting av informasjon om for eksempel hvilke abonnenter som har oppholdt seg på et bestemt sted til et bestemt tidspunkt. Med mindre det at man faktisk var til stede skulle anses som en tilstrekkelig definisjon av kategorien av personer som kan bli utsatt for de relevante tiltak, vil datalagring være avhengig av at EMD oppstiller andre kriterier for at datalagring skal være konvensjonsmessig enn det som er gjort for kommunikasjonskontroll med mer begrenset rekkevidde.

7.8 Hvilken betydning spiller lagringstiden hos teletilbyderen og oppbevaringstiden hos politi eller påtalemyndighet?

Både i saker om individuell og strategisk telefonavlytting har EMD, som ledd i vurderingen av om det foreligger tilfredsstillende garantier mot misbruk, uttalt at loven som hjemler overvåkningen må sette begrensninger for overvåkningens varighet. EMD har imidlertid ikke etablert en generell lengstetid for overvåkning før en rettsordre må fornyes. Samtidig har EMD ikke blitt forelagt spørsmål om rettmessigheten av regelverk som hjemler overvåkning i lenger enn seks måneder.

DLD fastsetter i artikkel 6 at lagringsperioden skal være minst seks måneder og maksimalt to år. Det innebærer at medlemsstatene kan fastsette lagringsperioden innenfor det handlingsrommet, og selv om det ikke er uttalt eksplisitt i artikkel 6, synes det klart at lagringsperioden kan være forskjellig for de forskjellige kategorier av data som skal lagres etter artikkel 5. Slik er det også tolket av de tyske myndighetene. DLD legger imidlertid ingen ytterligere føringer på medlemsstatenes valg enn de to yttergrensene. Det var blant de forhold EU-domstolen kritiserte i dommen av 8. april 2014:

> *Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.*
>
> *Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary." (avsnitt 63 og 64).*

EU-domstolen ser ved dette ut til å etterspørre konkrete vurderinger av hvor lenge politiet vil ha den nødvendige nytte av de forskjellige formene for data, og EU-domstolen

– slik vi leser den – synes også å stille spørsmål ved minsteperioden på seks måneder. Vi forstår den altså slik at dersom politiets vesentligste nytte av en bestemt type data vil være i en periode som er kortere enn seks måneder, bør lagringstiden forkortes tilsvarende. Dette er i tråd med det alminnelige synspunktet om at et inngrep for å være nødvendig ikke må strekke seg lenger enn det konkrete behovet tilsier, hvilket er den tradisjonelle tilnærming også etter EMK. Rettslig sett handler dette altså ikke om foreseeability-elementet i lovskravet. Enhver positivrettslig tidsbegrensning vil for så vidt skape den nødvendige forutsigbarhet. Derimot handler det om nødvendighetsvurderingen: Inngrepet vil ikke anses å være forholdsmessig hvis det går lenger enn den konkete nytten tilsier.

Det konkrete valget av lagringstid – om den for eksempel settes til 3, 6, 12 eller 24 måneder – har ikke vi forutsetninger for å belyse utover disse generelle synspunktene. Det må gjøres en konkret politifaglig vurdering der myndighetenes oppgave vil være å underbygge hvor lenge man vil ha den nødvendige nytte av dataene. Ettersom lagringen av data kan oppfattes som et rent overvåkningstiltak, og utvilsomt i seg selv utgjør et inngrep i rettighetene beskyttet i EMK artikkel 8 (1), kunne man også resonnert slik at lagringstiden ikke er så sentral. Synspunktet er i så fall at det store spørsmålet er overvåkningselementet som sådan, og at varigheten ikke har vesentlig betydning for inngrepets styrke. Vi leser Datatilsynets høringsuttalelse i den retning når de hevder at "*spørsmålet om implementering av datalagringsdirektivet først og fremst er et prinsipielt spørsmål, og at det derfor er av underordnet betydning hvordan direktivet eventuelt implementeres (med tanke på for eksempel lagringstid og –sted)*".[55]

Som vi allerede har vært gjennom i avsnitt 7.4, er vi enige i at direktivet, selv om det ikke gjelder innholdet i kommunikasjonen, utfordrer retten til privatliv på et mer vidtfavnende og prinsipielt nivå enn hva som har vært tilfellet i saker vurdert av EMD tidligere. Det er derfor risiko for at EMD ikke vil akseptere tiltak som innebærer en form for overvåkning av tilnærmet hele befolkningen uten noen mistanke om eller engang tilknytning til en straffbar handling. Dersom datalagring imidlertid først passerer det hinderet, det vil si at EMD aksepterer at man på gitte vilkår kan pålegge at lagring av bestemte data kan skje uten annen begrunnelse enn at dataene vil kunne ha vesentlig betydning som etterforskningsmateriale i saker som kan oppstå, er det grunn til å tro at EMD vil prøve forholdsmessigheten av tiltaket. Derunder vil domstolen se på om pålagt lagringstid går utover det som kan begrunnes faglig. For å øke mulighetene for at en lagringslov skal anses konvensjonsmessig, vil vi derfor anbefale at det gjøres en konkret vurdering av hvor lenge politiet vil ha betydelig nytte av de forskjellige formene for data.

Lagringsloven stiller krav til hvor lenge data skal lagres hos teletilbyderen. Uten at det er sagt eksplisitt i DLD artikkel 6, antar vi at det er det samme som reguleres der. Så langt vi kan forstå, vil det imidlertid også ha betydning for inngrepets omfang hvor lenge dataene blir lagret hos politiet eller påtalemyndigheten etter at det er utlevert til etterforskningsformål. I lagringsloven er det ikke gitt egne regler om politiets bruk og behandling av de utleverte opplysningene. Det er i forarbeidene forutsatt at dette blir

[55] Prop. 49 L (2010-2011) s. 66

regulert av politiregisterloven. Denne loven inneholder regler om bruk av informasjonen, men begrenser ikke denne bruken til de formålene som dataene er utlevert for. Loven har ikke regler om tilintetgjøring av utlevert informasjon, og ingen regler om kontroll med politi og påtalemyndighet. Dette tilfredsstiller neppe kravene til behandling av kommunikasjonsdata som må stilles i henhold til EMK

Blant de "minimum safeguards" EMD har oppstilt i saker om kommunikasjonskontroll er "*the circumstances in which recordings may or must be erased or the tapes destroyed*", se avsnitt 95 i *Weber and Saravia v. Germany*, sitert i avsnitt 7.2. I lys av det og EMDs generelt strenge utlegning av kravet til forutsigbarhet i saker om kommunikasjonskontroll, er det grunn til å forvente at lagringslovens manglende regulering ikke vil bli godtatt av EMD.

I fravær av klarere føringer vil det alminnelige utgangspunktet være at politiet eller påtalemyndigheten ikke bør beholde materialet lengre enn de har bruk for det. Det er i den sammenheng grunn til å minne om at DLD innebærer unntak[56] fra den alminnelige plikten etter kommunikasjonsvernsdirektivet[57] artikkel 6 til å slette eller anonymisere trafikkdata når det ikke lenger er behov for materialet, se også ekomloven § 2-7 tredje ledd som sier at "trafikkdata, lokaliseringsdata og data nødvendige for å identifisere abonnenten eller brukeren skal slettes eller anonymiseres så snart de ikke lenger er nødvendig" for de formål de er lagret, derunder for å oppfylle plikten etter den nye § 2-7 a til å lagre data. Heller ikke disse utgangspunktene gir imidlertid særlig klarhet. Dersom man skulle foreslå en ny lov, vil vår anbefaling være at man eksplisitt vurderer lagringstiden også hos politi og påtalemyndighet og legger klarere føringer på rettens fastsettelse av tidsrommet.

En viktig del av proporsjonalitetsvurderingen er videre at de data som er lagret ikke er tilgjengelige til andre formål enn det som begrunner lagringen og politiets tilgang. Dette er både spørsmål om en presis angivelse av formålene i lovene som gir tilgang til de lagrede opplysningene, kontroll med utleveringen og bruk av opplysningene og tekniske og andre sikkerhetsmessige tiltak for å sikre at opplysningene ikke kommer på avveie eller blir misbrukt til andre formål. Dette må reguleres både overfor tjenestetilbyderen som lagrer data etter lovens pålegg, og også overfor politiet og påtalemyndigheten som har fått data utlevert. I de reglene om datalagring som er vedtatt, er det bare regler om lagringen hos den som er lagringspliktig. Det er imidlertid ingen regler om hvordan den som har fått kommunikasjonsdata utlevert skal lagre og behandle dataene.

Når det gjelder kommunikasjonskontroll, så har straffeprosessloven andre og mer betryggende regler i kapittel 16 a og 16 c. I strprl. § 216 finnes regler om bruken av opplysninger til andre forhold enn det som begrunner utleveringen av dem. I reglene om behandlingen av opplysninger innhentet ved kommunikasjonskontroll er det krav om tilintetgjøring, jf. strprl. § 216 g. Opplysningene skal snarest mulig tilintetgjøres i den utstrekning de er uten betydning for forebyggelsen eller etterforskningen av de straffbare

[56] Se DLD artikkel 3

[57] Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon

forhold. Disse bestemmelsene er presise og klare og tilfredsstiller antakelig kravene etter EMK.

7.9 Betydningen av hvem som kan få tilgang til det utleverte materialet

Det må tas hensyn også til annet enn politiet og påtalemyndighetens nytte av materialet og de berørtes rett på personvern. Hvis det tas ut tiltale, må også den tiltaltes rett til tilgang til etterforskningsmaterialet etterleves. Det materialet som politiet har plukket ut og vil benytte som bevis i straffesaken må nødvendigvis kunne beholdes i alle fall frem til dommen er rettskraftig, og kanskje også lenger i tråd med alminnelige rutiner for arkivering av straffesaker og tilhørende bevis. Det er imidlertid heller ikke fritt frem for å slette det resterende materialet. Tiltalte vil normalt ha krav på å få gå gjennom tilleggsmaterialet for å se om det inneholder noe tiltalte mener er til hans fordel. Saken *Natunen v. Finland*, dom av 30. juni 2009, gjaldt nettopp et tilfelle der politiet hadde gjennomført telefonavlytting i utstrakt grad og hadde plukket ut den delen av materialet de mente var relevant. Resten var slettet. Klageren hevdet at det var i strid med EMK artikkel 6 og da mer presist prinsippet om *equality of arms,* og vant frem med det. EMD uttalte bl.a.:

> *Failure to disclose to the defence material evidence, which contains such particulars which could enable the accused to exonerate himself or have his sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence, and therefore a violation of the right guaranteed in Article 6 § 3 (b) of the Convention. (avsnitt 43)*

I forlengelsen av spørsmålet om siktede eller tiltaltes rett til etterforskningsmaterialet, oppstår det spørsmål om de andre aktørenes tilgang til materialet i straffesaken kan ha personvernmessige konsekvenser som kan ha betydning i vurderingen av konvensjonsmessigheten av datalagringen. Dersom materialet som utleveres til politiet skal benyttes i en straffesak, kan som nevnt ikke tilgangen begrenses til politiet og påtalemyndigheten. Hvis lagrede data skal benyttes som bevis i straffesaken, vil – som nevnt i avsnitt 6.2.5 – både tiltalte, eventuelt medtiltalte, forsvarere og domstolen få tilgang til det materialet som er plukket ut fra aktoratets side. Det samme gjelder fornærmede og eventuelt bistandsadvokater. Med mindre særlige begrensninger skulle få anvendelse, vil beviset også måtte føres i åpen rett med den virkning at allmennheten også får tilgang. I tillegg kommer siktede/tiltalte og forsvarernes rett til det materialet påtalemyndigheten ikke anser relevant som bevis.

Vi har som nevnt i avsnitt 6.2.5 ikke sett at de personvernmessige virkninger av andre aktørers tilgang til det utleverte materialet har vært reist som problemstilling tidligere. Vår oppfatning er imidlertid at denne tilgangen kan ha en betydning for personvernet som ikke kan ses bort fra i den forholdsmessighetsvurderingen som må gjøres etter EMK artikkel 8 (2). Ganske særlig vil det gjelde data om andre enn de siktede/tiltalte, hva enten det er trafikkdata eller opplysninger hentet inn gjennom basestasjonssøk.

7.10 Særlig om data fra advokater og andre med sterk taushetsplikt samt pressens kilder

Et særlig problem med lagring av kommunikasjonsdata er at lagringen vil komme til å omfatte kommunikasjon med personer hvis kommunikasjon nyter en særlig beskyttelse så som leger, prester, advokater og journalister. I sin dom peker EU-domstolen på, som en innvending mot DLD, at det ikke inneholder noen unntaksbestemmelser som gjør at det ikke kommer til anvendelse på personer hvis kommunikasjon er underlagt taushetsplikt, se avsnitt 58. Det er ikke helt klart om domstolen mener at dette er et moment i proporsjonalitetsvurderingen, eller om et slikt unntak er en betingelse for at lagring av kommunikasjonsdata i det hele tatt skal være lovlig. Det fremgår imidlertid av avsnitt 65 at det må foretas avgrensninger som må sikre at inngrepet i de grunnleggende rettighetene er begrenset til det strengt nødvendige, og at disse avgrensningene må følge av klare og presise regler. Siden inngrep i privilegert kommunikasjon reiser særlige spørsmål, må det i det minste foreligge klare regler for hvordan denne dataen skal skilles ut fra den øvrige mengden av data, samt hvordan de skal behandles.

Også den tyske forfatningsdomstolen underkastet den privilegerte informasjonen en særlig vurdering. Den uttalte i avsnitt 238 at en lagringslov må sette et absolutt utleveringsforbud "i det minste" for data om en "engere krets" av beskyttet kommunikasjon, særlig når det gjelder kommunikasjonen til personer, ansatte og organisasjoner på det sosiale og kirkelige området. Dette anså den nødvendig for å beskytte retten til personer i "sjelelig og sosial nød" anonymt å henvende seg for å få hjelp hos personer med lovfestet taushetsplikt. Domstolen ga imidlertid ingen anvisning på hvordan en slik beskyttelse kan utformes i praksis.

Viktigheten av å beskytte kommunikasjonen til bestemte grupper som advokater og journalister, også mot politiets etterforskning, har vært oppe i en rekke saker for EMD.

Om advokater uttalte EMD i *Wieser and Bicos Beteiligungen GmbH v. Austria* avsnitt 65:

> *With regard to the first applicant this manner of carrying out the search incurred the risk of impinging on his right to professional secrecy. The Court has attached particular weight to that risk since it may have repercussions on the proper administration of justice.*

Denne saken dreide seg om generelle beslag av elektronisk materiale på et advokatkontor.

Tiltak som setter pressens kildevern i fare kommer i en særstilling siden kildevernet er en viktig del av og forutsetning for ytringsfriheten i EMK artikkel 10, se blant annet *Goodwin v UK*. Spørsmålet kom særlig på spissen blant annet i *Tillack v. Belgium*. Saken dreide seg om etterforskningsskritt i form av ransakning og beslag mot en journalist som var mistenkt for å ha bestukket tjenestemenn i kommisjonen for å få tilgang til konfidensielle dokumenter.

I innledningen til sine vurderinger presiserer domstolen følgende (avsnitt 53):

> *Freedom of expression constitutes one of the essential foundations of a democratic society and the safeguards to be afforded to the press are of particular importance. Protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.*

Videre tilføyde den i avsnitt 55:

> *In cases concerning the press, such as the present one, the national margin of appreciation is circumscribed by the interest of a democratic society in ensuring and maintaining a free press. Similarly, that interest will weigh heavily in the balance in determining, as must be done under paragraph 2 of Article 10, whether the restriction was proportionate to the legitimate aim pursued.*

I avsnitt 65 sa retten som ledd i sin vurdering av forholdsmessigheten til beslaget hos journalisten:

> *The Court emphasises that the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution.*

Dommen føyer seg inn i rekken av tidligere avgjørelser som stiller meget strenge krav til at statene respekterer pressens kildevern. EMD har i avgjørelsene slått fast at pressens kildevern er en av de grunnleggende forutsetningene for pressefrihet og at begrensinger i kildevernet vil bli møtt med en meget grundig undersøkelse fra EMDs side ("most careful scrutiny").

Det er på den annen side klart at vernet ikke er absolutt.[58] Det er imidlertid strenge krav som må oppfylles for å gjøre unntak fra det. For norsk rett er kildevernet og dets grenser omhandlet i flere saker fra Høyesterett, blant annet Rt. 2010 s. 1381. Her uttaler Høyesterett blant annet i avsnitt 62:

> *Ved vurderingen av om det her skal gjøres unntak fra kildevernet, finner jeg det riktig å legge til grunn den mer langsiktige effekten av å skulle*

[58] Se Jon Petter Rui Johansen, Fra menneskerettighetsdomstolen - Utvalgte avgjørelser for perioden 15. august 2007 til 23. januar 2008, Tidsskrift for strafferett 2008 s 93-103.

> *gjøre unntak - den såkalte "chilling effect", som ble fremholdt blant annet i Rt-1992-39 (på side 49) og Goodwinsaken (EMD-1990-17488). I det lange løp er det en risiko for at en mer utstrakt bruk av vitneplikt vil kunne medføre at viktige kilder blir borte. Etter mitt syn tilsier derfor vesentlige samfunnsinteresser at media i størst mulig utstrekning bør kunne bevare anonymitet om sine kilder.*

For kommunikasjonsdata kommer for pressen det særlige hensynet inn at det er kildens identitet som nyter vern, like mye som innholdet av den kommunikasjonen som har foregått mellom kilden og en journalist. Rene kommunikasjonsdata er derfor uten videre mer inngripende i pressens kildevern enn i for eksempel kommunikasjonen med advokater og leger hvor det i hovedsak er innholdet av kommunikasjonen som er beskyttet. Det er neppe teknisk mulig å utforme en lagringsplikt som unntar data om kommunikasjon som kan røpe privilegert informasjon fra lagring. I teorien kan man kanskje tenke seg et system hvor de personer som har særlig krav på beskyttelse melder inn til tjenesteyteren at deres apparater eller adresser skal beskyttes mot lagring eller utlevering. Et system med en slik registrering vil imidlertid i seg selv kunne representere en krenkelse fordi man da i praksis vil få et register over kommunikasjonsmidler som kan representere særlig sensitiv kommunikasjon, og vil uansett være umulig å få fullstendig eller holde à jour. Dersom EMK må antas å stenge for udiskriminerende lagring av kommunikasjon som kan inneholde privilegert informasjon uten at det foreligger en konkret situasjon eller mistanke som kan begrunne også en slik lagring, vil dette innebære at datalagring ikke kan innføres uten å komme i konflikt med EMK.

Det er uansett klart at en datalagringsordning må differensiere mellom privilegert informasjon og annen informasjon når det gjelder tilgangen til og bruken av de lagrede data. Skal man beskytte denne typen kommunikasjon må det derfor være gjennom forbud mot utlevering og anvendelse av opplysninger kombinert med kontrollmekanismer. I størst mulig grad må det settes inn barrierer mellom dem som samler inn data og dem som er involvert i oppklaring eller etterforskning av saker. Ved siden av et forbud mot å anvende opplysninger som kan røpe kommunikasjon med personer som er unntatt fra vitneplikt på grunn av yrkes- og kallsmessig taushetsplikt eller pressens kildevern, kan tenkes regler om sletting av slike data samt protokollering av at sletting er foretatt.

Spørsmålet om overvåkningstiltak som gjør det nødvendig å skille ut privilegert informasjon var oppe for EMD i saken *Kopp v. Switzerland*. Advokaten Kopp var mistenkt for å være innblandet i hvitvasking og for sammen med sin kone som arbeidet i en høy offentlig stilling å ha solgt fortrolig informasjon. Påtalemyndigheten etterforsket saken som et mulig brudd på taushetsplikt i offentlig tjeneste, og Kopp var dermed ikke selv under mistanke. Han var inne i saken som en tredjeperson som kunne sitte inne med opplysninger som kunne bidra til oppklaring av saken. Etter sveitsisk rett kunne ikke advokater avlyttes i saker uten at de selv var mistenkt for noe straffbart, men denne begrensningen gjaldt bare korrespondanse og samtaler knyttet til selve advokatgjerningen. Påtalemyndigheten beordret avlytting av til sammen 13 telefonlinjer, herunder både den private telefonen til Kopp og hans forretningstelefon. I

avlyttingsordren var det angitt at advokatsamtalene hans ikke skulle avlyttes. Et sentralt punkt i saken var hvordan myndighetene skulle skille ut de samtalene som Kopp førte i egenskap av advokat og de samtalene han hadde i andre sammenhenger. Om dette uttalte domstolen i avsnitt 73:

> "*However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel.*"

Løsningen i det sveitsiske systemet var at en ansatt ved postvesenets juridiske kontor skulle foreta den nødvendige sorteringen. Domstolen fant et slikt system, hvor en offentlig ansatt, uten judisielt oppsyn, skulle foreta denne oppgaven, "astonishing". Den fant at den sveitsiske ordningen krenket artikkel 8 fordi "*Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter*".

I norsk rett reguleres forholdet til privilegert informasjon av straffeprosessloven § 216g tredje ledd som har slik ordlyd:

> *"Opplysninger fra kommunikasjonskontrollen som retten etter §§ 117 til 120 er avskåret fra å motta forklaring om, og opplysninger fra personer som etter §§ 122 er fritatt fra forklaringsplikt, skal slettes så snart som mulig etter at det er fastslått at materialet omfatter slike opplysninger. Dette gjelder likevel ikke dersom vedkommende kan mistenkes for en straffbar handling som opplysningene kan ha betydning for."*

Slik denne bestemmelsen er utformet tilfredsstiller den ikke de kravene til presisjon og klarhet som EMD har oppstilt blant annet i *Kopp v. Switzerland* idet den ikke gir anvisning på hvordan materialet skal gjennomgås med sikte på å fastslå om det inneholder privilegert informasjon, hvem som skal foreta en slik gjennomgang, hvilke kriterier og metoder som skal benyttes eller mekanismer for kontroll med gjennomgangen.

Høyesterett behandlet bestemmelsen i Rt. 2015 s. 81. Her la Høyesterett til grunn at det er påtalemyndigheten som skal foreta den gjennomgangen som loven gir anvisning på. Under henvisning til *Kopp v. Switzerland* kom Høyesterett til at så lenge det ikke er etablert noen særskilt ordning, må påtalemyndigheten slette samtaler som den vet er med en advokat uten å gjennomhøre dem for å finne ut av om det dreier seg om klientsamtaler eller ikke. Et annet alternativ er å oversende slike samtaler til tingretten til gjennomgang. Høyesterett var således ikke enig med lovgiveren som i proposisjonen

uttalte at "politiet i en viss utstrekning må ha mulighet til å høre gjennom materiale som kan være omfattet av reglene om vitneforbud eller –fritak".

Selv om datalagringen ikke skal omfatte kommunikasjonens innhold, vil i noen tilfeller selve det forholdet at det har vært kontakt mellom en person og for eksempel en advokat, lege eller journalist i seg selv kunne røpe opplysninger som er beskyttet av taushetsplikten. Det er gjerne når slik informasjon ses i sammenheng med annen informasjon som politiet har, at den fortrolige karakteren av kommunikasjonsdata kan tre frem. Dette kan ikke minst være problematisk for pressen, hvor rene kommunikasjonsdata kan røpe pressens kilder. Det er store praktiske problemer forbundet med å foreta den nødvendige silingen før materialet utleveres. Man kunne selvsagt tenke seg en ordning hvor dette ble utført av tingretten. Men det vil ofte dreie seg om store mengder av data som må gjennomgås. Ofte vil det dessuten ikke være mulig ut fra de rene data å identifisere hva som dreier seg om kommunikasjonen til personer med særlig taushetsplikt uten å ha opplysning om hvem som er innehaver av bestemte telefonnumre og IP-adresser. Slike opplysninger fremkommer kanskje på et langt senere stadium under politiets analyse av materialet, men da vil det jo alt være utlevert og informasjonen kjent for politiet.

Problemene med i det hele tatt å skille ut privilegert informasjon fra det materialet som utleveres av de lagrede kommunikasjonsdata, er forhold som i seg selv trekker i retning av at datalagring ikke kan gjennomføres uten å komme i konflikt med EMK. Uansett må det legges til grunn at uten at man etablerer ordninger som kan sikre dette på en betryggende måte, vil en lagringsordning ikke stå seg. Det å utforme en slik ordning vil kreve en betydelig teknisk innsikt og en innsikt i arten av data som vil bli omfattet av en lagring. Dette er en type innsikt vi ikke har, og vi vil derfor ikke begi oss inn på en konstruksjon av en slik ordning. Den som skal utforme en slik ordning må imidlertid oppfylle de kravene som EMD og EU-domstolen har satt til klarhet, forutberegnelighet og sikkerhet. Det betyr at ordningen klart må angi hvem som skal foreta silingen, hvilke kriterier og metoder den skal bygge på, retningslinjer for det skjønnet som må utøves i vurderingen av om kommunikasjonsdata kan røpe fortrolig informasjon og for vurderingen av om fortrolig informasjon likevel i unntakstilfeller skal utleveres. Silingen må skje ved en instans som er uavhengig av påtalemyndigheten og forvaltningen, og i den utstrekning den ikke skjer ved en domstol, være underlagt judisiell kontroll.

7.11 Muligheten for og betydningen av effektive rettsmidler for alle som berøres av lagringen

Som nevnt innledningsvis i avsnitt 7 er muligheten for kontroll og effektiv rettsbeskyttelse en sentral del av vurderingen av om et tiltak er "nødvendig i et demokratisk samfunn". EMD har i flere saker gjentatt at "*powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse,*" se for eksempel *Kennedy v. UK* avsnitt 153, *S. and Marper v. UK* avsnitt 103 og *Weber and Savaria v. Germany* avsnitt 93-95. Særlig viktig i denne forbindelsen er uttalelser i *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, om at "*the domestic*

law must provide some protection against arbitrary interference with Article 8 rights" og "*this assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law*".

Ut fra rettspraksis kan det således oppstilles en rekke konkrete krav til muligheten for kontroll og effektiv rettsbeskyttelse. Det første kravet som kan oppstilles på grunnlag av EMDs praksis er at loven på en tilstrekkelig klar måte gir borgerne en treffende indikasjon på i hvilke situasjoner og under hvilke betingelser myndighetene kan pålegge utlevering av de lagrede dataene. Dette innebærer at de straffbare handlingene som kan gi grunnlag for et krav om utlevering av kommunikasjonsdata må være klart angitt, se nærmere avsnitt 7.7.2 ovenfor. Likeledes må det være klart angitt i loven under hvilke omstendigheter politiet kan kreve informasjon utlevert, det vil si krav til grad av mistanke eller fare. Her vil nok den gjeldende lagringsloven langt på vei tilfredsstille kravene, i alle fall for de konkrete straffebudene som er oppregnet. Det kan som nevnt ovenfor være mer tvilsomt om den generelle henvisningen til straffbare handlinger som etter loven kan medføre straff av fengsel i 4(5) år eller mer tilfredsstiller kravet til presisjon. Selv om borgerne i teorien kan skaffe seg oversikt over hvilke handlinger dette er gjennom å slå opp i loven, vil dette i praksis være utilgjengelig for mange. I tillegg kommer det forholdet at det bør kreves at lovgiveren har tatt stilling til den enkelte straffbare handling som kan gi grunnlag for et så inngripende overvåkningstiltak for at man skal kunne si at det foreligger en forsvarlig vurdering av nødvendigheten fra lovgiverens hånd.

EMD har videre uttalt at det er i strid med grunnleggende rettssikkerhetskrav om en dommer eller et forvaltningsorgan kan avgjøre omfanget av en utlevering ut fra et fritt skjønn. Loven må således angi hvor omfattende et utleveringspålegg kan være og hvordan det skal avgrenses slik at borgerne er beskyttet mot vilkårlighet.

Dagens lov legger beslutningsmyndigheten til å gi tilgang til kommunikasjonsdata til retten. Dette må i seg selv oppfylle kravene i EMK. Når det gjelder de nærmere omstendighetene kan retten pålegge utlevering av trafikkdata for et bestemt tidsrom, og lokaliseringsdata innenfor et nærmere bestemt geografisk område. I tillegg sier loven at utlevering bare kan pålegges dersom det må antas at opplysningene vil være av vesentlig betydning for etterforskningen. Utover dette setter ikke loven begrensninger med hensyn til mengden av trafikkdata og lokaliseringsdata som kan utleveres. Den gir ingen kriterier for vurderingen av hva som er av vesentlig betydning for etterforskningen, og den gir ingen veiledning med hensyn til hvordan et utleveringspålegg skal avgrenses ut over at trafikkdata kan avgrenses i tid og lokasjonsdata geografisk. Det kunne for eksempel være relevant å avgrense til ulike kommunikasjonsmedier, til trafikk mellom geografiske lokasjoner etc. Dette innebærer at loven åpner for utlevering av store mengder av data som senere viser seg å være betydningsløse for den konkrete saken som foranlediget utleveringsbegjæringen. Hvorvidt, og på hvilken måte begjæringen og utleveringspålegget skal avgrenses er overlatt til rettens skjønn. Dette tilfredsstiller opplagt ikke kravene i EMK.

Tilgang til kommunikasjonsdata vil gi opplysninger om et stort antall personer og dermed berøre disses interesser. Dagens regler gir anvisning på at det skal oppnevnes en advokat som skal ivareta den mistenktes interesser, men det er ingen regler som sikrer at interessene til andre berørte blir representert når retten skal ta stilling til en utleveringsbegjæring. Det er derfor heller ingen ordning som gjør at det kan anvendes rettsmidler mot en utleveringsbeslutning på vegne av andre berørte. Betenkelighetene ved datalagring er ikke først og fremst knyttet til konsekvensene for dem som er mistenkt i en straffesak, men til konsekvensene for et stort antall mennesker hvis kommunikasjonsdata blir lagret og gjort tilgjengelig for politiet. At disse ikke har rettigheter under avgjørelsen av om data skal utleveres til politiet, er derfor en svakhet ved lovens ordning. Dette må endres om datalagring skal kunne være i samsvar med EMK.

Som nevnt ovenfor må loven også angi hvordan og ut fra hvilke kriterier privilegert informasjon skal skilles ut fra det som omfattes av utleveringspålegget. Heller ikke her tilfredsstiller loven EMK.

EMD krever ikke bare at skjønnet er begrenset og at beslutninger om utlevering er styrt av klare regler. I tillegg må det stilles et materielt krav som sikrer at de data som utleveres er relevante og ikke i sitt omfang går ut over de formål som har begrunnet lagringen. Dette går både på beslutningen om utlevering og på regler og kontrolltiltak som styrer politiets behandling av de utleverte dataene. I de foreslåtte tyske reglene er det for eksempel regler som forbyr bruken av opplysningene i andre saker enn den som har begrunnet utleveringen, med mindre det er tale om et forhold som i seg selv kunne ha begrunnet et krav om utlevering av data. Videre foreslås det at dataene skal slettes når de ikke lenger er nødvendige for etterforskning, avverging av fare eller rettslig overprøving. I tilfeller hvor dataene kan være relevante for rettslig overprøving av etterforskingsskritt eller straffesaksbehandling, skal de sperres slik at de ikke kan aksesseres ut fra andre formål.

I tillegg til de grunnleggende straffeprosessuelle reglene om bruken av opplysningene og tilintetgjøring av de som ikke trengs, kreves det etter EMDs praksis at det finnes prosedyrer for hvordan data som er innhentet blir undersøkt, brukt og oppbevart. Slike regler finnes hos oss i kommunikasjonsforskriften. Denne gir regler om hvordan begjæring skal fremsettes, hvem som kan forestå kommunikasjonskontroll, kontakten med tilbydere av kommunikasjonstjenester mv. Den bestemmer også at en etablert kommunikasjonskontroll skal stanses hvis vilkårene ikke lenger foreligger eller den ikke lenger anses hensiktsmessig, se § 5. Videre skal det føres en protokoll for hver kommunikasjonskontrollsak. Forskriften inneholder også regler om kontrollutvalget for kommunikasjonskontroll. Kapittel 3 gir regler om opplysning om kommunikasjonskontroll har vært foretatt. Underretning om foretatt kommunikasjonskontroll gis etter begjæring av kontrollutvalget.

Forskriften oppfyller etter vårt syn EMKs krav til klare og presise regler. Det kan som en svakhet innvendes at den ikke uttrykkelig omhandler de særlige utfordringene som behandling av data som er utlevert etter datalagring innebærer. Dessuten kan det være noen områder som kan kreve en særskilt regulering. For eksempel kan det være behov

for regler som balanserer hensynet til rettssikkerhet mot faren for misbruk når store mengder opplysninger som angår andre personer og forhold gjøres tilgjengelige for tiltalte og forsvarere fordi de har vært gjennomgått av politiet som ledd i forberedelsen av en straffesak.

Endelig kreves effektive virkemidler for å sikre at data som innhentes ikke blir misbrukt. Slike virkemidler må i første rekke bestå i en intern kontroll med politiets og påtalemyndighetens behandling og bruk av informasjon. En viss kontroll skjer i forbindelse med beslutningen om å tillate at politiet får tilgang til data. Det kan imidlertid også være behov for en mer løpende kontroll, og en etterfølgende kontroll etter at behandlingen er avsluttet. Etter de norske reglene skjer denne etterfølgende kontrollen gjennom kontrollutvalget opprettet i medhold av strprl. § 216 h. Dette utvalgets skal kontrollere at politiets bruk av kommunikasjonskontroll skjer innenfor rammen av lov og instrukser, at bruken av kommunikasjonskontroll begrenses mest mulig, og at kommunikasjonskontroll ikke skjer av hensyn til etterforskning i andre saker enn dem som er nevnt i straffeprosessloven § 216 a eller § 216 b, se kommunikasjonskontrollforskriften § 14. Utvalget skal herunder særlig ha for øye den enkeltes rettssikkerhet.

Etter vårt syn tilfredsstiller ordningen med kontrollutvalg for kommunikasjonskontroll de krav EMK setter til rettslige garantier og overprøvingsmekanismer. EMD har uttrykkelig tatt stilling til om et uavhengig utvalg kan erstatte domstolskontroll i slike tilfeller i *Klass and others v. Germany*. Her uttalte domstolen i avsnitt 56:

> *"The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.*
>
> *Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling."*

Ut fra dette mener vi at ordningen med kontrollutvalg i strprl. § 216 h og forskriften er tilfredsstillende etter EMK. Disse reglene må også gis anvendelse på data som er utlevert etter datalagring for at ordningen skal tilfredsstille EMK.

7.12 Oppsummering og konklusjoner

I mandatet for utredning ber Justis- og beredskapsdepartementet og Samferdselsdepartementet om å få utredet "hvilke konkrete tilpasninger i den norske lagringsloven med tilhørende forskrifter som eventuelt er nødvendig for at loven skal kunne settes i kraft uten at Norge krenker retten til personvern etter Grunnloven § 102 samt våre menneskerettslige forpliktelser slik disse må forstås i lys av EU-domstolens dom av 8. april 2014 om datalagringsdirektivet". EU-domstolen kom i sin dom til at datalagringsdirektivet er ugyldig og at EU-lovgiveren hadde overskredet de grenser som EUs charter setter for å beskytte personvernet.

En del av EU-domstolens argumenter mot at direktivet oppfylte unntaksvilkårene i charterets artikkel 7 gikk på manglende klarhet og presisjon. Gjennomgangen av EMDs utlegning av foreseeability-elementet i lovskravet i saker om kommunikasjonskontroll, viser etter vår oppfatning at samme type betraktninger kan ha betydning for vurderingen av om EMK artikkel 8 er oppfylt.

Vi har gjennomgått relevante bestemmelser i EMK og praksis fra EMD. Vi har også gjennomgått diverse nasjonale rettsavgjørelser og vurderinger av forholdet mellom datalagring og personvernet. EMD har ikke tatt stilling til den type kommunikasjonskontroll som datalagring innebærer, men det foreligger en rekke andre avgjørelser om kommunikasjonskontroll og andre etterforskningstiltak som kan gi veiledning for spørsmålet om forholdet mellom datalagring og personvernet slik det er nedfelt i EMK.

Den internasjonale juristkommisjonen ga i sin høringsuttalelse til DLD uttrykk for at EMDs avgjørelser "*viser at ikke-målrettet, tvangsmessig og generell masselagring av alminnelige borgeres personopplysninger, uavhengig av noen konkret etterforskning, vil ha store problemer med å passere EMDs normale krav til proporsjonalitet*".[59] Vi kan langt på vei slutte oss til denne vurderingen.

Det er etter vår oppfatning stor prinsipiell forskjell på regler som gir politiet og påtalemyndigheten tilgang til opplysninger som av andre grunner allerede finnes, og regler, som ut fra hensynet til oppklaring av *mulige* straffesaker, pålegger lagring av data som ellers ikke ville blitt lagret.

Når data lagres utelukkende ut fra formålet om å bekjempe og oppklare mulige straffbare handlinger dreier det seg i realiteten om en form for overvåkning. Selv om ikke innholdet i kommunikasjonen lagres, er det snakk om systematisk innsamling av opplysninger som er egnet til å kartlegge enkeltindividers kommunikasjon og bevegelser. Det er data som kan fortelle om private forbindelser, preferanser, vaner, sympatier, antipatier og en rekke andre forhold av strengt privat karakter. Dataene kan i tillegg gi informasjon om profesjonelle forbindelser, forretningsstrategier og andre tilsvarende forhold av faglig eller yrkesmessig karakter. Selv om slike forhold ikke kan defineres som en del av privatlivet i snever forstand, nyter de åpenbart vern etter EMK artikkel 8.

[59] Prop. 49 L (2010-2011) s. 17

I saker som gjelder individuell og strategisk overvåkning av løpende kommunikasjon har EMD fastslått at dette kan være akseptabelt om kravene i EMK artikkel 8 (2) er oppfylt. Man har ingen garanti for at EMD også i en sak om DLD-inspirert datalagring vil ta det utgangspunkt at slik innsamling i utgangspunktet er tillatelig så lenge lovgivningen er tilstrekkelig klar og tilgjengelig, skaper den nødvendige forutsigbarhet og ivaretar grunnleggende rettsikkerhetsgarantier*. Det kan etter vår oppfatning ikke utelukkes at de personvernmessige betenkelighetene ved overvåkningselementet er så fremtredende og tungtveiende at man simpelthen ikke kan anse det nødvendig i et demokratisk samfunn.* Uttalelser i EU-domstolens dom kan tolkes i samme retning, selv om det også er uttalelser i dommen som kan tolkes dit hen at datalagring under visse betingelser kan være i overensstemmelse med personvernet.

Hvis datalagring skal kunne være akseptabelt, vil det bare være under den forutsetningen at strenge rettslige krav er oppfylt med hensyn til (i) å ha hjemmel i lov, (ii) å ivareta nærmere angitte formål og (iii) å være nødvendig i et demokratisk samfunn. Vilkåret om at inngrepet må være i samsvar med loven inndeles av EMD i tre elementer. For det første må overvåkningen ha hjemmel i lov. For det andre må loven være "accessible", hvilket innebærer at loven må være offentlig tilgjengelig. For det tredje må loven gi borgerne mulighet til å forutse og forstå under hvilke omstendigheter overvåkning kan skje (kravet til "foreseeability"), det vil i korthet si at reglene som åpner for overvåkning må være tilstrekkelig klare og presist utformet. Det tredje vilkåret om at inngrepet må være nødvendig i et demokratisk samfunn byr på en konkret forholdsmessighetsvurdering av inngrepet og de formål det skal ivareta.

Departementet har lagt til grunn at datalagringsloven bygger på en grundig vurdering av kravet til forholdsmessighet, og at lovgiveren har en stor skjønnsmargin i vurderingen av om datalagring er nødvendig. Vi er ikke enige i dette. Etter vårt syn er ikke vurderingene i proposisjonen som ligger til grunn for den gjeldende loven særlig grundige. Vi tror heller ikke at EMD eller norske domstoler vil innrømme lovgiver nevneverdig skjønnsmargin på dette området.

Vi ser to grunnleggende innvendinger som må løses av lovgiveren for at datalagring skal kunne aksepteres etter EMK. Begge kan by på store utfordringer. For det første antar vi at domstolene vil stille strenge krav til dokumentasjonen av nødvendigheten av å lagre kommunikasjonsdata til etterforskningsøyemed eller for å avverge straffbare handlinger. I det materialet som er lagt frem hittil finnes ikke en slik dokumentasjon ut over generelle påstander og anekdoter. Dokumentasjonskraften svekkes av at myndighetene i forskjellige land gir uttrykk for sprikende vurderinger av nødvendigheten av datalagring. Med mindre myndighetene kan fremlegge bedre dokumentasjon for behovet, antar vi at det er stor sannsynlighet for at regler om datalagring vil bli underkjent.

For det andre vil generell lagring av kommunikasjonsdata også omfatte data som har beskyttelse mot å bli brukt som grunnlag for politiets arbeid, slik som personers kontakt med sjelesørgere og helsepersonell, pressens kilder og advokaters klientforhold. Slik informasjon kan ikke gjøres kjent for politi og påtalemyndighet uten å krenke personvernet, og etter omstendighetene også ytringsfriheten og retten til en rettferdig rettergang.

Det er store praktiske problemer forbundet med å foreta den nødvendige silingen før materialet utleveres. Man kunne selvsagt tenke seg en ordning hvor dette ble utført av tingretten. Men det vil ofte dreie seg om store mengder av data som må gjennomgås. Ofte vil det dessuten ikke være mulig ut fra de rene data å identifisere hva som dreier seg om kommunikasjonen til personer med særlig taushetsplikt uten å ha opplysning om hvem som er innehaver av bestemte telefonnumre og IP-adresser. Slike opplysninger fremkommer kanskje på et langt senere stadium under politiets analyse av materialet, men da er det jo alt utlevert og informasjonen kjent for politiet.

Problemene med i det hele tatt å skille ut privilegert informasjon fra det materialet som utleveres av de lagrede kommunikasjonsdata, er forhold som i seg selv trekker i retning av at datalagring ikke kan gjennomføres uten å komme i konflikt med EMK. Vi kan vanskelig se at en lagringsordning vil stå seg uten at man finner en løsning som kan sikre utskillelse av privilegert informasjon på en betryggende måte. Det å utforme en slik ordning krever en teknisk innsikt vi ikke har, og vi vil derfor ikke begi oss ut på å konstruere en slik ordning.

På bakgrunn av de særlige prinsipielle spørsmål som datalagring reiser sammenliknet med annen kommunikasjonskontroll, de særlige kravene til dokumentasjon av nødvendigheten av et slikt tiltak og behovet for å finne ordninger som på en betryggende måte kan skjerme privilegert informasjon, mener vi at det mest sannsynlige er at regler om datalagring ikke kan innføres uten å komme i konflikt med menneskerettighetene. I tillegg kommer det forhold at EMD så langt har ansett det nødvendig å begrense kontrolltiltak til (forholdsvis) klart definerte tilfeller av straffbare handlinger og klart definerte kategorier av personer. Også dette etterlater tvil om hvorvidt EMD i det hele tatt vil tillate at datalagring kan skje på nærmere bestemte vilkår. Det forutsetter i så fall at EMD forlater sin praksis for så vidt gjelder de to nevnte kriterier, og i stedet utvikler nye kriterier for datalagring.

Under forutsetning av at datalagring generelt sett lar seg forene med EMK, må loven likevel endres på en rekke punkter for å oppfylle kravene i EMK.

1) Lagringsloven bestemmer at informasjon skal kunne hentes til etterforskning eller avverging av straffbare handlinger med en minste strafferamme på henholdsvis fire år for trafikkdata og fem år for basestasjonssøk, samt for enkelte andre nærmere oppregnede straffbare handlinger med lavere strafferamme. Det er neppe tvil om at de særskilt oppregnede handlinger tilfredsstiller EMDs krav om foreseeability. Spørsmålet er imidlertid om spesifikasjon gjennom anvisning på en minste strafferamme skaper den nødvendige forutsigbarhet. Vi har ikke gjennomgått den norske straffeloven for å anslå hvor stor andel av straffebudene som har en strafferamme på minst fire år, men med mindre det er en vesentlig andel, burde den norske loven anses å skape den nødvendige forutsigbarhet. For å bedre muligheten for at en lagringslov skal overleve EMDs prøving, vil vi likevel anbefale at man presiserer de straffbare handlinger nærmere. Det bør gjøres en nærmere gjennomgang av for hvilke forbrytelser lagrede data skal kunne innhentes til etterforskning av, og de forbrytelsene bør listes opp spesifikt. En slik

gjennomgang er fordelaktig ikke bare av hensyn til forutsigbarhet, men også av hensyn til å dokumentere nødvendigheten av datalagring.

2) Muligheten for kontroll og effektiv rettsbeskyttelse er en sentral del av vurderingen av om et tiltak er "nødvendig i et demokratisk samfunn". Ut fra rettspraksis kan det oppstilles en rekke konkrete krav til muligheten for kontroll og effektiv rettsbeskyttelse. EMD har uttalt at det er i strid med grunnleggende rettssikkerhetskrav om en dommer eller et forvaltningsorgan kan avgjøre omfanget av en utlevering ut fra et fritt skjønn. Loven må således angi hvor omfattende et utleveringspålegg kan være og hvordan det skal avgrenses slik at borgerne er beskyttet mot vilkårlighet.

   Dagens lov legger beslutningsmyndigheten til å gi tilgang til kommunikasjonsdata til retten. Dette må i seg selv oppfylle kravene i EMK. Retten kan pålegge utlevering av trafikkdata for et bestemt tidsrom, og lokaliseringsdata innenfor et nærmere bestemt geografisk område. I tillegg sier loven at utlevering bare kan pålegges dersom det må antas at opplysningene vil være av vesentlig betydning for etterforskningen. Ut over dette setter ikke loven begrensninger med hensyn til mengden av trafikkdata og lokaliseringsdata som kan utleveres. Den gir ingen kriterier for vurderingen av hva som er av vesentlig betydning for etterforskningen, og den gir ingen veiledning om hvordan et utleveringspålegg skal avgrenses ut over at trafikkdata kan avgrenses i tid og lokasjonsdata geografisk. Det kunne for eksempel være relevant å avgrense til ulike kommunikasjonsmedier, til trafikk mellom geografiske lokasjoner og så videre. Dette innebærer at loven åpner for utlevering av store mengder av data som senere viser seg å være betydningsløse for den konkrete saken som foranlediget utleveringsbegjæringen. Hvorvidt og på hvilken måte begjæringen og utleveringspålegget skal avgrenses, er overlatt til rettens skjønn. Det tilfredsstiller ikke kravene i EMK.

3) Tilgang til kommunikasjonsdata vil gi opplysninger om et stort antall personer og dermed berøre disses interesser. Dagens regler gir anvisning på at det skal oppnevnes en advokat som skal vareta den mistenktes interesser, men det er ingen regler som sikrer at interessene til andre berørte blir representert når retten skal ta stilling til en utleveringsbegjæring. Det er derfor heller ingen ordning som gjør at det kan anvendes rettsmidler mot en utleveringsbeslutning på vegne av andre berørte. Betenkelighetene ved datalagring gjelder ikke først og fremst konsekvensene for dem som er mistenkt i en straffesak, men heller konsekvensene for et stort antall andre mennesker hvis kommunikasjonsdata blir lagret og gjort tilgjengelig for politiet. Disses interesser må beskyttes om datalagring skal kunne være i samsvar med EMK.

4) EMD krever ikke bare at skjønnet er begrenset og at beslutninger om utlevering er styrt av klare regler. I tillegg må det stilles et materielt krav som sikrer at de data som utleveres er relevante og ikke i sitt omfang går ut over de formål som har begrunnet lagringen. Dette går både på beslutningen om utlevering og på regler og kontrolltiltak som styrer politiets behandling av de utleverte dataene. I

strprl. § 216 i finnes regler om bruken av opplysninger til andre forhold enn det som begrunner utleveringen av dem. I tillegg er det regler om tilintetgjøring i strprl. § 216 g. Opplysningene skal snarest mulig tilintetgjøres i den utstrekning de er uten betydning for forebyggelsen eller etterforskningen av de straffbare forhold. Disse bestemmelsene er presise og klare og tilfredsstiller antakelig kravene etter EMK, og bør derfor også gjøres gjeldende for data som blir utlevert etter datalagring.

5) I tillegg til de grunnleggende straffeprosessuelle reglene om bruken av opplysningene og tilintetgjøring av de som ikke trengs, kreves etter EMDs praksis at det finnes prosedyrer for hvordan data som er innhentet blir undersøkt, brukt og oppbevart. Slike regler finnes hos oss i kommunikasjonsforskriften. Denne gir regler om hvordan begjæring skal fremsettes, hvem som kan forestå kommunikasjonskontroll, kontakten med tilbydere av kommunikasjonstjenester m.v. Den bestemmer også at en etablert kommunikasjonskontroll skal stanses hvis vilkårene ikke lenger foreligger eller den ikke lenger anses hensiktsmessig, se § 5. Videre skal det føres en protokoll for hver kommunikasjonskontrollsak. Forskriften inneholder også regler om kontrollutvalget for kommunikasjonskontroll. Kapittel 3 gir regler om opplysning om hvorvidt kommunikasjonskontroll har vært foretatt. Underretning om foretatt kommunikasjonskontroll skal etter begjæring gis av kontrollutvalget. Forskriften oppfyller etter vårt syn EMKs krav til klare og presise regler. For at en datalagringslov skal tilfredsstille EMKs krav, bør forskriften gjøres gjeldende også for data som utleveres etter denne loven.

6) Endelig kreves effektive virkemidler for å sikre at data som innhentes ikke blir misbrukt. Slike virkemidler må i første rekke bestå i en intern kontroll med politiets og påtalemyndighetens behandling og bruk av informasjon. En viss kontroll skjer i forbindelse med beslutningen om å tillate at politiet får tilgang til data. Det kan imidlertid også være behov for en mer løpende kontroll, og en etterfølgende kontroll etter at behandlingen er avsluttet. Etter de norske reglene skjer denne etterfølgende kontrollen gjennom kontrollutvalget opprettet i medhold av strprl. § 216 h. Dette utvalget skal kontrollere at politiets bruk av kommunikasjonskontroll skjer innenfor rammen av lover og instrukser, at bruken av kommunikasjonskontroll begrenses mest mulig, og at kommunikasjonskontroll ikke skjer av hensyn til etterforskning i andre saker enn dem som er nevnt i straffeprosessloven § 216a eller § 216b, se kommunikasjonskontrollforskriften § 14. Utvalget skal herunder særlig ha for øye den enkeltes rettssikkerhet. Etter vårt syn tilfredsstiller ordningen med kontrollutvalg for kommunikasjonskontroll de krav EMK setter til rettslige garantier og overprøvingsmekanismer.

Konklusjoner

Det kan etter vårt syn ikke utelukkes at de personvernmessige betenkelighetene ved datalagring er så fremtredende og tungtveiende at tiltaket ikke vil bli ansett nødvendig i et demokratisk samfunn uansett hvordan det begrunnes eller utformes. Dersom EMK ikke er til hinder for datalagring som sådan, er det grunn til å vente at nødvendigheten av et

slikt tiltak vil være strengt. Det er neppe oppfylt i de begrunnelser som hittil er gitt. I tillegg kommer at det er vanskelig å utvikle gode løsninger til beskyttelse av privilegert informasjon ved utlevering av data til politiet. Samlet sett gjør dette at vi mener at det er tvilsomt om regler om datalagring vil la seg forene med EMK.

Under forutsetning av at de grunnleggende innvendingene mot datalagring lar seg løse, er det uansett forhold som må endres i den nåværende lagringsloven for at den skal oppfylle kravene i EMK. De straffbare handlingene som kan begrunne utlevering av informasjon til politiet bør konkretiseres nærmere enn bare gjennom en henvisning til strafferammen. I tillegg bør det gis mer presise retningslinjer for den vurderingen som retten skal foreta når den tar stilling til en begjæring om utlevering. Det bør også være regler som sikrer at berørtes interesser er representert og ivaretatt under behandlingen.

8 VEDLEGG: OPPSUMMERING AV SÆRLIG RELEVANTE EMD-AVGJØRELSER

8.1 Klaas and others v. Germany (6. september 1978)

Bakgrunnen for klagen var at tysk lovgivning under visse omstendigheter tillot nasjonale myndigheter å åpne og undersøke post, samt å overvåke telefonsamtaler. Overvåkningen måtte være begrunnet i en overhengende fare mot nasjonal orden eller landets eksistens og sikkerhet. Overvåkning etter loven var for det første betinget av at det forelå faktiske indikasjoner på ovennevnte forhold. Vurderingen ble foretatt av høytstående offentlige representanter i samråd med nasjonal etterretning. Videre kunne overvåkningen ikke vare i lenger enn tre måneder uten at nytt samtykke ble gitt. For det tredje hadde subjektet utsatt for overvåkningen krav på å bli orientert om dette etter overvåkningens avslutning, dersom dette kunne gjøres uten å undergrave formålet med overvåkningen. Videre ble overvåkningen kontrollert av en jurist, og komiteer i nasjonalforsamlingen måtte holdes orientert om bruk av loven.

Klagerne anførte at lovgivningen var i strid med blant annet artikkel 8 fordi det ikke forelå tilfredsstillende mekanismer for å sikre at personer som ble utsatt for overvåkningen ble gjort kjent med dette etter at overvåkningen var avsluttet. Det ble særlig vist til at overvåkningen ikke var underlagt domstolskontroll.

Det avgjørende i saken var om lovgivningen oppfylte nødvendighetskravet. EMD uttalte at vilkårene for å tillate unntak etter artikkel 8 måtte tolkes strengt, og at "*powers of secret surveillance of citizens, characterising as they do the police State, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions*". EMD uttalte videre at domstolskontroll generelt er ønskelig for å ivareta borgernes rettssikkerhet. EMD konkluderte imidlertid med at fraværet av domstolskontroll i det konkrete tilfellet ikke medførte et brudd på artikkel 8, som følge av de øvrige tiltakene for å unngå misbruk.

8.2 Malone v. The United Kingdom (2. august 1984)

Klageren i denne saken mente seg urettmessig utsatt for hemmelig overvåkning i forbindelse med mistanke om heleri. Han anførte at slik overvåkning var i strid med artikkel 8. Det avgjørende spørsmålet var om overvåkningen oppfylte kravet til foreseeability.

EMD fant at den britiske lovgivingen ga politiet vide fullmakter til å foreta telefonavlytting og innhente informasjon om telefonisk kommunikasjon. Reglene for overvåkning var ikke tilstrekkelig klare og avgrensede, og den konkrete vurderingen av om vilkårene for overvåkning var oppfylt lå derfor i for stor grad i politiets hender. En side av dette var også at det etter engelsk rett ikke var ubetinget nødvendig med en rettsordre for å gjennomføre overvåkning. Borgerne hadde derfor ikke et tilstrekkelig vern mot misbruk. EMD konkluderte på bakgrunn av dette med at kravet til "foreseeability" ikke var møtt, og at det forelå et brudd på artikkel 8.

8.3 Rotaru v. Romania (4. mai 2000)

Spørsmålet i saken var om det medførte et brudd på klagerens privatliv at rumenske myndigheter nektet å slette arkiver og filer hvor det fremgikk at klageren hadde vært

medlem av en opposisjonell bevegelse. Klageren bestred opplysningene som fremgikk av arkivene.

EMD konkluderte med at det forelå et brudd på artikkel 8 som følge av at kravet til foreseeability ikke var oppfylt. Den rumenske lovgivningen fastslo at informasjon av betydning for landets sikkerhet kunne samles, registreres og arkiveres i hemmelige filer. Etter EMDs syn inneholdt lovgivningen ingen bestemmelser som fastsatte begrensninger for utøvelse av myndighet i den forbindelse. Som eksempler viste EMD til at loven manglet bestemmelser om hva slags informasjon som kunne lagres, hvem overvåkingstiltak kunne igangsettes mot, nærmere vilkår for overvåkingstiltak og rutiner for håndtering av innsamlet informasjon. Loven oppstilte blant annet ikke begrensninger med hensyn til lagringstid.

EMD minnet også om at hemmelig overvåkning kun er i tråd med artikkel 8 dersom det foreligger tilstrekkelige og effektive mekanismer for å forhindre misbruk. Under henvisning til *Klass and others v. Germany* viste EMD til at dette blant annet innebærer at krenkelser av borgernes rettigheter må være underlagt uavhengige organers kontroll, fortrinnsvis domstolene. Den rumenske lovgivningen hadde ingen mekanismer for å forhindre misbruk av informasjon.

Som følge av regelverkets manglende klarhet, presisjon og detaljgrad, samt adekvate garantier mot misbruk, konkluderte EMD med at myndighetenes omfattende diskresjon var uakseptabel, og at det forelå et brudd på artikkel 8.

8.4 Weber and Saravia v. Germany (29. juni 2006)

Spørsmålet i saken var om tysk lovgivning om hemmelig overvåkning av elektronisk kommunikasjon medførte et brudd på blant annet artikkel 8. Lovgivningen åpnet for såkalt "strategisk overvåkning". Formålet med slik overvåkning var å oppdage og avverge alvorlige trusler mot Tyskland, uten at det forelå en konkret mistanke om slike trusler. Overvåkningen omfattet trådløs telefonkommunikasjon, typisk mobiltelefoner. Overvåkningen var ikke rettet mot konkrete individer, men derimot mot internasjonale samtaler hvor konkrete, utvalgte ord ble benyttet for å fange opp samtalene.

Klagerne anførte at både avlyttingen, lagringen av informasjon, bruken av den, rutinene for sletting og hemmeligholdet overfor den avlyttede var i strid med deres grunnleggende rettigheter, derunder retten til privatliv. Både lovskravet og nødvendighetsvilkåret ble utfordret. EMD konkluderte med at den tyske lovgivningen på en klar og presis måte regulerte alle sidene av overvåkningen. Det forelå også adekvate mekanismer for å hindre misbruk. Lovskravet var derfor oppfylt.

I nødvendighetsvurderingen ble det vist til at EMD i tidligere saker har lagt til grunn at statene har en forholdsvis vid skjønnsmargin i spørsmål om hemmelig overvåkning for å opprettholde nasjonal sikkerhet. EMD fant at den tyske lovgivningen oppstilte strenge vilkår for å kunne gjennomføre den strategiske overvåkningen, og at det var en rekke sikkerhetstiltak mot misbruk tilknyttet ethvert ledd av overvåkningen. Det ble blant annet vist til at strategisk overvåkning krevde en begrunnet søknad fra lederen i den nasjonale etterretningstjenesten, at det krevde tillatelse fra en minister oppnevnt av

forbundskansleren, at overvåkningen var betinget av at andre midler ble ansett utjenlige, at overvåkningen var begrenset til tre måneder, og at det var strenge regler knyttet til lagring og sletting av informasjon. Under henvisning til statenes skjønnsmargin og de adekvate garantiene mot misbruk konkluderte EMD med at reglene om strategisk overvåkning var nødvendig i et demokratisk samfunn av hensyn til nasjonal sikkerhet og bekjempelsen mot alvorlig kriminalitet.

8.5 The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (28. juni 2007)

Klagen gjaldt bulgarsk lovgivning som regulerte muligheten for individuell overvåkning som ledd i bekjempelsen mot alvorlig kriminalitet. Klagerne anførte at lovgivningen ikke oppfylte lovskravet, fordi den manglet tilstrekkelig klare og presise bestemmelser, og fordi den ikke ga et adekvat vern mot misbruk.

EMD konkluderte med at den bulgarske lovgivningen oppfylte lovskravet hva gjaldt vilkårene for å igangsette overvåkning. Derimot fant retten at lovgivningen var mangelfull når det gjaldt de etterfølgende stadiene av overvåkningen. Det forelå ikke tilfredsstillende mekanismer for å sikre at gjennomføringen av overvåkningen faktisk skjedde i tråd med utstedte rettsordre, at innhentet informasjon ble filtrert og at innhentede data faktisk ble slettet. Domstolskontrollen på gjennomførings- og behandlingsstadiet var begrenset til at dommeren som godkjente overvåkningen ble informert om når overvåkningen var avsluttet. Det var heller ikke andre uavhengige organer som hadde noen form for kontroll med overvåkningen. Det ble også poengtert at lovgivningen ga innenriksministeren full kompetanse i spørsmålet om hva som skulle skje med overskuddsinformasjon, og at myndighetene ikke under noen omstendigheter eller på noe tidspunkt hadde plikt til å informere de som ble rammet av overvåkningen. Endelig viste retten til statistikk som tilsa at hemmelig overvåkning i Bulgaria var svært omfattende sammenliknet med antall straffesaker hvor informasjon innhentet gjennom overvåkning ble benyttet.

EMD konkluderte derfor med at den bulgarske lovgivningen ikke ga tilstrekkelige garantier mot misbruk, og at lovskravet ikke var oppfylt.

8.6 S. and Marper v. The United Kingdom (4. desember 2008)

Saken hadde sin bakgrunn i lovgivning i England, Wales og Nord-Irland som åpnet for at enhver som ble anholdt og mistenkt for straffbare handlinger, skulle avgi DNA-prøve og fingeravtrykk. Den innsamlede informasjonen ble lagret uavhengig av om den mistenkte ble siktet, og uavhengig av utfallet av en eventuell videre straffeforfølgning.

Klagerne anførte at det medførte et brudd på retten til privatliv at politiet nektet å destruere deres fingeravtrykk og DNA-prøver, etter at straffeforfølgningen mot dem ikke førte frem. Det omtvistede forhold var om reglene om lagring av nevnte informasjon oppfylte nødvendighetskravet. EMD fant at det var europeisk konsensus om at slik informasjon måtte destrueres der saker endte uten dom mot den mistenkte. Storbritannias skjønnsmargin var derfor snever, og krenkelsen etter artikkel 8 bestod ikke forholdsmessighetsvurderingen.

8.7 Liberty and others v. The United Kingdom (1. juli 2008)

I likhet med Weber and Saravia v. Germany gjaldt denne saken såkalt strategisk overvåkning. Storbritannia hadde på 1990-tallet opprettet et kommunikasjonsanlegg som kunne fange opp kommunikasjon fra 10 000 telefonlinjer samtidig. Informasjonen som ble fanget opp var både fra telefoner, e-post og fax, med det fellestrekk at enten avsenderen eller mottakeren befant seg utenfor Storbritannia. Enhver som var avsender eller mottaker av elektronisk kommunikasjon som gikk mellom Storbritannia og et annet land, risikerte å bli rammet av overvåkningen. Overvåkningen ble begrunnet i formål som nasjonal sikkerhet og forebyggelse og avdekking av grov kriminalitet.

Spørsmålet i saken var om den britiske lovgivningen oppfylte kravet til foreseeability.

I en generell uttalelse la EMD til grunn at prinsippene for vurdering av om kravet til foreseeability er møtt ikke er annerledes i spørsmål om strategisk overvåkning enn i spørsmål om individuell overvåkning (avsnitt 63).

Som ledd i den konkrete vurderingen sammenlignet EMD det britiske regelverket med det tyske som hadde vært vurdert i Weber and Saravia v. Germany. Sammenlikningen viste at den britiske lovgivningen på en rekke områder var mindre klar og presis, og at den ikke oppstilte like gode sikkerhetsmekanismer for å hindre misbruk. EMD viste til at overvåkningsfullmaktene kunne ha et svært bredt nedslagsområde, og at lovgivningen lot det i stor grad være opp til nasjonale myndigheters skjønn om overvåkning skulle tillates. I motsetning til den tyske lovgivningen oppstilte den britiske ikke klare regler om hvordan innhentet informasjon ble behandlet. Dette gjaldt både rutiner for filtrering, lagring, deling, bruk og sletting. EMD konkluderte på denne bakgrunn med at den britiske lovgivningen som tillot strategisk overvåkning medførte et brudd på retten til privatliv etter artikkel 8.

8.8 Iordachi and others v. Moldova (10. februar 2009)

Klagerne i denne saken var menneskerettighetsjurister som bistod borgere i Romania som mente seg utsatt for menneskerettighetsbrudd. Som følge av sin opposisjon mot den sittende regjeringen antok klagerne at de ble overvåket. Klagerne anførte at den nasjonale lovgivningen som åpnet for overvåkning ikke oppfylte kravet til "foreseeability" fordi den ikke var tilstrekkelig klar og presis, og fordi den ikke ga et adekvat vern mot misbruk. Konkret ble det blant annet vist til statistikk som underbygget at nærmest samtlige rettsanmodninger om å foreta overvåkning ble godkjent. Det ble også anført at lovgivningen ikke oppfylte nødvendighetskravet, ettersom overvåkning var tillatt i etterforskningen i en uforholdsmessig stor andel av straffesaker.

EMD konkluderte med at den rumenske lovgivningen på flere områder manglet klarhet, presisjon og et adekvat vern mot misbruk. Det ble særlig lagt vekt på at lovgivningen ikke i tilstrekkelig grad definerte hvem som kunne overvåkes i forbindelse med en etterforskning. Videre ble det lagt vekt på at domstolskontrollen var av nærmest formell karakter, og at lagring og sletting av innhentet informasjon ikke var underlagt klare rutiner. Kravet til foreseeability var derfor ikke oppfylt, og det forelå et brudd på artikkel 8.

8.9 Kennedy v. The United Kingdom (18. mai 2010)

Kennedy v. The United Kingdom (18. mai 2010) gjaldt spørsmålet om det forelå brudd på artikkel 8 som følge av hemmelig overvåkning. Klageren var en mann som var dømt for drap. Rettssaken mot ham var omdiskutert, og etter soning engasjerte han seg i kampen mot justismord. Han hevdet at britisk etterretning overvåket hans telekommunikasjon utelukkende for å undertrykke ham og for å ødelegge hans forretningsvirksomhet. Det var ikke bevist at han ble overvåket.

Klageren anførte både at (den eventuelle) overvåkningen av ham og selve lovgivningen som åpnet for slik overvåkning var i strid med artikkel 8. Den angrepne lovgivningen åpnet for overvåkning av konkrete personer eller lokaler når det var nødvendig av hensyn til nasjonal sikkerhet, for å avverge eller oppdage alvorlig kriminalitet, eller for å ivareta visse andre nasjonale hensyn. Bruddet på EMK artikkel 8 ble anført å bestå i at reglene ikke oppfylte kravet til foreseeability.

EMD fant ikke holdepunkter for at klageren hadde blitt overvåket, og vurderte derfor kun hans anførsel om at regelverket som åpnet for overvåkningen i seg selv var i strid med artikkel 8. EMD konkluderte med at det ikke forelå et brudd på artikkel 8, og viste særlig til at vilkårene for å foreta hemmelig overvåkning var klare og presise, at det var klare regler om sletting av innhentet materiale, samt at det var gode rutiner for å avverge misbruk av innhentet informasjon.