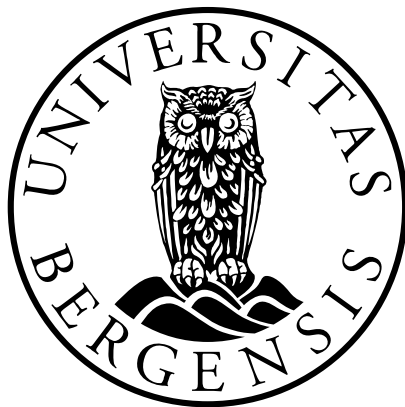


Kildevernets stilling etter innføring av Etterretningstjenestens adgang til tilrettelagt innhenting

*Er kildevernet i etterretningstjenesteloven
forenlig med EMK Artikkel 10?*

Kandidatnummer: 157

Antall ord: 14 989



JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

11.12.2023

Innholdsfortegnelse

1	Innledning	3
1.1	Tema og problemstilling	3
1.2	Tilrettelagt innhenting – system og terminologi	6
1.3	Metode og rettskildebildet	9
1.4	Avgrensninger	11
1.5	Videre fremstilling	13
2	Rettslige utgangspunkter	14
2.1	Generelt om kildevernet etter EMK Artikkel 10	14
2.2	Nærmere om EMDs krav til kildevern ved bulkinnhenting av elektronisk kommunikasjon	15
2.3	Tilrettelagt innhenting etter e-loven. De ulike stadiene av innhentingsprosessen og E-tjenestens tilgang til kildevernet materiale på disse	17
2.4	Hovedregelen om kildevern i e-loven § 5-2 og § 9-6.....	19
3	Kildevernets personkrets – hvilke aktører er vernet?	21
3.1	Opplysninger « <i>betrodd noen i deres journalistiske virke</i> ».....	21
3.2	Kildevernet i prosesslovgivningen	22
3.3	Utvikling og norsk rettspraksis – et styrket og teknologinøytralt kildevern	23
3.4	Menneskerettslige føringer etter EMD-praksis	24
3.5	Konklusjon og operasjonalisering av et EMK-forenlig kildevern	27
4	Vern av innholdet i journalistisk materiale – hvilke opplysninger er vernet?	29
4.1	Kravet om at opplysningen « <i>kan</i> » identifisere en kilde	29
4.2	Menneskerettslige føringer: Vern for opplysninger <i>egnet</i> til kildeavsløring	30
4.3	Konklusjon og operasjonalisering av et EMK-forenlig kildevern	33
5	Materielle og prosessuelle krav til E-tjenestens inngrep i kildevernet	35
5.1	Generelt om E-tjenestens adgang til inngrep.....	35
5.2	Inngrepet må ha hjemmel i lov	36
5.2.1	Krav om formell hjemmel i nasjonal rett.....	36
5.2.2	Lovens kvalitet (legalitet)	36
5.3	Inngrepet må forfølge et legitimt formål	38
5.4	Inngrepet må være nødvendig og forholdsmessig.....	39

5.4.1	Innledende om nødvendighet og forholdsmessighet ved kildeverninngrep under tilrettelagt innhenting.....	39
5.4.2	Lagring.....	41
5.4.3	Sletting.....	41
5.4.4	Deling	42
5.4.5	Domstolskontroll	43
5.4.6	EOS-utvalgets mandat	46
5.4.7	Samlet vurdering.....	47
6	Konklusjon og avsluttende betraktninger.....	49
6.1	Oppsummering og konklusjon	49
6.2	Avsluttende betraktninger	50
	Litteraturliste.....	52

1 Innledning

1.1 Tema og problemstilling

I 2020 la Stortinget frem ny etterretningstjenestelov (heretter e-loven), som gir oppdaterte regler for virksomhet og metoder for informasjonsinnhenting i etterretningstjenesten (heretter E-tjenesten).¹ Det ble samtidig vedtatt innføring av *tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon* (heretter «tilrettelagt innhenting»).

Tilrettelagt innhenting er et verktøy som på nærmere vilkår gir E-tjenesten tilgang til store mengder kommunikasjonsstrømmer som passerer landegrensen gjennom kabler og elektronisk infrastruktur. Innhenting skjer ved at ekomtilbydere pålegges en plikt til å speile og gjøre tilgjengelig utvalgte kommunikasjonsstrømmer for E-tjenesten.² Fordi kommunikasjonsstrømmene kan inneholde vernede data, gir loven særlige regler for hvordan E-tjenesten skal forholde seg til kildevern, herunder en rett for pressens kilder til å forbli anonyme i møte med mediene. Kildevern er en forutsetning for ytrings- og informasjonsfrihet som er vernet av Den europeiske menneskerettskonvensjonen (EMK) Artikkel 10.

Hovedregelen etter e-loven er derfor at kildeavslørende kommunikasjonsdata er vernet mot inngrep. Det kommer til uttrykk gjennom lovens § 9-6 første ledd, som oppstiller *behandlingsforbud* for kildevernet materiale. Vernet gjelder også allerede på *innhentingsstadiet*, ved at e-loven § 5-2 andre ledd oppstiller utgangspunktet om vern mot målrettet innhenting av kildevernet materiale. Temaet for avhandlingen er om kildevernet etter e-loven § 9-6 og § 5-2 er utformet i samsvar med EMK Artikkel 10.

Formålet med tilrettelagt innhenting er utenlandsetterretning, og det er informasjon som krysser landegrensen verktøyet tar sikte på å innhente.³ Formålsbegrensningen innebærer at E-tjenesten som hovedregel ikke skal innhente opplysninger om norske borgere. Det kommer til uttrykk i e-loven § 4-1 som oppstiller et generelt forbud mot å benytte lovens innhentingsmetoder overfor personer i Norge. Problemet med tilrettelagt innhenting er at det norske elektroniske kommunikasjonsnett i stor grad er tilknyttet servere/databaser i utlandet. Tilnærmet alle kommunikasjonskanaler nordmenn bruker, passerer følgelig landegrensen som

¹ Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven).

² Tilbydere som omfattes av ekomloven § 1-5 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten, jf. e-loven § 7-2, se nærmere i Prop. 80 L (2019–2020) s. 214.

³ E-loven § 7-1, jf. § 1-1; Prop. 80 L (2019–2020) s. 86 flg.

følge av nettets infrastruktur. Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon vil derfor innebære at også innenlands kommunikasjon, inkludert kildevernede data, kan bli gjenstand for innhenting og lagring.⁴

Det er samtidig utvilsomt behov for modernisering av E-tjenestens metoder i lys av dagens digitale trusselbilde. Norge er et av verdens mest digitaliserte land. Store deler av vår daglige kommunikasjon foregår over nett. Utviklingen gjør oss sårbar for moderne digitale trusler mot samfunnet og menneskerettighetene.⁵ Forsvarsdepartementet trekker frem særlig tre hovedtrusler: 1) Statlige og private aktører bruker i dag det digitale rom til angrep, sabotasje, påvirkning og spionasje, 2) digitale kommunikasjonsplattformer brukes til planlegging og koordinering av blant annet terrorhandlinger og 3) de fleste etterretningsmål kommuniserer i dag over nett.⁶ Effektiv sikkerhetstjeneste krever at myndighetenes metoder tilpasses slik at E-tjenesten kan operere på samme arena som trusselaktørene – nemlig det elektroniske kommunikasjonsnett.

Tilrettelagt innhenting skal bidra til å imøtegå moderne digitale sikkerhetstrusler i tråd med E-tjenestens formål om å beskytte nasjonale sikkerhetsinteresser, jf. e-loven § 1-1. Å ivareta Norges suverenitet, territorielle integritet, politiske handlefrihet samt borgeres rett til liv, frihet og sikkerhet er både en menneskerettslig plikt for myndighetene og i kjernen av E-tjenestens formål.⁷ Mer konkret skal tilrettelagt innhenting styrke myndighetenes evne til å oppdage, følge, varsle og motvirke utenlandske trusler mot Norge.⁸ Det innebærer at tilrettelagt innhenting er et tiltak i tråd med statens positive plikt til å beskytte demokratiske verdier under et moderne trusselbilde.⁹ For eksempel vil innhentede kommunikasjonsdata kunne bidra til å avdekke utenlandske hybride trusler og cyberangrep.

Ekomtilbydere, som pålegges såkalt tilretteleggingsplikt, er enhver som «omfattes av ekomloven § 1-5 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten».¹⁰ Tilretteleggingsplikten kan altså ramme tradisjonelle ekomtilbydere og kommunikasjonstjenester så vel som moderne digitale plattformer, fra

⁴ Prop. 92 L (2022-2023) s. 19.

⁵ Prop. 80 L (2019–2020) s. 88.

⁶ Høringsnotat fra Forsvarsdepartementet av 12. november 2018 side 193.

⁷ Grunnloven § 92, jf. EMK artikkel 1; e-loven § 1-1.

⁸ Prop. 80 L (2019–2020) s. 92.

⁹ Prop. 80 L (2019–2020) s. 18.

¹⁰ E-loven § 7-2; Prop. 80 L (2019–2020) s. 214. Plikten omfatter enhver tilbyder av elektronisk kommunikasjonsnett eller -tjeneste og såkalte over the top-tjenester (OTT-tjenester).

telefoni og telefonnett til sosiale medier som Facebook og Instagram samt medier, nettaviser og andre virksomheter som tilbyr kommunikasjonstjenester på nett. For folk flest er konsekvensen at myndighetene kan få tilgang til vår private kommunikasjon på nett. For ytrings- og informasjonsfriheten kan konsekvensen bli at brukere vegrer seg for å kommunisere digitalt.

Innføring av regler om tilrettelagt innhenting har vekket debatt og møtt motstand.¹¹ Det er ikke uten grunn. Systemet innebærer et grunnleggende skifte fra utgangspunktet om at E-tjenesten kun i unntakstilfeller befatter seg med nordmenns kommunikasjon, til at slik befatning ved tilrettelagt innhenting blir «hovedregelen» fordi innenlands kommunikasjon masselagres, også kjent som at det lagres i «bulk». Det representerer et avvik fra utgangspunktet i norsk rett om at staten ikke skal benytte inngripende virkemidler uten konkret mistanke om straffbar handling og etter en individuell vurdering fra en domstol.¹² Med det nye systemet er alle personer i Norge som kommuniserer på nettet i utgangspunktet utsatt for en uoverskuelig risiko for at E-tjenesten får tilgang på personlig kommunikasjonsdata. For medievirksomheter og andre selskaper som besitter fortrolig kommunikasjonsdata må en forvente at tilretteleggingsplikten ikke kan gjennomføres uten risiko for at kildevernets stilling svekkes.

Utgangspunktet er som nevnt at e-loven beskytter mot inngrep i kildevernet kommunikasjon, jf. § 9-6 første ledd og § 5-2 andre ledd. E-tjenesten kan likevel få tilgang på nærmere bestemte vilkår. Kildevernreglens formål er å treffe riktig balanse mellom de legitime interesser som gjør seg gjeldene.¹³ Et spørsmål som reiser seg er om hensynet til langsiktige konsekvenser for kildevernet står i fare for å overskygges av behovet for å beskytte den norske befolkning mot hybride trusler, cyberangrep og terror. Kildevern er som del av ytrings- og informasjonsfriheten en av grunnsteinene i et demokratisk samfunn.¹⁴ Det er avgjørende for sikring av en opplyst offentlig debatt at myndighetene ikke opererer på en måte som kan gi en nedkjølende effekt på borgernes ytringsvilje. Det er treffende at Den Europeiske menneskerettsdomstol (EMD) beskriver bulklagring for sikkerhetsformål som et dilemma

¹¹ Stiftelsen Tinius, hovedeier i Schibsted, har varslet søksmål mot staten om lovligheten av tilrettelagt innhenting. Flere norske presseorganisasjoner har tredd inn som partshjelpere. Se mer på Tinius.com.

¹² I samme retning NIMs høringsuttalelse om forslag til ny lov om Etterretningstjenesten, s. 5.

¹³ Prop. 80 L (2019–2020) s. 160.

¹⁴ Goodwin mot Storbritannia [GC] no. 17488/90 avsnitt 39.

hvor «*a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.*»¹⁵

Problemstillingen i denne avhandlingen er om e-lovens kildevernregler ved tilrettelagt innhenting er utformet i samsvar med EMK Artikkel 10. Avhandlingen undersøker utformingen av reglene i e-loven § 5-2 og § 9-6, med særlig fokus på § 9-6 som hovedregel for kildevernets innhold og rekkevidde etter e-loven. Oppgaven vil først analysere hva som skal til for at kommunikasjonsdata er underlagt det særlige vern kildevernreglene oppstiller (rettighetens rekkevidde), og dernest om reglene er forenlig med de krav EMK Artikkel 10 oppstiller for inngrep i kildevernet.

1.2 Tilrettelagt innhenting – system og terminologi

Analysen krever en kort forklaring av etterretningsverktøyet som e-loven kapittel 7 og 8 regulerer og relevante begrepsavklaringer.

Tilrettelagt innhenting er betegnelsen på et etterretningsverktøy som innebærer «masselagring (såkalt bulklagring) av metadata om elektronisk kommunikasjon som passerer den norske landegrensen».¹⁶ Lagringen skjer gjennom midtpunktinnhenting, det vil si innhenting av kommunikasjon i transitt mellom to endepunkter.¹⁷ Tilrettelagt innhenting er en form for midtpunktinnhenting som er avhengig av tilrettelegging fra ekomtilbydere.¹⁸ Fordi innhenting skiller seg fra annen midtpunktinnhenting ved at den i betydelig grad berører norsk innenlands kommunikasjon, er det gitt særregler for tilrettelagt innhenting i e-loven kapittel 7 og 8.¹⁹

Verktøyet tas i bruk ved at E-tjenesten pålegger en ekomtilbyder såkalt «tilretteleggingsplikt». Tilbyder skal speile og gjøre tilgjengelig utvalgte kommunikasjonsstrømmer slik at E-tjenesten kan kopiere og lagre metadataene i bulk.²⁰ Tillatelse til å pålegge

¹⁵ Big Brother Watch m.fl. mot Storbritannia [GC], no. 58170/13, 62322/14 og 24960/15 avsnitt 339.

¹⁶ Prop. 92 L (2022–2023) s. 22.

¹⁷ Prop. 80 L (2019–2020) s. 103.

¹⁸ Prop. 92 L (2022–2023) s. 22

¹⁹ Prop. 80 L (2019–2020) s. 106.

²⁰ E-loven § 7-2, jf. § 7-3.

tilretteleggingsplikt må gis av retten, jf. e-loven § 7-3. E-tjenesten får altså ikke direkte tilgang til bulklagret informasjon, men kan få tilgang etter domstolens tillatelse.²¹

Dataene som speiles skal lagres i bulk. Bulk er legaldefinert i e-loven § 1-3 første ledd bokstav i som «informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål». Formålet med bulklagring er å etablere informasjonsgrunnlag for etterretningsformål.²² Bulklagring bidrar til dette ved å muliggjøre analyse, utvalg og filtrering av kommunikasjonsdata i transitt (som ikke er teknisk mulig å analysere i sanntid). Dermed kan E-tjenesten senere gjøre søk etter etterretningsrelevant informasjon i en større informasjonssamling (bulken).²³ Tilrettelagt innhenting innebærer dermed en mulighet for storskala lagring av personopplysninger på myndighetenes hånd som ikke tidligere har forekommet i norsk rett.

Speiling av ekomtilbyders kommunikasjonsdata vil i praksis innhente «rådata». Rådata er «ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert.»²⁴ Når det er nødvendig for å etablere informasjonsgrunnlag for etterretningsformål, kan tilrettelagt innhenting iverksettes enten som grunnlag for søk etter «metadata» og/eller målrettet innhenting av «innholdsdata».²⁵

Tilrettelagt innhenting åpner for det første for innhenting og lagring av «metadata» i bulk. Metadata er «data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, herunder data som beskriver typen eller formatet på innholdet, hvem som er avsender og mottaker, og størrelse, tidspunkt og varighet for kommunikasjonen».²⁶ Bulkinnhenting skal ikke lagre innholdsdata.²⁷

I tillegg åpner verktøyet for målrettet innhenting og lagring av innholdsdata.²⁸ Innholdsdata er negativt definert og omfatter «data som ikke er metadata», jf. e-loven § 7-9. Innholdsdata sier noe om innholdet i dataene, og vil typisk inneholde opplysninger av mer sensitiv grad enn metadata. For eksempel kan det gjelde innholdet i en tekstmelding eller e-post. Innhenting og

²¹ Prop. 92 L (2022–2023) s. 22; Innst.402 L (2022–2023) s. 3.

²² E-loven § 7-3 første ledd første punktum.

²³ Prop. 92 L (2022–2023) s. 22.

²⁴ E-loven § 1-3 første ledd bokstav h.

²⁵ Se e-loven § 7-3 første ledd.

²⁶ Prop. 80 L (2019-2020) s. 109.

²⁷ Ibid s. 110.

²⁸ Ibid s. 92.

lagring av innholdsdata skal alltid regnes som «målrettet innhenting» etter loven.²⁹ Målrettet innhenting skiller seg ellers fra bulkinnhenting ved at det er «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål».³⁰

Tilrettelagt innhenting åpner altså for to typer innhenting: 1) innhenting og lagring av metadata i bulk og 2) målrettet innhenting og lagring av innholdsdata. I praksis er skillet sentralt fordi det innebærer at E-tjenesten ikke har faktisk tilgang til *innholdet* i kommunikasjonsdata før retten gir tillatelse til målrettet innhenting. Vel og merke kan også metadata være kildeavslørende, for eksempel dersom innhenting avdekker IP-adressen til en kilde. For analyse av kildevernets stilling er det likevel et sentralt skille mellom bulkinnhenting og målrettet innhenting, da innhentingsmetodene berører kildevernet materiale i ulik grad.³¹ Departementet uttaler at «kombinasjonen [av de to innhentingsmetodene] ventes å gi stor etterretningsmessig verdi».³²

Tilrettelagt innhenting gikk lenge under betegnelsen «digitalt grenseforsvar».³³ I mediene har verktøyet blitt omtalt som «digital masseovervåkning», fordi store mengder innenlands kommunikasjon innhentes. Da den nye e-loven skulle utformes, fikk verktøyet navnet «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon».³⁴ Avhandlingen vil bruke kortformen «tilrettelagt innhenting».

Avhandlingen kan ikke gi fullverdig oversikt over hvordan tilrettelagt innhenting fungerer teknisk og faktisk. E-loven er teknologinøytral, og praktiseringen av systemet er underlagt legitime behov for hemmelighold ved etterretningsvirksomhet.³⁵ Analysen av e-lovens kildevern må utføres på grunnlag av hvordan reglene er utformet, og hvordan disse ut ifra forarbeid og andre åpne kilder synes å være ment å fungere i praksis.

²⁹ Prop. 80 L (2019–2020) s. 111.

³⁰ E-loven § 1-3 bokstav f.

³¹ Mer om dette i kapittel 2.

³² Prop. 80 L (2019–2020) s. 92.

³³ Lysne II-utvalget.

³⁴ Prop. 80 L (2019–2020) s. 87.

³⁵ Ibid s. 78.

1.3 Metode og rettskildebildet

Avhandlingen anvender rettsdogmatisk metode. Det innebærer at avhandlingen analyserer rettskilder for å klarlegge gjeldende rett, herunder ta standpunkt til kildevernets rekkevidde etter innføringen av tilrettelagt innhenting.³⁶ Analysen vil vurdere om e-lovens kildevernregler samsvarer med EMK Artikkel 10.

Primært rettsgrunnlag er e-loven § 9-6 og § 5-2. Loven avløser etterretningstjenesteloven av 1998.³⁷ Kildevernbestemmelsene er i likhet med reglene om tilrettelagt innhenting nye av etterretningstjenesteloven av 2020, og både § 5-2 og § 9-6 ble endret 1. oktober 2023.³⁸ Under arbeidet med avhandlingen er reglene ikke enda trådt i kraft, slik at kildeomfanget til e-loven er begrenset. Mangel på praksis innebærer at sentrale rettskilder er lovens ordlyd og forarbeider.

Kildeomfanget suppleres av at e-loven skal tolkes og anvendes innenfor rammene av internasjonale menneskerettigheter. Et utvalg menneskerettigheter fremgår av Grunnloven direkte.³⁹ Grunnlovens menneskerettigheter skal, for de bestemmelser som er basert på internasjonale paralleller, tolkes i lys av internasjonale menneskerettighetskonvensjoner.⁴⁰ Flere menneskerettskonvensjoner, inkludert EMK, gjelder som norsk lov med forrang over alminnelig lov, jf. menneskerettsloven § 2, jf. § 3.

Pressens ytringsfrihet, herunder kildevern, er beskyttet av Grunnloven § 100 og EMK Artikkel 10. Fordi Grunnloven § 100 har spilt en beskjeden rolle i rettspraksis,⁴¹ er relevant rettspraksis for kildevernets innhold i hovedsak tilknyttet EMK Artikkel 10, både for norsk og internasjonal praksis. Analysen vil bygge på EMK Artikkel 10 i det følgende.

EMK Artikkel 19 oppnevner Den europeiske menneskerettsdomstolen (heretter EMD), som har avgjørende ord ved tolkning og anvendelse av EMK.⁴² EMD har med utgangspunkt i Wien-konvensjonen utviklet en egen menneskerettslig tolkningsstil, som innebærer at EMK

³⁶ Graver (2008) s. 157 flg.

³⁷ Lov 20. mars 1998 nr. 11 om Etterretningstjenesten (etterretningstjenesteloven).

³⁸ Lov 18. juni 2023 nr. 54 om endringer i etterretningstjenesteloven (domstolskontroll i saker om kildevern og ved speiling av kommunikasjonsstrømmer mv.)

³⁹ Grunnlovens menneskerettighetskatalog finnes i Grunnlovens kapittel E.

⁴⁰ Dok. nr. 16 (2011–2012) s. 177.

⁴¹ For eksempel Kierulf 2016, s. 185–189.

⁴² EMK artikkel 32.

skal tolkes helhetlig, formålsrettet og dynamisk.⁴³ Norske domstoler er bundet av EMDs tolkning av EMK,⁴⁴ og plikter å innrette seg etter EMDs avgjørelser der Norge er part.⁴⁵ EMD er «prejudikatdomstol i norsk rett på sitt område».⁴⁶ EMD sine avgjørelser mot andre konvensjonsstater er først og fremst relevant for tolkning av e-loven i den utstrekning EMD gir føringer for *tolkningen* av kildevern og bulklagring. Den konkrete vurderingen vil kunne falle ut ulikt som følge av nasjonale variasjoner. Når avhandlingens spørsmål er om e-lovens kildevernregler ved tilrettelagt innhenting samsvarer med EMK Artikkel 10, vil EMD-praksis primært ha normativ kraft som rettskilde ved utpenslingen av generelle krav til kildevern og bulklagringsregimer.

Høyesterett er øverste instans og prejudikatdomstol,⁴⁷ og har siste ord ved tolkning av kildevernet i norsk rett. Norske domstoler foretar en selvstendig tolkning av EMK, men anvender de samme tolkningsprinsipper som EMD.⁴⁸ Forholdet mellom Høyesterett og EMD har hittil ikke skapt problemer. Suverenitetshensyn innebærer likevel at Høyesterett kan fravike EMD-praksis dersom rettsutviklingen skulle gå i uønsket retning.⁴⁹

Regler om kildevernet fremgår også av norsk prosesslovgivning, herunder straffeprosessloven (strpl.) § 125 og tvisteloven (tv1.) § 22-11.⁵⁰ Kildevernet under prosessreglene er likelydende og rettighetens innhold skal tolkes likt.⁵¹ Reglene skal i likhet med e-lovens kildevernregler tolkes i lys av EMK Artikkel 10. E-tjenestens datainnsamling er inngripende i stor grad og kan deles med andre myndigheter, deriblant politi, slik at inngrep kan ha nedkjølingseffekt på kildevernet.⁵² Sammenhengen tilsier at rettigheten etter e-loven skal forstås på samme måte som i prosesslovgivningen.⁵³ Prosesslovgivningens kildevernregler og tilhørende rettspraksis er følgelig sentrale for tolkningen av kildevernets personkrets og rekkevidde etter e-loven.

⁴³ Vienna Convention on the Law of Treaties, Wien, 23 mai 1969; *Golder mot Storbritannia* [P], no. 4451/70 avsnitt 29 flg.

⁴⁴ Nygård nederst på s. 221.

⁴⁵ EMK artikkel 46 nr. 1.

⁴⁶ Nygård (2004) s. 82.

⁴⁷ Grunnloven § 88 og § 89.

⁴⁸ Rt. 2000 s. 996 P (Bøhler).

⁴⁹ Rt. 2015 s. 93 A avsnitt 57.

⁵⁰ Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker; Lov 1. januar 2008 om mekling og rettergang i sivile tvister.

⁵¹ Rt. 1992 s. 10 A s. 42.

⁵² Mer om deling i kapittel 5.4.4.

⁵³ Prop. 80 L (2019–2020) s. 156.

Analysen må foretas i lys av at avhandlingen ikke kan forutse hvordan kildevernreglene i e-loven vil virke i praksis. Det må understrekes at den faktiske praktiseringen av tilrettelagt innhenting, inkludert hvordan rettslige skranker etterleves og håndheves, vil ha avgjørende betydning for spørsmål om systemets forenlighet med EMK. Fordi reglene ikke er trådt i kraft under arbeidet med masteren, vil avhandlingens metode særpreges av at analysen vurderer *kvaliteten* av reglene i e-loven § 5-2 og § 9-6 i lys av EMK, herunder lovgivers utforming av kildevernets rekkevidde og adgang til inngrep.

1.4 Avgrensninger

Tilrettelagt innhenting griper inn i flere rettigheter enn kildevernet. Særlig retten til respekt for privatliv og kommunikasjon etter EMK Artikkel 8 kunne vært tema.⁵⁴ Det er imidlertid utenfor avhandlingens rammer å drøfte tilgrensende konvensjonsrettigheter eller lovligheten av tilrettelagt innhenting generelt.

Kildevernet er beskyttet i FNs konvensjon om sivile og politiske rettigheter (SP) Artikkel 19.⁵⁵ Rettighetsvernet er i all hovedsak tilsvarende etter EMK.⁵⁶ Avhandlingen avgrensner derfor mot behandling av SP.

Under e-lovens høringsrunder har det vært diskutert hvorvidt EU-direktiv 2002/58/EF (kommunikasjonsverndirektivet) har virkninger for E-tjenestens adgang til tilrettelagt innhenting.⁵⁷ Direktivet beskytter fortrolig kommunikasjon, er innlemmet i EØS-avtalen og bindende for Norge.⁵⁸ Tiltak som skal ivareta etterretningsformål omfattes imidlertid hverken av EU-retten eller EØS-avtalens saklige virkeområde.⁵⁹ EU-domstolen har i nyere praksis likevel fastslått at direktivet etter omstendighetene kan få anvendelse.⁶⁰ Avgjørelsene skaper uklarhet om og i hvilken utstrekning EU-rettskildene har virkninger for e-lovens kildevernregler.⁶¹ EU-rettsakter vil derfor kun benyttes som tolkningsbidrag i den grad de gir uttrykk for en felleseuropeisk forståelse av kildevernet.

⁵⁴ Prop. 80 L (2019–2020) s. 19 flg.

⁵⁵ De forente nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter.

⁵⁶ Rt. 2015 s. 1467 A avsnitt 45.

⁵⁷ For eksempel Prop. 92 L (2022–2023) s. 27.

⁵⁸ Avtale om Det europeiske økonomiske samarbeidsområde; Prop. 92 L (2022–2023) s. 7.

⁵⁹ EU-traktaten artikkel 4(2) fastslår at nasjonal sikkerhet er medlemsstatenes eneansvar; Kommunikasjonsverndirektivet Artikkel 1 nr. 3 og Prop. 80 L (2019–2020) s. 101.

⁶⁰ Forente saker C-511/18, C-512/18 og C-520 (La Quadrature du Net) og C-623/17 (Privacy International).

⁶¹ Mer i Prop. 92 L (2022–2023) s. 27 flg.

Grenseoverskridende datainnhenting aktualiserer spørsmål om EMKs såkalte ekstraterritoriale virkning. Avhandlingen behandler ikke jurisdiksjonsspørsmål. Norske myndigheters overvåking av utenlandske borgere skal uansett skje i samsvar med statens menneskerettslige forpliktelser, jf. menneskerettsloven §§ 2 og 3. Forpliktelsene kan etter forholdene også omfatte utenlandske borgere i utlandet.⁶²

Avhandlingen kommenterer ikke informasjonssikkerhet for kildevernedede opplysninger i etterretningsvirksomhet. Det forutsettes at fortrolige opplysninger oppbevares sikkert. Avhandlingen avgrensar også mot testinnhenting etter e-loven § 7-5.

Avhandlingen gir ikke en generell behandling av E-tjenestens innhentingsmetoder for elektronisk kommunikasjon.⁶³ Utgangspunktet er at det gjelder forbud mot innhenting av informasjon overfor personer i Norge, jf. e-loven § 4-1. Tilrettelagt innhenting er imidlertid *særpreget* ved at verktøyet innhenter store mengder data om norsk innenlands kommunikasjon.⁶⁴ Dette særpreget gjør tilrettelagt innhenting særlig inngripende, og skaper behov for klarlegging av kildevernet i lys av innføringen.

Som nevnt skal avhandlingen ikke gi en analyse av E-tjenestens kildeverninngrep i praksis, herunder hva som skal til for at inngrep etter § 5-2 og § 9-6 mer konkret kan forsvares i etterretningsvirksomhet etter en interesseavveining. E-tjenesten er en hemmelig tjeneste, reglene er nylig trådt i kraft og sikker informasjon om E-tjenestens metodebruk kan ikke oppdrives. Vurderingen av om kildevernreglene samsvarer med EMK beror på eksistensen av materielle og prosessuelle garantier mot misbruk.⁶⁵ Det innebærer også at i den grad e-lovens kildevernregler tolkes i lys av reglene i strpl. § 125 og tvl. § 22-11, er det kildevernets subjektive og objektive rekkevidde som sammenlignes.⁶⁶ Dette fordi avhandlingens hovedfokus er *utformingen* av kildevernreglene i e-loven.

⁶² Milanovic (2022); Big Brother Watch mot Storbritannia [GC] avsnitt 272.

⁶³ Dette innebærer blant annet avgrensning mot E-tjenestens adgang til midtpunktinnhenting etter e-loven § 6-9.

⁶⁴ Prop. 92 L (2022–2023) s. 19.

⁶⁵ Sml. EMDs tilnærming til overprøving av bulklagringssystemer i Big Brother Watch mot Storbritannia [GC] avsnitt 322–323.

⁶⁶ Kapittel 3 og 4.

1.5 Videre fremstilling

Kapittel 2 redegjør for rettslige utgangspunkter. Kapitlet introduserer de krav EMK Artikkel 10 oppstiller til kildevern generelt og under bulklagringssystemer. Dermed introduseres hvilke inngrep tilrettelagt innhenting utgjør for kildevernet, og hovedregelen om kildevern etter e-loven.

Kapittel 3 og 4 analyserer kildevernets rekkevidde etter e-loven (rettigheten). Denne delen klarlegger rettighetsvernet i e-loven § 9-6 og EMK Artikkel 10, samt eventuelle spenningsforhold mellom reglene. Kapittel 3 undersøker *hvilke aktører* vernet omfatter (rettighetens subjektive innhold). Kapittel 4 undersøker *hvilke opplysninger* vernet omfatter (rettighetens objektive innhold). Begge kapitlene gir en avsluttende analyse av om kildevernets rekkevidde etter e-loven § 9-6 samsvarer med Artikkel 10.

Kapittel 5 analyserer om reglene i e-loven § 9-6 og § 5-2 (inngrepet) oppfyller de krav EMK Artikkel 10 oppstiller for inngrep. Kapitlet undersøker om E-tjenestens adgang etter e-loven til kildeverninngrep som ledd i tilrettelagt innhenting kan forsvares.

Kapittel 6 konkluderer og gir avsluttende betraktninger om kildevernets stilling etter innføring av tilrettelagt innhenting.

2 Rettslige utgangspunkter

2.1 Generelt om kildevernet etter EMK Artikkel 10

EMK Artikkel 10 nr. 1 fastslår at ytringsfriheten omfatter «frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser». Det følger av bred EMD-praksis at pressens ytringsfrihet, herunder kildevern, er en sentral del av ytringsfriheten som nyter særlig vern.⁶⁷ Kildevern innebærer en rett og plikt til å beskytte mediernes anonyme kilder.⁶⁸ EMD legger til grunn at beskyttelse av journalistiske kilder er «one of the cornerstones of freedom of the press» og at «safeguards to be afforded to the press are of particular importance».⁶⁹

Kildevernet er ikke absolutt.⁷⁰ Det følger av EMK Artikkel 10 nr. 2 at inngrep i kildevernet må oppfylle tre krav: 1) Inngrepet må ha hjemmel i lov, 2) forfølge et legitimt formål og 3) være nødvendig (forholdsmessig).⁷¹ Praksis viser at terskelen for inngrep i pressefriheten er høy, og EMD foretar en intensiv prøving («special scrutiny») når inngrep berører kildevernet.⁷² EMD har uttalt at inngrep som berører kildevern må være «justified by an overriding requirement in the public interest».⁷³ Videre har EMD understreket at inngrep i kildevernet må underlegges adekvate rettssikkerhetsgarantier, blant annet uavhengig kontroll.⁷⁴ Det innebærer at E-tjenestens befatning med kildevernet materiale må underlegges betryggende kontrollmekanismer.

Den høye terskelen for inngrep i kildevernet materiale må forstås i lys av rettighetens samfunnsmessige begrunnelse: Vern om kilders rett til å forbli anonym er en nødvendig forutsetning for en opplyst at pressen skal kunne utføre sine samfunnsroller som «offentlig vaktbikkje», informasjonskanal og tilrettelegger for den offentlige samtale.⁷⁵ Et sterkt kildevern tilrettelegger for at pressen og offentligheten kan få tilgang til informasjon fra kilder

⁶⁷ Se for eksempel Goodwin mot Storbritannia [GC] avsnitt 39; Understreket i relasjon til bulklagring i Big Brother Watch mot Storbritannia [GC].

⁶⁸ NOU 2022: 9 s. 241.

⁶⁹ Big Brother Watch mot Storbritannia [GC] avsnitt 442.

⁷⁰ EMK artikkel 10 nr. 2.

⁷¹ Noe ulikt formulert i Grunnloven § 100, SP art. 19 og regler om kildevern i nasjonal lov, men vurderingen er i hovedsak sammenfallende i praksis.

⁷² Big Brother Watch mot Storbriannia [GC] avsnitt 442.

⁷³ For eksempel Goodwin mot Storbritannia [GC] avsnitt 39–40.

⁷⁴ Big Brother Watch mot Storbritannia [GC] avsnitt 444.

⁷⁵ Goodwin mot Storbritannia [GC] avsnitt 39–40.

som ønsker å være anonyme. Kildevernet bidrar til å sikre ytrings- og informasjonsfriheten og er begrunnet i hensynet til samfunnet som helhet.⁷⁶ Vernet kan i praksis beskrives som «en beskyttelse av journalistiske arbeidsmetoder for å ivareta samfunnets informasjonsfrihet».⁷⁷

Kildevernets begrunnelse innebærer at spørsmål om inngrep må vurderes ikke bare konkret, men særlig i lys av mulige ringvirkninger for samfunnet som helhet. Inngrep i kildevernet kan medføre svekkelse av fremtidige kilders tillit til at deres anonymitet blir ivaretatt, noe som kan gi nedkjølende effekt på pressens kildetilfang. Viktig informasjon for allmenheten kan på sikt gå tapt. Denne langsiktige samfunnseffekten – en såkalt «chilling effect» – av å gjøre unntak fra kildevernet blir i rettspraksis ofte veklagt med tyngde ved vurderingen av om inngrep er forholdsmessig.⁷⁸ Spørsmål om kildevernets innhold og rekkevidde bør ikke miste av synet at det dreier seg om «noe større enn bare spørsmål om innsyn kan forsvares i den enkelte sak».⁷⁹

Behovet for inngrep må avveies mot kryssende hensyn i den enkelte sak. På etterretningsområdet kan tungtveiende samfunnsmessige hensyn gjøre unntak fra kildevern nødvendig. Ved tvil om at kildevernet skal vike, har Høyesterett likevel lagt til grunn at tvilen skal falle ut til fordel for kildevernet.⁸⁰

2.2 Nærmere om EMDs krav til kildevern ved bulkinnhenting av elektronisk kommunikasjon

Statlig masseinnhenting og -lagring av data for etterretningsformål er ikke et særnorsk fenomen. Lignende systemer er innført i flere land. Noen har vært oppe til vurdering for EMD. Særlig retningsgivende for rettstilstanden er to storkammeravgjørelser avsagt av EMD i 2021: *Big Brother Watch m.fl. mot Storbritannia* og *Centrum for rättvisa mot Sverige*.⁸¹ På bakgrunn av en konkret vurdering av det britiske og svenske bulkagringsregimet, konstaterte EMD i begge sakene krenkelse av Artikkel 8. Dommen mot Storbritannia fant også krenkelse av Artikkel 10, herunder kildevernet. I den svenske saken var ikke Artikkel 10 anført. Fokus her vil derfor være bulkagringsregimets forenlighet med Artikkel 10 etter avgjørelsen i *Big*

⁷⁶ Rt. 2010 s. 1381 A avsnitt 52.

⁷⁷ NOU 2022:9 En åpen og opplyst offentlig samtale side 242.

⁷⁸ Goodwin mot Storbritannia [GC]; Rt. 2013 s. 1290 A og Rt. 1992 s. 39 A.

⁷⁹ Kierulf (2021), s. 69.

⁸⁰ Rt. 2015 s. 1286 A avsnitt 72.

⁸¹ Big Brother Watch mot Storbritannia [GC]; Centrum for rättvisa mot Sverige [GC].

Brother Watch. Avgjørelsen gir retningslinjer for krav til kildevernbeskyttelse etter Artikkel 10 under innhenting av kommunikasjonsdata i bulk.

Big Brother Watch stadfester for det første at det ligger innenfor statens skjønnsmargin å opprette et regime for innhenting av kommunikasjonsdata i bulk av hensyn til nasjonal sikkerhet.⁸² På grunn av misbrukspotensialet i et slikt regime, oppstilles samtidig krav til garantier mot misbruk og vilkårlighet. EMD uttaler at «in operating such a system the margin of appreciation afforded [...] must be narrower and a number of safeguards will have to be present.»⁸³ Den viktigste rettsikkerhetsgarantien er at det oppnevnes en dommer eller annen uavhengig instans som utøver reell kontroll over hvorvidt vilkårene for inngrep er oppfylt.⁸⁴

EMD anerkjenner at et bulkinnhentingsregime griper inn i kildevernet allerede på stadiet for speiling og lagring av kommunikasjonsdata i bulk, i form av at kildevernet materiale lagres i bulk og at journalistiske kilder kan bli avskrekket fra å dele informasjon via e-kommunikasjon.⁸⁵ At kildevernet materiale «fanges opp» i bulk som en utilsiktet konsekvens av bulklagringsregimets system kan imidlertid ikke *alene* anses EMK-stridig, ettersom dette er en uunngåelig konsekvens av etterretningsverktøyet. EMD har gjentatt uttalt at kildeverninngrep i form av strategisk overvåkning ikke er et særlig alvorlig inngrep i Artikkel 10, så lenge innhenting ikke rettes mot kildevernet virksomhet, for eksempel medievirksomhet.⁸⁶

EMD fastslår at et bulkinnhentingsregime må forstås som en gradvis prosess hvor graden av inngrep i individets rettigheter øker etter hvert som prosessen skrider frem.⁸⁷ Rettslige krav til inngrepet skjerpes proporsjonalt med inngrepets styrke. Det innebærer at kravene blir strengere jo lenger inn i «bulkinnhentingsprosessen» en kommer. Det innledende stadiet, herunder speiling og lagring av vernet kommunikasjonsdata i bulk, regnes som mindre alvorlig. Senere stadier, herunder målrettet innhenting av journalistisk materiale og videre behandling, er mer alvorlig og kravene til inngrep skjerpes tilsvarende.

Ettersom bulklagringsregimer innebærer en risiko for ulovlig inngrep i kildevernet materiale, krever Artikkel 10 at nasjonal lovgivning inneholder «robust safeguards regarding the storage,

⁸² *Big Brother Watch mot Storbritannia* [GC] avsnitt 322–323.

⁸³ *Ibid* avsnitt 347.

⁸⁴ *Ibid* avsnitt 445.

⁸⁵ *Weber og Saravia mot Tyskland* [A], no. 54934/00 avsnitt 143–145.

⁸⁶ *Big Brother Watch mot Storbritannia* [GC] avsnitt 450.

⁸⁷ *Ibid* avsnitt 325.

examination, use, onward transmission and destruction of such confidential material».⁸⁸

Kapittel 5 vil gi en nærmere vurdering av om e-lovens kildevern oppfyller disse krav.

2.3 Tilrettelagt innhenting etter e-loven. De ulike stadiene av innhentingsprosessen og E-tjenestens tilgang til kildevernet materiale på disse

Gjennomgangen over tilsier at det norske systemet for tilrettelagt innhenting kan gjøre inngrep i kildevernet på flere måter og i varierende grad avhengig av hvor i innhentingsprosessen en befinner seg. Innsamling, lagring, undersøkelse og bruk utgjør selvstendige inngrep, og både innholdsdata og metadata er kommunikasjon som omfattes av rettighetsvernet.⁸⁹ Tilrettelagt innhenting etter e-loven kan i hovedsak deles inn i fire trinn hvor graden av inngrep er økende:⁹⁰

- 1) Tilrettelegging i form av speiling og tilgjengeliggjøring av utvalgte kommunikasjonsdata for E-tjenestens lagring i bulk (tilretteleggingsplikt for selskaper som E-tjenesten utpeker)
- 2) Bruk av spesifikke selektorer på bulklagrede data til målrettet innhenting eller målsøking, med formål om å innhente informasjon til etterretningsvirksomhet
- 3) Behandling/undersøkelse av innhentede kommunikasjonsdata etter innhenting har samlet rådata i bulk
- 4) Oppbevaring og videre bruk av kommunikasjonsdata, inkludert eventuell deling med tredjeparter

Første steg i innhenting er E-tjenestens speiling og lagring av data i tråd med «tilretteleggingsplikten». Tilretteleggingsplikten gir E-tjenesten adgang til å pålegge virksomheter å tilgjengeliggjøre kommunikasjonsstrømmer. For eksempel kan E-tjenesten pålegge Telenor å tilgjengeliggjøre alle sine kabler til utlandet, fordi E-tjenesten mistenker at et ulovlig hacker-miljø som truer nasjonale sikkerhetsinteresser har sendt phishing-meldinger

⁸⁸ Ibid avsnitt 450.

⁸⁹ Prop. 80 L (2019–2020) s. 96.

⁹⁰ Sml. EMDs metode og trinnvise inndeling ved overprøving av det britiske bulklagringsregimet i Big Brother Watch mot Storbritannia [GC] avsnitt 325.

til norske brukere av telefonabonnement hos Telenor. Dette kan utgjøre inngrep i kildevernet kommunikasjon utilsiktet, for eksempel dersom dataene inneholder informasjon om en norsk journalist som har mottatt kildeidentifiserende opplysninger fra trusselaktøren under arbeid med en gravejournalistisk sak om phishing.

Som nevnt har staten vid skjønnsmargin etter EMK ved innføring av etterretningsverktøy av sikkerhetshensyn. At kildevernede kommunikasjonsdata fanges opp i bulken til E-tjenesten, som et «biprodukt» av speilingen, er derfor ikke til å unngå. Ettersom tilrettelagt innhenting ikke har som formål å innhente kildevernet materiale, er ikke bulkinnhenting i seg selv uforholdsmessig etter Artikkel 10. Det er de materielle og prosessuelle skranker for myndighetenes bruk av vernet kommunikasjon som er avgjørende.

Tilrettelagt innhenting er underlagt strenge prosessuelle skranker mot myndighetsmisbruk. Beslutning om tilrettelegging skal forelegges retten, jf. e-loven § 7-3. E-tjenesten skal ikke ha tilgang til data som innhentes på det innledende stadiet av tilretteleggingen: «Det er først etter at domstolen med hjemmel i kapittel 8 har gitt tillatelse til å gjøre søk i lagrede metadata etter § 7-8, eller gitt tillatelse til målrettet innhenting og lagring av innholdsdata etter § 7-9, at Etterretningstjenesten kan benytte informasjon fra tilrettelagt innhenting til etterretningsproduksjon».⁹¹ Videre tilgang for E-tjenesten er gjenstand for forhåndskontroll, løpende kontroll og etterfølgende kontroll.⁹² Utgangspunktet er at tilrettelegging og bulklagring av kildevernede data utgjør et lovlig inngrep i kildevernet etter EMK artikkel 10.

Det kan likevel tenkes at selve eksistensen av tilrettelagt innhenting kan ha en nedkjølende effekt på pressefriheten, ettersom reglene og systemet er uoversiktlig og til dels hemmelig. Kildevernets formål tilsier at kontrollmekanismer må utformes på en måte som gjør at reglene ikke bare bidrar til at kildevernet ivaretas i seg selv, men slik at også *tilliten* til kildevernet ivaretas.

Fokus for analysen videre er e-lovens materielle og prosessuelle skranker for E-tjenestens videre befatning med kildevernet materiale (etter bulkinnhenting og -lagring av metadata). Spørsmålet er om e-lovens kildevernregler i § 5-2 og § 9-6 samsvarer med EMK Artikkel 10.

⁹¹ Prop. 80 L (2019–2020) s. 22.

⁹² Ibid s. 109.

2.4 Hovedregelen om kildevern i e-loven § 5-2 og § 9-6

Ved tilrettelagt innhenting beskytter e-loven kildevernet spesielt i to situasjoner: ved bruk av selektorer på bulklagrede data med formål om innhenting (trinn 2 i listen ovenfor) og ved undersøkelse/behandling av innhentede kommunikasjonsdata (trinn 3 ovenfor), jf. hhv. e-loven § 5-2 og § 9-6. EMD har skissert at beskyttelse av kildevernet materiale er påkrevd i disse to situasjoner.⁹³ At e-loven oppstiller kildevern i disse to tilfellene, må anses som et minstekrav etter EMK Artikkel 10.

Det følger av § 5-2 andre ledd at målrettet innhenting mot «journalister som er omfattet av 9-6 første ledd» eller der det er «stor sannsynlighet for at innhenting vil frembringe kildeidentifiserende opplysninger som er omfattet av § 9-6 første ledd» bare kan iverksettes dersom det er «strengt nødvendig» at «de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser». Bestemmelsen oppstiller vern mot *målrettet innhenting* mot kildevernede opplysninger, det vil si innhenting som skjer med formål om eller høy sannsynlighet for å innhente kildevernede opplysninger.

Kravet i § 5-2 om «stor sannsynlighet» må forstås i lys av at E-tjenesten på forhånd av innhenting ikke nødvendigvis har oversikt over hvilke data innhenting fremskaffer. Kravet innebærer at det «basert på særskilte holdepunkter, må fremgå med høy grad av sannsynlighet at innhenting vil frembringe kildeidentifiserende opplysninger».⁹⁴ Dersom målrettet innhenting skjer overfor personer omfattet av § 9-6 første ledd, er utgangspunktet at sannsynlighetskravet anses oppfylt.⁹⁵ Sannsynlighetskravet bygger på føringer i *Big Brother Watch*, hvor EMD oppstiller krav om kildevernbeskyttelse ved «high probability» for at innhenting frembringer kildeidentifiserende opplysninger.⁹⁶ Bestemmelsens ordlyd og forarbeider gir ellers uttrykk for at kildevernet etter § 5-2 skal omfatte den samme personkrets og innhold som etter § 9-6. Kildevernets materielle innhold og rekkevidde etter e-loven beror følgelig på en tolkning av § 9-6.

Etter § 9-6 første ledd skal E-tjenesten som hovedregel ikke behandle opplysninger som er «betrodd noen i deres journalistiske virke» og som «kan avsløre hvem som er kilde for opplysningen», dersom «den som betror seg eller som er betrodd opplysningen, er bosatt i

⁹³ Big Brother Watch. mot Storbritannia [GC] avsnitt 447–450.

⁹⁴ Prop. 92 L (2022–2023) s. 17.

⁹⁵ Ibid.

⁹⁶ Big Brother Watch. mot Storbritannia [GC] avsnitt 448.

Norge, norsk statsborger eller arbeider på oppdrag for virksomhet i Norge som omfattes av mediefridomslova § 2». Det samme gjelder dersom «vedkommende ikke lenger bor i Norge eller arbeider for virksomheten, men gjorde dette da opplysningen ble gitt».

Lovteksten i § 9-6 oppstiller et generelt forbud mot behandling av kildeidentifiserende opplysninger i etterretningsvirksomhet, og gir samtidig en beskrivelse av kildevernets rekkevidde (rettighetens innhold) etter e-loven. Kildevern krever at følgende kumulative vilkår er oppfylt: 1) Opplysningene må være «betrodd noen i deres journalistiske virke», 2) opplysningen «kan avsløre hvem som er kilde» og 3) mottaker eller giver av opplysningene må ha en slik tilknytning til Norge som beskrevet. Vilkåret om persontilknytning forutsetter norsk jurisdiksjon, men behandles ikke nærmere da avhandlingens tema er kildevernet overfor norske borgere.⁹⁷ Ordlyden i § 9-6 skal tolkes på bakgrunn av kildevernet etter EMK Artikkel 10 samt rettspraksis fra Høyesterett og EMD.⁹⁸

Utgangspunktet om e-lovens forbud mot kildeverninngrep gjelder altså både på tidspunktet for målrettet innhenting og for videre behandling av dataene. Gjennomgangen videre undersøker kildevernets innhold og rekkevidde med utgangspunkt i tolkning av e-loven § 9-6. Spørsmålet er om utformingen av kildevernets beskyttelse i § 9-6 samsvarer med den trinnhøyere rettigheten i EMK Artikkel 10. Klarlegging av kildevernregelens innhold og samsvar med EMK Artikkel 10 nødvendiggjør en analyse av vilkårene i § 9-6: Hvilke aktører er vernet (kildevernets *personkrets*) og hvilke opplysninger er vernet (vern av *innholdet* i journalistisk materiale)?

⁹⁷ Se kapittel 1.4.

⁹⁸ Prop. 92 L (2022–2023) s. 22.

3 Kildevernets personkrets – hvilke aktører er vernet?

3.1 Opplysninger «betrodd noen i deres journalistiske virke»

Første steg for å avgjøre om dataene E-tjenesten innhenter og behandler skal underlegges den særskilte beskyttelse kildevernet oppstiller, er å vurdere hvilke aktører kildevernet omfatter (rettighetens personkrets). E-loven § 9-6 krever at opplysningene er «betrodd noen i deres journalistiske virke». Spørsmålet er *hvilke aktører* § 9-6 beskytter, og om vernets subjektive rekkevidde er i samsvar med EMK Artikkel 10.

Kravet om at opplysninger må være «betrodd noen i deres journalistiske virke» for å ha kildevern, tilsier at E-tjenesten som hovedregel ikke skal behandle data som inneholder fortrolig informasjon med journalister eller andre i journalistisk virksomhet. Lovteksten beskytter både den som mottar betroelsen og avsenderen (kilden).

Ordlyden «journalistisk virke» definerer mottakergruppen vagt. Den omfatter i sin kjerne pressen og redaksjonsstyrte medier, men rekker videre. Lovforarbeidene uttrykker at også annen medievirksomhet omfattes, herunder frilansere, dokumentarfilmskapere, forfattere og journaliststudenter.⁹⁹ E-loven § 9-6 og § 5-2 skal bidra til å «styrke journalister mv. sin rettsstilling på innhentingsstadiet».¹⁰⁰ Departementet forutsetter at «journalistisk virke» tolkes i lys av EMK Artikkel 10 og EMD-praksis.¹⁰¹

At kilden må ha «betrodd» opplysningen, forutsetter at kilden ønsker å være anonym. En streng ordlydstolkning avgrenser mot vern for andre enn kilden og den som mottar opplysninger under betroelse. Det utelukker for eksempel kolleger/samarbeidspartnere som besitter kildeidentifiserende materiale gjennom annen kjennskap. Det utelukker også vern for utradisjonelle arbeidsmetoder, for eksempel såkalt «undercover»-journalister.

⁹⁹ Prop. 80 L (2019–2020) s. 226.

¹⁰⁰ Prop. 92 L (2022–2023) s. 21.

¹⁰¹ Prop. 80 L (2019–2020) s. 160.

Lovteksten avgrensner ellers mot vern for aktører som utgir seg for å være journalister på en måte som utnytter/misbruker kildevernet. Etterretningsfaglige hensyn nødvendiggjør en slik avgrensning, da omgåelse av regelverket kan hindre E-tjenesten fra å innhente legitim etterretningsinformasjon. Forståelsen har støtte i forarbeidene, som understreker at avgrensning mot omgåelsestilfeller skal vurderes konkret.¹⁰² Avgrensningen er aktuell for eksempel for produksjon av propaganda for en terrororganisasjon, eller dersom en spion utgir seg som journalist for å unngå E-tjenestens datainnsamling.

3.2 Kildevernet i prosesslovgivningen

Tvl. § 22-11 og strpl. § 125 gir bevisfritaksregler for ivaretagelse av pressens kildevern i hhv. sivilprosess og straffeprosess. Reglene gjør unntak fra bevisplikt under rettergang for «redaktøren av et trykt skrift», «andre som har fått kjennskap til forfatteren eller kilden gjennom sitt arbeid for vedkommende forlag, redaksjon, pressebyrå eller trykkeri» og medarbeidere i «annen medievirksomhet som i hovedtrekk har samme formål som aviser og kringkasting». Kildevernet favner i sin ordlyd bredt. Forarbeidene uttrykker at sistnevnte blant annet omfatter nettaviser, debattforumer på nett, mv.¹⁰³ Kildevernets rekkevidde skal tolkes i lys av EMK Artikkel 10. Det oppstiller en presumpsjon om at den beskyttede personkrets etter e-loven tolkes i lys av rettergangsvernet.

Pressens arbeidsvilkår er stadig under diskusjon. Departementet har nylig foreslått en modernisering av strpl. § 125 og tvl. § 22-11 til å verne ikke bare redaktør og kilde, men enhver som driver «journalistisk virke».¹⁰⁴ Departementet understreker at endringsforslaget ikke representerer en realitetsendring, men en språklig oppdatering som skal bringe kildevernreglene i tydeligere overensstemmelse med EMK Artikkel 10.¹⁰⁵ Lovforslagets vern for den som betros noe i sitt «journalistiske virke» er identisk med ordlyden i § 9-6. Det tilsier at lovgiver har ment at kildevernets personkrets skal være den samme.

Departementet uttaler i sammenheng med endringsforslaget at ordlyden «journalistisk virke» angir en fleksibel personkrets som legger opp til en teknologinøytral tolkning i tråd med utviklingen av mediebildet. Dermed er tradisjonelle medier så vel som nettbaserte aktører

¹⁰² Prop. 80 L (2019–2020) s. 226.

¹⁰³ NOU 2001: 32 B s. 963.

¹⁰⁴ Høringsnotat fra Justis- og beredskapsdepartementet, snr. 18/4856, 24. september 2018.

¹⁰⁵ Ibid.

omfattet. Det innebærer at vernet også omfatter «privatpersoner som enten gjør slikt på fritiden eller som ledd i en rent profesjonell virksomhet».¹⁰⁶

Endringsforslaget verner også «andre som har fått kjennskap til kilden eller opphavspersonen gjennom sitt arbeid i tilknytning til [journalistisk virke]». Også her utgjør lovteksten en språklig oppdatering som viderefører rettstilstanden.¹⁰⁷ Dermed er kolleger/samarbeidspartnere til aktører i «journalistisk virke» omfattet av kildevernet under rettergang. Det innebærer altså at aktører som ikke direkte er «betrodd» opplysningen, har vern.

Hensynet til et koherent og forutberegnelig kildevern i norsk rett taler for at e-loven tolkes i samsvar med kildevernets beskyttede personkrets under rettergang. Det innebærer at ordlyden i § 9-6 tolkes fleksibelt med sikte på et bredt vern. For eksempel vil § 9-6 også beskytte kolleger/samarbeidspartnere til journalistisk virksomhet dersom de besitter kildeidentifiserende opplysninger, selv om disse ikke direkte har mottatt opplysningene i kildebetroelse.

3.3 Utvikling og norsk rettspraksis – et styrket og teknologinøytralt kildevern

Tradisjonelt har kildevernet omfattet medievirksomheter med en ansvarlig redaktør eller leder med tilsvarende oppgaver, og som er tilsluttet pressens selvdømmeordning og etiske retningslinjer.¹⁰⁸ Teknologisk utvikling og moderne informasjonsspredning innebærer imidlertid at flere aktører enn tidligere oppfyller pressefrihetens formål. Tendensen er at kildevernet gis sterkere vern enn før, og personkretsen og type medier som nyter vern er utvidet.¹⁰⁹ E-loven må tolkes dynamisk i tråd med samfunnsutviklingen. For å oppfylle kildevernets formål om å ivareta allmenhetens behov for informasjon, må e-loven underlegges en moderne forståelse, slik at personkretsen etter § 9-6 omfatter enhver aktør i mediene som bidrar til å oppfylle pressefrihetens formål, herunder formidlere av informasjon i det offentlige interesse.

¹⁰⁶ NOU 2016: 24 s. 279–280.

¹⁰⁷ Det samme følger av dagens strpl. § 125 og tvl. § 22-11, om noe kronglete formulert.

¹⁰⁸ Prop. 80 L (2019–2020) s. 226.

¹⁰⁹ Aarli (2015) s. 407–456.

Det innebærer at også enkeltpersoner som formidler informasjon uten redaktør etter en nærmere vurdering kan være omfattet av kildevernet. Allerede i 1992, ved tolkning av dagjeldende tvistemålsloven § 209a (videreført i tvl. § 22-11) la Høyesterett prinsipielt til grunn at kildevernets personkrets rammer videre enn den tradisjonelle pressen.¹¹⁰ Saken reiste spørsmål om forfatterne av boken *Edderkoppen – Historien om en møbelhandler* kunne pålegges å avgi forklaring om kilder til bokens opplysninger. Opplysningene antydde kritikkverdige forhold hos overvåkningstjenesten, og overvåkningstjenesten krevde derfor at forfatterne ble avhørt. Forfatterne arbeidet til daglig som journalister. På bakgrunn av en fleksibel tolkning av tvistemålsloven § 209a og bokens formål om å «fremme debatt om samfunnsspørsmål» konkluderte Høyesterett med at boken og dens forfattere måtte «likestilles med de trykte skrifter som gir kildevern».¹¹¹ Forfatterne ble fritatt for å avgi forklaring, under henvisning til at «[d]et er pressens *funksjoner* som skal vernes gjennom kildevernet og anonymitetsretten» (min utheving).¹¹²

«Edderkopp-saken» er ikke et enkeltstående eksempel på at Høyesterett tolker kildevernets personkrets med fleksibilitet. I «Rolfesen-saken» anerkjente Høyesterett at en dokumentarfilmskaper hadde krav på vern etter strpl. § 125.¹¹³ En tilsvarende moderne tolkning anla Høyesterett i «Runestein-saken», hvor et innlegg fra en leser på et debattforum tilknyttet en nettavis ble ansett omfattet av kildevernet i strpl. § 125.¹¹⁴ En samlet lesning illustrerer at Høyesterett anlegger en funksjonell og formålsrettet tolkning av kildevernets rekkevidde.

3.4 Menneskerettslige føringer etter EMD-praksis

EMD anlegger en funksjonell tilnærming til hvilke aktører som har krav på kildevernbeskyttelse som følge av den samfunnsrolle de ivaretar.¹¹⁵ Tilnærmingen har støtte internasjonalt. Europarådets ministerråd har uttalt at «the definition of media actors has expanded as a result of new forms of media in the digital age. It therefore includes others who contribute to public debate and who perform journalistic activities to fulfil public watchdog

¹¹⁰ Rt. 1992 s. 39 A

¹¹¹ Ibid side 47–48.

¹¹² Ibid side 46.

¹¹³ Rt. 2015 s. 1286 A.

¹¹⁴ Rt. 2010 s. 1381 A.

¹¹⁵ Youth Initiative for Human Rights mot Serbia, [J], no. 48135/06.

functions».¹¹⁶ Rekomendasjonen uttrykker en felleseuropeisk forståelse om at realiseringen av kildevernets funksjon ikke kan begrenses til media eller profesjonelle journalister.

Den nylig avsagte EMD-avgjørelsen i *Big Brother Watch* berører spørsmål om krav til nasjonale myndigheters inngrep i journalistisk materiale ved bruk av bulklagring. Avgjørelsen var en forent sak der tre grupper klagere hevdet at deres kildevernsrettigheter etter Artikkel 10 var krenket som følge av britiske etterretningsmyndigheters bulkinnsamlingsregime. Den første gruppen klagere var tre NGO-er og en akademiker: Big Brother Watch, Open Rights Group, English Pen og Dr. Constanze Kurz. Klagerne var alle aktører som driver formidling av ytringsfrihet og personvern. Den andre gruppen besto av en NGO for nyhetsinnsamling og en journalist: Bureau of Investigative Journalism og Alice Ross. EMD aksepterte at det britiske bulklagringsregimet utgjorde inngrep i den andre gruppens kildevernsrettigheter etter Artikkel 10, altså journalisten og NGO-en for nyhetsinnsamling.¹¹⁷ Den tredje gruppen klagere fikk saken avvist på prosessrettslig grunnlag. Det fremstår uklart hvorfor den første klagegruppen ikke ble nevnt. Avgrensningen gjenstår ubegrunnet. En kan dermed hevde at avgjørelsen sår tvil om kildevernets personkrets under moderne bulklagring.

Big Brother Watch slår samtidig fast at bulklagringssystemer må beskytte pressens ytringsfrihet slik vernet fremgår av EMK Artikkel 10.¹¹⁸ Spørsmål om hvilke aktører som er omfattet av kildevernet når inngrep skjer i form av bulklagringsregimer kan ikke tolkes i et vakuum. Hensynet til sammenheng tilsier at EMD-praksis om pressens ytringsfrihet og kildevern generelt er veiledende for spørsmålet om rekkevidden av den vernede personkrets ved bulklagring.

I flere saker om pressefrihetens rekkevidde har EMD uttalt at andre samfunnsaktører enn tradisjonelle journalistiske virksomheter kan fylle en rolle som minner om pressens og ha krav på tilsvarende beskyttelse etter Artikkel 10. I en EMD-avgjørelse hvor klager var en menneskerettighetsorganisasjon, uttalte EMD følgende om kildevernets rekkevidde:

«[...] when a non-governmental organisation is involved in matters of public interest, such as the present applicant, it is exercising a role as a public watchdog of similar

¹¹⁶ Recommendation CM/Rec (2016) fortalepunkt 4.

¹¹⁷ Big Brother Watch mot Storbritannia [GC] avsnitt 451.

¹¹⁸ Ibid avsnitt 442 flg.

importance to that of the press [...]. The applicant's activities thus warrant similar Convention protection to that afforded to the press [...] ». ¹¹⁹

En funksjonell tilnærming forelå også i *Társaság a Szabadságjogokért*, hvor domstolen anerkjente at Den Ungarske union for sivile rettigheter hadde krav på pressefrihetsbeskyttelse, fordi organisasjonen bidro til å ivareta informasjonsfrihetens formål gjennom forum for offentlig debatt. ¹²⁰

EMD-praksis stiller ellers ikke krav om at opplysningen må være «betrodd» journalisten for å ha vern. *Nordisk Film & TV A/S* er illustrerende. Avgjørelsen utfordrer den tradisjonelle forståelsen av journalistiske kilder. Utgangspunktet etter EMD-praksis er at en journalistisk kilde er «any person who provides information to a journalist». ¹²¹ EMD anerkjente at det utgjorde inngrep i kildevernet etter Artikkel 10 at politiet påla et tv-selskap å overgi upublisert materiale som inneholdt samtaler med personer mistenkt for pedofili. ¹²² Journalisten hadde samlet informasjonen «undercover». Ettersom personene journalisten snakket med ikke hadde vært klar over at han var journalist, uttalte EMD at de ikke var journalistiske «kilder» i tradisjonell forstand, fordi *betroelseshandlingen* manglet. Likevel understreket EMD at inngrep i kildevernet etter EMK Artikkel 10 forelå. ¹²³ Avgjørelsen viser at kildevernet omfatter enhver person som mottar opplysninger i journalistisk virksomhet, selv der opplysningen ikke er «betrodd» i tradisjonell forstand.

Den funksjonelle tilnærmingen bidrar samtidig til en skranke for kildevernet basert på hvem som anses beskyttelsesverdig. I avvisningskjennelsen *Stichting Ostade Blade* la EMD til grunn en snever tolkning av kildebegrepet, begrunnet i at kildens motivasjon ikke var å informere allmennheten om opplysninger av beskyttelsesverdig offentlig interesse. ¹²⁴ En gruppe hadde i brev til magasinet *Ravage* påtatt seg ansvaret for flere bombebrev i Nederland. EMD fant at informanten ikke kunne betraktes som en journalistisk kilde beskyttet av Artikkel 10, da informanten hadde til hensikt å utnytte kildevernet for å påta seg ansvar for en forbrytelse. ¹²⁵ Det funksjonelle kildevernet etter EMK avgrenser i likhet med e-loven mot

¹¹⁹ Youth Initiative for Human Rights mot Serbia [J] avsnitt 20; Rosianu mot Romania [J], no. 27329/06, avsnitt 64.

¹²⁰ Társaság a Szabadságjogokért mot Ungarn [J], no. 37374/05 avsnitt 27.

¹²¹ Nagla mot Latvia [J], no. 73469/10, avsnitt 81.

¹²² Nordisk Film & TV A/S mot Danmark [J], no. 60685/02.

¹²³ Ibid.

¹²⁴ Stichting Ostade Blade mot Nederland [A], no. 8406/06 avsnitt 62 flg.

¹²⁵ Ibid.

personer som misbruker kildevernet. For eksempel vil en terroraktør som under dekke av anonymitet forsøker å unngå E-tjenestens datainnsamling, ikke ha vern.

3.5 Konklusjon og operasjonalisering av et EMK-forenlig kildevern

Gjennomgangen viser at det foreligger en viss spenning mellom e-lovens ordlyd og rettskildene ellers ved spørsmål om hvilke aktører som kan påberope vern for opplysninger «betrodd noen i deres journalistiske virke». En ordlydsstreng tolkning av § 9-6 tilsier en snevrere rekkevidde av aktører enn den funksjonelle tolkning av kildevernet som er lagt til grunn av Høyesterett og EMD ved tolkning av EMK Artikkel 10.

Ordlyden «journalistisk virke» er riktignok vag nok til at kildevernet etter e-loven åpner for fleksibilitet, og gir adgang til å innfortolke et funksjonelt EMK-rettslig kildevern.

Journalistisk «virke» kan omfatte presselignende aktører eller andre som oppfyller kildevernets formål. Rettsanvender kan dermed tilpasse kildevernets virkeområde i tråd med rettspraksis og samfunnsutviklingen ellers. Høyesteretts tilnærming til tolkning av kildevernreglene under rettergang viser at norsk rett gir rom for en funksjonell tilnærming til hvilke aktører som omfattes.¹²⁶

Spenning mellom rettskildene oppstår når e-loven § 9-6 i tillegg krever at opplysningene må være «betrodd noen» i journalistisk virke. Her oppstår en særlig utfordring for en EMK-konform tolkning av rettighetens rekkevidde, fordi e-loven oppstiller et tilleggsvilkår for kildevern, herunder krav om at opplysningen er gitt under betroelse. Tatt på ordet avgrenser vilkåret mot kildevern for aktører som mottar opplysninger på andre måter. Ordlyden vanskeliggjør vern for visse journalistiske arbeidsmetoder, som for eksempel «undercover»-journalistikk eller dersom en aktør besitter kildeidentifiserende materiale gjennom annen kjennskap. Tilleggsvilkåret i e-loven fremstår unødvendig innsnevrende for det rettighetsvern opplysninger mottatt i journalistisk virke er gitt etter EMD-praksis og høyesterettspraksis. Spørsmålet er hvordan spenningen mellom reglene skal løses.

EMK Artikkel 10 har forrang over e-loven og går foran ved motstrid, jf. menneskerettsloven § 2 nr.1, jf. § 3. Rettighetsvernet i § 9-6 har imidlertid ikke et absolutt preg som kan

¹²⁶ Rt. 1992 s. 39 A.

karakteriseres som *motstridende* til EMK.¹²⁷ Spenning mellom et uheldig utformet vilkår i e-loven og EMK kan avdempes gjennom tolkning. Det innebærer at vilkåret «betrodd noen» må tolkes utvidende slik at kildevernets personkrets etter e-loven samsvarer med Artikkel 10. For at § 9-6 skal være forenlig med Artikkel 10, må kildevernets personkrets tolkes funksjonelt, slik at det omfatter enhver aktør i mediene som bidrar til å oppfylle pressefrihetens formål, herunder formidlere av informasjon i det offentliges interesse. Som nevnt krever EMD-praksis for eksempel at opplysningene også har vern der en journalist har samlet opplysninger «undercover», selv om kilden i denne situasjon ikke «betror» opplysninger i tradisjonell forstand.

For E-tjenestens databefatning under tilrettelagt innhenting, innebærer en funksjonell tolkning av e-lovens kildevern for det første at kildevernet omfatter data om tradisjonelle journalister og medievirksomheter så vel som moderne aktører og digitale arenaer for offentlig kommunikasjon. Videre skal «betrodd noen» ikke tolkes strengt etter sin ordlyd, men verne om journalisters arbeidsmetoder i tråd med rettsutviklingen i EMD. Det innebærer at kommunikasjonsdata E-tjenesten innhenter er underlagt e-lovens kildevern dersom dataene gjelder en aktør i mediene som bidrar til å oppfylle pressefrihetens formål, herunder enhver formidler av informasjon i det offentliges interesse.

¹²⁷ Kontra LA-2021-157502, hvor lagmannsretten tilsidesatte den absolutte femårsfristen for begjæring om gjenåpning i tvistemålsloven 2015 § 408 annet ledd (opphevet), av hensyn til EMK Artikkel 6, jf. Artikkel 13.

4 Vern av innholdet i journalistisk materiale – hvilke opplysninger er vernet?

4.1 Kravet om at opplysningen «*kan*» identifisere en kilde

Dersom en journalistisk aktør er innenfor den vernede personkretsen (kapittel 3), er neste steg for å avgjøre om kildevernet etter e-loven kommer til anvendelse, en vurdering av hvorvidt opplysningenes innhold er vernet. Sammenholdt skisserer vilkårene i § 9-6 første ledd kildevernets objektive rekkevidde, herunder krav til innholdet i kildevernet materiale. Dermed gjenstår å analysere kravet til at opplysningene «kan avsløre hvem som er kilde for opplysningen». Spørsmålet er *hvilke opplysninger* § 9-6 beskytter, og om vernets objektive rekkevidde er i samsvar med EMK Artikkel 10.

Kravet om at opplysningen «kan avsløre hvem som er kilde for opplysningen» tilsier at dataene er vernet dersom det er *risiko* for at innholdet av dataene leder til innsyn i identiteten til en journalistisk kilde. Ordlyden «kan» krever en lav grad av sannsynlighet for kildeavsløring, men avgrenser mot data som hverken direkte eller indirekte kan avsløre kilders identitet.¹²⁸ En streng ordlydstolkning tilsier at E-tjenestens behandling av fortrolige data ikke er et inngrep dersom E-tjenesten har positiv forhåndskunnskap om at innholdet i dataene ikke er kildeavslørende, for eksempel dersom kilden er kjent for E-tjenesten forut for datainnhenting.

Lovforarbeidene understreker at vernets innhold omfatter «opplysninger som kan identifisere kilden ved navn, bilde eller annen personidentifikasjon, samt uredigert og upublisert materiale såfremt informasjonen kan avsløre journalistens kilder».¹²⁹ Den aktuelle opplysningen må være egnet til å avsløre identiteten til den som har avgitt den.¹³⁰ Formuleringen «egnet» tyder på at lovgiver har ment at opplysningenes *karakter* er av betydning for vurderingen av om opplysningen «kan» være kildeavslørende. Det indikerer at det ikke stilles høye krav til grad av risiko for at dataene regnes kildeavslørende.

¹²⁸ Prop. 80 L (2019–2020) s. 155.

¹²⁹ Ibid.

¹³⁰ Ibid s. 226.

Lovgiver har nylig foreslått språklig fornyelse av kildevernreglene under rettergang, blant annet med formål om å bedre reflektere EMK-vernet.¹³¹ Et av forslagene har vært å kodifisere at kildevernet omfatter alle opplysninger som er *egnet* til å avsløre kilder. Departementet uttaler at endringsforslagene ikke innebærer en endring av gjeldende rett, bare en språklig oppdatering.¹³² Uttalelsene her sammenholdt med hensynet til en koherent tolkning av kildevernet i norsk rett taler for at lovgiver ikke kan ha ment i e-lovens forarbeider at kildevernet etter e-loven skal være snevrere. Følgelig må «kan» og «egnet til» i denne kontekst forstås synonymt.

4.2 Menneskerettslige føringer: Vern for opplysninger *egnet* til kildeavsløring

Kildevernets objektive innhold etter EMD-praksis beror på om opplysningene er «likely to lead to the identification of a source».¹³³ Dette inkluderer «the factual circumstances of acquiring information from a source by a journalist» og «the unpublished content of the information provided by a source to a journalist».¹³⁴ Opplysningene har dermed også etter EMD-praksis vern dersom de er *egnet* til å avsløre kildevernet materiale. Det kreves ikke at opplysningene *faktisk* inneholder kildeidentifiserende informasjon, men at kildeavsløring er en risiko av en viss sannsynlighetsgrad, jf. «likely to lead to». Kildevernets utforming i e-loven § 9-6 har klare likhetstrekk med vurderingstemaet etter EMD, som begge oppstiller en risikovurdering. Utformingen av § 9-6 bidrar dermed til en EMK-konform tolkning av kildevernets rekkevidde.

Utgangspunktet er at dataenes risiko for kildeidentifisering er styrende for vurderingen av om opplysningene «kan avsløre hvem som er kilde». Spørsmålet er hvilken grad av risiko for kildeidentifisering som kreves for at dataene er underlagt kildevern.

EMK-vernet er grundig behandlet i Rt-2015-1286, som gjaldt kildevern under straffeprosess. Etter en gjennomgang av EMD-praksis stadfester Høyesterett at «det sentrale for kildevernets utstrekning er [...] om beslaget kan ha en dempende – og derved skadelig – virkning på

¹³¹ Høringsnotat fra Justis- og beredskapsdepartementet, snr. 18/4856, september 2018; NOU 2016: 24.

¹³² Ibid.

¹³³ Rekommandasjon No. R (2000) 7.

¹³⁴ Nagla mot Latvia [J] avsnitt 81.

pressens tilgang til kilder».¹³⁵ Høyesterett fant at det ikke var avgjørende om materialet *faktisk* inneholdt kildeopplysninger, såfremt «ransakingsbeslutningen var utformet slik at beslaget kunne ha avslørt journalistens kilder».¹³⁶ Følgelig kreves ikke at opplysningene rent faktisk *er* fortrolige. Kildevernet rekker videre. Avgjørelsen oppstiller en formodning om at journalistisk materiale anses kildevernet, fordi inngrep kan ha skadevirkninger uavhengig av om inngrepet er kildeavslørende. Vurderingen av om data E-tjenesten innhenter «kan» avsløre en kilde, må tilsvarende ivareta kildevernets formål. Følgelig må e-loven forstås slik at kildevern foreligger allerede når data i liten grad gir risiko for kildeavsløring.

Også EMD-praksis illustrerer at det ikke skal mye til for at journalistiske data anses kildevernet. *Financial Times* gjaldt utlevering av materiale som ikke direkte avslørte kildens identitet, men der dokumentene «upon examination» kunne lede til kildeidentifisering. EMD la avgjørende vekt på at *formålet* med å kreve dokumentene utlevert var å identifisere kilden:

«[...] 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.»¹³⁷

Ettersom kildevernets hovedformål er å unngå en langsiktig nedkjølingseffekt på kilders vilje til å yte informasjon, kan allerede risikoen for nedkjøling tilsi vern. Dermed blir det av betydning for risikovurderingen at nedkjølingsrisiko foreligger uavhengig av om deling av data *faktisk* avslører en kilde. At nedkjølingshensynet får betydning for vurderingen av risikoen for kildeavsløring, underbygger at det skal lite til for at journalistisk materiale anses kildevernet.

Hensynet til å unngå nedkjøling av pressefriheten kan innebære at også opplysninger som hverken direkte eller indirekte kan avsløre en kilde, kan være kildevernet. Praksis fra Høyesterett og EMD underbygger dette. Med henvisning til EMDs praksis har Høyesterett uttalt obiter dictum at «i spesielle tilfelle [kan] også upublisert materiale som ikke inneholder informasjon som kan føre til avsløring av en kildes identitet, nyte et visst vern.»¹³⁸ EMD-avgjørelsen *Nordisk Film & TV A/S* illustrerer. Det omstridte materialet i saken inneholdt ikke

¹³⁵ Rt. 2015 s. 1286 A avsnitt 54.

¹³⁶ Ibid avsnitt 56.

¹³⁷ *Financial Times mot Storbritannia* [J], no. 821/03, avsnitt 70.

¹³⁸ Rt. 2015 s. 1286 A avsnitt 57.

kildeopplysninger, og mistenktes identitet var kjent for politiet før beslagstidspunktet. EMD bemerket at kildevernets styrke for disse tilfellene er svakere, men konkluderte med at opplysningene var kildevernet.¹³⁹ Det var nok at *selve plikten* til overlevering av materialet kunne ha skadevirkninger – en nedkjølingseffekt for pressefriheten. At Høyesterett og EMD stadfester at kildevern også omfatter opplysninger som ikke kan avsløre kilder, er prinsipielt retningsgivende og klarlegger omfanget av hvilke data E-tjenesten må hensynta etter behandlingsforbudet i § 9-6. Avgjørelsene må leses dithen at journalistisk materiale som hverken direkte eller indirekte kan avsløre en kilde, dersom inngrep skaper risiko for nedkjøling av pressefriheten.

Etter dette kreves som hovedregel en lav grad av risiko for å konstatere at journalistiske data etter § 9-6 er egnet til å identifisere en kilde. Når dataene berører den beskyttede personkretsen i § 9-6, er terskelen lav for at en opplysning «kan» avsløre en kilde. Dataene kan også være kildevernet selv om opplysningene ikke skaper risiko for kildeavsløring, fordi hensynet til å unngå en langsiktig nedkjøling av pressefriheten tilsier vern.

Inngrep i kildevernet kan foreligge allerede ved speiling og innhenting av data i bulk, dersom kildeidentifiserende materiale blir utilsiktet bulkinnhentet. Inngrepets alvorlighet øker dersom E-tjenesten målrettet innhenter og behandler data om den berørte personkretsen.

Både metadata og innholdsdata om en aktør etter personkretsen i § 9-6 er omfattet av vernet. Innholdsdata vil typisk utgjøre et mer alvorlig inngrep i kildevern enn metadata, og derav oftere være egnet til å avsløre en kilde. Dette fordi dataene typisk inneholder tekst, bilder, video eller annen kommunikasjon som kan avsløre personlige opplysninger og fortrolig dialog mellom for eksempel en journalist og kilde.

Innhenting av metadata utgjør i utgangspunktet et mindre alvorlig inngrep, ettersom dataene inneholder mindre sensitiv informasjon om den de gjelder. Metadata er underlagt behandlingsforbudet i den utstrekning dataene skaper risiko for kildeavsløring. Innhenting av metadata rettet mot en journalistisk aktør vil vanligvis skape denne risiko, fordi for eksempel innsyn i en IP-adresse som journalisten kommuniserer med kan være egnet til å avsløre

¹³⁹ Nordisk Film & TV A/S mot Danmark [J].

kildens identitet like mye som det nærmere innholdet i kommunikasjonsdataene. Til sammenligning er utlevering av IP-adresse underlagt kildevern også i straffeprosess.¹⁴⁰

Dersom E-tjenesten anvender en kombinert innhenting av metadata og innholdsdata, økes risikoen for kildeavsløring betraktelig. Dette fordi metadata og innholdsdata sammenstilt utvider E-tjenestens informasjonsgrunnlag, for eksempel ved at en IP-adresse kobles til kildens navn, utseende eller motiver. Dataene vil videre kunne avsløre en kildes identitet dersom dataene bidrar til å «sirkle inn» kilden. Det innebærer at datainnhenting/-behandling vil utgjøre et kildeverninngrep dersom dataene i avledet forstand bidrar til å identifisere kilden. For eksempel gjelder dette dersom dataene sammenstilles med andre tilgjengelige opplysninger på E-tjenestens hånd, slik at kildens identitet fremgår av sammenhengen.¹⁴¹

Ettersom praksis viser at opplysninger også kan ha kildevern allerede fordi inngrepet utgjør en nedkjølingsrisiko, kan i teorien alt materiale en medieaktør besitter være vernet. Dersom etterretningsapparatet brukes til å søke etter opplysninger som pressen er betrodd i kraft av sin samfunnsoppgave, kan dette ha en dempende virkning på kildetilgangen og dermed svekke arbeidsvilkårene for den kritiske presse. Det gjelder uavhengig av om kildeidentifiserende opplysninger *faktisk* fremgår av e-kommunikasjonen som innhentes – det er *muligheten* for inngrepet som kan gi nedkjølingseffekt. Kildevernets formål taler for at muligheten for at E-tjenestens befatning med journalistiske data kan ha nedkjølingseffekt, er nok til å anse innholdet av dataene vernet etter § 9-6. I praksis er den mengde datainnhenting tilrettelagt innhenting åpner for dessuten så uoversiktlig, at en betryggende sikring av kildevernet tilsier at alle data som stammer fra en aktør underlagt den beskyttede personkrets etter 9-6 må anses prinsipielt vernet av hovedregelen om behandlings- og innhentingsforbud, jf. §§ 9-6 og 5-2.

4.3 Konklusjon og operasjonalisering av et EMK-forenlig kildevern

Kravet i e-loven § 9-6 om at opplysningen «kan avsløre hvem som er kilde for opplysningen», innebærer at dataene må skape en grad av risiko for kildeavsløring for å ha vern. Vilåret har stor grad av likhet med det vurderingstema EMD-praksis oppstiller for kildevernets objektive rekkevidde etter Artikkel 10. Det kreves lav grad av risiko for å anse opplysningene egnet til

¹⁴⁰ Rt. 2010 s. 1381 A.

¹⁴¹ Prop. 80 L (2019–2020) s. 226.

kildeidentifisering. Fordi formålet er å hindre nedkjøling av kildevernet, kan også journalistisk materiale som ikke inneholder kildeidentifiserende opplysninger være vernet. Vilkåret er utformet i samsvar med Artikkel 10 og er egnet til å tolkes i lys av EMD-praksis.

Kildevern for innholdet i journalistisk materiale avhenger av hvilke opplysninger § 9-6 samlet verner. Inngrep i kildevernet foreligger dersom opplysningene er «betrodd noen i deres journalistiske virke» og «kan avsløre hvem som er kilde for opplysningen», jf. § 9-6.¹⁴² Hvorvidt kildevernets objektive rekkevidde samsvarer med EMK Artikkel 10, beror derfor på en vurdering av om vilkårene i § 9-6 samlet oppstiller et EMK-konformt kildevern.

Gjennomgangen har vist at kravet om at opplysningen «kan avsløre hvem som er kilde» ikke skaper utfordringer til EMK-vernet. Vernets objektive rekkevidde skal tolkes i lys av Artikkel 10 og EMD-praksis.

Det innebærer at E-tjenestens forbud mot å behandle opplysninger som er «betrodd noen i deres journalistiske virke» «og» som «kan avsløre hvem som er kilde» skal tolkes funksjonelt i samsvar med en formålsrettet tilnærming til hvilke aktører som er vernet, og ut fra en lav terskel for opplysninger som anses *egnet* til å avsløre kildevernet materiale. Inngrep må vurderes konkret avhengig av i hvilken grad dataene er av en karakter som gir mulighet for kildeidentifisering. Både metadata og innholdsdata kan være omfattet. Av hensyn til formålet om å hindre nedkjøling av kildevernet, må utgangspunktet være en formodning om behandlingsforbud for alle data om den beskyttede personkrets etter § 9-6.

¹⁴² Se kapittel 3.

5 Materielle og prosessuelle krav til E-tjenestens inngrep i kildevernet

5.1 Generelt om E-tjenestens adgang til inngrep

Som avhandlingen så langt illustrerer, utgjør tilrettelagt innhenting inngrep i kildevernet på flere stadier og i ulik styrke etter hvert som innhentingsprosessen skrider frem. Spørsmål om inngrepenes forenlighet med EMK må vurderes konkret. E-tjenestens adgang til målrettet innhenting av kildevernet materiale etter e-loven § 5-2 og videre behandling etter § 9-6 utgjør selvstendige inngrep i EMK Artikkel 10, men vil her behandles i fellesskap.

Etter § 9-6 andre ledd kan E-tjenesten behandle kildevernede opplysninger dersom det er «strengt nødvendig» at «de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser». Likelydende vilkår for inngrep følger av § 5-2 andre ledd, som gir E-tjenesten adgang til målrettet innhenting mot kildevernet materiale dersom det er «strengt nødvendig». Spørsmålet er om utformingen av reglene i e-loven § 9-6 og § 5-2 om unntaksvis behandling av kildevernet materiale til etterretningsformål oppfyller kravene til inngrep etter EMK Artikkel 10.

Etter EMK Artikkel 10 nr. 2 kan inngrep bare skje dersom det er «foreskrevet ved lov», ivaretar et legitimt formål og er «nødvendig i et demokratisk samfunn». Det innebærer at E-tjenestens befatning med kildevernet materiale må ha lovhjemmel, forfølge et legitimt formål og være nødvendig og forholdsmessig. Nødvendighetskravet innebærer for det første at e-lovens kildevernregler må være *egnet* til å ivareta formålet. Dernest må inngrepet være *nødvendig* og en samlet vurdering må tilsi at regelverket er *forholdsmessig*, herunder at interessene som begrunner inngrepet er mer tungtveiende enn interessene som krenkes. Vurderingen må foretas i lys av statens skjønnsmargin.

Myndighetene har vid skjønnsmargin ved valg av midler for å ivareta nasjonal sikkerhet og trusler mot liv og helse.¹⁴³ Skjønnsmarginen er imidlertid mer begrenset når det gjelder utforming av rammeverk for sikring av menneskerettighetene under et bulklagringsregime.¹⁴⁴

¹⁴³ Weber og Saravia mot Tyskland [A], avsnitt 106.

¹⁴⁴ Big Brother Watch mot Storbritannia [GC] avsnitt 347.

Ettersom tilrettelagt innhenting utgjør en overhengende risiko for nedkjøling av kildevernet, stilles strenge krav til garantier for kildevernets beskyttelse.

Skjønnsmarginen blir snevrere i takt med at myndighetenes kunnskapsgrunnlag om inngrepet øker. Det innebærer at krav til inngrep blir strengere etter hvert som bulkinnhentingsprosessen skrider frem og E-tjenesten får tilgang til informasjon om dataene. Det er illustrerende at EMD uttaler at kildeverninngrep ikke er «*particular serious*» når strategisk dataovervåking utilsiktet innhenter kildevernet materiale i bulk. Til kontrast er målrettet innhenting av kildevernet materiale sammenlignbart med ransaking av en journalist sitt hjem eller arbeidsplass.¹⁴⁵ Dermed gjelder strenge krav til garantier for kildevernet på stadiet for målrettet innhenting og videre behandling, og statens skjønnsmargin er tilsvarende snever.

Kapittelet undersøker om e-loven § 5-2 og § 9-6 oppfyller de krav EMK Artikkel 10 oppstiller for regler som tillater kildeverninngrep under bulklagringsregimer.

5.2 Inngrepet må ha hjemmel i lov

5.2.1 Krav om formell hjemmel i nasjonal rett

E-tjenestens befatning med kildevernet materiale er bare tillatt i den utstrekning inngrepet har hjemmel i lov.¹⁴⁶ Lovkravet etter EMK er tosidig: Inngrepet må ha hjemmel i nasjonal rett, og loven må oppfylle kvalitative krav til tilgjengelighet og klarhet.¹⁴⁷

Målrettet innhenting av kildevernet materiale må følge krav nedfelt i e-loven § 5-2. Krav til videre behandling av dataene fremgår av § 9-6. Tilrettelagt innhenting er ellers utfyllende regulert i e-loven kapittel 7 og 8. Det formelle hjemmelskravet er klart oppfylt.

5.2.2 Lovens kvalitet (legalitet)

Det kvalitative lovkravet innebærer at lovgivningen må angi myndighetenes inngrep så tilgjengelig og presist som forholdene tillater.¹⁴⁸ Behovet for hjemmelighet ved E-tjenestens datainnsamling innebærer imidlertid at full forutberegnelighet for borgerne hverken er

¹⁴⁵ Ibid avsnitt 448.

¹⁴⁶ EMK Artikkel 10 nr. 2. Legalitetsprinsippet følger også av Grunnloven § 113.

¹⁴⁷ Sunday Times mot Storbritannia [J], no. 6538/74, avsnitt 49.

¹⁴⁸ Roman Zakharov mot Russland [J], no. 47143/06, avsnitt 228.

hensiktsmessig eller mulig. For etterretningsregler har EMD tilpasset kravet til lovreglenes forutberegnelighet deretter. Reglene må utformes i tråd med behovet for hemmelighold, men klart nok til at myndighetskontroll ivaretas. EMD stiller krav til rettsgrunnlagets klarhet og at reglene gir garantier mot misbruk.¹⁴⁹

E-loven § 5-2 og § 9-6 angir rettslige rammer for de situasjoner hvor E-tjenesten etter bulkinnhenting kan gjøre inngrep i kildevernet.¹⁵⁰ Reglene oppstiller strenge krav, herunder at unntak fra innhenting- og behandlingsforbudet skal være «strengt nødvendig». Lovteksten gir innsikt i den høye terskelen for at kildevernet materiale havner på E-tjenestens skrivebord. Utgangspunktet om forbud mot inngrep bidrar også til å betrygge. Mangel på forutberegnelighet med hvilke opplysninger som innhentes og under hvilke omstendigheter, må aksepteres i lys av E-tjenestens behov for fordekt innhenting. Risikoen for myndighetsmisbruk avdempes ved at reglene skisserer prosedyrer for kontroll, gjennom krav om at inngrep skal autoriseres av domstolene og kontrolleres av EOS-utvalget.¹⁵¹

Lovgivers utforming av § 5-2 og § 9-6 skaper en viss tvil om kildevernets rekkevidde. Som gjennomgått over, angir § 9-6 i sin utforming et snevrere vern enn kildevernets rekkevidde etter EMK.¹⁵² Det samme gjelder for § 5-2, som eksplisitt henviser til kildevernet § 9-6 angir. Spenningen til EMK-vernet er uheldig med hensyn til lovens kvalitet. Det er e-lovens regler som er primært rettsgrunnlag når E-tjenesten skal bruke reglene, og når domstolene skal kontrollere om inngrep foreligger. Konsekvensen er at et EMK-forenlig kildevern er avhengig av E-tjenestens utvidende tolkning av kildevernets rekkevidde, og tilsvarende hos den enkelte kontrollør (domstoler/EOS-utvalget). Det svekker rettighetens beskyttelse og øker risiko for vilkårlighet. Videre kan en upresis nasjonal kildevernregel ha nedkjølende effekt på pressens kildetilfang i et langsiktig perspektiv, fordi reglene skaper usikkerhet om hvem som egentlig er vernet.

Kildevernet etter § 9-6 og § 5-2 kunne vært utformet klarere av hensyn til et betryggende vern mot inngrep. En uheldig lovtekst av denne karakter er imidlertid ikke nok til å bringe e-lovens kildevernregler i uforenlighet med EMK Artikkel 10. Spenning skal avdempes gjennom

¹⁴⁹ Big Brother Watch mot Storbritannia [GC] avsnitt 333.

¹⁵⁰ Se kap. 2.4.

¹⁵¹ Se kapittel 5.5.

¹⁵² Kapittel 3 og 4.

tolkning av e-lovens kildevernregler i lys av EMK-vernet. Lovens kvalitet er dermed akseptabel.

Spørsmål om kildevernreglens kvalitet er tett tilknyttet vurderingen av nødvendighet og forholdsmessighet, ettersom reglene utgjør selve inngrepet.¹⁵³ Ved spørsmål om regler som hjemler etterretningsfaglig datainnsamling er forenlig med EMK Artikkel 10, har EMD uttalt at vilkårene må ses i sammenheng.¹⁵⁴ Lovreglens utforming vil dermed kunne få betydning ved den samlede vurderingen av inngrepets forholdsmessighet.¹⁵⁵

5.3 Inngrepet må forfølge et legitimt formål

Kildeverninngrep må forfølge minst ett av formålene EMK Artikkel 10 nr. 2 angir. E-lovens regler for E-tjenestens kildeverninngrep må altså ivareta et av disse legitime formålene.

Tilrettelagt innhenting skal beskytte «Norges suverenitet, territoriale integritet og politiske handlingsfrihet samt borgernes rett til liv, frihet og sikkerhet».¹⁵⁶ Formålet sammenfaller med flere formål etter Artikkel 10 nr. 2, herunder «den nasjonale sikkerhet», «territoriale integritet» og «verne andres rettigheter». Innføringen av reglene om tilrettelagt innhenting har et legitimt formål. Det innebærer at også adgang til målrettet innhenting (§ 5-2) og behandling av kildevernede data (§ 9-6), som ledd i bulkinnhentingprosessen, forfølger legitime formål. Til sammenligning fastslo EMD i *Big Brother Watch* at formålskravet var oppfylt for det britiske bulklagringsregimet, som også forfulgte etterretningsformål.¹⁵⁷

¹⁵³ Centrum för rättvisa mot Sverige [GC] avsnitt 248; Big Brother Watch mot Storbritannia [GC] avsnitt 334.

¹⁵⁴ Ibid.

¹⁵⁵ Se kapittel 5.4.7

¹⁵⁶ Prop. 80 L (2019–2020) s. 19; NOU 2022: 9 s. 61.

¹⁵⁷ Big Brother Watch mot Storbritannia [GC] avsnitt 365.

5.4 Inngrepet må være nødvendig og forholdsmessig

5.4.1 Innledende om nødvendighet og forholdsmessighet ved kildeverninngrep under tilrettelagt innhenting

E-tjenesten adgang til kildevernet materiale etter e-loven § 5-2 og § 9-6 er bare tillatt i den utstrekning inngrepene er «nødvendig i et demokratisk samfunn», jf. EMK Artikkel 10 nr. 2. Det innebærer som nevnt at kildevernreglene må være *egnet* til å ivareta formålet, *nødvendig* og *forholdsmessig* på bakgrunn av en samlet interesseavveining. Vurderingen må hensynta statens skjønnsmargin, og hensynet til at norske myndigheter har primæransvaret for sikring av menneskerettighetene (subsidiaritetsprinsippet).

E-loven § 9-6 og § 5-2 er egnet til å ivareta formålet med tilrettelagt innhenting, blant annet ivaretagelse av «den nasjonale sikkerhet», ettersom reglene gir E-tjenesten adgang til kommunikasjonsdata for etterretningsformål. Verktøyet forventes å gi stor etterretningsverdi.¹⁵⁸ For eksempel kan det være effektivt å innhente kommunikasjonsdata mellom en hemmelig kilde og en journalist dersom E-tjenesten mistenker at kilden har betrodd planlegging av en terroroperasjon.

Det foreligger et presserende behov for tilrettelagt innhenting av kildevernet materiale. Teknologisk utvikling har ført til at E-tjenesten har behov for økt tilgang på e-kommunikasjon for å styrke E-tjenestens adgang til å oppdage og følge opp utenlandske trusler mot Norge.¹⁵⁹

Det må videre legges til grunn at ikke mindre inngripende tiltak vil gi samme effekt som tilrettelagt innhenting. Uavhengige utredninger og høringsrunder har vist at alternative løsninger ville gitt liten etterretningsmessig verdi.¹⁶⁰

Spørsmålet er om e-lovens kildevernregler samlet fremstår forholdsmessig. Staten har som nevnt snever skjønnsmargin ved operasjonaliseringen av bulklagringsystemer, herunder utforming av garantier som ivaretar menneskerettighetene. Ettersom kildevernet er beskyttet av EMK Artikkel 10 som en forutsetning for pressefrihet, er skjønnsmarginen for utforming

¹⁵⁸ Prop. 80 L (2019–2020) s. 92.

¹⁵⁹ Ibid s. 97.

¹⁶⁰ Ibid s. 94.

av garantier for kildevernet relativt begrenset.¹⁶¹ Spørsmålet er om samfunnsinteressene som begrunner kildeverninngrep er mer tungtveiende enn interessene som krenkes.

Utgangspunktet er at sterke legitime samfunnshensyn begrunner at tilrettelagt innhenting unntaksvis innhenter og behandler kildevernet materiale. Verktøyet skal verne demokratiske verdier under et moderne trusselbilde. Det taler med tyngde at en rekke demokratiske rettsstater som Norge sammenligner seg med, for eksempel Sverige, har funnet det nødvendig å innføre lignende bulklagringsregimer.¹⁶²

Tilrettelagt innhenting kan samtidig ha negative virkninger for rettsstaten, deriblant en nedkjølingseffekt for kildevernet. Tilrettelagt innhenting må beskytte demokratiske verdier på en måte som lar seg forene med dem.

Formålet med inngrepet må avveies mot inngrepets karakter. Etter e-loven § 5-2 og § 9-6 kan E-tjenesten målrettet innhente/behandle kildevernet materiale dersom det er «strengt nødvendig». Lovteksten legger opp til en nødvendighetsvurdering i tråd med alminnelig menneskerettslig metode og i samsvar med EMK Artikkel 10 nr. 2. En ytterligere beskyttelse for kildevernet er inntatt i ordlyden «strengt», som angir en høy terskel slik at kildeverninngrep er forbeholdt unntakstilfeller. Inngrepvilkåret kan anvendes på ulike tilfeller og legger opp til forholdsmessige avveininger i praksis. Samtidig vil allerede adgangen til bulkinnhenting kunne utgjøre utilsiktede kildeverninngrep i innenlands kommunikasjon, som et «biprodukt» av innhenting. Slike kildeverninngrep gir ikke § 5-2 og § 9-6 beskyttelse mot. E-lovens inngrep i kildevernet fremstår dermed moderat.

Kildevernets stilling avhenger av hvordan reglene anvendes i praksis. Avgjørende for forholdsmessighetsvurderingen er derfor hvorvidt regelverket gir effektive garantier mot misbruk og vilkårlighet.¹⁶³ Spørsmålet er om e-loven § 5-2 og § 9-6 er underlagt effektive garantier mot misbruk slik at reglene samlet fremstår forholdsmessig.

Analysen videre vurderer e-lovens sentrale rettsikkerhetsgarantier, herunder lagring, sletting og deling av kildevernet data, domstolskontroll og EOS-utvalgets mandat. Avslutningsvis foretas en samlet vurdering av reglenes forholdsmessighet.

¹⁶¹ Rt. 2003 s. 593 A avsnitt 49.

¹⁶² Prop. 80 L (2019–2020) s. 88 flg.

¹⁶³ Big Brother Watch mot Storbritannia [GC] avsnitt 450; Se kapittel 2.2.

5.4.2 Lagring

Det følger av § 7-9 at E-tjenesten kan målrettet innhente og lagre innholdsdata med tilhørende metadata «innenfor rammen av rettens kjennelse etter kapittel 8». Det innebærer at når målrettet innhenting avgjøres etter § 5-2, kan retten stille vilkår for lagringens varighet som del av forholdsmessighetsvurderingen.

Inngrepshjemmelen «strengt nødvendig» etablerer også domstolens adgang til å begrense E-tjenestens befatning med kildevernet materiale, både for målrettet innhenting etter § 5-2 og videre behandling etter § 9-6. Det innebærer at domstolen ved inngrep i kildevernet kan stille vilkår for befatningen, for eksempel gjennom krav til lagringen. EMD har lagt til grunn at kontrolløren (dommeren) ikke bare kan «refuse to make a disclosure order», men også «to make a limited or qualified order» «to protect sources from being revealed».¹⁶⁴ Det innebærer at e-lovens «strengt nødvendig» må tolkes dithen at domstolene kan stille vilkår til E-tjenestens datatilgang eller gi en begrenset tilgang. Adgangen gir rom for forholdsmessige løsninger i praksis, ved at domstolene kan begrense omfanget av E-tjenestens datatilgang og varigheten av lagringen.

5.4.3 Sletting

Etter e-loven § 7-7 tredje ledd skal lagrede metadata som hovedregel slettes senest 18 måneder etter innhenting. En spesifisert sletteplikt for kildevernede opplysninger følger av § 9-8. Regelen stadfester at «personopplysninger» og «kildeidentifiserende opplysninger som det er gitt tillatelse til å behandle etter § 9-6 tredje ledd og som ikke er personopplysninger», skal slettes når de ikke lenger er nødvendige for formålet med behandlingen.

Kildevernede opplysninger vil i mange tilfeller være «personopplysninger». I den utstrekning opplysningene ikke er personopplysninger, for eksempel dersom opplysningene avslører en organisasjon som kilde, vil de omfattes av alternativet «kildeidentifiserende opplysninger som det er gitt tillatelse til å behandle etter § 9-6 tredje ledd». Samlet verner § 9-8 alle opplysninger som etter e-loven regnes som kildevernet, både metadata og innholdsdata.

Den spesifiserte sletteplikten for kildevernet materiale bidrar til kildevernreglens forholdsmessighet. Forarbeidene understreker at kildeidentifiserende opplysninger «står i en

¹⁶⁴ Big Brother Watch mot Storbritannia [GC] avsnitt 445.

særstilling» sammenlignet med andre opplysninger E-tjenesten behandler.¹⁶⁵ Dersom E-tjenesten får tillatelse til å behandle slike opplysninger etter § 9-6, vil formålsbegrensningen skjerpes. I praksis betyr det at E-tjenesten plikter å slette kildeidentifiserende opplysninger uten unødig opphold når behandling ikke lenger er nødvendig for formålet etter rettens tillatelse.

5.4.4 Deling

E-loven kapittel 10 gir regler om E-tjenestens utlevering av informasjon av interesse for utenlandsetterretningsformål. Etterretningsrelevant informasjon *skal* deles med Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og andre relevante myndigheter.¹⁶⁶ Vilkår for utlevering til andre myndigheter og stater/organisasjoner følger av hhv. §§ 10-2 og 10-3. Blant annet må utleveringen være forholdsmessig etter § 5-4, jf. § 10-2 bokstav d. Risikoen for kildeverninngrep overfor norske borgere under disse delingsreglene avdempes av at E-tjenestens datainnhenting er formålsbegrenset til utenlandsetterretning. Data som videredeles andre myndigheter etter kapittel 10 er dermed begrenset til data om utenlandske trusler. Slik deling vil sjelden ramme norske borgere, men det er ikke utenkelig at delingsadgangen likevel kan ha dempende virkning på det norske kildevernet. For eksempel vil det være mindre attraktivt for utenlandske kilder å kommunisere med norske journalister.

Tilrettelagt innhenting særpreges av at ikke bare opplysninger om utenlandsetterretning innhentes, men også store mengder opplysninger uten interesse for etterretningsformål – såkalt *overskuddsinformasjon*.¹⁶⁷ Spørsmålet er om e-lovens delingsregler gir en forholdsmessig garanti for kildevernets beskyttelse når kildevernet materiale kan bli bulkinnhentet i form av overskuddsinformasjon.

Det gjelder som hovedregel et forbud for E-tjenesten mot å utlevere overskuddsinformasjon som stammer fra tilrettelagt innhenting, jf. e-loven § 7-13 første ledd. Bestemmelsen stadfester eksplisitt at slik informasjon ikke utløser avvergings- eller opplysningsplikter etter annen lov. Dette utgangspunktet bidrar til å avdempe en potensiell nedkjølingseffekt ved

¹⁶⁵ Prop. 92 L (2022–2023) s. 20.

¹⁶⁶ Prop. 80 L (2019–2020) s. 137.

¹⁶⁷ E-loven § 1-3 bokstav g.

inngrep i kildevernet, ettersom det gir trygghet om at opplysninger uten etterretningsinteresse som utgangspunkt ikke utleveres til andre myndigheter, for eksempel politi.

Etter § 7-13 annet ledd «kan» videredeling til andre myndigheter likevel skje dersom det er «nødvendig» for å «forhindre alvorlig fare for noens liv, helse eller frihet» eller at «noen blir uriktig tiltalt eller domfelt for en straffbar handling». Forarbeidene viser at unntaksadgangen er snever, men aktuell for eksempel «dersom målrettet innhenting av innholdsdata fra et godkjent etterretningsmål viser at etterretningsmålet utsetter sine nærstående for alvorlig vold eller seksuelt misbruker barn». ¹⁶⁸ I slike tilfeller vil det neppe være adgang til å unnlate å varsle uten å bryte statens plikt til å sikre menneskerettighetene. ¹⁶⁹ Dermed kan det i særtilfeller bli påkrevd å utlevere informasjonen til andre myndigheter.

Når E-tjenestens datatilgang som følge av tilrettelagt innhenting kan medføre deleplikt, kan hverken kilder, medieaktører eller e-komtilbydere være trygge på at kilder forblir anonym. At opplysninger i særtilfeller videredeles er imidlertid en uunngåelig konsekvens av rettighetskollisjoner som oppstår under systemet med tilrettelagt innhenting. Når tilrettelagt innhenting anses som et legitimt etterretningsverktøy, er deling i særtilfeller en forholdsmessig konsekvens.

5.4.5 Domstolskontroll

E-loven § 9-6 tredje ledd krever at «[a]vgjørelse om å behandle opplysninger» skal treffes av «retten» etter reglene i e-loven kapittel 8. Det samme følger av e-loven § 5-2 tredje ledd for iverksetting av målrettet innhenting. Dermed må beslutning forelegges retten dersom E-tjenesten ønsker å målrettet innhente eller behandle kildevernede data. Unntak fra innhenting- og behandlingsforbudet krever kjennelse i Oslo tingrett. ¹⁷⁰ E-tjenesten får ikke tilgang til data før etter domstolstillatelse. ¹⁷¹

Domstolskontrollen skjer skriftlig eller for lukkede dører av hensyn til E-tjenestens behov for fordekt innhenting, jf. § 8-3, jf. § 8-1 tredje ledd. Utfyllende garantier for domstolskontrollen følger av e-loven kapittel 8. For eksempel skal retten som hovedregel oppnevne særskilt advokat for ivaretagelse av kontradiksjonshensyn, jf. § 8-5. Kontroll ved uavhengige norske

¹⁶⁸ Prop. 80 L (2019–2020) s. 219.

¹⁶⁹ EMK Artikler 2, 3 og 8; O’Keeffe mot Irland [GC], no. 35810/09.

¹⁷⁰ E-loven § 9-6 tredje ledd, jf. § 8-2.

¹⁷¹ Innst. 402 L (2022–2023) s. 3.

domstoler gir en grunnleggende garanti mot misbruk, og bidrar til å styrke tilliten til kilevernet.

Målrettet innhenting etter e-loven § 5-2 krever rettslig forhåndskontroll, som innebærer at E-tjenesten må gis rettens tillatelse til å bruke aktuelle selektorer for å innhente ønsket informasjon. Forhåndskontroll er en effektiv garanti for kildevernets beskyttelse, så langt domstolene forelegges tilstrekkelig kunnskap til at de kan foreta en informert vurdering av om inngrepet er forholdsmessig.

E-loven § 9-6 legger opp til at domstolskontroll av inngrep i behandlingsforbudet skjer *etter* innhenting.¹⁷² I utgangspunktet er kontroll etter innhenting mindre effektivt som rettssikkerhetsgaranti, da skaden (ulovlig inngrep) kan inntre før kontrollen finner sted. Forhåndskontroll for behandling av data er imidlertid ikke mulig hvor kildevernet materiale innhentes utilsiktet – som «biprodukt» av innhenting. EMD godtar derfor at behandlingen forelegges rettslig kontroll «if and when it becomes apparent that the communication or related communications data contain confidential journalistic material».¹⁷³ Opplysningene skal dermed holdes adskilt og ikke tilgjengeliggjøres for bruk til etterretningsformål inntil retten har truffet beslutning etter § 9-6. Kildevernet materiale som innhentes utilsiktet skal ellers ikke behandles, men slettes.¹⁷⁴ Dermed er behandlingen av dataene i praksis også underlagt forhåndskontroll, ettersom kontroll skal skje før dataene *behandles*.

Det innebærer at det er E-tjenesten som må vurdere når kravet om domstolsprøving etter § 9-6 inntre. Det samme gjelder for målrettet innhenting.¹⁷⁵ Retten prøver ikke lovligheten av E-tjenestens innhenting og behandling på eget initiativ. Domstolsautorisasjon blir et mindre effektivt virkemiddel mot misbruk når det er opp til den som kontrolleres å avgjøre hvorvidt vurdering skal forelegges retten.

Domstolskontrollens effektivitet utfordres også av at et EMK-forenlig kildevern er avhengig av en utvidende tolkning av kildevernets rekkevidde etter § 9-6 og § 5-2.¹⁷⁶ Det medfører risiko for vilkårlighet, både gjennom risiko for at E-tjenesten forelegger færre beslutninger til kontroll og ved at et EMK-forenlig kildevern avhenger av den enkelte dommers tolkning.

¹⁷² Prop. 92 L (2022–2023) s. 13.

¹⁷³ Big Brother Watch mot Storbritannia [GC] avsnitt 450.

¹⁷⁴ Prop. 92 L (2022–2023) s. 16.

¹⁷⁵ Ibid s. 19.

¹⁷⁶ Se kapittel 3 og 4.

Det er videre grunn til å stille spørsmål ved domsapparatets reelle mulighet for kontroll på tidspunktet for E-tjenestens begjæring om målrettet innhenting mot kildevernet materiale. Etter § 5-2 kan målrettet innhenting iverksettes når «konkrete holdepunkter gir grunn til å undersøke om innhenting kan frembringe informasjon». Ved bruk av selektorer mot for eksempel journalister vil en i praksis ha liten kunnskap om *hvilke* data innhenting vil frembringe, samtidig som at innhenting sannsynligvis inneholder store mengder slike data. Målrettet innhenting mot journalistiske aktører er derfor sammenlignbart med ransakelse av en journalists hjem eller arbeidsplass.¹⁷⁷ Ettersom slik innhenting er mer inngripende enn pålegg om å oppgi en kilde, stilles strenge krav til forholdsmessighet. Det er vanskelig å forutse praktiske eksempler på at et alvorlig inngrep i kildevernet kan forsvares som forholdsmessig av hensyn til «å undersøke om innhenting kan frembringe informasjon». Det må kreves at E-tjenesten begrunner behov for inngrep på en måte som er egnet for reell prøving, og det må alltid kreves noe mer enn en generell henvisning til «nasjonale sikkerhetsinteresser».¹⁷⁸ Det stilles strenge krav til E-tjenestens begrunnelse.¹⁷⁹ Det bidrar til å styrke kontrollen at retten alltid kan be om ytterligere informasjon fra E-tjenesten dersom behov.¹⁸⁰ For at inngrepets forholdsmessighet skal være oppnåelig, må domstolene settes i stand til å foreta en tilstrekkelig opplyst forhåndskontroll.

Til sammenligning vil domstolene ha økt mulighet for kontroll på stadiet etter innhenting, når spørsmålet er om E-tjenesten kan behandle dataene, jf. § 9-6. Når dataene har blitt innhentet utilsiktet (som overskuddsinformasjon), er kunnskapsgrunnlaget om dataene større, fordi en har oversikt over hvilke data innhenting har fremskaffet. Det tilrettelegger for en informert forholdsmessighetsvurdering. Da vil det fungere som en «sikkerhetsventil» for kildevernet at domstolskontroll skal skje forut for E-tjenestens behandling av dataene.

Et spørsmål som oppstår i relasjon til domstolskontrollen er om målrettet innhenting og videre behandling av kildevernet materiale krever *to separate kjennelser* fra retten. Alternativet vil være at tillatelse til målrettet innhenting etter § 5-2 *også* automatisk tillater behandling av dataene. Forarbeidene gir ikke svar på spørsmålet. Ettersom reglene i § 9-6 og § 5-2 krever rettslig kjennelse for separate situasjoner, taler loven for at domstolen må ta konkret stilling til reglenes separate vurderingstema. Forsvarsdepartementet har uttalt støtte til denne

¹⁷⁷ Big Brother Watch mot Storbritannia [GC] avsnitt 448.

¹⁷⁸ Prop. 92 L (2022–2023) s. 20.

¹⁷⁹ Ibid s. 47.

¹⁸⁰ Ibid.

tolkningen.¹⁸¹ Dersom E-tjenesten ønsker å innhente og bruke kildevernedede data for etterretningsformål, kan E-tjenesten dermed ikke nøye seg med én kjennelse etter § 5-2, men må også ha tillatelse etter § 9-6.

Dermed oppstår også spørsmål om domstolen i en og *samme* kjennelse kan gi tillatelse til både innhenting og behandling *på forhånd* av E-tjenestens innhenting. Forsvarsdepartementet har antydning at E-tjenesten kan begjære rettens tillatelse etter begge regler forut for innhenting, dersom det før innhenting kan forutses hvilke kildeidentifiserende opplysninger innhenting med stor sannsynlighet vil frembringe.¹⁸²

Mot en slik løsning kan innvendes at kvaliteten av forholdsmessighetsvurderingen svekkes dersom vurderingen av § 9-6 skjer forut for innhenting. Kunnskapsgrunnlaget om inngrepet i kildevernet vil vanligvis være betraktelig mindre før innhenting finner sted, sammenlignet med etter innhenting når konkrete data er fremskaffet. En betryggende sikring av kildevernet nødvendiggjør at domstolen tar konkret stilling til både målrettet innhenting og behandling av opplysningene. Dermed kan det være nødvendig med to separate kjennelser i tid, fordi tilstrekkelig kunnskap om inngrep i form av behandling av dataene ikke kan oppnås forut for innhenting. For at § 9-6 skal kunne fungere som en adekvat sikkerhetsventil for kildevernet, må domstolskontrollen av behandlingen av dataene etter § 9-6 som hovedregel skje etter innhenting.

5.4.6 EOS-utvalgets mandat

Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) er et uavhengig kontrollorgan som fører løpende kontroll med EOS-tjenestene, deriblant E-tjenesten.

E-tjenesten er underlagt EOS-utvalgets alminnelige etterfølgende kontroll, jf. e-loven § 2-6. I tillegg er E-tjenestens etterlevelse av tilrettelagt innhenting gjenstand for EOS-utvalgets løpende kontroll etter e-loven § 7-11 og kan bringes inn for retten etter § 7-12. Det må tolkes

¹⁸¹ Kommunikasjon per e-post med Ianneke Karlsen, saksbehandler i Forsvarsdepartementet 10. november 2023. Gjengitt med samtykke.

¹⁸² Ibid.

dithen at E-tjenestens etterlevelse av kildevernreglene er gjenstand for løpende uavhengig kontroll på alle stadier av bulkinnhentingprosessen.¹⁸³

EOS-utvalgets løpende kontroll er en sentral rettsikkerhetsgaranti for kildevernet, fordi kontrollen gir mulighet for en rask reaksjon dersom ulovligheter foregår. Kombinert med alminnelig etterhåndskontroll gir EOS-utvalgets mandat en viktig garanti for lovmessig, nødvendig og forholdsmessig etterlevelse av e-loven. Videre kan kontrollen gi økt tillit til E-tjenestens virksomhet utad.

Kontrollen bidrar også til å avdemppe ulempene ved at domstolskontrollen inntreffer på E-tjenestens begjæring. Dersom E-tjenesten anlegger en uriktig tolkning av hvilke tilfeller som krever rettens kontroll etter § 5-2 og § 9-6, skal EOS-utvalget følge opp uriktig lovanvendelse og praksis. For eksempel kan EOS-utvalget dersom det avdekkes aktivitet i strid med kildevernet, etter § 7-12 fremme begjæring for domstolene om stans i pågående innhenting og sletting av dataene.

5.4.7 Samlet vurdering

Utgangspunktet for forholdsmessighetsvurderingen er som nevnt at sterke samfunnsbehov begrunner innføringen av tilrettelagt innhenting, inkludert regler som griper inn i kildevernet materiale som ledd i innhentingprosessen. Tilrettelagt innhenting er videre formålsbegrenset til utenlandsetterretning, og loven gir strenge vilkår i saker som berører kildevernet. Loven åpner i moderat grad for kildeverninngrep.¹⁸⁴

E-loven oppstiller ellers adekvate krav til innhenting, lagring, sletting og deling av kildevernet materiale. Inngrep er ellers underlagt uavhengig domstolskontroll og EOS-utvalgets kontroll. Rettsikkerhetsmekanismene gir garantier for kildevernets beskyttelse, og bidrar til at kildevernreglene utgjør forholdsmessige inngrep i Artikkel 10. At reglene skal tolkes i lys av EMD-praksis, underbygger dette.

En kan rette kritikk til at lovgivers utforming av § 5-2 og § 9-6 indikerer at kildevernet har snevrere rekkevidde enn EMK Artikkel 10. Det kan gi nedkjølingseffekt på den vernede personkretsen.¹⁸⁵ Spenningen til EMK kan og skal likevel avdempes gjennom tolkning.

¹⁸³ Prop. 92 L (2022–2023) s. 16–19.

¹⁸⁴ Se kapittel 5.4.1.

¹⁸⁵ Se kapittel 3.

Myndighetskontroll ved domstolene og EOS-utvalget skal sikre en EMK-konform tolkning. Ettersom reglene er underlagt effektive rettsikkerhetsmekanismer, står ikke lovtekstens utforming i veien for at kildevernreglene i § 9-6 og § 5-2 samlet fremstår forholdsmessig.

Samlet oppstiller e-loven et forholdsmessig vern for kildevernet kommunikasjon. I praksis må forholdsmessighetsvurderingen av inngrep alltid skje konkret. Faren for misbruk kan aldri helt elimineres, men reglene i § 5-2 og § 9-6 og tilhørende rettsikkerhetsgarantier tilsier at kildevernreglene fremstår forholdsmessige. Det innebærer at e-loven § 5-2 og § 9-6 er «nødvendig i et demokratisk samfunn» og utgjør lovlige inngrep i kildevernet etter EMK Artikkel 10 nr. 2.

6 Konklusjon og avsluttende betraktninger

6.1 Oppsummering og konklusjon

Tilrettelagt innhenting utgjør et lovlig inngrep i kildevernet etter EMK Artikkel 10, ettersom moderne digitale sikkerhetstrusler tilsier at myndighetene har legitimt behov for innføringen. Fordi bulklagring i hemmelig etterretningstjeneste har et iboende misbrukspotensiale, må imidlertid regler som hjemler inngrep ivareta materielle og prosessuelle krav til kildevernets beskyttelse.

Gjennomgangen har vist at kildevernet etter e-loven § 5-2 og § 9-6 er utformet i en viss spenning til kildevernets rekkevidde etter EMK Artikkel 10, slik det er tolket av EMD og Høyesterett. Spenningen skal avdempes gjennom en funksjonell tolkning i lys av EMD-praksis og prinsipielle Høyesterettsavgjørelser om kildevern i norsk rett. Vernets utforming etter e-loven er dermed ikke til hinder for en EMK-konform tolkning og praktisering av kildevernets rekkevidde.

Avgjørende for om e-lovens kildevern er i samsvar med EMK Artikkel 10, er om § 5-2 og § 9-6 oppfyller krav til inngrep etter Artikkel 10 nr. 2. Reglernes formål er klart legitimt. Reglene kunne vært utformet i klarere harmoni med EMK-vernet, men lovkravet er oppfylt ettersom de norske reglene gir tolkningsrom for en EMK-forenlig praktisering. Videre gir e-loven effektive kildeverngarantier gjennom vilkår for innhenting, lagring, deling, sletting, domstolskontroll og EOS-utvalgets kontroll. I lys av at sterke legitime samfunnsinteresser begrunner tilrettelagt innhenting, fremstår e-lovens kildevernregler i § 5-2 og § 9-6 og tilhørende garantier samlet som forholdsmessig.

Kildevernreglene i e-loven § 5-2 og § 9-6 oppfyller krav til inngrep etter EMK Artikkel 10 nr. 2. Det innebærer at kildevernet i e-loven er utformet i samsvar med EMK Artikkel 10.

6.2 Avsluttende betraktninger

Selv om tilrettelagt innhenting utgjør lovlige kildeverninngrep etter EMK, kan verktøyet *i seg selv* ha en nedkjølende virkning på pressens kildetilfang. Systemet er teknisk komplisert og regelverket uoversiktlig. I tillegg foregår etterretningsvirksomhet hemmelig for befolkningen, slik at praktiseringen av tilrettelagt innhenting er utilgjengelig. For allmennheten kan verktøyet gi assosiasjoner til et «overvåkningssamfunn», og tilhørende frykt for privatliv og kildevern. I tillegg må en forvente at teknologisk utvikling medfører nye utfordringer som ikke kunne forutses da regelverket ble til. Da er det avgjørende at e-loven gir et sterkt kildevern som verner funksjonelt, slik at reglene pedagogisk angir kildevernets beskyttelse overfor E-tjenesten, og at kontrollmyndigheter kan utføre sin rolle som voktere for rettssikkerhet.

Innføring av et datainnsamlingsystem av denne dimensjon åpner dessuten for risiko for misbruk, for eksempel formålsutglidning. Misbruk i de hemmelige tjenestene har skjedd før. Det er risiko for at hensynet til langsiktige konsekvenser for kildevernet kan havne i skyggen av behovet for å beskytte den norske befolkning mot hybride trusler. Desto viktigere blir det at E-tjenestens virksomhet er underlagt kontroll, og at menneskerettslige skranker respekteres.

Det er derfor grunnleggende uheldig at e-loven § 5-2 og § 9-6 er egnet til å skape usikkerhet om kildevernets rekkevidde. På sikt kan konsekvensen bli en nedkjølende effekt på pressens ytringsfrihet, og viktige bidrag til den offentlige debatt kan gå tapt. Det er denne langsiktige nedkjølingseffekt på ytringsfriheten kildevernet først og fremst skal hindre. Det er ønskelig med en avklaring fra EMD om kildevernets rekkevidde under bulklagringsregimer.

Det blir stadig vanligere at ekomtilbydere tilbyr kommunikasjonsløsninger med brukerkrypterte data, som er en type kryptering som hindrer E-tjenestens tilgang gjennom tilrettelagt innhenting, fordi dataene er ende-til-ende-kryptert.¹⁸⁶ Den personvernbevisste holder seg ofte unna for eksempel Facebook, som åpent innsamler brukernes personopplysninger. Krypteringsløsninger kan flytte den digitale kommunikasjonen, fordi kryptering bidrar til trygge miljøer for ytrings- og informasjonsfrihet. Det er en uheldig konsekvens for etterretningsformålet dersom kommunikasjon flyttes til utilgjengelige forumer fordi E-tjenestens metoder fremstår upålitelige. Kildevernet bør håndheves strengt av hensyn

¹⁸⁶ Prop. 80 L (2019–2020) s. 116.

til å sikre tilliten til myndighetene. Det er fordelaktig for alle demokratiets medlemmer at e-lovens kildevern tolkes og anvendes strengt.

Ettersom e-lovens kildevernregler nylig har trådt i kraft, er det ikke enda mulig å si noe om kildevernets stilling *i praksis*. Etter hvert som reglene praktiseres, vil kontrollmyndigheter kunne avdekke om reglene håndheves i tråd med EMK. Tilrettelagt innhenting skal være gjenstand for en uavhengig, offentlig evaluering senest fire år etter full ikrafttredelse, det vil si innen 2. september 2026.¹⁸⁷ Uforutsette problemer kan oppstå teknologisk, rettslig og samfunnsmessig. Det er å forvente at en offentlig, uavhengig evaluering vil gi et bredere grunnlag for å løse de interessekonflikter E-tjenestens metoder reiser.

¹⁸⁷ Prop. 92 L (2022–2023) s. 8

Litteraturliste

Norske lover og forskrifter

Kongeriket Norges Grunnlov, Lov 17. mai 1814.

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

Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).

Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven).

Lov 20. mars 1998 nr. 11 om Etterretningstjenesten (etterretningstjenesteloven).

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

Lov 1. januar 2008 om mekling og rettergang i sivile tvister (tvisteloven).

Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).

Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven).

Lov 18. juni 2023 nr. 54 om endringer i etterretningstjenesteloven (domstolskontroll i saker om kildevern og ved speiling av kommunikasjonsstrømmer mv.).

FOR-2022-09-1626, Instruks om innskrenking av sjefen for Etterretningstjenestens beslutningskompetanse etter etterretningstjenesteloven § 7-3.

Norske lovforarbeider, stortingsmeldinger og forhandlinger i Stortinget

NOU 1988: 2 Kildevern, offentlighet i rettspleien.

NOU 1993: 18 Lovgivning om menneskerettigheter.

Ot.prp.nr.55 (1997–1998) Om lov om endringer i rettergangslovene m.m. (kildevern og offentlighet i rettspleien).

NOU 1999: 27 «Ytringsfrihet bør finde Sted»: Forslag til ny Grunnlov § 100.

NOU 2001: 32 B Rett på sak: Lov om tvisteløsning (tvisteloven).

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

Innst. S. nr. 270 (2003–2004) Innstilling fra kontroll- og konstitusjonskomiteen om endring av Grunnloven § 100.

Innst. S. nr. 75 (2005–2006) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Ågot Valle, Martin Engeset, Kjell Engebretsen, Carl I Hagen og Modulf Aukan om endring av Grunnloven § 100 (ytringsfrihet).

DOK.nr.16 (2011–2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven.

DOK 7:2 (2015–2016) Særskilt melding fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.

NOU 2016: 24 Ny straffeprosesslov.

Rapport avgitt av Lysne II-utvalget 26. august 2016 om digitalt grenseforsvar (DGF).

Innst. 164 S (2016–2017) Innstilling fra kontroll- og konstitusjonskomiteen om Særskilt melding fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.

Høring – Endringer i reglene om kildevern i straffeprosessloven og tvisteloven, Justis- og beredskapsdepartementet, snr. 18/4856, 24. september 2018. Regjeringen.no.

Høring – Forslag til ny lov om Etterretningstjenesten, Forsvarsdepartementet, snr. 2016/2773-5/FD II 4/SIH, 12. november 2018. Regjeringen.no.

Prop. 80 L (2019–2020) Lov om etterretningstjenesten.

Innst.357 L (2019–2020) Innstilling fra utenriks- og forsvarskomiteen om Lov om Etterretningstjenesten.

Høring – Forslag til endringer i etterretningstjenesteloven, Forsvarsdepartementet, snr. 16/2773, 27. juni 2022. Regjeringen.no.

NOU 2022: 9 En åpen og opplyst offentlig samtale – Ytringsfrihetskommisjonens utredning.

Prop. 92 L (2022–2023) Endringer i etterretningstjenesteloven (domstolskontroll i saker om kildevern og ved speiling av kommunikasjonsstrømmer mv.).

Innst. 402 L (2022–2023) Innstilling fra utenriks- og forsvarskomiteen om Endringer i etterretningstjenesteloven (domstolskontroll i saker om kildevern og ved speiling av kommunikasjonsstrømmer mv.).

Internasjonale konvensjoner og rettslige dokumenter

Europarådets konvensjon av 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (Den europeiske menneskerettighetskonvensjonen, ofte forkortet til EMK).

Vienna Convention on the Law of Treaties, Wien, 23 mai 1969 (Wien-konvensjonen).

De forente nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter (SP).

EU- og EØS-rettslige kilder

Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen).

Europarådets ministerkomité's Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information.

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

personvern og elektronisk kommunikasjon (Datapersonverndirektivet - kommunikasjonsverndirektivet).

Europarådets ministerkomité's Recommendation CM/Rec (2016) 4 [1] On the protection of journalism and safety of journalists and other media actors.

EU-domstolens dom 6. oktober 2020 [GC], Privacy International, C-623/17, ECLI:EU:C:2020:790.

EU-domstolens dom 6. oktober 2020 [GC], *La Quadrature du Net and others*, forente saker C-511/18, C-512/18 og C-520, ECLI:EU:C:2020:791

Norske rettsavgjørelser

Rt. 1992 s. 39 A (Edderkopp).

Rt. 2000 s. 996 P (Bøhler).

Rt. 2003 s. 593 A (Valebrokk).

Rt. 2008 s. 489 A (Plata).

Rt. 2010 s. 1381 A (Runestein).

Rt. 2015 s. 93 A (Maria).

Rt. 2015 s. 1286 A (Rolfsen).

HR-2015-2536-A (Oslo Legevakt).

HR-2016-2554-P (Holship).

LA-2021-157502 (Fetteren) (Agder lagmannsrett).

LB-2023-91585 (Dagbladet) (Borgarting lagmannsrett).

Rettsavgjørelser fra EMD

Golder mot Storbritannia [P], no. 4451/70, 21. februar 1975.

Sunday Times mot Storbritannia [J], no. 6538/74, 26. april 1979.

Goodwin mot Storbritannia [GC], no. 17488/90, 27. mars 1996.

Carbonara og Ventura mot Italia [GC], no. 24638/94, 30. mai 2000.

Weber og Saravia mot Tyskland [A], no. 54934/00, 29. juni 2006.

S. og Marper mot Storbritannia [GC], no. 30562/04 og 30566/04, 4. desember 2008.

Társaság a Szabadságjogokért mot Ungarn [J], no. 37374/05, 14 april 2009.

Financial Times mot Storbritannia [J], no. 821/03, 14. mars 2010.

Youth Initiative for Human Rights mot Serbia [J], no. 48135/06, 25. juni 2013.

Nagla mot Latvia [J], no. 73469/10, 16. juli 2013.

O’Keeffe mot Irland [GC], no. 35810/09, 28. januar 2014.

Stichting Ostade Blade mot Nederland [A], no. 8406/06, 27 mai 2014.

Rosiianu mot Romania [J], no. 27329/06, 24. september 2014.

Roman Zakharov mot Russland [J], no. 47143/06, 4. desember 2015.

Nordisk Film & TV A/S mot Danmark [J], no. 60685/02, 8. desember 2015.

Becker mot Norge [J], no. 21272/12, 5. januar 2018.

Big Brother Watch m.fl. mot Storbritannia [GC], no. 58170/13, 62322/14 og 24960/15, 25. mai 2021.

Centrum för rättvisa mot Sverige [GC], no. 35252/08, 25. mai 2021.

Litteratur

Aall, Jørgen, *Rettsstat og menneskerettigheter*, Fagbokforlaget 2018.

Aarli, Ragna, «Massemedienes kildevern», i Aarli, Hedlund og Jebens Aarli, red., *Bevis i straffesaker. Utvalgte emner*, Gyldendal Akademisk 2015.

Høgberg, Alf Petter, Øyrehagen Sunde, Jørn (red.), «Juridisk metode og tenkemåte», Universitetsforlaget 2019.

Kierulf, Anine, «Grunnloven som irrelevant rettskilde», *Lov og rett* 2016/3, s. 185-189.

Kierulf, Anine, *Hva er ytringsfrihet*, Universitetsforlaget 2021.

Kierulf, Anine, «Hvilken rolle spiller Grunnloven § 100 i Høyesteretts ytringsfrihetspraksis?» *Lov og Rett* 2012/2, s. 131–150.

Kierulf, Anine, Rolfsen-saken: Høyesterett som kildevernets rettsavklarer, *Kritisk juss*, årgang 42 nr. 1, s. 55–61.

Kjølbrot, Jon Fridrik, *Den Europæiske Menneskerettighedskonvention: for praktikere*, Djøf Forlag 2023.

Milanovic, Marko, «Surveillance and Cyber Operations» i Mark Gibney, red., *Routledge Handbook on Extraterritorial Human Rights Obligations*, Routledge, 2022.

McDonald, Ian og Williams, John, *Big Brother Watch and ors v. The United Kingdom*, 4 New Square Chambers, Global Freedom of Expression, Columbia University Press, 17. oktober 2018.

Nygård, Nils, *Rettsgrunnlag og standpunkt*, Universitetsforlaget 2004.

Skoghøy, Jens Edvin A, «Nasjonal skjønnsmargin etter EMK», *Lov og rett* 2011, årgang 4.

Solheim, Stig Harald «Rettsanvendelsesprosessen på EMK-rettens område» i Høgberg, Alf Petter (red.) og Øyrehagen Sunde, Jørn (red.), *Juridisk metode og tenkemåte*, Universitetsforlaget 2019.

Uttalelser fra andre organer og institusjoner

Rettslig analyse: «Etterretningstjenesteloven kapittel 7 og 8 i lys av dommer fra Den europeiske menneskerettsdomstolen og EU-domstolen» 26. august 2021. Regjeringen.no.

Personlig kommunikasjon mottatt per e-post med Ianneke Karlsen, saksbehandler i Forsvarsdepartementet 10. november 2023. Gjengitt med samtykke.

Vedlegg: Personlig kommunikasjon mottatt per e-post med Ianneke Karlsen, saksbehandler i Forsvarsdepartementet 10. november 2023.



DET KONGELIGE
FORSVARSDPARTEMENT

Annelin Sødal

Deres ref

Vår ref

Dato

23/00823-2

10. november 2023

Vedrørende spørsmål om etterretningstjenesteloven § 9-6 og § 5-2 i forbindelse med masteroppgave

Det vises til spørsmål vedrørende §§ 9-6 og 5-2 i lov om etterretningstjenesten av 19. juni 2020 nr.77. Det bemerkes innledningsvis at bestemmelsene det vises til nylig har trådt i kraft, det samme gjelder relevante bestemmelser om domstolskontroll etter lovens kapittel 8. Det foreligger således ingen praksis knyttet til de etterspurte forhold.

Det konkrete rettsspørsmålet er ikke direkte adressert i forarbeidene, men loven oppstiller krav til rettslig kjennelse i begge bestemmelsene og det følger etter dette krav til at domstolen skal ha tatt konkret stilling til både målrettet innhenting etter § 5-2 og behandling av opplysninger etter § 9-6. Dette innebærer at det vil kunne være nødvendig med to separate kjennelser. Det vises for øvrig til formålsavgrensing og lovens strenge vilkår i saker som berører kildevernet. Dersom det før den målrettede innhenting kan forutses hvilke kildeidentifiserende opplysninger som innhenting med stor sannsynlighet vil frembringe og som vil være ønskelig å behandle for etterretningsformål vil det være hensiktsmessig å begjære domstolens kjennelse både etter § 5-2 og etter § 9-6, slik at domstolen tar stilling til begge spørsmål i en og samme kjennelse.

Med hilsen

Helle Falkman
avdelingsdirektør

Ianneke Borgersen Karlsen
Seniorrådgiver

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer

Postadresse
Postboks 8126 DEP
0032 OSLO
postmottak@fd.dep.no

Kontoradresse
Glacisgata 1
regjeringen.no/fd

Telefon
23098000
Org.nr 972417823

Avdeling
II 6 Informasjon og
beslutningsstøtte

Saksbehandler
Ianneke Borgersen
Karlsen