Datalagringsdirektivet og pressens kildevern:

- En oversikt

Universitetet i Oslo

Det juridiske fakultet

Kandidatnummer: 590

Leveringsfrist: 25. april

(* regelverk for masteroppgave på:
www.uio.no/studier/emner/jus/jus/JUR5030/reglement/vedlegg_emnebeskrivelse_masteroppgaver_JUR5030_5060.html)

Til sammen 17 988 ord

24.04.2012

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema og problemstillinger

Pressens kildevern er gitt en særstilling i norsk rett fordi det innebærer et unntak fra den alminnelige forklarings- og bevisplikten. Hensynet til kildevernet kan begrunnes både i grunnlovens § 100 og etter Den europeiske menneskerettighetskonvensjonen (heretter "EMK") artikkel 10 nr.1. Kildevernet er en integrert del av ytringsfriheten som igjen er en forutsetning for reell pressefrihet.[1]

Beskyttelsen av pressens kildevern er ikke absolutt, siden retten unntaksvis kan pålegge bevisplikt av hensyn til sakens opplysning o.l. Likevel er kravene så strenge, både etter norsk lov og EMK, at man kan spørre om det i viktige områder for informasjonsformidling nærmer seg et absolutt bevisfritak. I forhold til dette spørsmålet har jeg sett på praksis fra menneskerettsdomstolen [2](heretter "EMD").

Den rettslige problemstillingen jeg har tatt for meg, er hvorvidt implementeringen av datalagringsdirektivet vil påvirke pressens kildevern.

Spørsmål jeg har tatt opp er om implementeringen av datalagringsdirektivet vil kunne føre til brudd på menneskerettighetene med de kravene som stilles etter EMK artikkel 10. nr. 1. om ytringsfrihet.

Videre har jeg spurt om lagring av trafikkdata og lokalisasjonsdata kan tillates dersom lagringen truer de rettighetene som er gitt i norsk lovgivning, både gjennom Grunnloven, EMK og formell lov i forhold til kildevernet. Da har jeg spesielt lagt vekt på hvorvidt lagringen kan forsvares ved at den kommer innenfor unntaket i EMK artikkel 10 nr. 2.

Et like viktig spørsmål er hvorvidt man i lovgivningen kan sette vilkår for uthenting av opplysninger fra pressens medarbeidere på en slik måte at kildevernet beholder sin nåværende rettsposisjon. Kan man, med kontroll- og tilsynsordninger herunder også

[1] Jon Wessel Aas, 2010.
[2] Den europeiske menneskerettsdomstol. Den har kompetanse til å prøve individklager mot stater som har gjennomført menneskerettskonvensjonene se EMK artikkel 33.

domstolskontroll, beholde det vernet kildevernet gir etter EMD idag på en tilfredsstillende måte?

1.2 Bakgrunn og aktualitet

1.2.1 Datalagringsdirektivet

EU-direktiv 2006/24/EF,[3] populært kalt datalagringsdirektivet eller bare DLD, ble vedtatt av Stortinget 4.april 2011 etter mye diskusjon. Mange forskjellige aktører har hatt sterke meninger om direktivet, og det har kommet argumenter både for og imot. Datalagringsdirektivet har engasjert politikere, journalister og fagmiljøer innenfor blant annet jus og teknologi. Også den alminnelige borger har engasjert seg i forskjellige debattfora.

Datatilsynet, Forbrukerrådet, Advokatforeningen, og Den internasjonale juristkommisjonen, norsk avdeling, er bare noen av alle de som har uttalt seg mot direktivet. I tillegg, få dager før direktivet ble vedtatt, demonstrerte samtlige ungdomspartier mot direktivet foran Stortinget. Direktivet ble likevel vedtatt.

Argumentene for direktivet er at justismyndighetene får et bedre verktøy for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet. Sterke forkjempere for direktivet har blant annet vært Politiets Sikkerhetstjeneste (PST) og Kripos.

Noen av hovedargumentene mot direktivet er at det strider mot Grunnloven og Den europeiske menneskerettskonvensjonens (EMK)[4] beskyttelse av retten til fortrolig, privat kommunikasjon og retten til ytringsfrihet.

Jeg skal ikke vurdere alle sider ved implementeringen av datalagringsdirektivet i denne avhandlingen. I hovedsak skal jeg konsentrere meg om hvilken betydning direktivet vil ha for pressens kildevern, og også om lagringen kan forsvares med tanke på kildevernets styrke etter norsk rett og EMD. Videre vil det være av betydning hvordan politiet får tilgang til opplysningene, krav til lagring etc. og spesielt domstolskontrollen i forhold til uthenting av opplysninger.

---

[3] Europa-parlamentets og rådets direktiv 2006/24/EF

[4] Den europeiske menneskerettskonvensjon, Roma 1950. Inkorporert i Norge gjennom menneskerettsloven av 21. mai 1999.

1.2.2 Kildevernet, ytringsfrihet og demokrati

I utgangspunktet er det er to måter interessekonflikter kan oppstå uttrykk mellom kildevernet og hensynet til oppklaring av straffesaker på. Den første typen konflikt er fremprovosert bevisst fra det offentlige. Med andre ord situasjoner der domstoler og påtalemyndigheter bevisst ønsker å avsløre pressens anonyme kilder. Dette kan de oppnå ved bruk av vitneplikt, ved beslag av pressens materiell eller krav på utlevering av dette. Dette er dog ikke vanlig praksis.

Mer vanlig er det å snakke om problemstillinger som kan oppstå som en ubevisst konsekvens mellom de prinsippene kildevernet skal ivareta og de problemer som kan oppstå på grunn av nye etterforskningsmidler. Her menes telefonavlytting og ikke minst lagring av kommunikasjonsopplysninger som et resultat av datalagringsdirektivet.

Årsaken til pressens bekymringer i forhold til implementeringen av datalagringsdirektivet, er at de er redde for at ”den alminnelige borger” skal bli mer forsiktig med å komme til pressen med opplysninger og informasjon. Dette blir ofte kalt ”the chilling effect”. Pressens posisjon som ”samfunnets vaktbikkje” blir da svekket.

En trussel pressen ser ved implementeringen av datalagringsdirektivet er den myndighetspålagte lagringen av data. Denne kan føre til at politiet, påtalemyndigheten og noen utvalgte andre[5] senere kan få tilgang til disse dataene.[6] I tillegg ligger det en fare for lekkasje av opplysninger til andre parter.

At det finnes lagrede kommunikasjonsdata gir en mulighet for at disse opplysningene kan hentes ut ved ulovlige metoder. For eksempel ved hacking av system som oppbevarer slike opplysninger. Selv om man prøver å sikre slike opplysninger best mulig, så vil det alltid foreligge et usikkerhetsmoment som må tas med i forhold til ”the chilling effect”

Justis- og beredskapsdepartementet mener at implementeringen av direktivet i norsk rett kun vil gi en begrenset ”nedkjølende effekt”. De begrunner dette med at det allerede i lang tid har vært lagret slike data rutinemessig, og at dette så langt ikke har gitt inntrykk

[5] Se punkt 2.2.5.
[6] Prop. 49 L (2010–2011) Punkt 3.3.3.

av å ha noen betydning for den frie meningsytring. Samtidig vektlegger departementet at det nå kommer enda strengere regler til krav til lagring og tilgang på opplysninger, noe som delvis vil rette opp i situasjonen og i enkelte tilfeller også gjøre den bedre. Sist og ikke minst så anser departementet at en eventuell negativ effekt lagring av data vil måtte ha, vil være rettferdiggjort etter EMK artikkel 10 nr.2: Av hensyn til å bekjempe alvorlig kriminalitet, ivareta nasjonal sikkerhet og andres rettigheter.[7]

En direkte konsekvens av implementeringen av direktivet er at pressens rett til å forholde seg taus om en kildes identitet blir truet. Selv om pressens medarbeidere fortsatt har rett til å tie om hvor de har fått sine opplysninger, kan opplysningene likevel bli fanget opp og dermed bli krevd utlevert med hjemmel i en kjennelse i en rettssak. Denne muligheten finnes også i dag, men mulighetene for avsløring øker, når lagringen av data nå blir mer systematisk og langvarig [8]

Vurderingen av om et inngrep kan foretas må skje konkret, der inngrepets alvorlighet og styrke må måles opp mot vilkårene for inngrep i EMK artikkel 10 nr. 2. I forhold til om informasjon skal bli frigitt, må man vurdere den norske lovgivningen etter at datalagringsdirektivet har trådt i kraft i forhold til om det er nødvendig i et demokratisk samfunn for å bekjempe "legitime formål," som her i hovedsak vil være "alvorlig kriminalitet."

1.3 Avgrensninger og presisering

Selv om EMK artikkel 8 er svært aktuell når det gjelder brudd på menneskerettighetene i forhold til datalagringsdirektivet, blir det for omfattende å skrive om dette når temaet er pressens kildevern. Likevel vil jeg presisere at artikkel 8 og 10 tar utgangspunkt i de samme faktorene i unntaksbestemmelsene i sine respektive andre ledd. Dette medfører at inngrep i disse bestemmelsene ofte har gitt svært sammenfallende vurderinger hos EMD. Jeg kommer derfor til å ta med noen EMD-avgjørelser som omhandler artikkel 8 i min besvarelse, siden de har stor overføringsverdi i forhold til blant annet nødvendighetsvurderingen etter EMK artikkel 10 nr. 2.

[7] Prop 49. L (2010-2011) Punkt 3.3.3.
[8] Ibid.

Videre velger jeg å avgrense avhandlingen til ikke å omfatte de hensynene som taler mot uthenting av data gjennom implementeringen av datalagringsdirektivet når det gjelder lovbestemt taushetsplikt. Dette gjelder blant annet, advokater, leger, psykologer, prester og lignende.

1.4 Metode

I avhandlingen skal jeg forsøke å gi en deskriptiv oversikt over hvilke regler som implementeringen av datalagringsdirektivet gir. Deretter skal jeg se på rettsreglene rundt kildevernet, og dets beskyttelse både i grunnloven, formell lov og internasjonalt i menneskerettighetene. Etter mitt syn er det viktig å ha en god forståelse av hvordan disse regelsettene fungerer hver for seg, før man ser på samspillet mellom dem.

Jeg kommer ved hjelp av tradisjonell juridisk metode til å vurdere Grunnlovens og norsk lovs betydning i forhold til om lagringen av data etter implementeringen av datalagrinsdirektivet i seg selv er uholdbar i forhold til pressens kildevern. EMK kommer til å være svært sentral i denne vurderingen. EMK, er gjennomført ved inkorporasjon i norsk rett gjennom menneskerettsloven § 2.[9] Videre er bestemmelser etter konvensjonen gitt forrang dersom de er i strid med annen norsk lovgivning. I forhold til EMK vil jeg legge vekt på Wienkonvensjonens[10] tolkningsbestemmelser. EMDs rettspraksis har også stor betydning, blant annet som utvikler av konvensjonen. Høyesterett har også uttalt at norske domstoler skal benytte samme metode som EMD når det gjelder tolkning av EMK[11], noe som vil ha betydning for mine vurderinger i avhandlingen.

Videre vil jeg benytte den samme metoden når jeg forutsetter at lagringen er ”nødvendig i et demokratisk samfunn” og spør om den kan forsvares til også å dekke kildevernet så lenge det stilles strenge nok krav til rettssikkerhet og domstolskontroll.

[9] Lov om styrking av menneskerettighetenes stilling i norsk rett
[10] Vienna Convention on the Law of Treaties av 23. Mai 1969. (Norge er ikke part i konvensjonen, men er likevel forpliktet av den gjennom folkerettslig sedvanerett.)
[11] Rt 2002 s. 557

1.5 Begrepsavklaring.

I denne oppgaven er det mange begreper som ikke er like kjent for alle. Eller rett og slett trenger en bedre forklaring. Derfor vil jeg prøve å lage en oversikt for å gjøre lesningen av denne oppgaven noe lettere. Noen av definisjonene har jeg funnet i utkastet til datalagringsforskrift,[12]andre har jeg hentet fra andre kilder.

Basestasjonssøk: ”Uthenting av lagringspliktige data generert i landmobile offentlige elektroniske kommunikasjonsnett innenfor et angitt område i et bestemt tidsrom.”[13] (Denne typen søk regnes som svært inngripende søk, siden de gir adgang til data om kommunikasjon for et stort antall mennesker.)

Data: Data betegner ”enhver fysisk representasjon av opplysninger, viten, meninger etc. i motsetning til innholdet, som kalles informasjon.”[14]

Datalagring: Når man lagrer data for en viss tidsperiode, gjerne for ulike formål. F.eks. faktureringsformål, eller for å tilfredsstille krav om lagring etter datalagringsdirektivet.

E-post: Elektronisk meldingstjeneste som blir tilbudt av en lagringspliktig.

Den registrerte: Den opplysningene gjelder.

Fasttelefontjeneste: Utkastet til datalagringsforskrift definerer dette som ”…lagringspliktig telefontjeneste som starter eller ender i en terminal tilknyttet en fast geografisk adresse.”[15]

Innholdsdata: Opplysninger om innholdet av en kommunikasjon.

Internettaksess: Tilgang til Internett over kablet eller radiobasert tilkobling.

Internettelefontjeneste: Utkastet til datalagringsforskrift definerer dette som ”..lagringspliktig telefontjeneste som originerer eller terminerer ved bruk av IP-protokoll.” [16]

---

[12] Utkast til datalagringsforskift § 1-3
[13] Ibid.
[14] Store norske leksikons definisjon av data i IT-betydning.
[15] Utkast til datalagringsforskrift §1-3

Lagringspliktig telefontjeneste: Elektronisk kommunikasjonstjeneste som oppretter og mottar innenlandske eller innenlandske og internasjonale toveis taleforbindelser direkte eller indirekte ved hjelp av et eller flere numre i en nasjonal eller internasjonal telefonnummerplan, samt tilleggstjenester og eventuelle meldings- og multimedietjenester.

Lokalisasjonsdata: Data som viser hvor mobilt utstyr befant seg da en samtale ble koblet opp. [17] Dette er aktuelt ved bruk av mobiltelefon eller trådløs internettkobling. Med andre ord, så vil lokalisasjonsdata kunne gi informasjon om hvor en enkeltperson befant seg under en konkret samtale eller en trådløs oppkobling.

Massemedier: Jeg vil bruke dette uttrykket på lik linje med "pressen" og vil ikke differensiere mellom disse begrepene.

Mobiltelefontjeneste: Utkastet til datalagringsforskrift definerer dette som "…lagringspliktig telefontjeneste som originerer eller terminerer i terminal tilknyttet et landmobilt kommunikasjonsnett."

Pressen: Se massemedier

Trafikkdata: Data som er nødvendig for overføring av kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring. Jeg vil også bruke uttrykket trafikkdata som et samlebegrep på det meste av data som lagres ved implementeringen av datalagringsdirektivet, men jeg vil ikke omfatte lokalisasjonsdata i dette begrepet.

Med trafikkdata menes for eksempel data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjenester. Med behandling av trafikkdata menes enhver bruk av trafikkdata, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.[18]

---

[16] Ibid.
[17] NOU 2009: .
[18] Definisjon fra merknadene til Ot.prp. nr. 58 (2002-2003) om lov om elektronisk kommunikasjon.

”The chilling effect”: Et uttrykk som brukes for å beskrive den ”langsiktige effekten” man kan få ved å gjøre unntak fra kildevernet. Det man her er redd for er at en mer utstrakt vitnebruk vil føre til at viktige kilder blir borte.[19]

[19] Runesteinsaken premiss 62

2 DATALAGRINGSDIREKTIVET

2.1 Generelt om direktivet og dets bakgrunn

EUs datalagringsdirektiv[20] ble vedtatt 15. mars 2006 etter en lang politisk prosess. Terrorangrepene i USA 11. september 2011, Madrid 11. mars 2004 og London 7. juli 2005 var blant årsakene som gjorde at forslaget til slutt fikk gjennomslag, til tross for at det i årene før var stor motstand mot denne typen forslag på grunn av personvernhensyn. [21]

Formålet med datalagringsdirektivet er todelt. Det skal harmonisere forholdene for tele- og datakommunikasjonstilbydere, hvorav målet er å unngå at det blir forskjeller innad i medlemslandene i forhold til økonomiske ulemper knyttet til datalagring. Datalagringsdirektivet skal også sikre at medlemsstatene har de samme verktøyene for å kunne bekjempe "alvorlig kriminalitet".[22]

Frem til hendelsene i Madrid og London hadde prosessen med utforming av et datalagringsdirektiv gått langsomt. En viktig årsak var flere innvendinger på bakgrunn av personvernhensyn. Men siden terrorangrepene hadde ført til lokale datalagringsinitiativ, ble det ønskelig å få til et direktiv som harmoniserte denne praksisen.[23]

Siden Norge er part i EØS-avtalen, og direktivet har blitt vedtatt av EØS-komiteen, så er vi som nasjon også i utgangspunktet forpliktet til å implementere direktivet, forutsatt at vi ikke bruker vetoretten vår. Selv om muligheten for å nedlegge veto ble diskutert, førte ikke dette fram. Datalagringsdirektivet ble vedtatt av Stortinget 4.april 2011, og bestemmelsene som implementerer dette venter på å tre i kraft. Ikrafttredelsen ble utsatt fra 1. april til 1. juli 2012 på grunn av vanskelige arbeidsforhold etter terrorangrepet 22.

---

[20] EU-direktiv 2006/24/*EF*
[21] Se bl.a. Declaration on Combating Terrorism of 25 March 2004 som kom kort etter terrorangrepet i Madrid.
[22] Datalagringsdirektivet artikkel 1
[23] Teknologirådet Fra rådet til tinget nr. 26, april 2010. (Teknologirådet *er et uavhengig, rådgivende organ for teknologivurdering. Det ble opprettet ved kgl. res.30.april 1999 etter initiativ fra Stortinget.)*

juli 2011. [24] Ikrafttredelsen er etter dette igjen blitt utsatt, og man vet nå ikke når bestemmelsene trer i kraft i norsk rett.

2.2 Implementeringen i norsk rett

Gjennomføringen av direktivet har krevd endringer i flere norske lover. Blant annet i ekomloven, personopplysningsloven og straffeprosessloven, se lovvedtak 46 (2010–2011). Det har blant annet vært nødvendig å innføre en lagringsplikt i stedet for sletteplikt for data. Se ekomloven § 2-7 (2).[25] Videre har det også måtte innføres regler for tilgang til de data som skal lagres i henhold til datalagringsdirektivet. Regler for dette finnes i straffeprosessloven, politiloven, tvisteloven og verdipapirhandelloven.

Alle reglene direktivet fører med seg er ikke lovregulert, og det er heller ikke planer om dette. I stedet er det lagt opp til i lovvedtaket at ytterligere regler kan bli gitt i forskrift.[26] Post og teletilsynet ble gitt i oppdrag av Samferdselsdepartementet å utarbeide og sende på høring: "utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (utkast til datalagringsforskrift)." Denne er nå kommet og høringsfristen er satt til 10. april.

Andre forskrifter som er av betydning for datalagringsdirektivet, er blant annet politiregisterforskriften. Den er hjemlet i politiregisterloven[27], og det er planlagt at den skal tre i kraft samtidig med endringene knyttet til gjennomføringen av datalagringsdirektivet i norsk rett. [28] Politiregisterlovens formål er å styrke personvernet, samtidig som den skal bidra til å hjelpe politiet og påtalemyndigheten å løse sine oppgaver på en effektiv måte. Regler som er av betydning i forhold til datalagringsdirektivet er blant annet deling av opplysninger med andre medlemsland i EØS. Et av grunnhensynene bak datalagringsdirektivet er nettopp å sikre at visse opplysninger "er tilgjengelige med sikte på etterforskning, avsløring og rettslig forfølging av alvorlige forbrytelser." [29]

---

[24] http://www.regjeringen.no/nb/dep/sd/tema/telekommunikasjon/datalagringsdirektivet.html?id=666723
[25] Lovvedtak 46 (2010–2011)
[26] Se også Prop. 49 L (2010-2011) og Innst. 275 L (2010-2011)
[27] Politiregisterloven
[28] Revisjon av datalagringsdirektivet: http://www.regjeringen.no/nb/sub/europaportalen/eos-notatbasen/notatene/2011/okt/datalagring---revisjon.html?id=661439
[29] Jf Datalagringsdirektivet artikkel 1

Datatilsynet vil også bli styrket, slik at de kan ivareta det kontrollansvaret de vil få som følge av bl.a. politiregisterloven.*" [30]*

2.2.1 Hvordan er dagens regelverk?

Også i dag lagres mange av de samme dataene som implementeringen av datalagringsdirektivet nå gir hjemmel for. Den prinsipielle forskjellen reglene som implementerer direktivet utgjør er likevel stor. I dag lagres trafikkdata, lokaliseringsdata og abonnementsdata utelukkende på grunn av kundeadministrasjon, opplysningstjenester, og faktureringshensyn hos tilbyderne. Reglene er slik at det foreligger en slette- og anonymiseringsplikt for tilbyderne så snart disse formålene er uttømt.[31] Etter dagens regelverk er maksimal lagringstid for disse loggene fastsatt til fem måneder dersom faktureringen skjer kvartalsvis, og tre måneder dersom faktureringen skjer månedlig. Når det gjelder informasjon om hvilke IP-adresser som tilhører hvilke kunder, så kan de etter dagens regelverk bare lagres i 3 uker, i motsetning til de 6 månedene som vi vil kreve etter implementeringen av direktivet.

Den store prinsipielle forskjellen implementeringen av datalagringsdirektivet vil utgjøre er altså at vi går fra en sletteplikt til en lagringsplikt med tilhørende sletteplikt. I tillegg vil lagringstiden bli lengre og flere data enn i dag vil bli lagret. Bakgrunnen for lagringen vil også bli en annen siden formålet nå ikke lenger bare vil gjelde tilbyder selv men også kriminalitetsbekjempelse.[32]

Selv om begrunnelsen for lagringen av data i dag ligger i faktureringshensyn, vil den likevel ofte inneholde trafikk- og lokaliseringsdata. Denne typen logger kan politiet også i dag få utlevert og benyttet som bevis i straffesaker eller som hjelpemidler under etterforskningen. Politiet har også muligheten til å "fryse" disse loggene, slik at de ikke blir slettet når fristen løper ut. Se straffeprosessloven § 215a i kapittel 16 om Beslag og utleveringspålegg. Jf. § 222d om bruk av tvangsmidler. (Mer om dette i punkt 2.2.6.2.) Denne muligheten blir videreført med implementeringen av datalagringsdirektivet.

---

[30] http://www.regjeringen.no/mobil/nb/dep/jd/dok/regpubl/prop/2011-2012/prop-1-s-20112012/6.html?id=657484

[31] Ekomloven § 2-7 (2). Denne loven ble endret ved lov 15. april 2011 nr. 11 med implementeringen av datalagringsdirektivet.

[32] Innst. 275 L (2010-2011)

Andre som også har hjemmel til å få tilgang til data i dag er Finanstilsynet. De har hjemmel for tilgang til data som er nødvendig for at de skal kunne utføre sine oppgaver.[33] Denne tilgangen vil bli videreført av hensyn til internasjonale forpliktelser. (Se mer om dette i punkt 2.2.6.3)

2.2.2 Hva skal lagres?

Direktivets artikkel 5 inneholder en oversikt over hvilke kategorier av opplysninger som Norge har plikt til å lagre. Denne oversikten er omfattende, og den er også noe uklar i forhold til nøyaktig hvilken betydning hvert enkelt punkt har. Helt overordnet så skal det være lagringsplikt for trafikkdata, lokaliseringsdata og abonnements/brukerdata som fremkommer ved bruk av elektroniske kommunikasjon som: fasttelefoni, mobiltelefoni, internettaksess, epost og bredbåndstelefoni.[34] (Se kapittel 1.1.2 for definisjoner.)

Plikten til å lagre data er nå tatt inn i ekomloven § 2-7a. Det som skal lagres er ifølge bestemmelsen: ”trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren” [35] Videre er det i § 2-7a, annet ledd lagt opp til at myndighetene ved forskrift kan utdype disse punktene. Dette følger opp forarbeidenes anbefaling om samarbeid mellom politimyndigheter, representanter fra tilbydere av ekomnett og tjenester samt fra Post- og teletilsynet. På denne måten vil uklarhetene i direktivet på sikt kunne avklares i forskriften. Nøyaktig hvordan dette skal foregå er fremdeles ikke endelig avgjort på det tidspunkt denne oppgaven skrives, men utkast til forskrift[36] kom i februar 2012, og skal på høring i april. Høringsfristen er satt til 10.april.2012. Jeg kommer til å bruke utkastet til forskrift som utgangspunkt for min oversikt over hva som kreves lagret.

Etter utkastet til forskrift er lagringen av data inndelt etter type tjeneste: Fasttelefontjeneste, mobiltelefontjeneste, internettelefontjeneste, internettaksess og epost.

---

[33] Innst 275 L (2010-2011)
[34] Ibid.
[35] Ekomloven § 2-7a, 1.punktum. Loven er foreløpig ikke trådt i kraft. Planlagt ikraftsetting 1.juli 2012.
[36] Utkast datalagringsforskrift

Fasttelefontjeneste:[37]

Det som kreves lagret er:

- Anroperens telefonnummer (A-nummer)
- Telefonnummer til den som blir anropt (B-nummer)
- Telefonnummeret som anropet viderekobles til (C-nummer)
- Abonnentens og den registrerte brukerens navn og adresse for A-, B- og C-nummer på tidspunktet for den aktuelle kommunikasjonen
- Dato og tidspunkt for start og avslutning av kommunikasjonen, og
- Den telefontjeneste som benyttes
- I tillegg skal mislykkede anrop og tapte anrop lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop

Mobiltelefontjeneste[38]

Det som kreves lagret er:

- A-, B- og C-nummer
- Abonnentens og den registrerte brukerens navn og adresse, for A-, B- og C-nummer på tidspunktet for den aktuelle kommunikasjonen
- Dato og tidspunkt for start og avslutning av kommunikasjonen
- Den telefontjeneste som benyttes
- Anroperens og den anroptes internasjonale kjennetegn for mobilabonnenter (IMSI)
- Anroperens og den anroptes internasjonale kjennetegn for mobiltelefoniutstyr (IMEI)
- Ved forhåndsbetalte anonyme tjenester: dato og klokkeslett for første aktivering av tjenesten samt den lokaliseringskoden (celleidentiteten) som tjenesten ble aktivert fra
- Lokaliseringskoden (celleidentiteten) ved kommunikasjonens begynnelse og slutt og opplysninger som identifiserer cellens geografiske lokalisering på de tidspunkt dataene blir lagret
- Som for fasttelefontjenester, skal også mislykkede anrop og tapte anrop lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop

Internettelefontjeneste[39]

Det som kreves lagret er:

- Anroperens telefonnummer (A-nummer) eller tildelt brukeridentitet
- Telefonnummer til den som blir anropt (B-nummer) eller tildelt brukeridentitet til den som blir anropt

[37] Utkast til forskrift om datalagring § 2-2
[38] Ibid.
[39] Utkast til forskrift om datalagring § 2-4

- Abonnentens eller den registrerte brukerens navn og adresse for A- og B-nummer eller tilsvarende ved tildeling av brukeridentitet på tidspunktet for den aktuelle kommunikasjonen
- Dato og tidspunkt for start og avslutning av kommunikasjonen, og
- Den tjeneste som benyttes
- Også her skal mislykkede og tapte anrop lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop

Internettaksess[40]

Lagringspliktige data for internettaksess er:

- Abonnentens og den registrerte brukerens bruker-ID eller tilsvarende identifikasjon,
- Tildelt IP-adresse for kommunikasjonen
- Abonnenten eller den registrerte brukerens navn og adresse på tidspunktet for den aktuelle kommunikasjonen
- Dato og klokkeslett for på- og avlogging hos Internett-tjenesten, basert på en bestemt tidssone, sammen med den IP-adressen som tilbyderen av Internett-tilgangstjenesten har tildelt kommunikasjonen, og abonnentens eller den registrerte brukerens brukeridentifikasjon
- Telefonnummer ved oppringt tilgang, og
- Den digitale abonnentlinjen (DSL) eller et annet sluttpunkt for kommunikasjonens avsender
- I tillegg skal lokaliseringskoden (celleidentiteten) ved kommunikasjonens begynnelse og opplysninger som identifiserer cellens geografiske lokalisering på det tidspunkt dataene blir lagret, også lages dersom mobilt kommunikasjonsutstyr benyttes for internettaksess

E-post[41]

Det som kreves lagret er:

- Avsender og mottakers e-postadresse samt bruker ID eller annen tilsvarende identifikasjon dersom dette er noe annet enn e-postadressen
- Abonnenten eller den registrerte brukerens navn og adresse på tidspunktet for den aktuelle kommunikasjonen. Slik informasjon skal lagres for både avsender og mottaker
- Dato og klokkeslett for på- og avlogging av e-posttjenesten

For alle tjenestene så er det også et krav at det skal angis hvilken tidssone de lagrede klokkeslett er angitt i.

Etter min oppfatning er fortsatt flere av disse punktene uklart definert i forskriften.

[40] Ibid. § 2-5
[41] Ibid. § 2-6

For eksempel er "epost" definert som en ”elektronisk meldingstjeneste som blir tilbudt av en lagringspliktig.” Om en ”elektronisk meldingstjeneste” kun er ment å gjelde tradisjonell epostkommunikasjon eller også andre meldingstjenester som for eksempel chatte-tjenester er ikke tydelig. Jeg kommer ikke til å gå nærmere inn på uklarhetene i forskriften, unntatt der jeg har ansett det relevant for problemstillingen.

2.2.3 Hvor lenge skal trafikkdataene lagres?

I Norge har man satt lagringstiden til 6 måneder,[42] som er den korteste lagringstiden direktivet tillater. Direktivet har overlatt til statene selv å velge lagringslengde, så lenge lagringstiden er innenfor et spenn fra 6 til 24 måneder[43].

Når lovens krav til lagring er gått ut, skal disse dataene slettes.[44] Dette gjelder selv om tjenesteleverandør eventuelt skulle ønske å lagre dem lenger. Påtalemyndigheten derimot kan ”som ledd i etterforskning” gi pålegg om ”sikring av elektronisk lagrede data som antas å ha ”betydning som bevis.” [45] Med sikring menes ”ethvert tiltak som ivaretar de aktuelle dataenes integritet, tilgjengelighet og autentisitet. Sikring kan skje ved at det tas kopi av dataene som saken gjelder, eller ved at disse gjøres utilgjengelige for andre enn den pålegget retter seg mot.”[46]

2.2.4 Lagringssted og informasjonssikkerhet.

Etter personopplysningslovens § 2 nr. 4, er hver enkelt tilbyder behandlingsansvarlig for data som er lagret for fakturerings- og administrasjonsformål. Dette kan skje enten hos tilbyderen selv, eller det kan benyttes en databehandler for ekstern lagring.

Justis- og politidepartementet har foreslått for Stortinget, og fått godkjent, at det skal være opp til den enkelte tilbyder å velge lagringsløsning. Man har foretrukket å ikke velge en sentralisert lagringsløsning, siden dette vil kunne bli svært kostbart og informasjonssikkerheten ved lokal lagring også vil kunne skje på en tilfredsstillende

[42] Jf Ekomloven § 2-7a
[43] Datalagringsdirektivet artikkel 6
[44] Jf Ekomloven § 2-7(2) se også definisjonen av data i punkt 1.5
[45] Straffeprosessloven § 215a
[46] Norsk lovkommentar: Note om sikring: av Geir Sunde Haugland jfr straffeprosessloven § 215a.. (Noten er sist hovedrevidert 23.02.2012)

måte.[47] Det vil likevel kunne være mulig for små tilbydere å gå sammen om en felles løsning for lagring. Lagrede data skal sikres i henhold til personopplysningslovens § 13 og den tilhørende forskriften kapittel 2.

Etter datalagringsdirektivets artikkel 1 er det tilbyder av en offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett som skal lagre opplysningene. I norsk rett utdypes dette i ekomlovens definisjon av tilbyder. Med andre ord ”enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste”.[48]

I utkastet til datalagringsforskrift er det også presisert at det er tilbyder som er lagringspliktig. Samtidig er det lagt opp til at myndighetene i særlige tilfeller kan gjøre unntak fra dette ved enkeltvedtak, enten ved å unnta tilbyder helt eller delvis fra lagringsplikt eller ved å pålegge lagringsplikt for annen virksomhet.[49]

Dette vil altså si at alle teleselskapene må ha en egen database for denne typen informasjon i tillegg til den databasen de allerede har for faktureringshensyn. Basene må skilles av rettssikkerhetshensyn for å kunne begrense tilgangen til informasjonen. Dagens standard til sikkerhet for disse dataene holder ikke mål. Et godt eksempel på dette er det som skjedde i 2007 da over 100 000 fødselsnummer, navn, adresser og kredittopplysninger fra Talkmores databaser kom på avveie.[50] Eller senest i mars 2012 da Altinn som man burde kunne stole på er et nettsted som er svært sikkert, viste seg å ha feil, noe som førte til at personlig informasjon om ”Kenneth” lå ute i flere timer.[51]

2.2.5 Hvem skal ha tilgang til trafikkdata? [52]

Etter datalagringsdirektivet artikkel 4 i er det opp til medlemsstatene selv i nasjonal lovgiving å sette vilkår for hvem som skal kunne få tilgang til de lagrede dataene.[53]

---

[47] Innst 275 L
[48] Ekomloven § 1-5 nr.10.
[49] Utkast datalagringsforskriften § 1-2.
[50] Datatilsynets årsmelding fra 2007, og Lillesund, 2007
[51] Sunnanå, 2012

[52] Utkast til datalagringsforskriften § 4-1
[53] Direktiv 2006/24/EF

For det første så må de personene som har ”tjenestelig behov for tilgang til lagringspliktige data” [54] ha mulighet til å aksessere dataene. For at man skal kunne få autorisasjon til å få slik tilgang til data, så er det satt krav om at disse personene må være vurdert som ”skikket” av den lagringspliktige virksomheten. I tillegg må vedkommende for å få slik autorisasjon fremvise politiattest og undertegne en erklæring om taushetsplikt.[55]

Det faller seg også naturlig at en person skal ha muligheten til å få innsyn i hvilken informasjon som er lagret om seg selv. Hjemmel for dette finner vi i personopplysningsloven § 18 (2), som gir innsyn for ”den opplysningene gjelder”.

Videre så er det også naturlig at politi og påtalemyndighet, samt Finanstilsynet kan få tilgang så lenge man har *samtykke* fra den registrerte. Jf. utkast til datalagringsforskrift § 4-1b og personopplysningsloven § 18 (2).

Det er også hjemmel for at ”andre myndigheter” kan få tilgang *abonnements- og brukerdata*, dersom noen vilkår er oppfylt. Merk at dette ikke gjelder alle typer data. (Se punkt. 2.2.6)

Politi og påtalemyndigheten kan også få tilgang til gitte data etter kjennelse eller hastekompetanse dersom vilkårene for dette er oppfylt. Dette gjelder da uthenting av data i etterforsknings- og forebyggende øyemed. (Vilkårene for dette vil jeg presentere i punkt 2.2.6)

2.2.6 Uthenting av data

Implementeringene av datalagringsdirektivet har gitt nye hjemmelsgrunnlag for uthenting av data. Her vil jeg redegjøre for både disse og de som allerede var en del av norsk rett.

[54] Utkast til datalagringsforskrift § 3-4
[55] Ibid. § 3-4 annet og tredje ledd.

2.2.6.1 Uthenting av data i etterforskingsøyemed

Ekomlovens § 2-9

Etter gjeldende rett er trafikkdata og lokaliseringsdata i utgangspunktet taushetsbelagte.[56] Derfor trenger man særskilt hjemmel i lov for å kunne utlevere slike.

Ekomlovens § 2-9 tredje ledd gir hjemmel for unntak fra taushetsplikten når det gjelder *abonnements- og brukerdata*. Dette vil si, etter § 2-9 tredje ledd:

> "avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse."

Disse opplysningene krever ikke kjennelse fra retten, og de regnes som mindre beskyttelsesverdige[57]. En naturlig årsak til dette er at disse opplysningene er mindre inngripende i forhold til personvernet. Det ble også uttalt av Høyesterett i Rt. 2010 s.774, at opplysninger etter ekomloven § 2-9 første ledd, første punktum har et svakere vern enn for eksempel trafikkdata.[58] Unntakene her gjelder etter tredje ledd påtalemyndigheten, politiet og i tillegg "annen myndighet i medhold av lov" etter tredje ledd, annet punktum.

Eksempler på hjemler for "annen myndighet" finnes blant annet i tolloven, ligningsloven, folketrygdloven og merverdiavgiftsloven.[59]

Straffeprosessloven § 210 b[60]

Her er utgangspunktet at utlevering til politiet bare kan skje etter kjennelse fra retten. Utleveringen vil gjelde trafikkdata og lokaliseringsdata som ikke omfattes av straffeprosessloven § 210 c. For at utlevering kan foregå må en del uttømmende vilkår være oppfylt:

For det første så må utleveringen være av "vesentlig betydning for etterforskningen".[61] For det andre så må det foreligge skjellig grunn til mistanke om en straffbar handling

[56] Ekomloven § 2-9(1)
[57] Innst 275. L s. 5.
[58] Rt 2010 s 774 avsnitt 41.
[59] Rønnevig 2011
[60] Ny strpl §§ 210 b og c. som ble vedtatt ved lovvedtak 46. Den 4. april.2011. (Fortsatt ikke trådt i kraft)
[61] Strpl § 210 b tredje ledd

som kan medføre fengsel i fire år eller mer. Utlevering av data kan også skje dersom handlingen er utøvet som ledd i organisert kriminalitet og kan straffes med fengsel i tre år eller mer[62].

Videre så er det mulig å utlevere opplysninger i enkelte andre saker som det ellers ville vært svært vanskelig å etterforske uten tilgang til data. Dette gjelder brudd på en rekke uttømmende straffebud i straffeloven og en bestemmelse i utlendingsloven jf. straffeprosessloven § 210(c). Dette er bestemmelser som omhandler rikets sikkerhet og statsforfatning, høyforræderi, informasjonstyveri, narkotikaforbrytelser, identitetstyveri, barnepornografi, bedrageri, heleri/hvitvasking og sjikane[63]

Straffeprosessloven § 210 c

Denne bestemmelsen er svært lik, men noe strengere enn § 210 b. Dette er fordi denne paragrafen også omfatter hjemmel for utlevering av data fra basestasjonssøk. Justis- og beredskapsdepartementet har vurdert at data fra basestasjonssøk bør reserveres for de alvorligste sakene siden de kan gi adgang til informasjon om kommunikasjon fra et stort antall mennesker.[64] Dette er et større inngrep i personvernet enn om det ble uthentet data fra bestemte brukere, IP-adresser, og lignende.

Her vil man altså, dersom man får kjennelse fra retten, kunne pålegge utlevering 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. Tilleggskravet som skiller denne bestemmelsen fra § 210 b er at dette gjelder for handlinger som kan medføre straff av fengsel i fem år eller mer, i motsetning til fire. Altså krever § 210 c. en høyere strafferamme for utlevering. Unntak fra dette er dersom det foreligger mistanke om at handlingen er utøvd som ledd i virksomheten til en organisert kriminell gruppe. I så fall gjelder det her som i § 210 b et krav på en strafferamme på 3 år. [65] Ellers kan basestasjonssøk bare skje dersom bestemte straffebud er brutt. Dette gjelder rikets sikkerhet, terrorisme, forræderi,

[62] Strpl § 210 b første led, bokstav a,b
[63] 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
[64] Prop. 49. L (2010-2011)
[65] Straffeprosessloven § 210 c. og Prop 49 L

narkotikaforbrytelse, heleri/hvitvasking og ulovlig innvandring. [66] Her har § 210 c et snevrere utvalg av bestemmelsene i § 210 b, noe som bekrefter at dette er en bestemmelse som krever mer alvorlige forhold enn § 210 b.[67]

Argumentet for at man vil tillate basestasjonssøk, på tross av at slike kan medføre alvorlige inngrep i personvernet, ligger i at politiet må få tilgang til slike data når det gjelder svært alvorlig kriminalitet med ukjent gjerningsperson eller ved terrorhandlinger. [68] Men dette kan ikke skje uten videre, derfor de strengere kravene for å tillate utlevering.

2.2.6.2 Uthenting av data i avvergende og forebyggende øyemed

Avvergende øyemed.

Et annet formål ved å hente ut informasjon fra tilbyderne gjelder politi og påtalemyndighetens bruk av "tvangsmidler" for å innhente informasjon for å prøve å *avverge* at bestemte former for organisert og annen alvorlig kriminalitet.[69] Dette er allerede hjemlet i straffeprosesslovens kapittel 17 b i dag, og det er ikke foreslått noen endringer i disse bestemmelsene i loven fra departementet sin side.[70] Grunnen til dette er at den viser tilbake på straffeprosesslovens kapittel 16 som nå har blitt endret. Straffeprosesslovens kapittel 16 inneholder blant annet §§ 210 b og c. fra foregående punkt, og § 215a fra punkt 2.2.1.

I § 222 d er det bestemt at retten ved kjennelse kan gi politiet tillatelse til å nytte slike tvangsmidler som ledd i etterforskning når det er "rimelig grunn til å tro at noen kommer til å begå en handling som rammes av" en rekke opplistede straffebud.[71]. Den samme tillatelsen kan også bli gitt til politiets sikkerhetstjeneste, men dette gjelder da flere straffebud.[72] Et tilleggsvilkår er også at det må antas at "inngrepet vil gi

---

[66] 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
[67] Disse bestemmelsene er utelatt fra § 210 c: 145 annet ledd, 145 a, 145 b, 190 a, 201 a, 203, 204 a, 270 første ledd nr. 2, og § 390 a
[68] Prop. 49 L
[69] Ibid. kapittel 13.
[70] Ibid. Kapittel 13.3.
[71] Straffeprosessloven § 222 d (1) a-c
[72] Straffeprosessloven § 222 d (2) a-d

opplysninger av vesentlig betydning" for å kunne avverge handlingen saken gjelder og at slik avverging ellers "i vesentlig grad vil bli vanskeliggjort".

I bestemmelsens fjerde ledd er det gitt unntak fra at tillatelsen må gis fra retten. Dersom behovet for avvergelse ikke kan vente, så kan ordre fra påtalemyndigheten tre i stedet for kjennelse. Dersom dette skjer, så skal denne beslutningen snarest mulig og senest innen 24 timer etter at tvangsmiddelet ble tatt i bruk legges frem for retten for godkjennelse.

Forebyggende øyemed

Politiets sikkerhetstjeneste (PST) kan også få kjennelse fra retten om å få bruke tvangsmidler i "forebyggende øyemed" [73], altså utenfor etterforskning når det er grunn til å undersøke om noen forbereder en handling som rammes av straffebud som er listet opp i politilovens § 17d første ledd. Etter bestemmelsens tredje ledd kan sjef eller assisterende sjef i PST gi hastekompetanse som trer inn i stedet for kjennelse fra retten. (Unntak fra denne er romavlytting.[74] Denne vil bli underlagt etterfølgende domstolskontroll.)

Straffeprosessloven § 170 a

Denne bestemmelsen gir vilkår for bruk av tvangsmidler. Det gjelder her en nødvendighets og forholdsmessighetsvurdering. Etter bestemmelsen så kan bare et tvangsmiddel brukes når det er "tilstrekkelig grunn til det." Videre i bestemmelsen presiseres det at inngrepet må være forholdsmessig i forhold til sakens art og forholdene ellers. Jeg vil diskutere denne paragrafen nærmere under punkt 4.2.2.2 om domstolskontroll.

2.2.6.3 Regler for tilgang til data for "andre"

Justis- og beredskapsdepartementet har fastslått at det prinsipielle utgangspunkt for etterforskning av lovbrudd skal tilligge politiet og påtalemyndigheten og ikke forvaltningen.[75] Det skal derfor ikke åpnes opp for at andre myndigheter også kan få

[73] Utkast til datalagringsforskrift § 4-1d cfr. Politiloven § 17 første og annet ledd.
[74] Politiloven § 17d (3) sml straffeprosessloven § 218m
[75] Innst. 275 L (2010-2011)

tilgang til trafikk- og lokaliseringsdata. Fra dette gjøres det et unntak, for Finanstilsynet. Dette unntaket gjelder kun abonnements-/brukerdata, jf. ekomloven § 2-9 og verdipapirhandelloven § 15-3 (2) nr.2 og 3.[76] Grunnen til at Finanstilsynet unntas, ligger i at bestemmelsen i verdipapirhandelloven § 15-3 (2) nr.3 oppfyller EØS-forpliktelser som følger av direktiv 2003/6/EF om markedsmisbruk artikkel 12 nr.2 d og direktiv 2004/39/EF om markeder for finansielle instrumenter artikkel 50 nr. 2 d. [77]

Sivile saker

Tvisteloven § 22-3 inneholder et unntak fra taushetsplikten hos "tilbyder eller installatør av elektronisk kommunikasjonsnett eller tjeneste". Tilgang kan skje dersom departementet samtykker i at beviset føres.[78] I praksis er det Post- og teletilsynet som har denne kompetansen etter delegering fra departementet. [79] I bestemmelsen står det:

> "Samtykke kan bare nektes når bevisføring kan utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold."

Retten er gitt kompetanse til å overprøve samtykke eller nektelse av å gi samtykke i tredje ledd. Dette skal skje etter "en avveining av hensynet til taushetsplikten og hensynet til sakens opplysning.

Justis- og beredskapsdepartementet har foreslått å endre tvistelovens § 22-3, siden det strider mot datalagringsdirektivets formål om lagring av data: kriminalitetsbekjempelse, at Post- og teletilsynet kan oppheve taushetsplikten. Hensikten med endringen er ikke å fjerne dagens adgang til å få utlevert abonnementsopplysninger, herunder elektronisk kommunikasjonsadresse se ekomloven § 2-9(3), men å ikke gi tilgang til trafikkdata og lokaliseringsdata som er mer inngripende i seg selv.

2.2.7 Implementeringen av datalagringsdirektivet i forhold til personvernhensyn

Pressens kildevern har ikke vært hovedhensynet i debatten rundt innføringen av datalagringsdirektivet i Norge. Selv om kildevernet er svært viktig i forhold til de

[76] Se også utkast til datalagringsforskrift § 4-1 (d)
[77] Se Prop. 49 L. kapittel 14.
[78] Jf Tvisteloven § 22-3 annet ledd.
[79] Se prop. 49 L kapittel 14.

rettighetene pressen skal beskytte for å sørge for en fri informasjonsflyt i samfunnet, noe som er igjen er en forutsetning for demokratiet, så har nok dette kommet i annen rekke i forhold til vurderingene som har vært foretatt rundt innføringen.

Lagring av trafikkdata vil berøre alle borgere i betydelig grad. Innhenting og lagring av personopplysninger er blant annet et inngrep i retten til respekt for privatliv og korrespondanse etter EMK artikkel 8. Retten til fri kommunikasjon er sett på som en av grunnpilarene i et demokratisk samfunn. Art 29 Working Party[80], har også uttalt at de mener lagring av trafikkdata vil krenke retten til fortrolig kommunikasjon etter EMK artikkel 8.[81]

Videre har Datatilsynet har uttalt at datalagringen kan ses på som en forskuttert etterforskningsmetode som retter seg mot hele samfunnet uten at det foreligger mistanke mot noen. Dette kan igjen sees på som et uttrykk for at hele folket blir satt under mistanke. [82] Man kan spørre seg om dette bryter med uskyldspresumsjonen etter EMK artikkel 6. Andre generelle farer ved en slik masselagring av opplysninger, er muligheten for at dataene kan misbrukes. Dette er noe det er svært vanskelig å garantere mot til tross for sterke sikkerhetsmekanismer.

Selv om personvernhensyn er svært viktig i forhold til implementeringen av datalagringsdirektivet, dekkes ikke dette av min problemstilling.

[80] En arbeidsgruppe, nedsatt etter art. 29 i direktiv 95/46/EF som fungerer som et uavhengig EU-rådgivningsorgan for personvernspørsmål og består av representanter fra alle EUs medlemsland
[81] Artikkel 29-gruppen vedrørende databeskyttelse, 2005
[82] Prop. 49 L (2010–2011) Punkt 3.2.3.

3 PRESSENS KILDEVERN

3.1 Bakgrunnen for kildevernet

Med kildevern vil man historisk mene anonymitetsrett. Før Grunnloven ble til, var anonym publisering forbudt. Etter Christian V-s danske lov fra 1683 var det fastsatt livstidsfengsel eller dødsstraff for anonyme krenkelser.[83] Det har blitt hevdet fra flere hold at anonymt forfatterskap ble innført i Norge gjennom det grunnlovfestede ytringsfrihetsvernet, selv om det ikke direkte fremkom av ordlyden i § 100 fra 1814.[84] På siste halvdel av 1800-tallet var det flere rettssaker i Norge hvor redaktører ble dømt til bøter eller fengselsstraff fordi de ikke ville oppgi hvem som var forfatter til en tekst.[85]

Først etter 2.verdenskrig blusset debatten om lovfesting av kildevernet opp for fullt. Og de første bestemmelsene som kom i 1951, ble hjemlet i straffeprosessloven og tvistemålsloven.[86] Pressens eget etiske regelverk, Vær Varsom-plakaten, fikk egne regler om kildevern i 1956, og i dag lyder de som følger:

> 3.4. Vern om pressens kilder. Kildevernet er et grunnleggende prinsipp i et fritt samfunn og er en forutsetning for at pressen skal kunne fylle sin samfunnsoppgave og sikre tilgangen på vesentlig informasjon.
> 3.5. Oppgi ikke navn på kilde for opplysninger som er gitt i fortrolighet, hvis dette ikke er uttrykkelig avtalt med vedkommende..

Kildevernet i presseetikken er i dag et absolutt yrkesetisk prinsipp for pressen. Ifølge Vær Varsom-plakaten skal en kilde som er blitt lovet fortrolighet aldri røpes, heller ikke når det er pålagt av retten.

Ina Lindahl[87] har laget en oversikt over samtlige kildevernsaker i Norge fra 1950 til 2009. Her kommer det fram at ingen pressefolk *noen sinne* har etterkommet pålegg fra domstolen om å oppgi kilder. Pressen har da heller valgt å akseptere sanksjoner. Dette har i hovedsak bestått av bøter.[88] (Se punkt3.3.6.3)

---

[83] Lindahl (2009)
[84] Ibid.
[85] NOU 2011:12 Punkt 12.2.
[86] Straffeprosessloven av 1887 § 177, og tvistemålsloven av 1915 §209
[87] Lindahl, (2009) s. 49-54.
[88] Rt 1987 s. 910 og Rt 1996 s. 1164.

Folkerettslig er kildevernet beskyttet av EMK artikkel 10 som et element i ytringsfriheten. Praksis ved EMD gir prinsippet stor gjennomslagskraft, selv om det ikke er absolutt.

3.2 Grunnlovsvern

Grunnloven er vår øverste rettskilde i Norge, og betegnes ofte som "lex superior". Utgangspunktet i § 100 er at *"*Ytringsfrihed bør finde Sted*"*.[89]

Forarbeidene til den nye grunnloven slår fast at § 100 også omfatter retten til å forholde seg taus. Denne retten omtales ofte som den "negative ytringsfrihet", og har to sider: Det å forholde seg taus om egne meninger, og det å forholde seg taus om faktiske opplysninger.[90] Det er gjennom denne retten at kildevernet blir beskyttet av Grunnloven. Dette fremkommer ikke direkte av ordlyden, men kan leses ut av henvisningen til Ytringsfrihet i § 100 første ledd.[91]

3.3 Lovregler

Rettsreglene som omhandler kildevernet til pressen i norsk rett er:

- Straffeprosessloven § 125
- Tvisteloven § 22-11, tidligere tvistemålsloven § 209 a.
- EMK artikkel 10

3.3.1 Hovedregelen er unntak fra vitneplikt.

Utgangspunktet i norsk rett er at enhver plikter å møte som vitne og forklare seg overfor retten[92], med mindre annet er bestemt ved lov. Reglene omhandler fri bevisføring og en allmenn forklarings- og bevisplikt. Kildevernreglene er et unntak fra dette. De gjelder både straffesaker og sivile saker, og bestemmelsene i straffeprosessloven § 125 og tvisteloven § 22-11 er tilnærmet identiske[93].

[89] Grl § 100 (1)
[90] St.meld. nr. 26 (2003-2004) s. 33
[91] NOU 1999:27 s 240 og St.meld. nr. 26 (2003-2004) s. 33-34. Se også Lindahl, 2009 s 34.
[92] Jf straffeprosessloven § 108 og tvisteloven § 21-5
[93] Strprl § 125 (1,2,3,5 ledd) tilsvarer tvl. § 22-11 og strprl § 125 (4), tilsvarer tvl. § 22-12 (2)1.setning

Pressens kildevern innebærer et bevisfritak fra vitneplikten. En forutsetning for slik fritakelse er at opplysningene er betrodd journalisten "til bruk i hans virksomhet**"** [94]**,** hvorvidt opplysningene er publisert har ingen betydning.[95] Dette er fordi journalisten kan ha gode grunner til å bringe informasjonen han har mottatt direkte videre til politi eller andre myndigheter i stedet for å publisere dem først.[96] Det er derfor ikke meningen at publisering skal være avgjørende for hvorvidt det foreligger kildevern.

Unntaket fra vitneplikt kommer som tidligere nevnt bl.a. fra straffeprosessloven § 125 første ledd, og lyder som følger:

> **"§125.** Redaktøren av et trykt skrift kan nekte å svare på spørsmål om hvem som er forfatter til en artikkel eller melding i skriftet eller kilde for opplysninger i det. Det samme gjelder spørsmål om hvem som er kilde for andre opplysninger som er betrodd redaktøren til bruk i hans virksomhet."

Denne regelen er sideordnet hovedregelen om vitneplikt, og legger stor vekt på de prinsipielle hensyn som taler for et sterkt kildevern.[97] I forarbeidene er det uttalt at:

> "Mediearbeidere har imidlertid som hovedregel rett til å nekte å svare på spørsmål om identiteten til en anonym kilde. Unntaksvis kan retten likevel pålegge slik vitneplikt." [98]

I Rt 1992 s.39 (Edderkoppen) blir det også uttalt at man i tolkningen av disse reglene må se på dem som likeverdige. Dette gjaldt da tvistemålsloven § 209a som nå er videreført av tvisteloven § 22-11 med en viss utvidelse i tredje ledd. Den omhandler medarbeidere i kringkasting og annen virksomhet som i hovedtrekk har samme formål som aviser og kringkasting. Kildevern er altså blitt den klare hovedregelen.[99]

3.3.2 Unntaket fra hovedregelen. Når kan man fravike kildevernet?

Vær varsom-plakaten gir et absolutt forbud mot å avsløre navnet på en kilde på opplysninger som er gitt i fortrolighet.[100] Eneste unntak fra dette er dersom kilden selv har godtatt tilkjennegjøring.

---

[94] Straffeprosessloven § 125 (1) annet punktum.
[95] Ot.prp.nr.55 (1997-1998) punkt3.2.1. avsnitt 11.
[96] Andenæs 2009
[97] Ot.prp.nr 55 (1997-1998)
[98] Ibid. s 5.
[99] Lindahl (2009)
[100] Vær Varsom-plakaten punkt 3.4 og 3.5

Selv om pressen selv ser på kildevernet som absolutt, er dette ikke den stillingen kildevernet har i lovverket. Her er bestemmelsene slik at domstolen etter en helhetsvurdering kan gjøre unntak fra prinsippet om kildevern dersom "vektige samfunnsinteresser" tilsier det, og det er av "vesentlig betydning for sakens oppklaring". Dette har i forarbeidene blitt kalt for avveiningsnormen.[101]

3.3.2.1 Den generelle unntaksbestemmelsen

Unntak fra kildevern kan bare gjøres etter en helhetsvurdering av hvorvidt det foreligger "vektige samfunnsinteresser" som videre må være av "vesentlig betydning for sakens oppklaring" [102]. Dette er absolutte vilkår. Uttrykket "vektige samfunnsinteresser" vil si at hensynene må være av "*betydelig styrke"*[103] før de gir grunnlag for å gjøre unntak fra kildevernet. Videre er uttrykket samfunnsinteresser svært vidt. Det omfatter ikke bare statens eller det offentliges interesser, men også fellesskapsinteresser eller allmenne interesser.[104] Rent private interesser derimot faller utenfor.[105]

I forhold til hvorvidt opplysningen er av "vesentlig betydning for sakens oppklaring" så følger det av ordlyden "vesentlig" at dette må være relevante opplysninger som må ha stor betydning for oppklaringen av saken. Ifølge forarbeidene så forutsettes det at alternative etterforskningsmetoder først må ha vært prøvd ut før man kan benytte seg av unntaket, til tross for at dette kan være mye mer ressurskrevende.[106]

3.3.2.2 Den særskilte unntaksregelen

Den særskilte unntaksregelen omhandler at kildevernet i enkelte tilfeller kan være spesielt sterkt. Dersom kilden "har avdekket forhold som var av samfunnsmessig betydning å få gjort kjent",[107] så gjør det ikke noe at vilkårene i den generelle unntaksbestemmelsen er oppfylt. Kildevernet vil da likevel gå foran vitneplikten, og

---

[101] NOU 2011:12 punkt 12.1.1.
[102] Jf strpl § 125 (3)1.setning og tvl § 22-11(2)1.setning.
[103] Lindahl 2009 og Ot.prp.nr. 55 (1997-98)
[104] Ot.prp.nr.55.(1997-98) Kapittel 3.2
[105] Ibid.
[106] Ibid.
[107] Tvl § 22-11 (1)1.setning, og strpl, § 125 (3)1.setning.

vitneplikt vil ikke bli pålagt. Så langt har ikke denne problemstillingen vært oppe for norsk rett.[108]

3.3.3 Interesseavveiningen

Det er domstolene som må foreta den konkrete avveiningen av vilkårene om hvorvidt det foreligger unntaksbestemmelser som gjør at vitneplikt kan bli pålagt.

3.3.4 Mellomløsningen

Både tvisteloven og straffeprosessloven inneholder en mellomløsning for vitneplikt og kildevern. Disse bestemmelsene speiler hverandre og innebærer at opplysning om kildens identitet bare kan gis til retten og partene i møte for lukkede dører og under pålegg om taushetsplikt.[109] Denne bestemmelsen kan også anvendes i tilfeller der pressemedarbeideren er villig til å oppgi navnet på kilden uten at det foreligger pålegg fra retten, noe som bør etterkommes i følge forarbeidene.[110]

At opplysninger gis for lukkede dører medfører tap av muligheten for kontradiksjon. Det er et spørsmål om denne formen for anonym vitneførsel er forenlig med kravet til "fair trial" i EMK artikkel 6 nr. 3. d. Dette problemet faller utenfor temaet for denne avhandlingen. For mer informasjon om det, se Ina Lindahls særavhandling fra 1999[111].

3.3.5 Pressens forhold til gjeldende rett

Som nevnt i kapittel 3.3.2 er det forskjellige oppfatninger mellom pressen og gjeldende rett om kildevernets styrke. Pressen ser på kildevernet som absolutt[112], men dette er ikke det Stortinget har ønsket når de har gitt pressen unntak fra vitneplikten. Ved å innføre vilkår som "vektige samfunnsinteresser" og "vesentlig betydning for sakens oppklaring" har lovgiver gitt domstolen rett til å kreve navn på kilden dersom det foreligger tungtveiende nok grunner for at kildens identitet bør opplyses.[113] Likevel har

[108] Lindahl 2009.
[109] Se tvisteloven § 22-12 og straffeprosessloven § 125 fjerde ledd
[110] Ot prp. Nr. 55 (1997-1998)
[111] Lindahl 1999: Pressens kildevern.(I dag jobber Lindahl som advokat hos Norsk Journalistlag.)
[112] Lindahl (2009) s. 54 og Vær Varsom Plakaten punkt 3.5 og Dommen der noen gikk i fengsel!
[113] Ot.prp. nr 55 (1997-98) s. 19

pressefolk aldri så langt i rettspraksis "etterkommet pålegg fra domstolen om å oppgi kilden" til opplysningene sine[114]

Rettspraksis har beskrevet det som at "kildevernet langt på vei er absolutt så lenge de opplysninger kilden har gitt er av samfunnsmessig betydning" [115] Dette bygger på praksis fra EMD, særlig Goodwin-saken. Selv om opplysningene ikke har slik betydning så er det også gjeldende rett at det skal meget tungtveiende hensyn til for å pålegge vitneplikt.[116]

3.3.5.1 Fare for misbruk

Kildevernet kan misbrukes. Påberopelse av kildevern kan brukes til å skjule dårlig kildearbeid.[117] Et eksempel er der noen ønsker å fabrikkere en sak ved å fremsette grunnløse beskyldninger mot private eller juridiske personer. I slike situasjoner vil kildevernet være til hinder for de som ønsker å rette ansvar mot den anonyme kilden til beskyldningene.

Lovgiver har funnet at slikt misbruk kan oppveies tilstrekkelig ved hjelp av ansvarsregler. Eksempler er straffelovens bestemmelser om æreskrenkelse, grove skildringer av vold og om privatlivets fred,[118] som alle kan gjøres gjeldende mot pressefolk. Samtidig har redaktøren et objektivt ansvar jf. straffelovens § 431, og kan bli erstatningsansvarlig jf. lov om skadeserstatning § 3-6. Dette gjør at man ikke blir stående uten ansvarssubjekt selv om kilden forblir anonym.

3.3.6 Virkeområdet for kildevernreglene

Dette avsnittet skal tydeliggjøre hvilke offentlige interesser som kildevernet tar sikte på å verne. Jeg vil ta for meg de personelle, materielle og prosessuelle reglene rundt kildevernet.

---

[114] Lindahl (2009) s 54.
[115] Se Rt 2004 s1400 avsnitt 46 på bakgrunn av EMD-praksis. Fulgt opp i Rt 2010 s 1945 avsnitt 61.
[116] Se Goodwin-saken, og Rt 2004 s 1400 premiss 46.
[117] NOU 2011:12 Ytringsfrihet og ansvar i en ny mediehverdag. Punkt 12.1.1.
[118] Jf straffelovens §§ 246, 247, 382, 390

3.3.6.1 De personelle reglene

Redaktøren

Det er viktig å kunne klargjøre nøyaktig hvem kildevernreglene gjelder for. I utgangspunktet er det i henhold til lovens ordlyd "Redaktøren av et trykt skrift" [119] som kan nekte å gi tilgang til bevis om hvem som er forfatter til en tekst eller kilden for opplysningene. "Med redaktør forstås den som treffer avgjørelse om innholdet i et trykt skrift." [120] Altså er det uten betydning om personen faktisk har tittelen redaktør. Det er det reelle ansvarsforholdet og hvorvidt han har myndighet til å treffe avgjørelser av redaksjonell karakter som er avgjørende. Dette kan utledes av redaktørens selvstendige ansvar for det som publiseres etter straffeloven § 431.[121]

Redaktøren er som siste instans strafferettslig ansvarlig for opplysningene han publiserer. Redaktøren har altså et selvstendig ansvar, og kan ikke fritas ved å oppgi hvem kilden til opplysningene er. Retten til kildevern medfører altså ikke ansvarsfrihet, og dette er i litteraturen blitt kalt kildevernets gjenytelse. Ifølge rettspraksis skjerpes aktsomhetsplikten når journalisten bygger sin fremstilling på anonyme kilder.[122]

En avis kan ha flere sideordnede redaktører som alle omfattes av bestemmelsen. Dette kan leses av ordlyden i straffeloven § 436.

Andre

Kildevernet beskytter ikke bare "redaktøren". Samme beskyttelse har også "andre som har fått kjennskap til forfatteren eller kilden gjennom sitt arbeid for vedkommende forlag, redaksjon, pressebyrå eller trykkeri" [123] Dette vil for eksempel være journalister, fotografer, teknisk personale og lignende arbeidsgrupper. Viktigst er likevel kildevernet i praksis for journalister, siden de skal være uavhengige og ivareta sin rolle som kritiske formidlere av informasjon.[124]

Kringkasting

"Medarbeidere i kringkasting"

---

[119] Straffeprosessloven § 125 (1)1.setning og Tvisteloven § 22-11(1)1.setn.
[120] Straffeloven 2005 § 270(4) som er en videreføring av straffeloven 1902 § 436
[121] Straffeloven, 2005, § 269
[122] Tønsberg Blad-saken Rt 2003 s. 928
[123] Straffeprosessloven § 125 (2) og § 22-11(3)a
[124] Manshaus, 2011.

Vitnefritaket gjelder tilsvarende også i kringkastingsvirksomhet. Se definisjonen i kringkastingsloven § 1-1.

> ”Med kringkasting menes utsending av tale, musikk, bilder og liknende med radiobølger eller over tråd, ment eller egnet til å mottas direkte og samtidig av allmennheten.”

Denne bestemmelsen kom inn i 1973 som følge av at den tekniske utviklingen nå hadde nådd så langt at man krevde en likestilling mellom trykt presse og kringkasting.[125]

”Annen medievirksomhet.”

Kildevernreglene gjelder også for ”annen medievirksomhet som i hovedtrekk har samme formål som aviser og kringkasting.” [126] Dette vil i hovedsak gjelde ”elektroniske medier”, i praksis formidling som skjer gjennom internett og nettbaserte medier[127]. Dette ble innført etter den siste lovendringen på området[128] og i forarbeidene presiseres det at bestemmelsen:

> ”… tar sikte på å fange opp den medievirksomhet som ikke er kringkasting eller avis i tradisjonell forstand, men hvor formålet er å spre informasjon og være et debattforum mv. på samme måte som gjennom aviser og kringkasting. Dette vil blant annet dekke nettaviser mv. og elektroniske overføringer av ‘kringkastings- eller fjernsynskarakter’ hvor tilgangen skjer via Internett og liknende. Sentrale kriterier her vil være om den aktuelle ‘nettavis’ har en ledende person med oppgaver tilsvarende en ansvarlig redaktør og om den fremtrer som en kilde for løpende informasjon og debatt.” [129]

Det viktige her er altså formålet med informasjonen, om den fremtrer som en kilde for løpende informasjon og debatt, og hvorvidt det finnes en person som har oppgaver tilsvarende en ansvarlig redaktør. Dette bekreftes i rettspraksis, blant annet i Runesteinsaken[130] hvor det blir bekreftet at redaktører for nettaviser også er omfattet.

Leserinnlegg o.l. i nettaviser og på nettsteder.

Runesteinsaken var en sak som omhandlet en mann som omtalte sitt funn og salg av en runestein i et debattforum på et nettsted. Til sammen skrev han fire innlegg. Disse innleggene ville, om de hadde vært tradisjonelle leserinnlegg i en papiravis, vært

---

[125] Definisjonen av kringkasting har siden da blitt endret flere ganger. Se Ot.prp. nr. 76 (2004-2005)
[126] Strpl § 125(5) og tvl § 22-11(3)b.
[127] Lindahl 2009 s 82.
[128] Tvisteloven 2005, straffeprosessloven § 125 første, annet, tredje og femte ledd er også endret.
[129] NOU 2001:32 Bind B side 963-964.
[130] Rt 2010 s 1381.

omfattet av kildevernet, ettersom de normalt ville ha vært gjenstand for en redaksjonell forhåndskontroll. I stedet forelå det her en form for sanntidsredigering ved at hvert nytt innlegg utløste et varsel til redaksjonen slik at innlegget kunne bli vurdert og eventuelt fjernet.

Høyesterett kom til at denne typen innlegg på debattfelt av denne typen nøt samme kildevern som for redaktører og medarbeidere, fordi nettsiden var undergitt redaktøransvar. Dette til tross for at det her var en anonym person som hadde skrevet et innlegg direkte på nettsiden, uten noen form for forutgående redaksjonell kontroll. Selv om det var av "vesentlig betydning for sakens oppklaring" at man fant ut hvem som hadde skrevet disse leserinnleggene, fant Høyesterett at det var viktigere å bevare den sentrale samfunnsinteressen kildevernet beskytter, nemlig "medias nyhetsformidling og frie formidling av synspunkter" [131]. Videre uttalte Høyesterett seg om den mer langsiktige effekten av å skulle gjøre unntak fra ytringsfriheten, som jeg diskuterer i kapittel 4.2.3.

Høyesterett har dermed stadfestet at leserinnlegg og debattinnlegg i nettaviser og nettsteder også beskyttes av kildevernet under visse forutsetninger.

3.3.6.2 De materielle reglene

Hvilke opplysninger omfattes av kildevernet?

Utgangspunktet for at opplysninger skal være omfattet av kildevernet er at" opplysningene er "betrodd" pressemedarbeideren "til bruk i hans virksomhet". I dette ligger det at opplysningene pressemedarbeideren har mottatt faktisk må ha vært betrodd ham i yrkessammenheng. Opplysninger han har mottatt som privatperson eller "mellommann" overfor politiet dekkes ikke.[132] Det gjør heller ikke opplysninger han har opparbeidet gjennom egne observasjoner.

Etter ordlyden i loven er det kildens identitet som skal beskyttes, altså *hvem som er forfatter eller kilde.*[133] Med andre ord er det kun personlige opplysninger som navn, adresse (både hjemme og arbeidsplassen), fødselsnummer, telefonnummer, e-

[131] Rt 2010 s 1381 avsnitt 52
[132] Lindahl, 1999 s.27.
[133] Tvisteloven § 22-11(1) og straffeprosessloven § 125(1)

postadresse, stemme og bilde som direkte beskyttes.[134] Men indirekte fører dette også til et forbud mot å stille spørsmål som vil føre til avsløring av kilden. Med andre ord kan sammenhengen mellom opplysningene og kilden føre til at man ikke kan kreve forklaring på enkelte spørsmål, selv om de isolert sett ikke direkte avslører kilden.[135] I Edderkoppsaken uttalte førstvoterende med et obiter dictum, at:

> "Kildevernet må gå så langt at det heller ikke kan stilles spørsmål hvor formålet ikke er å komme på spor etter kilden, men hvor det kan bli resultatet."[136]

Dette fører til at hvilke spørsmål som kan tillates, må avgjøres konkret fra sak til sak. I Europarådets rekommandasjon fra 2000 nr. 7, så ble det presisert at også de faktiske omstendigheter rundt hvordan man får tilgang til opplysninger også kan holdes tilbake.[137] Dette er svært interessant i forhold til hva datalagringsdirektivet tillater av innsamling. Selv om formålet ikke er å komme på spor etter kilden, så kan dette lett bli konsekvensen dersom informasjon om journalisters kommunikasjon blir hentet ut.

Betydningen av hvordan kildens opplysninger er brukt

Tidligere var det i norsk rett avgjørende at opplysningene var publisert for at kildevernet skulle gjelde. I 1981 kom det en lovendring som et resultat av kritikk av flere høyesterettsdommer fra de senere år, blant annet Klepslandsaken og Politimannsaken.[138]

Klepslandsaken gjaldt en redaksjonssekretær som gikk til politiet med tips han fikk om beruset mannskap på to rutefly som var gått fra Tromsø samme natt. Neste dag publiserte han saken i avisen, og ble senere bedt om å avsløre sin kilde. Høyesteretts kjæremålsutvalg kom til at kildevernet ikke fikk anvendelse siden han hadde varslet politiet før han offentliggjorde saken i avisen.

---

[134] Veiledningen til "Rekommandasjon (2000) 7 " kap. II, punkt 13 (ii).
[135] Ot.prp.nr. 55 (1997-1998) s. 15.
[136] Rt 1992 s.39 (s.51)
[137] Rekommandasjon (2000)7, d (ii)
[138] Rt 1966 s 176. (Klepplandsaken), og Rt 1977 s.966 (Politimannsaken)

Også i Politimannsaken[139] kom kjæremålsutvalget frem til at den betingede rett til kildebeskyttelse var knyttet til det "trykte ord", noe som førte til at de vanlige reglene for vitneplikt ble gjeldende.

På den tiden var det et krav i straffeprosessloven § 177 (3) at det måtte gjelde et "trykt skrift" for at kildevernet skulle komme til anvendelse. I ettertid ble saken kritisert siden det må være mulig for pressen å gå til politiet med opplysninger, uten at kildevernet måtte vike. [140] I dag er det gjeldende rett at kildevernet gjelder uansett om "kildens opplysninger har vært benyttet, er tenkt benyttet eller ikke vil bli benyttet" [141] Dette kan man blant annet lese ut av uttrykket "andre opplysninger" i tvisteloven § 22-11 og straffeprosessloven § 125.

Betydningen av samtykke

Samtykke fra kilden om formidling av opplysninger om hans identitet, vil i utgangspunktet føre til at opplysningene faller utenfor kildevernet. Begrunnelsen for kildevern vil ikke lenger foreligge. Unntak fra dette kan likevel forekomme:

I Rt. 1992 s. 39 (Edderkoppen) ble samtykkets betydning vurdert. Det kom fram at selv om det forelå samtykke fra konkrete kilder, så ville ikke dette nødvendigvis føre til et bortfall av kildevernet. I dommen legges det bl.a. vekt på at kildevernet har en allmenn interesse og bør beskyttes. Et eksempel som blir gitt er at dersom en av flere kilder nekter å gi samtykke, så vil dette lett gi inntrykk av at vedkommende har noe å skjule. Videre kan situasjonen være slik at journalisten bygger på flere kilder, og det kan være vanskelig for ham å forklare seg om en av dem uten samtidig å avsløre de andre. Dette kan også sette de andre under et uheldig press. Med andre ord er ikke samtykke alltid avgjørende for hvorvidt retten til å nekte å oppgi en kilde faller bort.

[139] Rt 1977 s.966 (Politimannsaken).
[140] Innst. O. nr 37 (1980-81) s 21-.22 jf Ot.prp. nr. 55 (1997-98) punkt 3.2.1
[141] Lindahl 2009 s 97.

3.3.6.3 De prosessuelle reglene

Saksbehandlingen

Dersom det blir tvist om hvorvidt et bevis[142] kan føres i en sak, så skal beslutning om dette treffes ved kjennelse, jf. tvisteloven § 19 (2)d., og straffeprosessloven § 137. Om bevisplikt blir pålagt, så kan denne ankes.[143] Dette kan, dersom retten krever det, måtte skje "straks",[144] for å sikre fortgang i saken.

Sanksjonsmidler

Bøter

Dersom et vitne nekter å avgi forklaring, til tross for rettskraftig pålegg om vitneplikt, kan retten pålegge vedkommende bøter eller erstatningsplikt for eventuelle omkostninger som følge av vegringen, se domstolloven § 206. Som tidligere nevnt i punkt 3.1, har hittil ingen pressefolk etterkommet pålegg fra domstolen om å oppgi sine kilder. Dette har ført til at det i flere saker er blitt gitt bøter til pressefolk. Bøtene har vanligvis ligget rundt 20 000 til 25 000 kroner.[145]

Fengslig Forvaring

Dersom det er snakk om en straffesak, og bevisplikt er pålagt ved rettslig kjennelse, kan retten beslutte ved ny kjennelse at vedkommende skal holdes i fengslig forvaring inntil plikten er oppfylt, se straffeprosessloven § 137. Denne retten har bare blitt brukt en gang, jf. Rt 1953 s. 127, Hall-Hofsø-saken, som gjaldt en redaktør som nektet å oppgi kilden for opplysningene som var brukt i reportasjen: "Forsøk på voldtekt i Harstad".[146] Saken endte med at kilden selv sto fram etter at redaktøren hadde sittet fengslet i 14 døgn.

Justis- og politidepartementet uttalte i Ot.prp. nr. 55 (1997-98), at de var enige i den tilbakeholdenhet som var vist så langt når det gjaldt fengslig forvaring, og at det ikke burde komme noen endringer når det gjaldt bruken av fengslig forvaring som tvangsgrunnlag. Departementet fulgte her de anbefalingene som kom fra

---

[142] For eksempel vitneførsel.
[143] Tvisteloven § 29-8 (2), og straffeprosessloven § 377.
[144] Tvisteloven § 29-5(3) og straffeprosessloven § 379 (2)
[145] Eksempler funnet i Lindahl, 2009, se Transplantasjonssaken II, Verstingsaken II, og MC-fotosaken.
[146] Lindahl, 2009, s 102.

utvalgsutredningen for NOU 1988; ”Kildevern og offentlighet i rettspleien”. De hadde uttalt at det å bruke et slikt tvangsmiddel var prinsipielt betenkelig.[147]

3.4 EMK artikkel 10

3.4.1 Innledning

Norge har gjennom menneskerettsloven blant annet gitt EMK forrang foran annen lovgivning[148] (med unntak av grunnloven). Dette vil si at den nasjonale terskelen for kildevern ikke kan legges lavere enn det som følger etter EMK.

EMK artikkel 10 slår fast i første ledd at:

> ”Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser…”

Dette er en den positive retten EMK artikkel 10 gir. Unntak fra dette må oppfylle tre kumulative vilkår i EMK artikkel 10 annet ledd. For det første så må inngrepet være foreskrevet ved lov. Videre må det være nødvendig i et demokratisk samfunn og oppfylle et av disse 11 legitime formålene:

> ”hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.” [149]

Hvis disse tre vilkårene er oppfylt, altså lovkravet, nødvendighetskravet og krav til legitimt formål, så kan det foretas unntak fra ytringsfrihetsbestemmelsen i første ledd.

3.4.2 EMK artikkel 10 andre ledd

3.4.2.1 Lovkravet, ”prescribed by law”

Det første vilkåret for at det skal kunne gis innskrenkninger i ytringsfriheten, innebærer at dette unntaket må være ”*foreskrevet ved lov”*. Dette vil si at det må foreligge en lov i intern norsk rett for at det skal være mulig å foreta et unntak fra hovedregelen. Videre

[147] NOU 1988:2 s 21.
[148] Menneskerettsloven §3
[149] EMK artikkel 10(2)

følger det av praksis i EMD, at denne loven må være tilstrekkelig presis, forutberegnelig, og tilgjengelig.[150] Dette er helt alminnelige krav til rettsstaten, siden borgerne skal ha mulighet til å forutse eventuelle inngrep i deres ytringsfrihet[151]

Lovvedtak 46 (2010-2011), som gjennomførte EUs datalagringsdirektiv i norsk rett, oppfyller kravet om at unntak fra ytringsfriheten må være ”foreskrevet ved lov” Reglene er likevel enda ikke fullstendig implementert, siden lovene ennå ikke har trådt i kraft. Men de gir likevel et utgangpunkt i forhold til ”lovkravet” etter EMK artikkel 10.

3.4.2.2 Kravet til legitimt formål

Inngrep i ytringsfriheten må som tidligere nevnt, være begrunnet i et av de tidligere nevnte formål i EMK artikkel 10 nr. 2. Det er her hele 11 konfliktområder, som i utgangspunktet kan deles inn i to hovedgrupper: Nemlig vern av individuelle interesser, (”andres omdømme” og ”andres rettigheter”) og vern av offentlige interesser (de øvrige 9 formålene).[152] Disse *uttømmende* formålene, setter skranker for hvilke argumenter det i det hele tatt er relevant å ta med i vurderingen om hvorvidt inngrepet er ”nødvendig i et demokratisk samfunn”.[153]

Formålene som ligger bak datalagringsdirektivet og som omfattes av EMK artikkel 10 nr. 2, er bekjempelse av alvorlig kriminalitet og hensynet til å ivareta den nasjonale sikkerhet, og andres rettigheter. Så i utgangspunktet er kravet til legitimt formål oppfylt. Hvorvidt formålet faktisk fremmes, trekkes først inn ved nødvendighetsvurderingen. EMD har gjennomgående brukt lite tid på å diskutere hvorvidt disse formålene er reelle, se for eksempel dommen Klaas v. Germany, premiss 44. Uttrykket samfunnsmessige hensyn er også brukt for å omtale uttrykket ”legitimt formål”.

3.4.2.2.1 Nødvendighetskravet ”necessary in a democratic society”

Nødvendighetskravet blir gjerne omtalt som en rettslig standard, som går ut på at man må veie de hensyn som begrunner inngrepet i ytringsfriheten mot de hensyn

[150] EMD: Leandersaken premiss 50 og Sunday Times premiss 49
[151] Kyrre Eggen, Ytringsfrihet Kapittel 4.4.2.1
[152] NOU 1999:27
[153] Kyrre Eggen, 2002 s 215.

ytringsfriheten skal ivareta.[154] Etter ordlyden: *nødvendig,* kan man innfor et krav om forholdsmessighet Nødvendighetsvurderingen inneholder flere elementer som må vurderes i den enkelte sak, og alle er ikke alltid like aktuelle. Det er ikke nok at inngrepet er nyttig eller hensiktsmessig i forhold til formålet. Det avgjørende er at det må ivareta et "presserende eller tvingende samfunnsmessig behov. Dette uttrykket legger føringer på hvor viktig begrunnelsen for inngrepet må være for å kunne rettferdiggjøre brudd på ytringsfriheten.

Videre så er det staten som i første rekke har ansvaret for å sikre rettighetene etter konvensjonen, noe som gir dem et visst skjønnsmessig spillerom, en "margin of appreciation". Det at de har blitt gitt et slikt spillerom faller naturlig, siden det er staten selv som er nærmest til å vurdere hva som er nødvendig og proporsjonelt til enhver tid. Dette spillerommet er dog ikke ubegrenset og EMD, har uttalt at de forbeholder seg det siste ord:

> "…the Court has underlined that the initial responsibility for securing the rights and freedoms enshrined in the Convention lies with the individual Contracting States. Accordingly, "Article 10 (2) (art. 10-2) leaves to the Contracting States a margin of appreciation. This margin is given both to the domestic legislator ... and to the bodies, judicial amongst others, that are called upon to interpret and apply the laws in force" (p. 22, para. 48). "Nevertheless, Article 10 (2) (art. 10-2*)* does not give the Contracting States an unlimited power of appreciation": "The Court ... is empowered to give the final ruling on whether a 'restriction' ... is reconcilable with freedom of expression as protected by Article 10 (art. 10). The domestic margin of appreciation thus goes hand in hand with a European supervision."[155]

Dette er senere fulgt opp og forsterket i en storkammeravgjørelse av EMD i 2007, der det ble uttalt:

> "Where freedom of the "press" is at stake, the authorities have only a limited margin of appreciation to decide whether a "pressing social need" exists"[156]

Pressen har med andre ord blitt gitt et svært sterkt vern.

Hvor stort skjønnsmessig spillerom staten har vil også bero på hvor stort inngrepet er, sammenholdt med hva slags type rettighet det er snakk om. Naturlig nok vil liv og helse veie tyngre enn økonomiske interesser. I forhold til kildevernet, så vil det naturlig nok

---

[154] Ibid. s 216
[155] The Sunday Times v United Kingdom
[156] Case of Stoll v. Switzerland

ha betydning at det ikke er avsløring av kilder som er formålet med lagringen av kommunikasjons- og lokaliseringsdata.[157]

EMD har i flere plenumsdommer sammenfattet det generelle innholdet i nødvendighetskravet i EMK artikkel 10 nr. 2. Selv om det selvfølgelig er nyanseforskjeller, har EMD stort sett konkludert med at nødvendighetsvilkåret innebærer at begrunnelsen bak inngrepet må være ”relevant” og ”sufficient”, og at inngrepet må være ”proportionate to the legitimate aim pursued”.[158] Når det gjelder relevanskravet, så er det bare en påminnelse om at inngrepet må forankres i et at de påberopte legitime formål. [159] Relevanskravet må også sees på i sammenheng med om inngrepet er ”sufficient” (tilfredsstillende). Minstekravet for at begrunnelsen skal være ”tilfredsstillende” er at inngrepet bidrar til å realisere det aktuelle formålet.[160] Sammenhengen mellom relevanskravet og hvorvidt begrunnelsen er ”sufficient”, beskrives godt i dommen om Sunday Times:[161]

> “Moreover, although this particular reason for the injunction might possibly have been "relevant" under Article 10 (2) (art. 10-2), the Court cannot decide whether it was" sufficient" without examining all the surrounding circumstances.”

Det må altså foretas en konkret vurdering.

Når alt kommer til alt så er nok den viktigste vurderingen man foretar under nødvendighetskravet, en *proporsjonalitetsvurdering.* Proporsjonalitetskravet som ligger innbakt i uttrykket ”necessary in a democratic society”, går i grove trekk ut på at det inngrepet som skjer i konvensjonsrettigheten må være proporsjonalt med de legitime formålene som staten ønsker å oppnå. Her må man også se på om det foreligger proporsjonalitet mellom individenes rettigheter og rettighetene til samfunnet som helhet. Et viktig spørsmål når man vurderer dette er, hvorvidt det etter omstendighetene var *nødvendig* å gå frem på en så inngripende måte. Dersom man kan oppnå formålet med mindre inngripende midler, eller at formålet ikke var tilstrekkelig tungtveiende i

[157] Weber og Saravia mot Tyskland premiss 145
[158] Kyrre Eggen, 2002 kap. 4.4.4.1. smh med Sunday Times, avsnitt 50, Observer and Guardian avsnitt 59, og Vogt avsnitt 52.etc. Se også Møse, 2005, Aall 2005 og Nordeide 2006
[159] Kyrre Eggen, 2002, avsnitt 4.4.4.2.
[160] Ibid. avsnitt 4.4.4.3.
[161] Sunday Times avsnitt 63.

forhold til å oppveie inngrepet, så er det et klart uttrykk for at inngrepet ikke var "necessary in a democratic society".[162]

Når vi ser på nødvendighetskravet i forhold til datalagringsdirektivet, så har EU ved vedtagelsen av direktivet, gitt uttrykk for, at det foreligger et presserende samfunnsmessig behov for å bekjempe alvorlig kriminalitet, og at tilgang til data kan være av avgjørende betydning for å kunne oppklare en rekke ulovlige og straffbare handlinger. Dette ble også fremhevet av politiet og påtalemyndigheten under høringen av datalagringsdirektivet. Hvorvidt inngrep i kildevernet til pressen vil være proporsjonalt i forhold til formålet: "å bekjempe alvorlig kriminalitet", vil måtte avgjøres ved en konkret forholdsmessighetsvurdering fra sak til sak. Dette vil i praksis være en vurdering som tas ved domstolskontrollen, som jeg skal diskutere videre, senere i avhandlingen. Jeg vil likevel vektlegge Kyrre Eggens uttalelse i boken Ytringsfrihet:

> "EMD, har anerkjent at journalisters kildevern er en viktig rettslig rammebetingelse for medias funksjon som "public watchdog", og at inngrep i kildevernet følgelig er et tungt inngrep i ytringsfriheten.[163]

Det skal med andre ord svært mye til før et inngrep i kildevernet, og dermed ytringsfriheten, kan forsvares i en proporsjonalitetsvurdering om hvorvidt det er "nødvendig i et demokratisk samfunn".

3.4.3 Rettspraksis etter den Europeiske menneskerettighetsdomstol (EMD).

3.4.3.1 Goodwin-saken[164] og dens betydning.

Goodwin-saken er en plenumsdom fra 1996 som stadfester at pressens kildevern er dekket av ytringsfrihetsbestemmelsen i EMK artikkel 10. Dommen er spesielt interessant siden den kommer med en del prinsipielle uttalelser som har vært fulgt opp i senere dommer om kildevern.

---

[162] Kyrre Eggen, 2002, avsnitt 4.4.4.4.
[163] Kyrre Eggen, 2002, avsnitt 4.4.4.4.
[164] Goodwin v. The United Kingdom

Saken handlet om at journalisten William Goodwin mottok opplysninger om selskapet Tetra Ltds finansielle problemer. Goodwin visste ikke at det dreide seg om konfidensielle interne dokumenter da han mottok opplysningene og forsøkte å få kontakt med selskapet for å innhente kommentarer og for å få bekreftelse på informasjonen han hadde mottatt. Dette førte til at det ble gitt pålegg om publiseringsforbud for opplysningene. Det viste seg at informasjonen stammet fra selskapsplanen til selskapet som bare fantes i 5 eksemplarer. Det ble videre gitt et rettslig pålegg, for at Goodwin skulle utlevere notatene sine om saken Pålegget om å utlevere notatene og avsløre kilden var begrunnet i ønsket om å identifisere kilden til lekkasjen, slik at selskapet kunne rettsforfølge kilden.

Grunnen til at Tetra Ltd kunne prøve saken under unntaket i EMK artikkel 10, var at de kom inn under kravet om legitime formål som "andre interesser". Dette viser at selv bedrifters private interesser kan være grunnlag for unntak for kildevernet.

Det viktige her var hvorvidt inngrepet var "*nødvendig i et demokratisk samfunn"*. I denne saken fant EMD at publiseringsforbudet kunne godtas, men at pålegget om å oppgi kilden var å trekke det for langt. I premiss 39 i dommen sies det at inngrep i artikkel 10 ikke kan rettferdiggjøres med mindre det er "justified by an overriding requirement in the public interest". Dette gir uttrykk for at vitneplikt bare kan pålegges dersom det kan la seg forsvare av dominerende offentlige interesser. Med andre ord så skal det svært mye til før et inngrep i kildevernet kan forsvares.

Premiss 40 i dommen understreker at inngrep i kildevernet "call for the most careful scrutiny by the Court".[165] Dette tolker jeg som at prøvingsintensiteten må være spesielt streng når det er snakk om inngrep i kildevernet.

I dommen blir det også understreket at pressens kildevern er en av de grunnleggende forutsetningene for pressefrihet og at

> "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." [166]

[165] Ibid. premiss 39
[166] Ibid. premiss 39

EMD gav her klart uttrykk for hvor viktig kildevernet er for den frie pressen:[167] Likevel så var det nødvendig å ta en proporsjonalitetsvurdering i forhold til selskapet Tetras interesser.

> "On the facts of the present case, the Court cannot find that Tetra's interests in eliminating, by proceedings against the source, the residual threat of damage through dissemination of the confidential information otherwise than by the press, in obtaining compensation and in unmasking a disloyal employee or collaborator were, even if considered cumulatively sufficient to *outweight the vital public interest in the protection of the applicant journalist's source*."[168] (min kursivering)

Goodwin-saken har hatt stor betydning for norsk rett, og er blitt sitert i flere høyesterettsdommer om kildevern.[169]

3.4.3.2 Financial Times-saken[170]

Klagerne i saken, fire aviser og et nyhetsbyrå, hadde mottatt dokumenter som inneholdt informasjon om at et belgisk bryggeri skulle komme med et mulig oppkjøpsbud av et sør-afrikansk bryggeri. De publiserte artikler om det mulige oppkjøpet, noe som førte til at aksjene til det sør-afrikanske bryggeriet steg kraftig. Det belgiske bryggeriet anla så sak mot klagerne, og fikk medhold i engelske domstoler i at de måtte utlevere dokumentene. Bryggeriet håpet dokumentene kunne bidra i deres etterforskning av hvem som hadde lekket informasjonen siden lekkasjene var alvorlige både overfor bryggeriene og aksjemarkedet. Bryggeriet mente også at dokumentene var manipulerte fordi aksjeprisene som avisene refererte til ikke stemte med prisene angitt i originaldokumentene. Engelsk rett opprettholdt avgjørelsen om utlevering i ankesaken. Begrunnelsen de gav, var at den offentlige interessen som lå i det å beskytte kilden, ikke var tilstrekkelig i forhold til den offentlige interessen som lå i å finne kilden til lekkasjen som de mente hadde et tydelig mål om å skade firmaet, da også muligens for egen personlig vinning. Dette formålet fant ikke EMD at var blitt fastslått med sikkerhet

---

[167] Høstmælingen, 2006, 259
[168] Goodwin v. the United Kingdom 1996 para 45.
[169] Rt-1996 s.1375 (MC-fotosaken), Rt-2002-489 (Biltyverisaken), Rt 2004 s. 1400 (Dørvaktskjennelsen), Rt-2010 s. 1150, Rt-2010-1381 (Runesteinsaken), Rt. 2011 s.1266
[170] Financial Times Ltd and others v. The United Kingdom,

hos de nasjonale domstolene, og pekte på at det kunne tenkes situasjoner hvor en slik hensikt kunne anses som en relevant nok og tilstrekkelig grunn til å treffe en beslutning om utlevering av dokumenter. Her derimot var ikke dette bevist godt nok i engelsk rett.

EMD slo fast, etter en konkret vurdering, at det ville være i strid med EMK artikkel 10 å kreve dokumentene utlevert.

EMK startet nødvendighetsvurderingen, med å understreke hvor viktig kildevernet er i et demokratisk samfunn.[171] De minnet om Goodwin-saken og uttalte at utleveringspålegg som kunne avsløre en kilde krevde en særlig god begrunnelse. I tillegg la de i premiss 63 i dommen stor vekt på verdien av kildevernet i seg selv.

> "In the case of disclosure orders, the Court notes that they have a detrimental impact not only on the source in question, whose identity may be revealed, but also on the newspaper against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on the members of the public, who have an interest in receiving information imparted through anonymous sources and who are also potential sources themselves."

Her fikk EMD fram hvilke skader slike utleveringspålegg kan påføre informasjonsfriheten generelt ved at den generelle tilliten til at kildevernet vil respekteres, svekkes, og ikke bare hvorvidt det vil virke skadelig på ytringsfriheten i den enkelte sak.[172]

Videre, ble saken sammenlignet med Goodwin-saken i forhold til at det også her var snakk om dokumenter som kunne avsløre kilden. Forskjellen lå i at det i Financial Times-saken ikke var snakk om utlevering av dokumenter som kunne avsløre kilden direkte. I forhold til dette uttalte EMD:

> "… the Court does not consider this distinction to be crucial. In this regard, the Court emphasises that a chilling effect will arise wherever journalists are seen to assist in the identification of anonymous sources. In the present case, it was sufficient that information or assistance was required under the disclosure order for the purpose of identifying X."

Det at EMD også her understreker hvor viktig det er å unngå "the chilling effect" som kan oppstå ved brudd på kildevernet, viser at kildevernet langt fra har mistet sin betydning siden Goodwin-saken, og antagelig heller har fått enda sterkere vern. Dette er

[171] Ibid, premiss 59
[172] Jon Wessel Aas, 2009

et hensyn som norske domstoler vil måtte ta hensyn til i en eventuell forholdsmessighetsvurdering etter § 170a når det gjelder utlevering av trafikkdata og lokalisasjonsdata etter implementeringen av datalagringsdirektivet. Denne oppfatningen er også blitt uttrykt i juridisk litteratur.[173]

[173] Ibid.

4 Er implementeringen av datalagringsdirektivet forenlig med EMK artikkel 10 og pressens kildevern?

Denne vurderingen må jeg foreta i to deler. Først er det nødvendig å fastsette hvorvidt lagringen i seg selv er i strid med EMK artikkel 10 og kildevernet. Videre vil jeg ta stilling til hvorvidt rettsikkerhetsgarantiene, og blant dem spesielt domstolskontrollen, kan beskytte kildevernet på en god nok måte dersom lagringen er forutsatt å være ”nødvendig i et demokratisk samfunn”.

4.1 Er lagringen i seg selv forenlig med ytrings- og informasjonsfriheten?

4.1.1 Innledning

Hovedargumentene for at lagringen av data kan tillates gjennom direktivet ligger ikke i at den enkelte stat har rett til å overvåke sine egne borgere. Dette ville ikke stått seg mot de rettigheter EMK gir i blant annet regler om privatliv og ytringsfrihet[174]. Det følger implisitt av direktivet at EU anser lagring av ”trafikkdata” forsvarliggjort så lenge selve behandlingen av de lagrede data og vilkårene for eventuell uthenting av data, tilfredsstiller de krav til ”rettssikkerhet og proporsjonalitet som EMK oppstiller”.[175] Dette svarer likevel ikke på spørsmålet om selve registreringen og lagringen av opplysningene kan forsvares, eller om de kan forsvares som ”nødvendig i et demokratisk samfunn”, se EMK artikkel 10 nr. 2.

Som jeg redegjorde for i avsnitt 3.4.2, så stiller EMK artikkel 10 nr. 2 tre vilkår for at man skal kunne foreta inngrep i ytringsfriheten. Inngrepet må være foreskrevet ved lov, oppfylle et legitimt formål, samt være nødvendig i et demokratisk samfunn. De to første vilkårene regner jeg som oppfylt.[176] Vurderingen min vil i hovedsak skje etter hvorvidt lagringen er forholdsmessig og oppfyller kravet om nødvendighet

Før jeg går inn på dette vil jeg redegjøre for de grunnprinsippene om personvern som lå til grunn i EU og EØS området forut for datalagringsdirektivet.

---

[174] EMK artikkel 8 og 10.
[175] Schartum, 2010, Fagbokforlaget
[176] Se punkt3.4.2

Tidligere prinsipper i forhold til lagring av personopplysninger.

Da datalagringsdirektivet kom, så endret det tidligere direktiver og konvensjoner på personvernområdet. Det ble endringer i persondatakonvensjonen, i personopplysningsdirektivet og i kommunikasjonsdirektivet.[177] Det som var felles for disse regelsettene var at de alle bygget på "utgangspunktet om vern av personopplysninger og av privatlivets fred, herunder kommunikasjonsfortroligheten.[178] Videre så satte de svært strenge krav til registrering og lagring av personopplysninger. Dette skulle begrenses til et minimum. (Trafikkdata og lokalisasjonsdata er dekkes helt klart av begrepet personopplysninger.)

Jon Wessel-Aas, beskriver i en artikkel,[179]i boken Overvåkning i en rettsstat[180], at kommunikasjonsdirektivet og de øvrige direktiver og konvensjoner, kan tolkes slik at de ser på registrering og lagring av personopplysninger som "et eventuelt nødvendig onde som bør begrenses i størst mulig grad". Det kan sies at EU, med datalagringsdirektivet, har valgt å vike bort fra de grunnprinsippene som til da hadde vært gjeldende på personvernområdet.

Datakriminalitetskonvensjonen[181] fra 2001, kom som et resultat av et ønske om å effektivisere kriminalitetsbekjempelsen i forhold til utviklingen av elektroniske kommunikasjonsmedier.[182] Dens artikkel 16 påla konvensjonsstatene (inkludert Norge) å gi kompetent myndighet "adgang til å sikre lagrede data som deretter kan benyttes som bevis i en straffesak." [183] I motsetning til datalagringsdirektivet, så var ikke dette en generell plikt til å lagre data, men en regel om bevissikring som ledd i etterforskningen av en straffesak. Norge implementerte bestemmelsen gjennom straffeprosessloven § 215 a i 2005. Bestemmelsen ga påtalemyndigheten, som ledd i etterforskning, mulighet til å gi pålegg om midlertidig sikring av elektronisk lagrede data som man antok kunne ha betydning som bevis. Merk at dette ikke gav

[177] Europarådets konvensjon av 20. januar 1981 nr. 108, EU-direktiv 1995/46/ og EU-direktiv 2002/58/EF.
[178] Schartum, 2010, Fagbokforlaget
[179] Datalagringsdirektivet – er dets krav om lagring av trafikkdata forenlig med Den europeiske menneskerettighetskonvensjonen?
[180] Schartum, 2010, Fagbokforlaget
[181] Europarådets konvensjon av 8. November 2001.
[182] Schartum, 2010, Fagbokforlaget.
[183] NOU 2003:27

påtalemyndigheten tilgang til opplysningene, men kun mulighet til å "sikre" dem i tilfelle de skulle få hjemmel til å få tilgang til dem senere. Etter forarbeidene ble det diskutert om det ikke burde vært strengere vilkår for at man skulle kunne *sikre* data på denne måten, for eksempel ved at det i tillegg ble stilt krav om "skjellig grunn til mistanke".[184] Til slutt forble ordlyden likevel som den er nå siden politiet tross alt ikke fikk *tilgang* til dataene gjennom bestemmelsen.

Hvis vi trekker dette opp mot implementeringen av datalagringsdirektivet, så kan det sies at Stortinget lovmessig har beveget seg svært langt på få år i forhold til hva man tillater av overvåkning overfor individet.

4.1.2 Nødvendighetsvurderingen etter EMK artikkel 10 nr.2[185]

I forhold til om lagringen av data er "nødvendig i et demokratisk samfunn" så vil jeg starte med å si at dette er et vanskelig spørsmål å besvare. Det er beskyttelsen av kildevernet som må vurderes opp mot en automatisk og systematisk registrering av data. Dette gjør at det for en generell lagring av data som også omfatter pressens kommunikasjonsdata, krever enda sterkere grunner enn om det bare gjaldt borgere ellers.

Hvis vi ser på rettspraksis fra EMD, så er ikke spørsmålet om generell lagring er *nødvendig i et demokratisk samfunn* noe det er praktisk for EMD å besvare. EMD har bare kunnet prøve en eller flere klageres konkrete rettigheter. Det sier seg selv at det vil kunne være store individuelle forskjeller på inngrep i forhold til hvem som er gjenstand for lagring. Likevel virker EMDs praksis, når det gjelder inngrep i kildevernet ganske entydig, selv om hensynet til kildevernet ikke har vunnet fram i absolutt alle tilfeller.

I sakene Liberty mfl. mot Storbritannia,[186] og Weber og Saravia mot Tyskland[187] var det snakk om en helt annen type kontroll og overvåkning enn den implementeringen datalagringsdirektivet nå hjemler. I disse sakene aksepterte EMD en forholdsvis vidtgående strategisk overvåkning av kommunikasjon så lenge systemene var underlagt tilstrekkelig kontroll. Her ble ikke all kommunikasjon lagret, det var snakk om systemer

[184] Ot.prp. nr. 40 (2004-2005) punkt 4.2 og Jon Wessel-Aas, 2010
[185] Se punkt:3.4.2.
[186] Liberty mfl. mot Storbritannia
[187] Weber and Saravia v. Germany

som baserte seg på automatiserte søk etter bestemte tekniske og/eller innholdsbaserte søkekriterier. Formålet med dette var "å sile ut" kommunikasjon som omhandlet trusler mot nasjonal sikkerhet eller annen alvorlig organisert kriminalitet. [188] Først på dette stadiet ble kommunikasjonen lagret.

Mellom hva som kreves lagret etter disse to EMD-dommene og hva som blir lagret etter implementeringen av datalagringsdirektivet er det likevel en forskjell. I de to EMD-dommene ble også innholdet av kommunikasjonen lagret. Dette er ikke det som blir tilfellet ved implementeringen av datalagringsdirektivet. Her er lagringen satt til kommunikasjonsdata og lokalisasjonsdata, innholdsdata blir ikke lagret. I Malone-dommen (inngrep etter artikkel 8), som omhandlet uthenting av "data obtained from metering"[189], som i mange tilfeller er de samme data som kreves lagret etter direktivet, ble det fastslått at også trafikkdata beskyttes av EMK.

I forhold til hvorvidt innholdsdata er mer beskyttelsesverdig enn trafikkdata og lokalisasjonsdata, så er nok dette tvilsomt i dag. På grunn av den teknologiske utviklingen kan man hente ut svært detaljert informasjon når man systematiserer informasjon om en brukers trafikkdata[190] og dette er etter min mening like inngripende som lagring av innholdsdata i seg selv.

Klageren i *Weber og Saravia*-saken var journalist, noe som gir saken større betydning i forhold til kildevernet enn Liberty-saken. Problemstillingen var om det at den tyske stat hadde gitt overvåkningstjenesten hjemmel for å drive strategisk overvåkning av kommunikasjon for å avsløre og avverge alvorlige angrep på rikets sikkerhet, var et inngrep i journalisters rett til ytringsfrihet og kildevern.

I utgangspunktet er bruk av etterforskningsmetoder som rammer kommunikasjonen mellom journalist og kilde, slik at kilders identitet kan avsløres, et inngrep i ytringsfriheten etter EMK artikkel 10. Men, i denne saken var spørsmålet om lagringen likevel kunne tillates selv om den innebar en trussel for kildevernet fordi det ikke ble foretatt en generell lagring av kommunikasjon. Kommunikasjon ble kun ble lagret etter en gjennomgående siling og analyse av disse dataene. Først dersom visse kriterier var

[188] Schartum, 2010, Fagbokforlaget
[189] Malone v. The United Kingdom, §84
[190] Nathan Eagle, 2009

oppfylt, ble det foretatt lagring. EMD uttalte under henvisning til tidligere praksis om retten til kildevern:

> ”The applicant communicated with persons she wished to interview on subjects such as drugs and arms trafficking or preparations for war, which were also the focus of strategic monitoring. Consequently, there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone.” [191]

Domstolen foretok her en konkret vurdering, hvor de påså at inngrepet var proporsjonalt i forhold til formålet. I forhold til artikkel 10 nr. 2, om inngrepet kunne anses ”nødvendig i et demokratisk samfunn,” så domstolen det som avgjørende at den strategiske overvåkningen ikke var rettet mot journalister eller mot å avdekke deres kilder. Den var en utilsiktet konsekvens av at andre personers telefoner var underlagt kontroll. Dette var i følge EMD et langt mindre alvorlig inngrep, og man kunne i utgangspunktet ikke kreve at det nasjonale regelverket måtte inneholde særlige regler for å kunne beskytte kilders identitet i slike tilfeller.[192] EMD har som tidligere nevnt gitt medlemsstatene en viss ”margin of appreciation”.

I proposisjon 49 L (2010-2011), ble det uttalt i forhold til den ovennevnte saken at:

> ”Avgjørelsen av om inngrepet likevel er uforholdsmessig må antas å bero på en vurdering av om regelverket er egnet til å sikre at inngrepene begrenser seg til det som var nødvendig for å oppnå det aktuelle formålet, og da særlig om vilkårene for inngrepet er tilstrekkelige og effektive med hensyn til å begrense avsløringen av journalisters kilder til et uunngåelig minimum.”

Kildevernets betydning og EMDs forholdsmessighetsvurdering blir altså igjen understreket. Den konkrete vurderingen som må foretas i forhold til implementeringen av datalagringsdirektivet, gjelder en formålsrettet lagring av kommunikasjonsdata. I forhold til de reglene som har kommet om implementering av datalagringsdirektivet blir det ikke foretatt noen siling i forhold til lagringen. Alt blir lagret. Hvis man ser på hva EMD sier i følge blant annet Weber og Saravia-saken, så kan man tolke det dit hen at en slik generell lagring som datalagringsdirektivet oppstiller ikke er forenlig med EMD, en tolkning som blant annet støttes av Jon Wessel-Aas[193]

---

[191] Weber og Saravia mot Tyskland premiss 145.
[192] Ibid, premiss 151.
[193] Schartum, 2010, Fagbokforlaget

EMD har også gått sterkt ut når det gjelder allmenn lagring av opplysninger. I S og Marper-dommen[194], som gjaldt myndighetenes fortsatte lagring av DNA-profiler etter at de mistenkte hadde blitt renvasket, uttalte retten at:

> "…the Court is struck by the blanket and indiscriminate nature of the power of retention"[195]

Retten fant her Statens anførsel, om at lagringen ikke ville ha noen betydning så lenge de mistenkte ikke gjorde noe straffbart i fremtiden som ville knytte dem til en kriminell handling, uakseptabel. EMDs vurdering her i forhold til allmenn lagring av informasjon, understreker hvor stort inngrep lagring av data er.

4.1.3 Oppsummering

Argumentene som taler for lagring av data er mange. Politi- og påtalemyndighet vil kunne ha stor nytte av at slike data blir lagret i en lengre periode i etterforskningssammenheng. Nøyaktig hvor stor nytteeffekt de vil gi er derimot ikke avklart siden vi foreløpig vet for lite om dette. At det trengs mer forskning og statistikk på dette er tydelig. Kripos foretok en kvantitativ undersøkelse av bruk av trafikkdata i mars 2010, som omhandlet bestemte sakstyper. Denne undersøkelsen var begrenset til saker fra 2008 som hadde ført til en positiv påtaleavgjørelse.[196] Selv om resultatene fra denne undersøkelsen viste at kommunikasjonsdata hadde stor nytte, så gir ikke undersøkelsen et fullstendig bilde av bruken av trafikkdata i alvorlige kriminalitetssaker. Dette ble også presisert av Kripos i vedlegg 1 i høringssvaret.

EMD har i de senere år, gitt uttrykk for at kildevernet har et svært sterkt vern i forhold til de viktige hensyn det skal ivareta som blant annet ytringsfrihet. Etter min forståelse, så er ikke hensynet til oppklaring av alvolig kriminalitet tungtveiende nok, til å gjøre opp for det "presserende samfunnsmessige behovet" kildevernet beskytter i henhold til ytringsfriheten.

---

[194] S and Marper v. The United Kingdom
[195] Ibid, premiss 119
[196] Høringssvar fra Kripos angående datalagringsdirektivet.

Selv om EMD operer med en såkalt "dynamisk tolkningsstil", noe som innebærer at rettighetene de beskytter må tolkes i lys av samfunnsutviklingen i medlemslandene,[197] kan jeg ikke se at de trusler vi opplever idag kan forsvares med så inngripende tiltak. Ordlyden i konvensjonsteksten setter også en grense mot hvor langt EMD kan strekke seg i forhold til en harmonisering med datalagringsdirektivet.

Jon Wessel-Aas nevner i en artikkel[198] muligheten for at EMD kan finne at "present day conditions" er så dramatisk endret i de senere år at de likevel vil tillate lagring til tross for tradisjonelle personvern- og rettsstatsprinsipper. At EMD skulle endre sin praksis i forhold til de rettigheter de har oppstilt mot personvern og kildevern de siste årene virker usannsynlig. Spesielt på grunn av at en slik allmenn lagring ikke tar hensyn til spesielt beskyttede grupper som for eksempel pressens medarbeidere. Den samme vurderingen kan foretas i forhold til andre grupper med taushetsplikt, for eksempel advokater, leger, prester, psykologer etc, men det er ikke en del av min problemstilling.

Sett i sammenheng med kildevernet og den "chilling effect"[199] som lagring av data gir, kan jeg ikke se at en allmenn lagring av data, til tross for nytteverdien den gir ved etterforskning av alvolig kriminalitet, kan sies å være forholdsmessig nok til å tillate et inngrep i EMKs artikkel 10 første ledd.

Etter dette finner jeg at en allmenn lagring av trafikk- og lokalisasjonsdata ikke kan gjennomføres uten å komme i strid med EMK artikkel 10 nr.1.

4.2 Gir rettsikkerhetsgarantier og domstolskontroll god nok beskyttelse?

4.2.1 Innledning og forutsetninger

Hvis sikkerheten rundt lagring av data, som diskutert i forrige kapittel, ikke er god nok, har det liten hensikt å vurdere spørsmålene rundt rettsikkerhetsgarantier og domstolskontroll på grunn av muligheten for at dataene kan havne i gale hender og dermed kan bli brukt til uønskede formål. Derfor når jeg nå skal vurdere om de krav som så langt er stilt av lovgiver om uthenting, er gode nok i forhold til de krav EMK og norsk rett setter i forhold til kildevernet, så forutsetter jeg en situasjon der lagringen er

[197] Tyrer mot Storbritannia 1978
[198] Schartum, 2010 Fagbokforlaget.
[199] Se punkt:4.2.3

sikret på en forsvarlig og hensiktsmessig måte. Kravene er *gode nok*, om de gir et tilfredsstillende vern av kildevernet.

4.2.2 Proporsjonalitetsvurderingen

Siden kravene til lovmessighet og formålsmessighet er oppfylt etter EMK artikkel 10, så vil jeg her vurdere om de rettsikkerhetsgarantier som norsk lov setter i forbindelse med uthenting av data i henhold til direktivet oppfyller de krav til nødvendighet og proporsjonalitet som EMK artikkel 10 nr. 2 stiller. Jeg vil først ta for meg de forskjellige rettsikkerhetsgarantiene, deriblant domstolskontrollen, før jeg avslutter med å vurdere om disse oppfyller kravet til proporsjonalitet etter EMK artikkel 10 nr. 2.

4.2.2.1 Rettsikkerhetsgarantiene

Underretting om uthenting av opplysninger

En sentral rettssikkerhetsgaranti er at mistenkte skal underrettes om uthenting av opplysninger som gjelder han, med mindre retten beslutter at underrettingen skal utsettes. I så fall skal det straks oppnevnes en offentlig advokat for mistenkte. Se straffeprosessloven § 100 a. Det at det oppnevnes en advokat for mistenkte når han selv ikke er klar over at det blir uthentet kommunikasjonsdata om seg begrunnes i kontradiksjonshensyn. Da kan advokaten ivareta den mistenktes rettigheter og påse at vilkårene for utleveringspålegg er oppfylt.[200]

Krav om autorisert personell

Kravet til autorisert personell har jeg behandlet i punkt 2.2.5. At det er satt krav til hvem som skal behandle kommunikasjonsdata er ikke overraskende, siden man ved et slikt påbud tvinger frem strenge krav om hvem som kan gis den tilliten det er å behandle så sensitiv informasjon. Det er klart at tilgangen til så sensitiv informasjon som innsamlingen av data i forhold til implementeringen av datalagringsdirektivet fører til, krever en særskilt beskyttelse. Det er også bakgrunnen for at man ønsker å begrense antall personer med slik autorisert tilgang til et minimum.

[200] Innst. 275 L (2010–2011), punkt 1.2

Krav om sporbarhet

Som et virkemiddel for å forhindre uautorisert bruk av lagrede data, så ble det forutsatt i innstillingen til Stortinget[201] at enhver bruk av de lagrede data skulle loggføres. Dette er nå hjemlet i utkast til datalagringsforskrift § 3-2 som bestemmer at ”Enhver behandling av lagringspliktige data skal dokumenteres i egen logg.” Loggen skal inneholde hva som er gjort med dataene, når dette skjedde, hvem som har behandlet dataene, hvem de er utlevert til og ”entydig identifisering” av pålegget om utlevering. Videre så skal loggen oppbevares i tre år. Det er gjort unntak fra loggføring når det gjelder ”tilføring eller sletting av lagringspliktige data med hjemmel i ekomloven § 2-7a første ledd eller § 2-7 annet ledd.”

Det at nesten all tilgang loggføres gjør også at muligheten for autorisert personell til å gå uhjemlet inn på lagrede data begrenses. Dette øker sikkerheten på de dataene som er lagret, siden dette vil gjøre det mindre attraktivt å misbruke den tilgangen som er gitt gjennom autorisasjonen. Det vil altså bli mindre fristende å motta bestikkelser, for eksempel fra kommersielle aktører, siden muligheten for oppdagelse vil være stor.

Hypotetisk, kan kommersielle aktører, være villig til å betale store summer for å få tilgang til kommunikasjonsdataene fra for eksempel en journalist. Dette kan være aktuelt for eksempel ved at en avis eller en annen nyhetskanal har avdekket at en bedrift bedriver giftdumping, eller blir beskyldt for korrupsjon. Denne bedriften kan hypotetisk være villig til å strekke seg langt for å få tilgang til hvem i bedriften som står bak lekkasjen. PST har selv uttalt at industrispionasje og hacking av databaser er en av de største truslene vi har mot vår nasjonale sikkerhet.[202] Dette gjør at det ikke bare er uautorisert tilgang fra autorisert personell vi må være på vakt etter.

Meldeplikt og tilsynsordning

Etter utkastet til datalagringsforskrift, så er det Post- og teletilsynet (gjennom samferdselsdepartementet) som skal føre tilsyn med de bestemmelsene som er angitt i forskriften. Dette er også hjemlet i ekomlovens § 10-1,

[201] Innst. 275 L (2010–2011)
[202] Jon Wessel Aas 12.04.2012 og http://www.pst.no/trusler/spionasje/

Når det gjelder lagringspliktige subjekter etter ekomloven så skal de data som lagres etter ekomloven § 2-7a første ledd være underlagt pliktene i ekomloven § 2-7 om kommunikasjonsvern og § 2-9 om taushetsplikt. Når det gjelder § 2-7a så vil også personopplysningsloven § 13 om informasjonssikkerhet og § 14 om internkontroll være hjemmel for behandlingsansvarlige av data etter ekomloven.[203]

Datatilsynet fører i dag kontroll etter personopplysningsloven. På grunn av den store kontroversen innføringen av direktivet førte med seg, er det gitt uttrykk for, blant annet i forarbeidene, at Datatilsynet i forbindelse med implementeringen skal styrke sin kontrollvirksomhet mot ekomtilbydere og justissektoren,

Videre har Datatilsynet fått i oppgave av Fornyings-, administrasjons- og kirkedepartementet å vurdere hvorvidt det er behov for kryptering av lagringspliktige data. Dette kom som et resultat av en avtale mellom Høyre og Arbeiderpartiet om Prop. 49 L (2010-2011).[204] I tillegg er det bestemt at det skal være krav om kryptering når det gjelder forsendelse av data til andre medlemsstater i EØS. Etter forarbeidene skal overføring av personopplysninger til utlandet også meldes til Datatilsynet. Datatilsynet skal også utarbeide forslag til hvilke andre områder det kan være behov for kryptering.

Nøyaktig hvilke oppgaver Datatilsynet har fått som resultat av implementeringen av direktivet er jeg ikke sikker på. Men det var enighet blant flertallet i Stortinget som stemte for implementeringen at det var viktig at de data som lagres gis nødvendig sikring.

Sikker lagring

Dersom vi først skal gjennomføre datalagringsdirektivet i norsk rett er det viktig at vi gjør dette på en forsvarlig måte. Det er en prosess som tar tid. Å lage gode datasystemer i forhold til sikkerhet og kryptering og en forsvarlig brukerbehandling er en omfattende prosess. Derfor er det viktig at vi hører på de som har erfaring på dette området og ikke stresser med å få til en rask gjennomføring. Bransjeforeningen IKT Norge, mener innføringen bør utsettes i nærmere 3 år.[205] I løpet av denne tiden vil vi ha opparbeidet mye mer kunnskap om nytten ved direktivet, og vil i tillegg ha et mer solid og trygt

[203] Utkast datalagringsforskrift, punkt 5.
[204] Avtale mellom Arbeiderpartiet og Høyre om Prop. 49 L (2010-2011)
[205] Færaas, 2012

verktøy til å hjelpe oss med lagringen. At vi ikke presser fram en hurtig gjennomføring vil etter min mening har stor betydning for dataenes sikkerhet i lagringsøyemed.

4.2.2.2 Krav om kjennelse (Domstolskontrollen)

Innledning

Selv om kravet om kjennelse er en rettsikkerhetsgaranti har jeg valgt å behandle denne under et eget punkt på grunn av dens store betydning i forhold til ivaretakelsen av de verdier som blant annet EMK artikkel 10 nr. 1 dekker.

I kapittel 2.2.6 har jeg tatt for meg hvilke lovregler som foreligger for å kunne hente ut data som blir lagret etter implementeringen av direktivet. Jeg vil ikke gjenta hvilke krav som gjelder for at domstolene skal kunne foreta utlevering av data, men nøyer meg med å henvise tilbake til dette kapittelet.

Med unntak av de opplysninger (abonnements- og brukerdata), som kan hentes ut etter ekomlovens § 2-9, kreves det altså som hovedregel kjennelse fra retten før politi eller påtalemyndighet kan få utlevert kommunikasjonsdata og lokalisasjonsdata. Et unntak fra dette er Politiets sikkerhetstjeneste som har hastekompetanse som trer inn i stedet for kjennelse fra domstolene.

Forholdsmessighetsvurderingen etter straffeprosessloven § 170a.

Straffeprosessloven § 170 a, lyder som følger:

> ”Et tvangsmiddel kan brukes bare når det er tilstrekkelig grunn til det. Tvangsmidlet kan ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep. ”

§ 170 a er en generell hensikt- og forholdsmessighetsvurdering som skal foretas ved bruk av ethvert tvangsmiddel, herunder også utlevering av data. Uthenting av trafikkdata og lokalisasjonsdata, kan bare skje etter at domstolene har foretatt en konkret vurdering av utleveringsbegjæringen mot hvorvidt det finnes andre alternative, mindre inngripende virkemidler. Domstolene vil her blant annet måtte vektlegge personvernhensyn i forhold til hvor alvorlig den konkrete handlingen begjæringen skal forsvare er. Videre vil hvor viktig utleveringen er for etterforskningen spille en rolle. Disse momentene vil også ha betydning for vurderingen i forhold til hvor langt tilbake i

tid man skal kunne utlevere data. Det at implementeringen av direktivet gir hjemmel for at det kan begjæres uthenting av data for seks måneder med lagring vil ikke si at domstolene behøver å utlevere data for hele denne perioden. Dette vil være en del av den forholdsmessighetsvurderingen de må foreta. Andre avgrensningsmuligheter retten kan bruke, er å begrense antall personer det skal innhentes data om eller legge begrensninger på tidspunkt og sted. Når det gjelder basestasjonssøk, så vil også befolkningstettheten i det geografiske området det ønskes data fra ha betydning.[206]

Metodekontrollutvalget[207] har uttalt at hensynet til pressens kildevern og EMDs syn på dette bør gjøres til momenter i forholdsmessighetsvurderingen etter § 170 a. På denne måten kan man unngå å komme i konflikt med EMK artikkel 10.[208]

De momenter som allerede finnes i norsk lovgivning i straffeprosessloven § 125 og tvisteloven § 22-11vil kunne bli viktige i spørsmålet om hvorvidt det er "tilstrekkelig grunn til" å tillate uthenting av data. Dersom det finnes rettslig grunnlag i norsk rett til å fravike kildevernet så er dette et svært sterkt moment til hvorvidt man kan tillate bruk av tvangsmidler etter § 170 a og dermed foreta uthenting av data.

4.2.3 De indirekte skadevirkningene / "The Chilling effect"

Implementeringen av datalagringsdirektivet vil ikke bare ha direkte skadevirkninger. Et problem er at mulige kilder i frykt for lekkasje ikke lenger kommer til pressen med aktuelle saker. Dersom de forholder seg tause i frykt for avsløring, vil kanskje informasjon av samfunnsmessig betydning aldri komme fram.

Selv om Domstolene avskjærer politiets tilgang til uthenting av data på grunn av at det gjelder kommunikasjonsdata til en journalist, så løser ikke dette problemet i seg selv. Her kan man ta utgangspunkt i en hypotetisk situasjon: Dersom politiet gjennom å lese et oppslag i pressen får rettet fokus mot en spesiell kriminell gruppe, så kan de gjennom etterforskning snevre ned antall mulige "kilder" til denne "lekkasjen." De kan deretter kreve uthenting av kommunikasjonsdata fra et fåtall av personer, begrunnet i etterforskingsøyemed. Politiet kan altså fortsatt kunne få bekreftet at en mistenkt person

[206] Prop. 49 L (2010-2011)
[207] Et utvalg opprettet av justis- og beredskapsdepartementet for å etterkontrollere lovgivningen om politiets inngripende etterforskningsmetoder, slik som for eksempel kommunikasjonskontroll.
[208] NOU 2009:15 kapittel 28.7

har vært i kontakt med den aktuelle journalist gjennom uthenting av data fra den mistenkte selv. Dette kan de få vite gjennom at de får oversikt over hvem den mistenkte har vært i kontakt med, gjennom såkalte "B-nummer" [209]. Dommeren som sitter og skal foreta vurderingen vil ikke her nødvendigvis ha kunnskap om forbindelsen til pressen noe som gjør at han ikke sitter på informasjon som er svært relevant i helhetsvurderingen i forhold til uthenting. Dette kan da føre til at han gir tilgang til uthenting av kommunikasjonsdataene, selv om det i utgangpunktet gjelder data beskyttet både etter Grunnloven og EMK. Dette er en enkel måte for politiet å få tak i regler som i utgangspunktet er beskyttet gjennom kildevernet, noe som kan medføre en "chilling effect".

Det er viktig å huske at kildevernet ikke bare er til for *pressens skyld*. Det er like fullt, om ikke mer, et vern for den alminnelige borger. Hvis ikke ytreren har sikkerhet for sin anonymitet når han går til media, så kan det hende at kritikkverdige forhold aldri ser dagens lys, og fortsetter å være ukjent for offentligheten. Dette er en del av grunnlaget for et åpent og demokratisk samfunn og en av grunnene til at man populært kaller pressen den "fjerde" statsmakt.

I Runesteinsaken som jeg omtalte i kapittel 3.3.6.1, la Høyesterett stor vekt på EMDs vurderinger i forhold til "the chilling effect":

> "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 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."[210]

Det vi kan trekke ut av om dette er at *the chilling effect* har stor betydning i den helhetsvurderingen domstolene må foreta i forhold til hvorvidt uthenting av data kan foretas. Dette gjør også at det blir særdeles viktig at lagringen foregår på en forsvarlig og sikker måte.

---

[209] Se avsnitt 2.2.2, om hva som lagres.
[210] Runesteinsaken premiss 62.

4.2.4 Oppsummering

At de bestemmelser om rettsikkerhetsom er foreslått i forhold til lagring og uthenting av data blir innført, er nok et minstekrav om man skal beholde den posisjon kildevernet er gitt både i norsk lovgivning, EMK og etter praksis fra EMD.

Det at det er innført vaktordning ved Oslo tingrett slik at saksbehandlingen vedrørende uthenting av data skal kunne skje raskest mulig[211] er også en viktig del av den sikkerhet som ligger i at hjemmel for utlevering blir kontrollert av et uavhengig organ.

Norge har tatt mange steg i retning av å harmonisere gjennomføringen av datalagringsdirektivet med EMK. Det som gjenstår er blant annet å finne gode nok lagringsløsninger og krypteringsmåter for å sikre den lagrede informasjonen på en god måte. Så lenge man godtar at en slik lagring harmoniserer med EMK, så er det kun trusselen som ligger i "the chilling effect" som gjenstår i forhold til kildevernet.

Man kan aldri garantere 100 prosent at lagrede data ikke kommer på avveie eller at uthentingshjemler ikke blir misbrukt. Dette er det vanskeligste ved å skulle harmonisere reglene i EMK med datalagringsdirektivet. For å oppnå en harmonisering må man finne en balanse mellom en generell lagring av opplysninger og kontroll- og tilsynsordninger.

Inngrepets nytteverdi har helt klart avgjørende betydning i forhold til hvilken konklusjon EMD vil komme til etter proporsjonalitetsvurderingen i artikkel 10 nr.2. Etter min oppfatning av hvor sterkt EMD har vektlagt beskyttelsen av kildevernet tidligere, så kan jeg ikke se for meg at det vil tillates uthenting av kommunikasjonsopplysninger og lokalisasjonsopplysninger så lenge det er snakk om data som kommer fra massemedia.

Dersom norske domstoler opprettholder sin praksis om å benytte samme tolkningsprinsipper som EMD i forhold til EMK[212] så kan jeg heller ikke se at dette blir et problem i forhold til domstolskontrollen. Domstolen kan da stoppe uthenting av data som stammer *direkte* fra *pressefolk.* Selv om det ideelt sett hadde vært ønskelig med klarere regler for beskyttelse av pressens kilder i forhold til uthenting av data. Et sted

---

[211] Utkast datalagringsforskrift
[212] Rt 2002 s.557

kontroll- og tilsynsordningene ikke vil gi god nok beskyttelse er der politiet går direkte på kilden for å få bekreftet kontakt med pressen. Som jeg omtalte i forrige kapittel, kapittel 4.2.3, så er dette en situasjon hvor kildevernet ikke får den beskyttelsen det har krav på.

Som jeg har prøvd å vise, blant annet gjennom eksempler fra rettspraksis fra EMD, i blant annet kapittel 3.4.2 og 4.1.2.så er mitt syn at svaret på hvorvidt rettsikkerhetsgarantier og domstolskontroll kan opprettholde den beskyttelsen kildevernet har i dag antagelig nei. Det er ikke tvilsomt at man med tilsyns- og kontrollordninger kommer svært langt i forhold til å gjøre opp for det inngrepet lagring av data gir, men etter min oppfatning er de hensyn som ligger bak kildevernet, så tungtveiende, at de ikke er forholdsmessige i forhold til en systematisk masselagring av data.

Spørsmålet man da må stille, er om de løsninger som kan utvikles ved hjelp av kontroll og tilsynsordninger gjør at datalagringsdirektivet kan godtas etter en helhetsvurdering på bakgrunn av "present day conditions".[213] Denne muligheten beholder jeg åpen, da jeg finner det vanskelig å konkludere. Et vurderingsmoment her, er at det kreves bedre kunnskap enn den vi har i dag om den nytten datalagringsdirektivet gir i relasjon til oppklaring av alvorlig kriminalitet.

5 Avsluttende kommentar.

Arbeidet med denne avhandlingen har vært en spennende prosess og har gitt meg et mye større innblikk i problemstillinger innføringen av datalagringsdirektivet har skapt i norsk rett. Mine vurderinger har i hovedsak har gått inn under nødvendighetsvurderingen etter EMK artikkel 10 nr.2, noe som har ført til at jeg har lagt stor vekt på rettspraksis fra EMD. Det skal bli spennende å følge utviklingen til direktivet både her i Norge og i Europa ellers fremover.

[213] Se punkt:4.1.3

6 Litteraturliste

Lover

1902 Almindelig borgerlig Straffelov (Straffeloven) 22. mai nr. 10

1915 Lov om rettergangsmåten for tvistemål (tvistemålsloven). 13. august 1915 nr 06. (opphevet)

1981 Lov om rettergangsmåten i straffesaker (Straffeprosessloven) 22. mai 1981 nr. 25

1988 Lov om utlendingers adgang til riket og deres opphold her (utlendingsloven). 24. juni

1988 nr. 64

1992 Lov om kringkasting [kringkastingsloven]. 04. desember 1992 nr. 127

1995 Lov om politiet (politiloven) 4 august 1995 nr 53

1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven av 21. mai 1999 nr. 30

2000 Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31

2003 Lov om elektronisk kommunikasjon (ekomloven). 04. juli 2003 nr. 83

2005 Lov om straff (straffeloven) 20 mai nr. 28

2005 Lov om mekling og rettergang i sivile tvister (tvisteloven). 17. juni 2005 nr. 90

2010 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) 28. mai 2010 nr. 16

2011 Lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) (Endringslov om datalagringsdirektivet) 15.april 2011
(Lovvedtak 46 (2010–2011)

Forarbeider

Prop. 1 S (2011–2012), http://www.regjeringen.no/mobil/nb/dep/jd/dok/regpubl/prop/2011-2012/prop-1-s-20112012/6.html?id=657484 (Sist hentet ut 24.04.2012)

Prop. 49 L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Ot.prp. nr. 76 (2004-2005) Om lov om endringar i lov 4. desember 1992 nr. 127 om kringkasting

Ot.prp. nr. 55 (1997-98) Om lov om endringer i rettergangslovene m m (kildevern og offentlighet i rettspleien)

NOU 2011:12 Ytringsfrihet og ansvar i en ny mediehverdag.

NOU 2009:15 Skjult informasjon – åpen kontroll (Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker)

NOU 2009: 1: Individ og integritet: Personvern i det digitale samfunnet.

NOU 2003:27 Lovtiltak mot datakriminalitet. Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi

NOU 2001:32 Rett på sak

NOU 1999:27 ”Ytringsfrihed bør finde Sted” Forslag til ny Grunnlov § 100

NOU 1988:2 s 21.

Høring - Utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften) Fastsatt av Post- og teletilsynet med hjemmel i lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83 §§ 2-7, 2-7a, og 2-8.

Innst 275 L (2010-2011): Innstilling fra transport- og kommunikasjonskomiteen om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Innst. O. nr 37 (1980-81)

St.meld. nr. 26 (2003-2004) Om endring av Grunnloven § 100

Traktater og konvensjoner

EMK Den europeiske menneskerettskonvensjonen, Roma 1950

EU direktiver

EU-direktiv 1995/46/EF: Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)

EU-direktiv 2002/58/EF: Europaparlaments- og rådsdirektiv av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon)

Europa-parlamentets og rådets direktiv 2006/24/EF

Europarådets konvensjoner

Vienna Convention on the Law of Treaties av 23. Mai 1969

Europarådets konvensjon av 20. januar 1981 nr. 108 om personvern i forbindelse med elektronisk behandling av personopplysninger,

Europarådets konvensjon av 8. November 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

Rettspraksis

Norsk rettspraksis

- Rt 1953 s. 127 (Hall-Hofsø-saken)
- Rt 1966 s 176. (Klepplandsaken)
- Rt 1977 s.966 (Politimannsaken
- Rt 1987 s. 910
- Rt 1992 s.39
- Rt 1996 s. 1164.
- Rt 1996 s.1375 (MC-fotosaken)
- Rt 2002 s. 557
- Rt 2003 s. 928 (Tønsberg Blad-saken)
- Rt 2004 s1400 (Dørvaktskjennelsen)
- Rt 2010 s 774
- Rt 2010 s. 1150
- Rt 2010 s 1381 (Runesteinsaken)
- Rt 2010 s 1945
- Rt 2011 s.1266

EMD-dommer

- Handyside v. United Kingdom, The European Court of Human Rights, Strasbourg, 7. desember 1976
- Klass and Others v. Germany, The European Court of Human rights, Strasbourg, 6. september 1978
- Sunday Times v. United Kingdom, The European Court of Human Rights, Strasbourg 26. april 1979
- Leander v. Sweden, The European Court of Human Rights, Strasbourg, 26. mars 1987
- Observer and Guardian v. the United Kingdom judgment of 26 November 1991
- Vogt v. Germany, The European Court of Human Rights, Strasbourg, 26. September 1995
- Goodwin v. The United Kingdom, The European Court of Human Rights, Strasbourg 27. Mars 1996
- Weber and Saravia v. Germany, The European Court of Human Rights, Strasbourg, 29. juni 2006
- Case of Stoll v. Switzerland, The European Court of Human Rights, Strasbourg, 10 December 2007
- Liberty and Others v. United Kingdom, The European Court of Human Rights, Strasbourg, 1. juli 2008
- S. and Marper v. United Kingdom, The European Court of Human Rights, Strasbourg 4. desember 2008
- Financial Times Ltd and others. V. The United Kingdom, The European Court of Human Rights, Strasbourg 15. Desember 2009

Juridisk litteratur

Aal, Jørgen, Kommentar til Ekomloven: Norsk lovkommentar nettversjon (Sist hentet ut 23.04.2012)

Andenæs 2009 Norsk straffeprosess (4.utg) Universitetsforlaget 2009

Eggen, Kyrre, Ytringsfrihet, 1.utg, J.W. Cappelens Forlag a.s, Oslo 2002

Høstmælingen, Njål, Internasjonale menneskerettigheter, 3.opplag, Universitetsforlaget, 2003

Lindahl, Ina. Massemedienes kildevern. Bergen 2009

Lindahl, Ina. Pressens kildevern. Særavhandling. Juridisk fakultet , Oslo 1999.

Manshaus, Halvor I Lov§Data nr.105-Mars 2011.

Møse, Erik, Kommentar til Ekomloven: Norsk lovkommentar nettversjon (Sist hentet ut 23.04.2012)

Nordeide, Ragnar: Kommentar til Ekomloven: Norsk lovkommentar nettversjon (Sist hentet ut 23.04.2012)

Wessel-Aas, Jon: Datalagringsdirektivet, I Schartum, Fagbokforlaget, Bergen 2010,

Wessel Aas, Jon: I blogginnlegget: Pressens kildevern utvides i ny dom fra Menneskerettsdomstolen: http://www.uhuru.biz/?p=29 (Sist hentet ut 23.04.2012)

Wessel-Aas, Jon, Ytringsfrihet: EMD befester kildevernet. I: Jusnytt 16. september 2010

Andre kilder

Artikkel 29-gruppen vedrørende databeskyttelse, 2005 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_en.pdf (sist hentet ut 22.04.2012)

Datatilsynets årsmelding fra 2007

Declaration on Combating Terrorism of 25 March 2004

Europaportalen: Revisjon av datalagringsdirektivet, 2011 http://www.regjeringen.no/nb/sub/europaportalen/eos-notatbasen/notatene/2011/okt/datalagring---revisjon.html?id=661439

Færaas, IKT-bransjen vil utsette datalagringsdirektivet i tre år. I Aftenposten, 18.04.2012 http://www.aftenposten.no/nyheter/iriks/IKT-bransjen-vil-utsette-

datalagringsdirektivet-i-tre-ar-6808486.html#.T5VqEdU2c21 (Sist hentet ut 24.04.2012)

Lillesund, Datatilsynet anmelder Talkmore, I Computerworld 13.11.2007 http://www.idg.no/bransje/bransjenyheter/article75163.ece Sist hentet ut 24.04.2012)

Nathan Eagle, 2009 http://reality.media.mit.edu/dyads.php (Sist hentet ut, 20.04.2012)

Norsk Redaktørforening, Kildevern, 2011 http://www.nored.no/Juss/Kildevern (Sist hentet ut 24. 04 2012)

Teknologirådet. Fra rådet til tinget nr. 26, april 2010

Samferdselsdepartementet, notat om Datalagringsdirekivet. http://www.regjeringen.no/nb/dep/sd/tema/telekommunikasjon/datalagringsdirektivet.html?id=666723 (Sist hentet ut 24.04.2012)

Samtale med Jon Wessel-Aas. 12.04.2012 (Advokat og leder i den internasjonale juristkommisjonens norske avdeling)

Sunnanå, Lars Magne. Brukte én time på å finne flere datahull hos staten. I Aftenposten 21.03.2012. http://www.aftenposten.no/okonomi/innland/Brukte-n-time-pa-a-finne-flere-datahull-hos-staten-6790346.html#.T4hJ6tW8XoY (Sist hentet ut 24.04.2012)

Veiledningen til Europarådets "Rekommandasjon (2000) 7"

Vær Varsom Plakaten, Norsk presseforbund. 2012 http://presse.no/Etisk-regelverk/Vaer-Varsom-plakaten (Sist hentet ut 24.04.2012)

7 Lister over tabeller og figurer m v

Se http://www.ub.uio.no/ujur/henvisninger/