UiO : Det juridiske fakultet

Dataavlesing og lovkravet i EMK

En vurdering av straffeprosesslovens regler om dataavlesing i lys av det materielle lovkravet i EMK artikkel 8

Kandidatnummer: 677

Leveringsfrist: 25.04.2017

Antall ord: 16 845

Innholdsfortegnelse

1 INNLEDNING 2

1.1 Tema for oppgaven 2

1.2 Problemstilling og fremstillingen videre 3

2 GENERELT OM GRUNNLAGENE FOR BESKYTTELSEN AV RETTEN TIL PRIVATLIV I NORSK RETT 4

2.1 Innledning 4

2.2 Den europeiske menneskerettskonvensjonen 5

2.3 Grunnloven 6

2.4 Den internasjonale konvensjonen om sivile og politiske rettigheter 7

2.5 Andre overordnede rettsnormer 7

2.6 Oppsummering 7

3 KRAV OM LOV VED INNGREP I RETTEN TIL PRIVATLIV 8

3.1 Kort om lovkrav 8

3.2 Lovkravet i EMK 9

3.3 Lovkravet ved statlig overvåkning 10

4 NÆRMERE OM KRAVET TIL "SAFEGUARDS" VED STATLIG OVERVÅKNING 11

4.1 Generelt om "safeguards" 11

4.2 Krav til innholdet i rettsgrunnlaget 13

4.2.1 Oversikt 13

4.2.2 Generelle innholdskrav 14

4.2.3 Retningslinjer og rammer for utøvelsen av skjønn 18

4.2.4 Sammenfatning 32

4.3 Kontrollmekanismer 32

4.3.1 Oversikt 32

4.3.2 Kravet til prosessuelle sikkerhetsmekanismer 33

4.3.3 Etterhåndskontroll 36

4.3.4 Sammenfatning 38

4.4 Oppsummering 39

4.5 Avsluttende kommentarer til dataavlesingsreglene 41

5 KONKLUSJON 43

LITTERATURLISTE 44

1 Innledning

1.1 Tema for oppgaven

Ved lov 17. juni 2016 nr. 54 vedtok Stortinget å innføre dataavlesing som nytt selvstendig tvangsmiddel, i nye kapittel 16 d i straffeprosessloven. Straffeprosessloven (strpl.) § 216 o hjemler nå *avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem* (dataavlesing) for å avdekke, avverge og forebygge alvorlig kriminalitet, terrorhandlinger og trusler mot rikets sikkerhet.[1] Metoden åpner blant annet for avlesing av data som lagres på pc og mobil, slik som filer og dokumenter, den gir tilgang til brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester, og adgang til å avlytte i sanntid kommunikasjon via for eksempel e-post, SMS og Skype. "Dataavlesing" betegner ikke noen klart avgrenset teknologisk fremgangsmåte, og inngrepspotensialet beror på de tekniske mulighetene og begrensningene i datasystemet.[2]

Metoden innebærer av politiet får utvidet adgang til skjult overvåkning sammenlignet med tidligere.[3] Bakgrunnen for innføringen er blant annet at politiet og andre etterforskningsorganer rapporterer at stadig mer avansert og utbredt bruk av kryptering og andre former for kommunikasjonsbeskyttelse har medført at bruken av de tradisjonelle formene for skjulte tvangsmidler, herunder blant annet kommunikasjonsavlytting og skjult ransaking, ikke gir like godt informasjonsutbytte som tidligere.[4] Politiets sikkerhetstjeneste uttaler seg om dette i sin høringsuttalelse til lovforslaget:

> "Gjennom dataavlesing kan objektets produksjon av viktige dokumenter, herunder krypterte filer, avdekkes. Dette kan gjelde dokumenter som kanskje ikke finnes på det tidspunktet en ransaking av pc-en finner sted, og som kanskje aldri blir sendt elektronisk og derfor heller ikke vil bli fanget opp i forbindelse med en kommunikasjonskontroll. ... Eneste mulighet for å gi politiet tilgang til slik informasjon er derfor gjennom dataavlesing."[5]

Dataavlesing vil kunne gi samme informasjonstilgang som eksisterende tvangsmidler, men har samtidig et langt større potensiale. Det er foreløpig uklart hvilket faktisk overvåkningspotensiale dataavlesing har og vil få.

---

1 Strpl. §§ 216 o første ledd og 222 d, og politiloven § 17 d

2 Prop. 68 L (2015-2016) s. 224

3 Tidligere har politiet hatt adgang til å benytte blant annet skjult ransaking (strpl. kap. 15, § 200 a), romavlytting og annen kommunikasjonskontroll (strpl. kap. 16 a) og telefonavlytting (strpl. kap 16 b)

4 Prop. 68 L (2015-2016) s. 249

5 Prop. 68 L (2015-2016) s. 250

Adgangen til overvåkning gjennom dataavlesing åpner opp for betydelige inngrep i den personlige sfære til den som etterforskes, og vil utgjøre et inngrep i retten til privatliv slik denne er beskyttet gjennom Den europeiske menneskerettskonvensjonen (EMK) artikkel 8.[6] På visse vilkår vil slike inngrep likevel ikke utgjøre en krenkelse av EMK. Et av disse er vilkåret om at inngrepet foretas "in accordance with the law." Dette er delvis et krav om at adgangen til å gjøre inngrep må ha grunnlag i nasjonal rett, men det er også et krav om at grunnlaget tilfredsstiller visse materielle krav.[7] Undersøkelsestemaet i oppgaven er om bestemmelsen om dataavlesing i strpl. § 216 o tilfredsstiller det materielle lovkravet i EMK slik dette er utviklet i rettspraksis.

1.2 Problemstilling og fremstillingen videre

I oppgaven søker jeg å redegjøre for og vurdere dataavlesingsreglene i lys av det materielle lovkravet i EMK. Jeg vil avgrense mot vern av privatliv etter Grl. § 102 første punktum, utenom å redegjøre kort for forholdet mellom EMK og Grunnloven (pkt. 2.3. i oppgaven).

Det særlig interessante ved innføringen av metoden er at "dataavlesing" ikke er et entydig juridisk begrep, men snarere et samlebegrep som omfatter en rekke ulike fremgangsmåter for å fremskaffe informasjon som produseres, lagres eller kommuniseres i eller mellom elektroniske informasjonssystemer.[8] Politiet kan gjennom dataavlesing få tilgang til all *kommunikasjon* til og fra et datasystem, for eksempel en mobiltelefon. Dette innbefatter e-poster, SMS-er, telefonsamtaler og andre kommunikasjonsprogrammer som Skype, Whatsapp, og Messenger. Politiet får også tilgang til alt materiale som er *lagret* på mobiltelefonen, herunder bilder, filmer, dokumenter, Facebookkonto og internettlogg. I tillegg kan politiet blant annet få adgang til mobilens GPS-koordinasjoner, og kan se gjennom mobilkameraet når dette er i bruk. Under samlebetegnelsen dataavlesing er det med andre ord åpnet opp for overvåkningstiltak som kombinerer flere ulike overvåkningsformer samtidig[9], og intensiteten av overvåkningen vil kunne være langt større enn ved anvendelsen av for eksempel kommunikasjonskontroll. Overvåkningspotensialet gjennom dataavlesing er betydelig.

Det oppstår et vidt handlingsrom for politiet ved anvendelsen av dataavlesing. Hvordan og i hvilken utstrekning politiet skal utnytte dette rommet når den rettslige terskelen for å anvende metoden dataavlesing er oppfylt, fremgår ikke av hjemmelsgrunnlaget i strpl. § 216 o. Den

---

6 Se bl.a. Kruslin v. The United Kingdom i avsn. 26, Szabo and Vissy v. Hungary avsn. 52, og Prop. 68 L (2015-2016) s. 38

7 Kjølbro (2010) s. 589

8 Prop. 68 L (2015-2016) s. 224

9 Strpl. § 216 o fjerde ledd

europeiske menneskerettsdomstolen (EMD) har gjennom sin rettspraksis utviklet til dels spesifikke krav knyttet til regler om og gjennomføring av statlige overvåkningstiltak, med det formål å forhindre misbruk av myndighetenes makt på dette området. Det sentrale spørsmålet i oppgaven vil være om regelverket rundt dataavlesing er i samsvar med de særkrav EMD har oppstilt på dette området. Herunder vil et særlig spørsmål være hvilken betydning det har at hjemmelen for dataavlesing ikke regulerer selve utøvelsen av overvåkningen, altså det handlingsrommet som oppstår etter at politi og etterforskningsmyndigheter har fått tillatelse til å anvende dataavlesing. For å svare på dette vil jeg se til rettspraksis fra EMD for å undersøke om det i lovkravet i EMK eksisterer et krav om nærmere regulering av politiets handlingsrom.

I oppgaven videre vil jeg redegjøre for retten til privatliv (kapittel 2) og kravet om lov som gjelder for inngrep i EMK artikkel 8, herunder si noe innledende om lovkravet som gjelder for statlig overvåkning (kapittel 3). På bakgrunn av den særlig inngripende naturen av slike tiltak, og risikoen for myndighetsmisbruk som normativt sett ligger latent i systemer for statlig overvåkning, har EMD på dette området oppstilt skjerpede krav til forholdsmessigheten. I kapittel 4 vil jeg redegjøre nærmere for lovkravet for statlig overvåkning, og vurdere dataavlesingsreglene opp mot dette. I kapittel 5 vil jeg oppsummere og forsøke å trekke noen konklusjoner ut fra det foreliggende kildematerialet.

Reglene om dataavlesing har bare virket siden september 2016, og det finnes ikke ennå offentliggjort rettspraksis eller rapporter som beskriver hvordan reglene hittil har fungert i praksis.[10] Oppgaven vil vurdere om dataavlesingsreglene generelt er i samsvar med det materielle lovkravet i EMK. EMD har i en rekke saker tatt klager til slik "in abstracto"-vurdering, fordi klagerne ofte ikke har kjennskap til om de har blitt utsatt for overvåkning.[11] Jeg vil følge systematikken EMD anvender ved slike vurderinger.

2 Generelt om grunnlagene for beskyttelsen av retten til privatliv i norsk rett

2.1 Innledning

Jeg vil innledningsvis i oppgaven redegjøre for retten til privatliv. Det rettslige utgangspunktet, og den helt sentrale bestemmelsen, er EMK artikkel 8. Innledningsvis vil jeg også redegjøre kort for andre grunnlag for beskyttelsen av retten til privatliv i norsk rett. Formålet er å vise omfanget vernet av privatlivet nyter etter norsk rett, og redegjøre for de grunnleggende

[10] Haugen (2017)

[11] Se Szabó and Vissy v. Hungary avsn. 32

vilkårene for inngrep i denne retten. Jeg vil også trekke frem samvirket mellom rettsgrunnlagene og hvordan de kan supplere hverandre.

2.2 Den europeiske menneskerettskonvensjonen

Den europeiske menneskerettskonvensjonen artikkel 8 første ledd (EMK artikkel 8-1) verner retten til privatliv, og retten til familieliv, hjemmet og korrespondanse. Bestemmelsen gir et generelt vern av respekten for disse rettighetene. Det fremgår av annet ledd (EMK artikkel 8-2) at vernet ikke gjelder absolutt, og at inngrep (”interference”) på visse vilkår er tillatt, blant annet dersom de forfølger et bestemt formål, herunder ”the prevention of disorder or crime”, altså å bekjempe og forebygge kriminalitet. EMD har anerkjent at overvåkning i etterforskingsøyemed utgjør et legitimt formål under EMK artikkel 8.[12] Videre kreves det at inngrepet skjer ”in accordance with the law”, og at det er “necessary” for å oppnå det ønskede formålet. I dette siste ligger et krav om forholdsmessighet i inngrepet.[13] Inngrep i de beskyttede rettighetene i EMK artikkel 8-1 vil være lovlig såfremt inngrepsvilkårene i artikkel 8-2 er tilfredsstilt. Problemstillingen i oppgaven knytter seg altså til det første av disse vilkårene, som fremholder at inngrep i en ellers konvensjonsbeskyttet rettighet må være i samsvar med lov. Det er en sammenheng mellom lovkravet og de øvrige vilkårene for inngrep, ettersom lovkravet til dels skal gjenspeile kravet om legitimt formål og forholdsmessighet. I noen grad vil jeg derfor indirekte komme inn på kravene til legitimt formål og forholdsmessighet, men da kun i relasjon til lovkravet.

EMK og vernet av privatlivet i artikkel 8 er gjort til norsk rett gjennom menneskerettsloven.[14] EMK er gitt forrang fremfor annen lovgivning gjennom menneskerettsloven § 3 jf. § 2. Det samme følger også av straffeprosessloven § 4, som innebærer at loven gjelder med de begrensninger som følger av folkeretten, herunder EMK. Den rettslige konsekvensen av dette er at strpl. § 216 o kan anvendes i den utstrekning den ikke kommer i strid med EMK. [15]

Ved spørsmålet om hvordan man fastlegger innholdet i de enkelte rettighetsbestemmelsene i EMK, gjelder i første rekke de sedvanerettslige tolkningsprinsipper som er kodifisert i Wienkonvensjonen om trakatretten.[16] I tillegg vil en sentral faktor være hvordan EMD selv tolker

---

[12] Klass and Others v. Germany avsn. 42, Szabó and Vissy v. Hungary avsn. 55. Se også Prop. 68 L (2015-2016) s. 40

[13] Prinsippet om forholdsmessighet anses for å være et produkt av den indre motstriden i en konvensjonstekst som inneholder både et inngrepsforbud og et krav om nødvendighet i samme bestemmelse. Det er således et sentralt og gjennomgående element ved vurderingen av tiltak som griper inn i konvensjonsbeskyttede rettigheter, slik Anett Beatrix Osnes Fause beskriver det i sin artikkel i Tidsskrift for norsk strafferett (1/2014).

[14] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett, se § 2

[15] Innst.169 S (2012-2013) s. 32

[16] Aall (2015) s. 36

konvensjonen.[17] I Rt. 2000 s. 996 (Bøhler) la Høyesterett til grunn at norske domstoler skal foreta en selvstendig tolkning av konvensjonen. Høyesterett skal benytte de samme prinsippene som EMD, men ikke anlegge en for dynamisk tolkning, slik at det i første rekke er EMD som har til oppgave å utvikle konvensjonen.[18] Det er uklart om denne ulikheten i tilnærmingen vil ha betydning for vurderingen av EMK artikkel 8 innenfor temaet i denne oppgaven. Jeg kommer ikke til å gå nærmere inn på dette, og vil i oppgaven følge EMDs rettsanvendelse fullt ut.

2.3 Grunnloven

Vernet av retten til privatliv ble ved Stortingets vedtak 13. mai 2014 om endringer i Grunnloven tatt inn i Grunnlovens (Grl.) § 102 første punktum. Med dette nyter retten til privatliv også etter Grunnloven et vern med forrang fremfor annen norsk lov. Det følger av rettspraksis at vernet i Grl. § 102, i likhet med vernet etter EMK artikkel 8, ikke er absolutt.[19] Samtidig gir Grl. § 102 første punktum ingen retningslinjer for når det er tillatt å gjøre inngrep gjennom for eksempel bruk av ulike politimetoder.[20] Høyesteretts praksis etter vedtakelsen av nye Grl. § 102 har lagt innholdet i vurderingen nært opp til det som følger av EMK, her sitert fra Rt. 2015 s. 93:

> ”Grunnloven § 102 [inneholder] ingen anvisning på om det overhodet kan gjøres lovlige begrensninger i privat- og familielivet. Men grunnlovsvernet kan ikke være - og er heller ikke - absolutt. I tråd med de folkerettslige bestemmelsene som var mønster for denne delen av § 102, vil det være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, jf. Rt-2014-1105 avsnitt 28”.[21]

For spørsmålet om grunnlovsbestemmelsens rekkevidde sett opp mot vernet i EMK, ble det i Menneskerettighetsutvalgets rapport lagt til grunn at for bestemmelser som ivaretar den samme rettigheten, må domstoler og forvaltning følge den lovbestemmelsen som går lengst i å gi den enkelte vern.[22] Dette også i lys av Grl. § 92, som pålegger staten ”å sikre og respektere menneskerettighetene” slik de er nedfelt i Grunnloven og i bindende traktater om menneskerettigheter. Høyesterettsdommer Hilde Indreberg drøfter dette i en artikkel i festskrift til Høy-

---

17 EMD tolker konvensjonen, jf. EMK art. 32 jf. art. 19

18 Rt. 2000 s. 996 s. 1007

19 Se Rt. 2015 s. 93 og Prop. 68 L (2015-2016) s. 34

20 Se Rt. 2015 s. 93 og Prop. 68 L (2015-2016) s. 34

21 Rt. 2015 s. 93 avsn. 60

22 Dokument 16 (2011-2012) s. 69

esteretts 200-årsjubileum, og konkluderer med at det er lite sannsynlig at Grl. § 102 vil bli tolket slik at den gir et snevrere vern enn EMK artikkel 8.[23]

2.4 Den internasjonale konvensjonen om sivile og politiske rettigheter

Ved siden av bestemmelsene i Grunnloven og EMK, er retten til privatliv vernet gjennom Den internasjonale konvensjonen om sivile og politiske rettigheter (SP) artikkel 17. Her følger det at ingen skal utsettes for "arbitrary or unlawful interference with his privacy, family, home or correspondence", og at "Everyone has the right to the protection of the law against such interference or attacks.". Konvensjonen er inntatt i menneskerettsloven med forrang foran andre norske lovbestemmelser, jf. § 3.

2.5 Andre overordnede rettsnormer

Også etter EØS-avtalen nyter privatlivet et vern i norsk rett, gjennom Den europeiske unions kommunikasjonsverndirektiv som er inntatt i EØS-avtalen.[24] Kommunikasjonsverndirektivet regulerer retten privatliv på et mer spesifikt område enn de ovennevnte rettsgrunnlagene, og har til hovedformål å beskytte personvernrettigheter innenfor området for elektronisk kommunikasjon.[25] Artikkel 5 i direktivet verner fortroligheten av elektronisk kommunikasjon, og forbyr enhver annen person enn brukerne av slike kommunikasjonstjenester å "avlytte, oppfange, lagre eller på andre måter oppfange eller overvåke kommunikasjonen og tilhørende trafikkopplysninger". Det kan vedtas lovgivningstiltak som begrenser dette vernet dersom tiltaket er "er nødvendig, egnet og rimelig i et demokratisk samfunn av hensyn til ... forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger." Etter EØS-loven § 2 har direktivet ved konflikt forrang fremfor andre bestemmelser som regulerer samme forhold.

2.6 Oppsummering

De ulike grunnlagene for vern av retten til privatliv overlapper hverandre i større eller mindre grad, og gir samlet sett uttrykk for at vernet av privatlivet står sterkt i norsk rett. Innholdet i bestemmelsene i Grunnloven, SP og EØS ligger nært opp til det som følger av EMK artikkel 8, herunder vilkårene for begrensninger i retten, slik som kravet om at inngrepet må forfølge et legitimt formål. I en viss grad utfyller de ulike grunnlagene hverandre, for eksempel har Høyesterett sett hen til bestemmelsen i EMK artikkel 8 ved tolkningen av Grl. § 102. EMD har i sine rettsavgjørelser om EMK artikkel 8 tatt i bruk argumentasjon fra relaterte spørsmål i

---

[23] Indreberg (2015) s. 410

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[25] St.prp. nr. 59 (2003-2004) s. 10

EU-domstolen, for eksempel EU-dommen Digital Rights Ireland.[26] Argumentasjon og prinsipper fra EU-retten vil på denne måten kunne inngå som en del av argumentasjon tilknyttet bestemmelsen i EMK.

Overvåkning gjennom dataavlesing utgjør inngrep i retten til privatlivet etter alle disse rettighetsgrunnlagene. Av de ulike grunnlagene er det EMK som går lengt i å verne retten til privatlivet, blant annet på bakgrunn av EMDs tolkning og anvendelse av konvensjonsbestemmelsen, inkludert innholdet i retten og vilkårene for begrensninger i denne. Det er derfor naturlig å foreta vurderingen av dataavlesingsreglene opp mot vernet som følger av EMK artikkel 8.

3 Krav om lov ved inngrep i retten til privatliv

3.1 Kort om lovkrav

Det gjelder ulike lovkrav i norsk rett. Etter Grunnloven § 113 må myndighetenes inngrep overfor den enkelte ha "grunnlag i lov." Dette er både et formelt og et materielt lovkrav.[27] For å være i samsvar med Grl. § 113 må inngrepet ha hjemmel i formell lov, eller forskrift gitt i medhold av lov. I henhold til det materielle kravet må rettsgrunnlaget også tilfredsstille visse innholdsmessige krav til presisjon og klarhet.

EMK artikkel 8 anses for å angi et materielt lovkrav. "Law"-begrepet i konvensjonen er annerledes enn det norske "lov"-begrepet. Etter EMK artikkel 8 kreves det ikke hjemmel i formell lov, såfremt grunnlaget for inngrepet er anerkjent etter det nasjonale rettssystemet.[28] Til sammenligning må det materielt tilfredsstillende grunnlaget for inngrep fremgå av formell lov for å være i samsvar med Grl. § 113.

Innholdet i det materielle lovkravet vil variere ettersom hvilket rettsområde vi befinner oss på, for eksempel gjelder andre krav, og i en viss grad andre hensyn, bak lovkravet på straffeområdet, sammenlignet med lovkravet for begrensninger i ytringsfriheten etter EMK artikkel 10-2, tvang i barnevernet etter EMK artikkel 8-2 – eller for statlige overvåkningstiltak.

---

[26] EU-dom C-293/12 and C-594/12, sitert iSzabó and Vissy v. Hungary avsn. 23

[27] Se eksempelvis Rt. 2014 s. 1105 avsn. 30

[28] Fause (2014) s. 49 og 50

Inngrep i retten til privatliv utløser det materielle lovkravet i EMK artikkel 8, og også det formelle lovkravet i Grl.§ 113. Disse utgjør dermed komplementære krav til regler om inngrep i denne retten.

3.2 Lovkravet i EMK

Lovkravet i EMK, slik dette fremgår av blant annet EMK artikkel 8-2, gjør seg gjeldende ved ethvert inngrep i konvensjonsrettigheten. EMD har i flere dommer fastslått at eksistensen av regler som tillater skjult overvåkning i seg selv utgjør et inngrep i individets rettigheter etter EMK artikkel 8.[29] Det er uomtvistet at overvåkning gjennom dataavlesing vil utgjøre et inngrep i rettigheten i EMK artikkel 8.

Lovkravet har som nevnt i innledningen tradisjonelt to komponenter: Et krav om grunnlag i nasjonal rett, og materielt krav rettet mot utformingen og innholdet av rettsgrunnlaget. Inngrepet må være forenelig med "rettsstatsprinsippet", eller "the rule of law", og lovgrunnlaget må av den grunn være tilgjengelig, og gi tilstrekkelig forutsigbarhet.[30] For å oppnå dette må lovgrunnlaget være tilstrekkelig presist eller klart.[31] På området for skjult overvåkning har EMD i tillegg fremholdt at loven må inneholde tilstrekkelige sikkerhetsgarantier mot myndighetsmisbruk.[32] Det er problemstillinger knyttet til dette siste som er særlig tema for oppgaven.

Kravet om grunnlag i nasjonal rett innebærer at inngrepet i en konvensjonsrettighet må ha substansiell forankring i nasjonal rett.[33] Foreligger ikke dette, vil inngrepet utgjøre en krenkelse av konvensjonen. Dette kravet kan etter praksis fra EMD anses oppfylt både dersom inngrepshjemmelen er inntatt i form av skreven, formell lov, og dersom den eksisterer som anerkjent ulovfestet rett.[34] Tilsvarende følger det av Grunnlovens § 113 at "Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov." Dette lovkravet går altså lenger enn lovkravet i EMK, og krever at inngrepet har hjemmel i formell lov. Reglene om dataavlesing er vedtatt i lovs form gjennom vedtakelsen av strpl. kap. 16 d, og fyller dermed helt klart kravet om grunnlag i nasjonal rett.[35]

---

29 Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 69, Malone v. The United Kingdom avsn. 64, m.fl.

30 Kjølbro (2010) s. 591

31 Munjaz v. The United Kingdom avsn. 88

32 Malone v. The United Kingdom avsn. 67

33 Fause (2014) pkt. 3 annet avsnitt, og Robathin v. Austria avsn. 40

34 Sunday Times v. The United Kingdom avsn. 47.

35 Se eksempelvis Szabo and Vissy v. Hungary, avsn. 60

Det materielle lovkravet innebærer at det stilles kvalitative krav til rettsgrunnlaget. Hjemmelen må være tilgjengelig, og gi tilstrekkelig forutberegnelighet overfor objektene. Kravet om tilgjengelighet er rettet mot at hjemmelens innhold må være faktisk tilgjengelig for borgerne, og kommer særlig på spissen der en rettsregel gradvis har vokst frem gjennom myndighets- og rettspraksis.[36] Dataavlesingsreglene er kunngjort i Norsk Lovtidend, og publisert i Norges lover, og reiser ikke spørsmål om tilgjengelighet.

Den andre komponenten i det materielle lovkravet er det såkalte forutberegnelighets- eller klarhetskravet. Dette knytter seg til rettsgrunnlagets utforming, og går kort sagt ut på at det må være så presist og klart at individet har mulighet til å innrette seg, eller forutberegne sin rettsstilling.

Forutberegnelighetshensynet er i første rekke knyttet til individets innrettelsesbehov, og gjør seg nødvendigvis ikke gjeldende tilsvarende for bestemmelser om skjulte tvangsmidler som for bestemmelser av handlingsregulerende art, som for eksempel straffebestemmelser.[37] For slike rettshåndhevende inngrep er det materielle kravet rettet mot rettsgrunnlagets klarhet eller presisjon, og har som formål å sikre individene mot myndighetsmisbruk.[38] For å sikre at inngrep ikke foretas etter myndighetspersoners eget forgodtbefinnende må rettsgrunnlaget likevel angi "the circumstances in which and the conditions on which" slike etterforskningstiltak kan iverksettes.[39] Hvorvidt hjemlene er utformet med tilstrekkelig klarhet må vurderes for de ulike delene av lovgivningen.

3.3 Lovkravet ved statlig overvåkning

Lovkravet i relasjon til statlig overvåkning har vokst frem i EMD gjennom en rekke dommer. Blant de første av disse var dommene Klass and Others v. Germany (1978) og Malone v. The United Kingdom (1985), som begge gjaldt skjult overvåkning gjennom telefonavlytting. Gjennom sine rettsavgjørelser har EMD utviklet til dels svært detaljerte krav til innholdet i lovgivning som regulerer statlige overvåkningstiltak.

Lovkravet på dette området skiller seg hermed noe fra lovkravet på områder som for eksempel tvang i psykiatrien eller barnevernet. Hensynet til grunn for dette, jamfør en rekke rettsavgjørelser i EMD, er at ved statlig overvåkning er risikoen for myndighetsmisbruk normativt ansett potensielt svært stor, ettersom lovene som tillater skjult overvåkning samtidig (og nød-

---

36 Til sammenligning, se eksempelvis Kruslin v. France, avsn. 20 flg.

37 Jf. Aall, side 120

38 Aall (2015) s. 120

39 Roman Zakharov v. Russia avsn. 229

vendigvis) tillater at myndighetene arbeider i det skjulte overfor borgerne.[40] En illustrerende uttalelse finner vi i Szabó and Vissy v. Hungary: ”A system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it”.[41]

Kort sammenfattet har EMD av denne grunn oppstilt som krav at regelverket må inneholde tilstrekkelige ”safeguards” (heretter også sikkerhetsmekanismer) mot myndighetsmisbruk.[42] Herunder er det oppstilt en rekke særlige krav knyttet til innholdet i lovgivningen (den regulatoriske gjennomføringen) og til kontrollmekanismer rundt iverksettingen og gjennomføringen av overvåkningen. Disse særkravene må i tillegg tilfredsstille det generelle kravet til tilgjengelighet og forutberegnelighet.

Det kan være verdt å peke på allerede nå at det er en klar forbindelse mellom kravet til rettsgrunnlagets klarhet og kravet til kontrollmekanismer, særlig ved forhåndskontroll i domstolene. Et klart rettsgrunnlag vil kunne bidra til en mer effektiv domstolskontroll. Jeg vil senere i oppgaven se nærmere på betydningen av å ha et klart og presist rettsgrunnlag ved utøvelsen av forhåndskontroll ved domstolene.

4 Nærmere om kravet til ”safeguards” ved statlig overvåkning

4.1 Generelt om ”safeguards”

Kravet til “safeguards” ved statlig overvåkning utgjør én komponent av lovkravet i EMK artikkel 8-2. Ved vurderingen av om det foreligger tilstrekkelige sikkerhetsmekanismer er det avgjørende om rettsreglene angir hvilke vilkår som må foreligge før inngrep kan foretas, og om de inneholder garantier mot vilkårlighet.[43] EMD formulerer dette som et krav om at det foreligger ”adequate and effective guarantees against abuse”,[44] eller “adequate protection against arbitrary interference.”[45] Dette kan knyttes til det jeg har sagt i det foregående om krav til henholdsvis den regulatoriske gjennomføringen og kontroll med etterlevelsen av lov-

---

40 Se eksempelvis Szabó and Vissy v. Hungary avsn. 62, og Klass and Others v. Germany

41 Szabó and Vissy v. Hungary avsn. 57. Se tilsvarende i Kennedy v. The United Kingdom avsn. 167: ”…In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole”

42 Szabó and Vissy v. Hungary avsn. 57

43 Kjølbro (2010) s. 595

44 Roman Zakharov v. Russia avsn. 236, Szabó and Vissy avsn. 57, Rotaru v. Romania avsn. 59

45 Malone v. The United Kingdom avsn. 68, sitert i blant annet Amann v. Switzerland avsn. 56 og Weber and Saravia avsn. 94

reglene. Den overordnede vurderingsnormen er hvorvidt lovverket er i samsvar med "the rule of law", eller rettsstatens prinsipper.[46]

Det fremgår videre av EMDs praksis at vurderingen av om de ulike sikkerhetsmekanismene er tilfredsstillende er relativ, på bakgrunn av de ulike omstendighetene i saken, herunder arten, omfanget og varigheten av de hjemlede overvåkningstiltakene, vilkårene for iverksettelsen av disse, og kontroll med vilkårene gjennom uavhengig myndighet.[47] I dommen Roman Zakharov v. Russia finner man et illustrerende eksempel på samspillet mellom de ulike komponentene i kravet. EMD trakk frem at myndighetene var tillagt nærmest ubegrenset skjønn ved vurderingen av hvilke handlinger som utløste en slik trussel mot rikets sikkerhet at det var nødvendig å iverksette overvåkningstiltak. I forlengelsen av dette uttaler EMD at det er av betydning at

> "Prior judicial authorisation for interceptions is required in Russia ... Such judicial authorisation may serve to limit the law-enforcement authorities' discretion."[48]

Med andre ord kan svakheter ved deler av lovverket avhjelpes av andre mekanismer, slik at regelverket samlet sett møter kravet til "adequate and effective guarantees against abuse."

Kjernen i disse kravene er å beskytte borgerne fra vilkårlige inngrep fra myndighetene.[49] Kravet har i naturlig forlengelse av dette en side til et annet av de generelle inngrepsvilkårene i EMK artikkel 8-2, kravet om at inngrep må være "necessary in a democratic society". Jeg siterer her fra Roman Zakharov v. Russia i avsnitt 236:

> "The "quality of law" … implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society"…."

Ved kravet til "necessary in a democratic society", er det i premissene i Klass and Others v. Germany og senest i Szabó and Vissy v. Hungary slått fast at for statlig overvåkning gjelder et krav om "strict necessity" mellom inngrepet og det ønskede formålet, ikke bare som en generell betraktning ved gjennomføringen av innføringen av overvåkningsreglene, men som en

---

46 Se blant annet Malone v. The United Kingdom avsn. 67

47 Szabó and Vissy v. Hungary avsn. 57

48 Roman Zakharov v. Russia avsn. 248-249

49 Dette går igjen i så og si alle dommene som omhandler dette temaet, i litt ulike formuleringer: "Arbitrary interference" (Malone v. The United Kingdom), "abuse" (Szabó and Vissy v. Hungary), "misuse of power" (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria)

konkret vurdering ved inngrepet i hver enkelt sak.[50] En konsekvens av dette er at *regelverket* må ivareta kravet til streng nødvendig. Jeg vil redegjøre nærmere for dette, og betydningen det har for kravet til utformingen av rettsreglene, etter hvert i oppgaven.

Formålet med kravet til "safeguards" er i siste rekke å sikre at de inngrepene som foretas, er i samsvar med et krav om "strict necessity" mellom inngrep og formål. Dette har én side til kvaliteten av rettsgrunnlaget, og en annen side til prosessen rundt iverksettingen av inngrepet. Kontrollmekanismer som sikrer prosessen rundt iverksettingen og gjennomføringen av statlige overvåkningstiltak hører derfor også til lovkravet, med det formål å begrense "The 'interference' to what is 'necessary in a democratic society.'"[51]

Oppsummert innebærer kravet til "safeguards" at loven må inneholde tilstrekkelige sikkerhetsmekanismer for å beskytte borgerne mot vilkårlige inngrep fra offentlig myndighet, det vil si sikre at inngrep som foretas er "strictly necessary" i henhold til artikkel 8-2. Dette stiller krav til henholdsvis den regulatoriske gjennomføringen og til kontrollmekanismer. De ulike delene av kravet virker i nær sammenheng, og er hver for seg og samlet av betydning for om rettsgrunnlaget tilfredsstiller kravet til "adequate and effective guarantees against abuse."

I det følgende vil jeg redegjøre nærmere for de ulike komponentene av lovkravet slik dette gjelder for statlige overvåkningstiltak, herunder dataavlesing. Jeg vil følge systematikken fra dommen Szabó and Vissy v. Hungary, og redegjøre først for kravene til innholdet i rettsgrunnlaget, og deretter kravet til kontrollmekanismer knyttet til iverksettingen og gjennomføringen av tiltaket. I relasjon til lovkravet er deler av lovgivningen ganske klart i samsvar med kravene i EMK, og jeg vil kort redegjøre for disse elementene. Jeg vil konsentrere hoveddelen av drøftelsen om den delen av lovreguleringen som kan tenkes å være problematisk sett opp mot lovkravet. Dette er knyttet særlig til det jeg pekte på i innledningen, at hjemmelen for dataavlesing ikke regulerer selve utøvelsen av overvåkningen, altså det handlingsrommet som oppstår etter at politi og etterforskningsmyndigheter har fått tillatelse til å anvende dataavlesing. Jeg vil komme nærmere inn på dette i punkt 4.2.3 og 4.3.

4.2 Krav til innholdet i rettsgrunnlaget

4.2.1 Oversikt

Kravene til innholdet i rettsgrunnlaget, eller det EMD betegner som "the quality of the law",[52] utgjør én side av kravet til "safeguards." Formålet med kravet er både å sikre at den regulatoriske gjennomføringen isolert sett ivaretar kravet om "strict necessity" mellom tiltak og for-

[50] Szabó and Vissy v. Hungary avsn. 73

[51] Szabó and Vissy v. Hungary avsn. 57

[52] Szabó and Vissy v. Hungary avsn. 59

mål, og å sikre at rettsgrunnlaget gir domstolene tilfredsstillende grunnlag for å vurdere om tiltaket er i samsvar med dette nødvendighetskravet. Et sentralt poeng i denne forbindelse er at det er samvirket mellom disse aspektene av lovkravet som bidrar til å begrense misbruksfaren.

Forbindelseslinjen mellom kravet til innholdet i rettsgrunnlaget og kravet om at inngrepet ikke må gå ut over det som er "strictly necessary" er også understreket av EMD. Følgende har gått igjen i flere av dommene på dette området, særlig der hvor domstolen har vurdert lovgivningen på generelt grunnlag:

> "The lawfulness of the interference is closely related to the question whether the 'necessity' test has been complied with … It is therefore appropriate for the Court to address jointly the 'in accordance with the law' and 'necessity' requirements."[53]

Her uttaler EMD at på bakgrunn av den nære sammenhengen mellom kravet til rettsgrunnlaget og kravet om at inngrepet er "necessary" er det hensiktsmessig å behandle disse kravene samlet. På bakgrunn av dette vil jeg knytte vurderingen av om den regulatoriske gjennomføringen er tilfredsstillende opp mot kravet om "strict necessity", altså vurdere om lovgrunnlaget er egnet til å ivareta dette kravet.

I det følgende vil jeg redegjøre for de innholdsmessige kravene som følger av EMK etter praksis fra EMD, og foreta en fortløpende vurdering av dataavlesingsreglene opp mot disse. Kravet kan grovt sett deles i to: Krav til hva lovgivningen innholdsmessig bør regulere (pkt. 4.2.2), og krav til hvordan rettsgrunnlaget må være utformet, gjennom et krav om at lovverket inneholder retningslinjer og rammer for utøvelsen av skjønn (pkt. 4.2.3). Jeg vil vurdere delene av kravet hver for seg, og deretter samlet (pkt. 4.2.4).

4.2.2 Generelle innholdskrav

EMD har fremholdt at ved statlig overvåkning må loven som et minstekrav angi "the scope of application of secret surveillance measures", det vil si under hvilke omstendigheter myndighetene har adgang til å iverksette skjult overvåkning.[54] I Roman Zakharov v. Russia sammenfatter EMD fra tidligere domspraksis en rekke minstekrav til reguleringen av statlig overvåkning:

> "The Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to

[53] Szabó and Vissy v. Hungary avsn. 58, Kennedy v. The United Kingdom avsn. 155, Kvasnica v. Slovakia avsn. 84, Roman Zakharov v. Russia avsn. 236

[54] Roman Zakharov v. Russia avsn. 243, Rotaru v. Romania avsn. 61

> an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed."[55]

EMD fremholder her at rettsgrunnlaget "should" angi disse vilkårene. Momentene inngår for seg i en helhetsvurdering av om lovkravet på dette punktet er ivaretatt. Betydningen av at lovgrunnlaget skulle være mangelfullt på for eksempel ett eller to av punktene, er ikke klart fastlagt i EMDs praksis. Veiledende på dette punkt er at kravet som nevnt er relativt, og vil variere på bakgrunn av inngrepets art, varighet, med mer. EMDs praksis har vist at loven på noen punkter kan være relativt vag og likevel være innenfor grensene av lovkravet.[56]

Et eksempel som likevel kan illustrere et "nedre sjikt" av oppfyllelsen av denne delen av lovkravet er dommen Amann w. Switzerland. EMD vurderte ordlyden i en bestemmelse som anga at "[the federal police] Shall provide an investigation and information service in the interests of the Confederation's internal and external security", herunder gjennom skjult overvåkning. EMD trakk frem at loven verken indikerte hvilke personer som kunne omfattes av overvåkningen, hvilke nærmere omstendigheter som kunne gi adgang til iverksettelse av slike tiltak, hvilke metoder politiet kunne benytte, eller hvilke prosedyrer som måtte følges. Retten konstaterte brudd på EMK art. 8, ettersom loven dermed ikke gav tilfredsstillende beskyttelse for borgerne mot konvensjonsstridige inngrep i deres rett til privatliv. [57]

Kravet innebærer altså at loven konkret bør regulere visse tema som er vurdert å være av betydning for en rettssikker anvendelse av regelverket, som for eksempel hvilke lovovertredelser som etter nasjonal rett kan danne grunnlag for statlig overvåkning. Her igjen ser man sammenhengen mellom de ulike vilkårene for inngrep i EMK, ettersom en angivelse av lovovertredelsen gir domstolene (i første rekke nasjonalt, og i siste rekke eventuelt EMD) mulighet til å vurdere om overvåkningstiltaket forfølger et formål som er legitimt under EMK artikkel 8-2. Hvor strengt kravet til innholdet i reguleringen er vil kunne avhenge delvis av hvilket tema det er snakk om, og delvis av om lovgrunnlaget etter en helhetsvurdering anses å tilfredsstille kravet. Dersom lovreguleringen er mangelfullt utbygget vil EMD, som i Amanndommen, kunne komme til at regelverket ikke møter kravet i EMK artikkel 8-2.

---

55 Roman Zakharov v. Russia avsn. 231, Szabó and Vissy v. Hungary avsn. 56, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 76

56 Se Roman Zakharov v. Russia avsn. 244 og Szabó and Vissy v. Hungary avsn. 64

57 Amann w. Switzerland avsn. 58

Jeg vil i det videre foreta en vurdering av dataavlesingsreglene opp mot kravet om hva det nasjonale regelverket bør regulere, etter modell fra premissene i Roman Zakharov v. Russia. Spørsmålet er både om loven regulerer disse temaene, og om lovreguleringen innholdsmessig sett er tilfredsstillende. Spørsmålet om samsvar mellom utformingen av rettsgrunnlaget og kravet til "strict necessity" ved et konkret tiltak vil jeg se nærmere på i pkt. 4.2.3 og avslutningsvis i 4.2.4. For spørsmålet om den generelle innholdsmessige reguleringen vil jeg se lovreguleringen opp mot det overordnede kravet om "adequate and effective guarantees against abuse." Dette fordi disse innholdskravene retter seg i større grad mot å forhindre misbruk og vilkårlighet generelt, mens de mer skjønnsmessige vilkårene er av større betydning for den konkrete forholdsmessigheten i inngrepet, som jeg vil komme tilbake til.

I strpl. § 216 o er det angitt en rekke vilkår knyttet til iverksettingen av overvåkning. Strpl. § 216 o første ledd angir "the nature of offences" gjennom å henvise til vilkåret om at det må foreligge mistanke om en handling eller forsøk på en handling med minimum ti års strafferamme *eller* en av de lovovertredelsene som er spesifisert ved henvisning til de aktuelle straffebudene i første ledd bokstav b.

Dataavlesing kan på visse vilkår anvendes i avvergende og forebyggende øyemed. I strpl. § 222d er det hjemlet tillatelse for henholdsvis politiet og Politiets sikkerhetstjeneste (PST) til å benytte dataavlesing for å avverge lovbrudd. I medhold av politiloven § 17d kan PST få adgang til å anvende dataavlesing i forebyggende øyemed. I disse hjemlene henvises det uttømmende til de straffebudene som gir adgang til å anvende dataavlesing.

EMD har presisert at det i utgangspunktet er tilstrekkelig at loven angir lovbruddets art ("nature"),[58] og i Roman Zakharov v. Russia godtok EMD som tilstrekkelig klart at loven gav adgang til overvåkning ved mistanke om lovovertredelser av "medium severity", "a serious offence" eller "an especially serious criminal offence."[59] En tolkning av dette tilsier at kravet på dette punktet ikke er svært strengt.[60] Strpl. §§ 216 o og 222d og politiloven 17d må anses å ivareta minstekravet slik dette følger av EMD.

Strpl. § 16 o angir "a definition of the categories of people liable to have their telephones tapped", gjennom å sette som vilkår at iverksettingen av slike tiltak kan foretas dersom det foreligger skjellig grunn til mistanke mot "noen". Det innebærer at adgang til skjult overvåkning bare skal iverksettes når det foreligger en konkret og kvalifisert mistanke mot én eller flere bestemte personer. Til sammenligning var det i premissene i Roman Zakharov v. Russia im-

58 Roman Zakharov v. Russia avsn. 244

59 Roman Zakharov v. Russia avsn. 244

60 Tilsvarende i Kennedy v. The United Kingdom avsn. 159

plisert at det var tilfredsstillende i henhold til EMK at loven bestemte at overvåkningen kunne foretas overfor en mistenkt eller tiltalt person.[61]

Straffeprosessloven inneholder videre "a limit on the duration of telephone tapping". Strpl. § 216 o femte ledd viser til at strpl. § 216 f gjelder tilsvarende. Etter denne bestemmelsen skal tillatelse til [dataavlesing] gis for et bestemt tidsrom, som må begrenses til det som er strengt nødvendig. Strpl. § 216 o femte ledd begrenser varigheten til maksimalt 2 uker av gangen. Etter strpl. § 216 f annet ledd må dataavlesingen i alle fall avsluttes dersom vilkårene for kontroll ikke lenger antas å være til stede, eller dersom tiltaket ikke lenger anses hensiktsmessig. Tilsvarende følger også av den generelle regelen i strpl. § 170 a, som krever at det må påvises "tilstrekkelig grunn" for ethvert tvangsmiddel, og at det ikke må utgjøre et uforholdsmessig inngrep.

Videre må det eksistere regler knyttet til "the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed." Strpl. § 216 o femte ledd viser til at strpl. §§ 216 d-216 k gjelder tilsvarende. Disse inneholder regler om tilintetgjøring av overskuddsmateriale (§ 216 g) og taushetsplikt om opplysningene som fremkommer (§ 216 i). I tillegg er det i lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) og i forskrift om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften) angitt utførlige regler knyttet til behandlingen av opplysninger innhentet i forbindelse med politietterforskning, og vilkårene for videreformidling, lagring og tilintetgjørelse av disse. Jeg vil ikke gå inn på en nærmere redegjørelse av innholdet i disse, men da norske regelverket på dette punkt er relativt grundig lovregulert er det nok ganske klart at det her foreligger samsvar med kravet i EMK.

Oppsummert fremstår straffeprosessloven å være i samsvar med kravet i EMK hva gjelder de generelle innholdsmessige kravene. Straffeprosessloven med tilstøtende regelverk adresserer alle de påkrevde temaene. Disse er i tillegg relativt detaljert regulert i lovgivningen. Detaljgraden fremstår tilfredsstillende sett opp mot kravet om "adequate and effective guarantees against abuse" også sammenlignet med lignende systemer i andre land, se for eksempel Kennedy v. The United Kingdom, og Weber and Saravia v. Germany. At regelverket fremstår tilfredsstillende på dette punkt, vil være av betydning ved helhetsvurderingen av regelverket.

---

[61] Roman Zakharov v. Russia avsn. 245. Se også Kennedy v. The United Kingdom avsn. 160

4.2.3 Retningslinjer og rammer for utøvelsen av skjønn

Den andre delen av kravet til lovens innhold er av mer overordnet karakter, og har sammenheng med "the rule of law"-idealet. Under denne fanen anses det som en viktig garanti mot myndighetsmisbruk at regelverket ikke overlater skjønnsutøvelse til myndighetene i form av et ubegrenset skjønn ("unfettered power").[62] I Szabó and Vissy v. Hungary utdypes dette, og konsekvensene det har for regelgjennomføringen:

> "Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity."[63]

Sitatet illustrerer sammenhengen mellom kravet til lovens innhold og kravet om å begrense faren for myndighetsmisbruk. I Roman Zakharov v. Russia kritiserer EMD den russiske lovgivningen for å overlate til myndighetene et nesten ubegrenset skjønn når det kommer til å definere innholdet i begrepet "national, military, economic or ecological security",[64] og i Gillan and Quinton v. The United Kingdom hadde den enkelte politimann under "stop and search"-reglene et for vidtgående skjønn ved avgjørelsen av hva som var "hensiktsmessig" (expedient) for å forhindre terrorhandlinger.[65] Fra dette kan man utlede at når en hjemmel angir "the nature of offences", kan den likevel komme til kort etter EMDs standard dersom myndighetene tillegges stort skjønn ved vurderingen av om en handling utgjør en (kvalifiserende) "offence". EMD fremholder derfor at myndighetenes spillerom bør begrenses, gjennom regulering i lov, eller ved annen form for ekstern kontroll, for eksempel, og fortrinnsvis, ved domstolene.[66] Domstolene vil kunne prøve vilkårene i skjønnsmessige begreper, eller etterse at politiet følger en konsekvent praksis.[67]

I et ideologisk perspektiv beskriver Jeremy Waldron det slik:

> "The Rule of Law is a multi-faceted ideal ... people in positions of authority should exercise their power within a constraining framework of public norms rather than on the basis of their own preferences, their own ideology, or their own individual sense of right and wrong."[68] (min utheving)

---

62 Roman Zakharov v. Russia avsn. 230

63 Szabó and Vissy v. Hungary avsn. 65

64 Roman Zakharov v. Russia avsn. 248

65 Gillan and Quinton v. The United Kingdom, sitert i Fause, Tidsskrift for strafferett (1/2014)

66 Se blant annet Rotaru v. Romania avsn. 59

67 Se Szabó and Vissy v. Hungary avsn.73

68 Waldron (2008) s. 5

Rent overordnet er det kravet om rammer for utøvelsen av skjønn, eller myndighetenes "discretionary powers", som må regnes som den mest grunnleggende bestanddelen av kravet til rettsgrunnlagets innhold. De øvrige innholdsmessige kravene er på et vis en utkrystallisering av dette overordnede ønsket om, eller behovet for, å sette rammer for myndighetspersoners utøvelse av skjønn ved iverksettingen av skjulte tiltak slik som overvåkning. Det sentrale formålet er å sikre at det ikke forekommer myndighetsmisbruk gjennom vilkårlighet, uforholdsmessige inngrep, eller inngrep med illegitime formål. Ser man dette i sammenheng med det rettsstatlige idealet som Waldron referer til, er det et spørsmål om å begrense myndighetenes makt, hvor det er risiko for at denne går på bekostning av andre, grunnleggende verdier i et demokratisk samfunn.

Videre under dette punktet vil jeg vurdere dataavlesingsreglene opp mot dette kravet. Spørsmålet er særlig om rammene for skjønn er egnet til å begrense utstrekningen av inngrepet til det som er "strictly necessary."

Det følger av strpl. § 216 o at det må foreligge "skjellig grunn" til mistanke om at lovovertredelsen er foretatt eller forsøkt foretatt. I tillegg må dataavlesingen være av "vesentlig betydning" for å oppklare saken, og oppklaringen må ellers i "vesentlig grad" bli vanskeliggjort. Strpl. kapittel 16 d må i tillegg anvendes i samsvar med strpl. § 170 a, som krever at inngrepet er hensiktsmessig og forholdsmessig.

Ved anvendelse av dataavlesing i medhold av strpl. § 222d og politiloven § 17d kreves det henholdsvis "rimelig grunn til å tro" og "grunn til å undersøke." Mistanketerskelen er senket, sammenlignet med kravet om "skjellig grunn" i strpl. § 216 o, men samtidig er straffeterskelen høy.

Innholdet i vurderingskriteriene i disse hjemlene er underlagt forhåndskontroll ved domstolene, jf. første ledd første punktum, og vurderingene er dermed etterprøvbare og underlagt uavhengig avgjørelsesmyndighet. Tillatelse etter strpl. § 216 o er også knyttet opp mot et "kanskjønn", slik at det i alle tilfeller vil være opp til retten å vurdere om iverksettelse av dataavlesing ut fra alle omstendighetene er et forholdsmessig tiltak.[69]

Så langt det gjelder vilkårene for iverksettelse av dataavlesing synes politiets skjønn å være underlagt rammer og begrensninger, i tråd med kravet i EMK.[70] Det jeg vil se nærmere på nå

[69] Prop. 68 L (2015-2016) s. 44

[70] Jf. også Kennedy v. The United Kingdom

er hvilke begrensninger som ligger i politiets skjønnsmakt ved gjennomføringen av dataavlesingen.

Det følger av strpl. § 216 o at retten kan "Gi politiet tillatelse til å foreta avlesing av ikke tilgjengelige opplysninger i et datasystem (dataavlesing)." Avlesingen kan bare gis i bestemte datasystemer eller brukerkontoer, jf. fjerde ledd. Og videre: "Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen."

Ordlyden tilsier at politiet er påkrevet å angi datasystemet eller brukerkontoen de ønsker å overvåke, og at avlesingen må begrenses til informasjonsstrømmene i disse.[71] Innenfor disse rammene er politiet ikke påkrevet å avgrense overvåkningen til deler av de tilgjengelige informasjonsstrømmene, ettersom de ulike dataene er opplistet som alternativer overvåkningen "kan" omfatte, innforstått også kombinasjon med hverandre.[72] Ordlyden i lovteksten tillegger politiet vide fullmakter for valg av hvilket informasjonsmateriale de ønsker å avlese og innhente, og hvilke kanaler de ønsker å anvende. En slutning fra dette tilsier at en tillatelse til å avlese noens mobiltelefon dermed vil kunne gi faktisk adgang til å lese SMSer, lytte til telefonsamtaler, få tilgang til e-post, logge tastetrykk, følge vedkommendes GPS, lese notater, få tilgang til mikrofon og kamera når disse er i bruk, med mer, i tråd med overvåkningspotensialet som ligger i metoden.

Heller ikke i forarbeidene til loven, Prop. 68 L (2015-2016), eller Metodekontrollutvalgets rapport fra 2009, berører dette, noe jeg vil komme nærmere tilbake til.

Kripos har bekreftet at politiet i utgangspunktet ikke må avgrense avlesingen til å gjelde for eksempel bare telefon- og SMS-kommunikasjon. Samtidig ble det opplyst om at retten i kjennelsen som tillater dataavlesingen har adgang til å begrense overvåkningen til å omfatte bare deler av datasystemet.[73] Denne adgangen fremgår ikke i direkte ordelag av strpl. § 216 o, utenom eventuelt implisitt i at dataavlesingen "kan" omfatte de nevnte formene for data. Dersom man legger til grunn at dette er en fullmakt retten har og i aktuelle tilfeller tar i bruk, vil det være relevant ved vurderingen av lovkravet, særlig i relasjon til kravet til kontrollmekanismer. Dette vil jeg komme tilbake til i pkt. 4.3.

Lovtekst og forarbeider isolert sett tillegger politiet frihet til etter eget skjønn til å velge hvordan og i hvilken utstrekning overvåkningen skal gjennomføres.

---

71 Jf. også Prop. 68 L (2015-2016) s. 264

72 Prop. 68 L (2015-2016) s. 265

73 Sætnan (2017)

Betydningen dette kan ha i praksis, sett opp mot bruk av andre skjulte tvangsmidler, kan illustreres slik: Dersom overvåkningsmetodene er begrenset til enten kommunikasjonsavlytting eller skjult ransaking kunne man ideelt sett se at domstolene får seg forelagt følgende problemstilling: "Er det "strictly necessary" å iverksette telefonavlytting for å etterforske en mistenkt i en sak om menneskehandel." Domstolene kan slik ta stilling til om det anvendte middelet er forholdsmessig sett opp mot det ønskede formålet. Denne testen lar seg langt vanskeligere svare på når det kommer til anvendelsen av dataavlesing: "Er det "strictly necessary" å iverksette telefonavlytting/GPS-tracking/key-logging/overvåkning av e-post - med mer, for å etterforske en mistenkt i den konkrete saken." Situasjonen kan tenkes å oppstå hvor det er ansett strengt nødvendig å avlytte kommunikasjonen til og fra et datasystem, men ikke å få adgang til GPS-tracking, data lagret i datasystemet slik som notater, dokumenter og bilder, eller aktivitet på applikasjoner eller andre programmer i datasystemet. For å trekke linjene tilbake til de grunnleggende delene av lovkravet, oppstår her etter mitt syn spørsmålet om den regulatoriske gjennomføringen er innholdsmessig tilstrekkelig til å forhindre misbruk og tvangsmiddelbruk ut over tilfeller hvor det er strengt nødvendig.

Temaet for drøftelsen videre er først om kravene til innholdet i rettsgrunnlaget omfatter regulering av selve gjennomføringen av overvåkningen. Videre er spørsmålet om det norske regelverket er i samsvar med et eventuelt krav på dette området, eller denne delen av overvåkningen i for stor grad er underlagt politiets skjønn. Med andre ord om lovens form og innhold, eller mangel på sådan, er i samsvar med kravet i EMK. Hertil hører spørsmålet om eventuelle mangler ved den regulatoriske gjennomføringen av reglene kan veies opp gjennom andre kontrollmekanismer, for eksempel domstolskontroll i forkant eller kontroll i etterkant, som jeg vil behandle nærmere under pkt. 3.4.

I sakene knyttet til temaet lovkravet og statlige overvåkningstiltak har EMD ennå ikke fått seg forelagt et spørsmål tilsvarende det som dataavlesingsreglene reiser. Det kan være ulike årsaker til dette, men en mulig grunn er at overvåkning gjennom dataavlesing er et relativt nytt fenomen. I noen dommer berører EMD likevel problemstillingen.

I dommen Rotaru v. Romania var et av spørsmålene hvorvidt regelverket etterretningstjenesten i Romania (RIS) handlet etter tilfredsstilte det materielle lovkravet i EMK artikkel 8-2, især spørsmålet om lovgivningen anga med tilstrekkelig klarhet under hvilke omstendigheter RIS kunne lagre og gjøre bruk av informasjon om klagerens privatliv.[74] Den aktuelle lovgiv-

[74] Rotaru v. Romania avsn. 56

ningen tillot RIS å samle, nedtegne og lagre informasjon av betydning for nasjonal sikkerhet. EMD viser til følgende:

> ”No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded … .”[75]

Her trekker EMD frem som et moment i kravet til nasjonal lovgivning at den regulerer hvilken type informasjon myndighetene har autorisasjon til å innhente.

Situasjonen EMD beskriver har visse likheter med den som oppstår under reguleringen av dataavlesing: Myndighetene får adgang til å foreta skjult overvåkning, men rettsgrunnlaget begrenser eller regulerer ikke omfanget eller formen av overvåkningen. I Rotaru v. Romania trekkes dette frem som manglende klarhet ved regelverket, og dette igjen innebærer en større fare for vilkårlig myndighetsinngrep.[76] Likheten i faktum tilsier at dette kan tillegges vekt ved vurderingen av de norske reglene om dataavlesing. Isolert tilsier uttalelsen at der problemstillingen aktualiserer seg, bør det nasjonale regelverket angi de nærmere grensene eller rammene for innhentingen av informasjon. For dataavlesingsreglene kunne det bety at loven burde angi nærmere hvordan gjennomføringen av overvåkningen vil foregå, for eksempel gjennom et pålegg til retten om å angi nærmere hvilke kategorier av informasjon politiet får adgang til å avlese.

I Rotaru var det ovenfor siterte imidlertid bare én av flere svakheter ved lovgivningen, og det kom i tillegg til et manglende system for kontroll med myndighetenes utøvelse av regelverket. Dommen gir derfor begrenset veiledning om hvor grensene går, ettersom dette inngikk som et moment i en helhetsvurdering. Dommen gir for eksempel ikke svar på hvordan det hadde forholdt seg dersom manglende angivelse av typen informasjon var den eneste ”mangelen” ved lovreguleringen. Jeg vil være forsiktig med å trekke noen avgjørende slutninger fra premissene i Rotaru. En så eksplisitt henvisning til reguleringen av typen av informasjon har jeg heller ikke gjenfunnet i noen av de andre dommene som omhandler statlig overvåkning. Det bør likevel kunne utledes fra dommen at det er et relevant moment, selv om vekten sett opp mot øvrige momenter ikke er klarlagt.

I en annen dom fra EMD var spørsmålet om omfanget av innhentingen av informasjon mer sentralt. Liberty and Others v. The United Kingdom gjaldt masseovervåkning, altså i utgangs-

---

[75] Rotaru v. Romania avsn. 57

[76] Utledet fra Malone v. The United Kingdom, sitert i Rotaru v. Romania avsn. 55

punktet ulikt den type tvangstiltak som gjelder målrettet overvåkning av enkelte mistenkte individer. I Liberty and Others fant retten likevel ingen grunn til å anvende andre prinsipper ved vurderingen av lovgrunnlaget for masseovervåkning enn de som gjelder ved individuell overvåkning, det vil si det lovkravet som gjelder for statlig overvåkning.[77] Interessant i relasjon til spørsmålet i denne oppgaven er uttalelsene i avsnitt 64 i dommen. Her uttaler EMD:

> "According to the applicants, warrants covered very broad classes of communications … The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered."

Spørsmålet i saken relaterte seg til et konkret saksforhold, hvor EMD fant at det hadde skjedd et inngrep i strid med EMK artikkel 8. Premissene har likevel, etter mitt syn, en generell overføringsverdi, blant annet til tilfellet med dataavlesing, jamfør at tillatelsen til dataavlesing etter sigende vil romme svært vide fullmakter for politiet. Avslutningsvis i dommen konkluderer EMD slik:

> "The Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications."[78]

I denne uttalelsen refererer EMD altså til kravet til rettsgrunnlaget. Når EMD i denne konteksten bruker ordet "clarity" knyttet til den innholdsmessige reguleringen, kan det tyde på at også for de nærmere delene av kravet til "safeguards" vil EMD vurdere om rettsgrunnlaget møter kravet til klarhet. Det er uklart om EMD i begrepet "clarity" har tiltenkt en distinksjonen mellom det overordnede klarhetskravet, og krav til klarhet ved den nærmere reguleringen av "safeguards." En mulighet er at begrepsbruken ikke er helt konsekvent.

Den "very wide discretion" EMD i sitatet sikter til må knyttes til uttalelsene i avsnitt 64, hvor myndighetene er gitt svært vide fullmakter til å samle inn kommunikasjonsmateriale. På dette punkt anså EMD rettsgrunnlaget for ikke å tilfredsstille klarhetskravet. Dette kan tas som et argument for at dette er et område av dataavlesing som burde være nærmere regulert i straffeprosessloven.

---

[77] Liberty and Others v. The United Kingdom avsn. 63

[78] Liberty and Others v. The United Kingdom avsn. 69

Også her må det tas visse forbehold om rekkevidden av dommen for spørsmålet om reguleringen av dataavlesing. For det første var de "wide discretions" ett av flere momenter i dommen. EMD kritiserte særlig at det ikke var tilgjengeliggjort for offentligheten hvilke prosedyrer som gjaldt for utvelgelsen, videreformidlingen, lagringen og tilintetgjørelsen av det innsamlede materialet.[79] Argumentet får derfor noe begrenset vekt, ettersom momentet inngikk som en del av en helhetsvurdering. Dommen gir ikke svar på om manglende rammer for politiets fullmakter i dette tilfellet alene hadde vært nok til å konstatere krenkelse av EMK. I tillegg gjaldt saken et tilfelle av masseovervåkning, som innebærer overvåkning og potensielle inngrep av svært stor skala, også sammenlignet med det potensialet som ligger i dataavlesing. I et slikt tilfelle vil kravet til et rettsgrunnlag som ivaretar kravet om "strict necessity" og målrettethet antas å være skjerpet, på bakgrunn av overvåkningens omfang og art. Det er ikke gitt at hensynet til å begrense hvilke typer informasjon vil veie like tungt i en sak om individuell overvåkning. Her vil skadepotensialet være mindre, relativt sett, enn ved masseovervåkning. EMD har ikke trukket opp denne distinksjonen eksplisitt, så en slik slutning må eventuelt foretas med forsiktighet, og på bakgrunn av den generelle rettssetningen om lovkravets relative karakter.[80]

Hvis man oppsummerer fra dommene Rotaru og Liberty and Others, mener jeg at man på det minste kan utlede at manglende rammer for gjennomføringen av overvåkningen inngår som et moment i en helhetsvurdering av om lovverket er tilfredsstillende i henhold til EMK artikkel 8-2. Det er uklart hvilken vekt det har i relasjon til andre momenter. Ikke i noen av disse dommene var det avgjørende at rettsgrunnlaget ikke anga nærmere fremgangsmåten for – eller begrensning av – innhentingen av materialet. Og i begge forelå det andre og til dels mer "graverende" mangler ved regelverket. I Rotaru var dette én av et såpass stort antall svakheter ved regelverket at det er vanskelig å konkludere noe om hvilken vekt dette ene momentet utgjorde. I Liberty and Others derimot ble manglende "clarity" ved angivelsen av myndighetenes skjønn trukket frem som én av to særlige svakheter ved regelverket, selv om premissene i dommen tyder på at EMD vektla i enda større grad at prosedyrene for håndtering av det innsamlede materialet ikke var offentlig tilgjengelig.[81]

På bakgrunn av dette vil utgangspunktet for drøftelsene videre være at det aktuelle spørsmålet vil kunne utgjøre et moment i helhetsvurderingen. Tema videre er om dette er et område straffeprosessloven derfor bør regulere nærmere, og eventuelt hvordan.

---

79 Liberty and Others v. The United Kingdom avsn. 69

80 Se igjen Szabo and Vissy v. Hungary avsn. 57

81 Se avslutningsvis i Liberty and Others v. The United Kingdom avsn. 69

Av prinsipiell karakter i relasjon til spørsmålet er premissene i dommen Szabó and Vissy v. Hungary. I avsnittene 72-73 refererer EMD fra tidligere domspraksis, og konkluderer med at inngrep av så alvorlig art som statlige overvåkningsordninger utgjør, må være "strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation"[82] (min utheving). Det referer seg altså til kravet om streng nødvendighet. På et tidspunkt senere i dommen, ved vurderingen av om det ungarske regelverket tilfredsstiller dette kravet, viser EMD igjen til "The requisite assessment of strict necessity with regard to the aims and the means at stake" i en konkret sak.[83] Fra dette kan man slutte at det ikke vil være tilstrekkelig å regulere de omstendighetene hvor et inngrep rent generelt anses som nødvendig, for eksempel for det formål å bekjempe og avverge en viss type alvorlig kriminalitet. Slik EMD her anvender EMK artikkel 8-2 kreves det i den enkelte sak konkret forholdsmessighet mellom det mål som søkes oppnådd og de etterforskingsskritt politiet foretar seg. Et tilsvarende krav til forholdsmessighet er lovfestet i strpl. § 170 a, som krever at et tvangsmiddel bare benyttes når det er tilstrekkelig grunn til det, og tiltaket ikke vil utgjøre et uforholdsmessig inngrep. Disse kildene sett i sammenheng tilsier at et tiltak ikke må gå lenger enn det som anses strengt nødvendig.

Anvender man dette på reguleringen av dataavlesing, kan man se det slik at kravet om konkret nødvendighet er etterkommet gjennom å sette som vilkår at etterforskningsmyndighetene må påvise at dataavlesing vil være av av "vesentlig" betydning i den enkelte saken, og at oppklaringen ellers i "vesentlig grad" blir vanskeliggjort.[84] Disse vilkårene knytter behovsprøvingen av dataavlesingen opp mot situasjonen i den konkret foreliggende saken. Med denne innfallsvinkelen kan dataavlesingsreglene synes å være i samsvar med kravet i Szabó and Vissy v. Hungary.[85]

Et annet synspunkt på dette er at lovreguleringer lik den i strpl. § 216 o, hvor reglene er utformet med sikte på å sikre at iverksettelsen av metoden i det konkrete tilfellet er "strictly necessary", har vært ansett tilfredsstillende når politiets metoder har begrenset seg til for eksempel kommunikasjonsavlytting.[86] Ved anvendelsen av dataavlesings tilligger det imidlertid politiet et langt større handlingsrom og langt større frihet i gjennomføringen av overvåkningen, og avlesingen kan skje i mer eller mindre inngripende former, og i større eller mindre utstrekning. I tråd med kravet i Szabó and Vissy v. Hungary, kunne dette tilsi at dataavlesingsreglene burde være spisset for bedre å sikre at den konkrete gjennomføringen ikke går ut

---

82 Szabó and Vissy v. Hungary avsn. 73

83 Szabó and Vissy v. Hungary avsn. 75

84 Strpl. § 216 o tredje ledd

85 Kennedy v. The United Kingdom, avsn. 159 og følgende, jf. 29-56

86 Se for eksempel Weber and Saravia v. Germany

over det som er "strictly necessary". Under denne synsvinkelen kan det være nærliggende å se til uttalelsene i Liberty and Others, hvor nettopp "wide discretions" i dette henseendet ble ansett kritikkverdig.[87]

I denne forbindelse er det interessant å se på lovforslaget som lå til grunn for vedtakelsen av straffeprosesslovens nye kapittel 16 d, og hvilke betraktninger som lå til grunn for regelutformingen.

I lovforslaget i Prop. 68 L (2015-2016) har departementet i pkt. 5.2 vurdert forholdet til EMK artikkel 8. Det er foretatt en gjennomgang av rettspraksis fra EMD og hvilke skranker EMK setter for politiets metodebruk. I proposisjonen blir det redegjort for kravet til tilgjengelighet og forutsigbarhet, lovkravets relative karakter, og betydningen av prosessuelle garantier.[88] På side 41 uttaler Departementet at "[EMD] vil ... prøve om hjemmelen er for vidt utformet, både om bestemmelsen som sådan er for vid og om en i forbindelse med en konkret bruk har gått utenfor det som er nødvendig i et demokratisk samfunn."

Videre drøfter de i pkt. 14.8.4. i kapittelet som omhandler dataavlesing spørsmålet om dataavlesing bør innføres som eget tvangsmiddel, og hvilke personvernrettslige utfordringer dette kan medføre. Departementet skriver at det ikke er hensiktsmessig å beskrive gjennomføringsmåten i detalj i lovteksten, med henvisning til den tekniske gjennomføringsmåten.[89] Om den nærmere avgrensningen av den konkrete informasjonsinnhentingen, sier departementet lite. Jeg siterer her fra lovproposisjonen:

> "Med hensyn til *hvilke typer informasjon* politiet bør kunne gjøre seg kjent med ved dataavlesing, mener departementet at metoden for det første må omfatte tilgang til samme type elektronisk informasjon som politiet ellers har rettslig adgang til gjennom kommunikasjonsavlytting og hemmelig ransaking og beslag".[90]

Og videre:

> "Med forslaget om å tillate dataavlesing vil departementet imidlertid også åpne for at politiet fortløpende gjør seg kjent med andre opplysninger knyttet til bruken av et datasystem som det ikke har anledning til å innhente etter gjeldende rett. Dette inkluderer opplysninger om inntastinger på et tastatur, bruk av programvare og behandling av

87 Op.cit

88 Prop. 68 L (2015-2016) s. 38-40

89 Prop. 68 L (2015-2016) s. 271

90 Prop. 68 L (2015-2016) s. 264

> ulike filer som ikke resulterer i data som blir lagret eller kommunisert, eller som senere blir utilgjengelig for politiet fordi dataene da lagres eller kommuniseres i kryptert form. Etter departementets oppfatning er en slik utvidelse nødvendig for å kunne møte utfordringene knyttet til kryptering og moderne kommunikasjonstjenester på en tilstrekkelig effektiv måte."[91]

Leser man dette i sammenheng, kan det synes som om departementet har tatt stilling til at dataavlesing som etterforskningsmetode innebærer et utvidet potensiale for inngrep og vil innebære ulike former for overvåkning. Konsekvensene dette har for lovreguleringen, og hvordan denne bør være utformet for å sikre forholdsmessigheten ved gjennomføringen av overvåkningen, er så langt jeg kan se ikke problematisert videre i lovproposisjonen. Departementet peker imidlertid på at dataavlesing åpner for mer målrettet informasjonsinnhenting.[92] De uttaler at beskyttelsen mot personverninngrep må sikres "gjennom passende vilkår for bruk av metoden."[93]

Ser man dette opp mot lovreguleringen i strpl. § 216 o, er denne i tråd med departementets forslag: Skrankene for dataavlesingen er satt gjennom vilkårene for bruk, og gjennom domstolskontroll av disse. Utstrekningen av overvåkningen gjennom av dataavlesingen er ikke videre problematisert, verken om dette burde reguleres nærmere i lov, eller om hjemmelen vil kunne være for "vid" i henhold til lovkravet i EMK, jamfør det ovenfor siterte.

Fra lovteksten og forarbeidene later det til å ha vært lovgivers intensjon å utelate fra lovreguleringen en begrensning eller regulering av utøvelsen av selve dataavlesingen. I lys av rettskildegrunnlaget referert hittil, kunne det nok ha vært grunn til å vurdere en nærmere regulering av utøvelsen av overvåkningen.

Til mulig støtte for et krav om at lovgrunnlaget skal speile kravet til streng, konkret forholdsmessighet mellom inngrep og formål er en dom avsagt i EU-domstolen i desember 2016, Tele2 and Watson. EU-domstolens avgjørelser er naturligvis ikke bindende for EMD, men EMD har selv trukket frem EU-domstolens avgjørelser som relevante kilder ved tolkningen av EMK.[94] Dommens uttalelser knytter seg i hovedsak til hva som vil være tillatt innenfor rammene av EU-charteret, men at dette har vekt i vår sammenheng følger av at samme spørsmål var sentralt i avgjørelsen i EU-dommen Digital Rights Ireland, som ble trukket frem i premis-

---

91 Prop. 68 L (2015-2016) s. 264

92 Prop. 68 L (2015-2016) s. 264

93 Prop. 68 L (2015-2016) s. 266

94 Se bl.a. i Szabó and Vissy v. Hungary i avsnitt 23, hvor det siteres fra EU-dommen C-293/12 and C-594/12 Digital Rights Ireland

sene i Szabó and Vissy v. Hungary, og utgjorde en sentral del av EMDs argumentasjon. De grunnleggende prinsippene vedrørende brudd på retten til vern av korrespondanse[95] er også nær sagt tilsvarende de som gjelder etter EMK, slik at inngrep i denne retten kan tillates i den utstrekning det er et "necessary, appropriate and proportionate measure within a democratic society" i lys av det angitte formålet.[96] I tillegg til at EMD selv ser hen til EU-domstolen, taler også likheten i saksforhold og vurderingsnormer for at uttalelsene kan være relevante kilder til tolkningen av EMK.

Saken gjaldt EU-direktiv 2002/58 (kommunikasjonsverndirektivet) i lys av en ordre fra Post- och telestyrelsen i Sverige til Tele2 om å lagre all trafikkdata fra Tele2s abonnenter og registrerte brukere. Spørsmålet var om Artikkel 15 (1) i direktivet, i lys av EU-charteret artikkel 7 og 8 som verner henholdsvis retten til privatliv og beskyttelse av personlig data, måtte tolkes slik at medlemsstatene var avskåret fra å innføre lovgivning som tillot "for the purpose of fighting crime, for the indiscriminate retention of all traffic and location of data of all subscribers and registered users with respect to all means of electronic communications."[97]

Saksforholdet samsvarer i utgangspunktet ikke med problemstillingen bruken av dataavlesing reiser, da spørsmålet gjaldt lagring av dataene til alle brukere av dataabonnementene, uavhengig av om det kunne rettes noen konkret mistanke mot noen av objektene og uten sammenheng med noen konkret etterforskning. Dommen er likevel interessant i vår sammenheng av to grunner: Domstolen kommer med flere prinsipielle uttalelser knyttet til spørsmålet om målrettet overvåkning i forbindelse med kriminaletterforskning, slik som bruk av dataavlesing. Og den form for overvåkning det er snakk om innebærer innhenting av en rekke ulike data, blant annet abonnentens navn, adresse, telefonnummer ringt til og fra, IP-adresse, tidspunktet for telefonsamtaler, stedet telefonsamtalene fant sted, med mer,[98] også dette sammenlignbart med anvendelsen av dataavlesing som metode.

I avsnittene 102-105 drøfter domstolene saksforholdet, og konkluderer med at masseinnhenting av en mengde av ulike data slik svenske Post- och telestyrelsen etterspurte, gikk langt utover det som var strictly necessary.[99] Den fremholder deretter at innhenting av slik massedata ville være lovlig under EU-charteret på det vilkår at myndighetene i staten foretok, og begrenset seg til: "The targeted retention of traffic and location data, for the purpose of

---

95 Vern av "The confidentiality of communications and the related traffic data", nedfelt i kommunikasjonsverndirektivet artikkel 5 (1), sitert i Tele2 and Watson avsn. 95

96 Jf. direktiv 2002/58 artikkel 15 (1). Til støtte for dette, se også Ingvild Bruce i Lov og Rett (05/2010)

97 Tele2 and Watson, avsn. 62

98 Tele2 and Watson avsn. 98

99 Tele2 and Watson avsn. 107

fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary"[100] (min utheving).

Dette sitatet kan etter sin ordlyd og i sin kontekst tolkes slik at EU-domstolen setter krav om at "strict necessity" må foreligge ikke bare mellom overvåkningen av den enkelte person og det ønskede formålet, men at overvåkningen må være rettet inn mot (bare) de kategorier av data og de former for kommunikasjon som er "strictly necessary". Hvis man anvender dette på reglene om dataavlesing, kunne det tilsi at lovgrunnlaget burde være utformet med sikte på at tillatelsen til inngrepet skal følge en tilsvarende konkret vurdering av forholdsmessigheten mellom inngrep og formål. Lovgrunnlaget i dag åpner for at politiet i enhver sak får adgang til å benytte dataavlesingens fulle potensiale. I tråd med premissene i Tele2 and Watson, kunne en se det slik at loven for eksempel bør gi anvisning på begrensninger av hvilke bestemte informasjonskanaler i et datasystem politiet skal få adgang til å avlese i den enkelte sak.

Et annet argument av mer overordnet art er lovkravets relative karakter, hvoretter kravet vil kunne skjerpes på bakgrunn av, blant annet, " the nature, scope and duration of the possible measures"[101] (min utheving). Det ligger for det første et svært stort "scope of possible measures" i anvendelsen av dataavlesingsmetoden. Metoden er også svært inngripende i sin natur. Isolert sett skulle EMD da legge til grunn en strengere vurdering av om det foreligger "adequate and effective guarantees against abuse". Disse momentene taler samlet sett i retning av at anvendelsen av dataavlesingen bør underlegges en nærmere regulering enn den som gjelder i dag, for å ivareta kravet om sikkerhetsmekanismer mot myndighetsmisbruk.

Osnes Fause argumenterer også for at det ligger et "minste inngreps prinsipp" i EMK artikkel 8-2.[102] Dette er i og for seg en annen formulering av at regelverket bør være egnet til å forebygge myndighetsmisbruk, ettersom inngrepet i motsatt fall vil kunne være uforholdsmessig. Men denne innfallsvinkelen kan likevel tas til inntekt for et annet viktig poeng. Regelverket bør ikke være utformet først og fremst med det øyemål at urettmessige inngrep ikke skjer, men med det formål å skåne individets privatliv i størst mulig grad, så langt det lar seg forene med begrunnelsen for inngrepet. Reglene om dataavlesing tar i stor grad hensyn til dette, gjennom å sette strafferammen for anvendelsen relativt høyt, og å kreve at dataavlesingen er av "vesentlig" betydning for etterforskningen. Det fremstår i mindre grad at dette hensynet er

[100] Tele2 and Watson avsn. 108

[101] Se Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 77, sitert fra Klass and Others v. Germany avsn. 50

[102] Fause (2014) s. 57

ivaretatt ved gjennomføringen av overvåkningen, ettersom reglene er utformet slik at politiet får nær sagt "blankofullmakt" ved overvåkningen av individet.

Et annet poeng til vurderingen av dataavlesingsreglene opp mot lovkravet er at domsutviklingen går i retning av stadig strengere krav til rettsregler om statlig overvåkning. Dette kan ses i sammenheng med at det råder en stadig større aksept for statlig overvåkning, og metodene for gjennomføringen er blitt stadig mer avanserte og vidtrekkende, med tilsvarende større risiko for myndighetsmisbruk. Godt utbygde sikkerhetsmekanismer kan bidra til å redusere dette risikopotensialet. Kravene til lovregulering retter seg også kanskje i større grad mot selve datainnsamlingen, jamfør Liberty and Others, og Tele2 and Watson. Selv om det ennå ikke er én enkel EMD-dom som slår fast at dette må gjelde som en del av kravet til lovreguleringen, eller begrensningen i skjønn, har EMD argumentert for det i relasjon til masseovervåkning (Liberty and Others), og det er slått fast rimelig klart i EU-domstolen (Tele2 and Watson) at ved individuell overvåkning kan slikt inngrep bare være lovlig dersom det foretas en begrensning og målretting av hvilken informasjon som innhentes. Til dette kommer også de prinsipielle uttalelsene i Szabó and Vissy v. Hungary, som er en dom av nyere dato, med andre ord avsagt i "vår tid " overvåkningsmessig sett.

Til dette kan man også trekke frem en annen uttalelse i Szabó and Vissy. I avsnitt 70 peker EMD igjen på det særlig inngripende ved moderne former for overvåkning. Teknologien i dag gjør det mulig for myndighetene å innhente "A detailed profile ... of the most intimate aspects of citizen' lives." EMD uttalte seg her på bakgrunn av en redegjørelse fra organisasjonen Center for Democracy & Technology (CDT), som fungerte som en hjelpepart i saken. Sitatet henviser til CDTs redegjørelse for masseovervåkningsordninger, og målrettet overvåkning av individer, for eksempel trekker CDT frem muligheten til å installere software i et datasystem, og derigjennom "record keystrokes, sounds, photos or videos, unbeknown to the owner."[103] Til dette uttaler EMD:

> "This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices."[104]

Ordrett sier domstolen her at de eksisterende garantiene i EMK, slik de følger av rettspraksis, må forsterkes for å imøtegå slik overvåkning som foregår i dag. Da det ungarske regelverket

[103] Szabó and Vissy v. Hungary avsn. 49

[104] Szabó and Vissy v. Hungary avsn. 70

ikke ble ansett å møte de eksisterende kravene til sikkerhetsgarantier, gikk EMD ikke nærmere inn på temaet. I lys av at en problemstilling lik den som oppstår under dataavlesingsreglene ennå ikke har vært til vurdering i EMD, gir dette sitatet en mulig pekepinn om hvor leden vil kunne gå i fremtiden.

For å sammenfatte fra drøftelsene under dette punktet, kan EMDs rettspraksis, senest i Szabó and Vissy v. Hungary, og EU-domstolens avgjørelse i Tele2 and Watson, etter mitt syn tolkes i retning av at lovkravet gir anvisning på en relativt streng, konkret vurdering av nødvendigheten og utstrekningen av et inngrep i den enkelte sak. I Szabó and Vissy v. Hungary begrunnes kravet om "strict necessity" blant annet med at systemet ellers vil være "prone to abuse", eller tilbøyelig til å misbrukes, tatt i betraktning de betydelige tekniske kapabilitetene som står myndighetene til rådighet.[105] De samme hensynene ligger til grunn for EMDs krav om at statlige overvåkningstiltak generelt må være "Based on a Law that is particularly precise."[106] De helt grunnleggende hensynene som ligger til grunn for lovkravet i EMK artikkel 8 som sådan, og for det særlige lovkravet lovkravet på det aktuelle området, gjør seg gjeldende med styrke ved anvendelsen av dataavlesing, på bakgrunn av metodens overvåkningspotensiale. Disse kildene og argumentene tilsier at kravene til kvaliteten av rettsgrunnlaget her skjerpes, for å forhindre at individene utsettes for inngrep i større utstrekning enn det som er "strictly necessary".

For dataavlesingsreglenes del kunne dette, de lege ferenda, tilsi at loven burde regulerer nærmere også utøvelsen av overvåkningen, for å gjenspeile det skjerpede kravet til forholdsmessighet. Dette kunne man eksempelvis oppnå gjennom å lovfeste i strpl. § 216 o at retten i kjennelsen må angi nærmere hvilke informasjonsstrømmer i datasystemet politiet har adgang til å avlese. Slik vil man i større grad kunne "spisse" overvåkningen, sett opp mot det konkrete formålet og øvrige omstendigheter i saken. Rent konkret kan en se for seg at dette vil begrense situasjoner der politiet gjennom dataavlesing overvåker SMS, e-poster, dokumenter, bilder, kamera og mikrofon, GPS, og så videre, uten en nærmere vurdering av om et slikt omfang av overvåkningen er "strictly necessary."

Oppsummert fra dette, så fremstår det klart at det fra EMDs rettspraksis kan utledes at regulering av utøvelsen av overvåkningen utgjør et moment i helhetsvurderingen av den innholdsmessige gjennomføringen. Flere argumenter kan tilsi at det norske regelverket kunne vært utformet mer presist sett opp mot dette kravet.

---

[105] Szabó and Vissy v. Hungary avsn. 73

[106] Op.cit

4.2.4 Sammenfatning

De norske reglene regulerer både under hvilke omstendigheter og på hvilke vilkår myndighetene kan iverksette inngrep i borgernes privatliv i form av dataavlesing. Vilkårene om vesentlig nødvendighet og kvalifisert mistankekrav bidrar til å sikre at begjæring om overvåkning gjennom dataavlesing bare foretas der inngrepet er "strictly necessary", og derigjennom begrenser faren for vilkårlig inngripen fra myndighetene. Slik regelverket er utformet, synes vilkårene å være utformet med tilstrekkelig presisjon slik at de også danner grunnlag for en tilfredsstillende domstolsprøving. På disse punktene er dataavlesingsreglene etter mitt syn i samsvar med de innholdsmessige kravene til rettsgrunnlaget. Dette er en nærliggende slutning også på bakgrunn av EMDs avgjørelse i saken Weber and Saravia v. Germany. Saken gjaldt masseovervåkningsordninger, men EMD la til grunn tilsvarende krav til "safeguards" som ved individuell overvåkning. Det tyske regelverket "Contained the minimum safeguards against arbitrary interference as defined in the Court's case-law." EMD fant at klagen var "åpenbart grunnløs" jf. EMK artikkel 35.[107] Reguleringen i straffeprosessloven fremstår vel så godt utbygd som det tyske hva gjelder kravene til innholdet i regelverket.[108]

Gjennomgangen under pkt. 4.2.3 kan tilsi at i tråd med kravet om retningslinjer og rammer for utøvelsen av skjønn kunne dataavlesingsreglene vært utformet med større grad av detalj. Dette for å møtegå kravet om at rettsgrunnlaget speiler kravet om "strict necessity", men også for å tilrettelegge for at domstolsprøvingen av dette vilkåret kan foretas på tilfredsstillende grunnlag. Vekten av dette momentet, sett opp mot de øvrige reguleringene i loven, er ikke åpenbar. Hertil kommer også spørsmålet om eventuelle mangler ved den regulatoriske gjennomføringen av reglene kan avhjelpes gjennom andre kontrollmekanismer, for eksempel domstolskontroll i forkant eller rapporteringer i etterkant, i lys av helhetsvurderingen av om det foreligger "adequate and effectve guarantees against abuse". Dette vil jeg komme inn på under pkt. 4.3.

4.3 Kontrollmekanismer

4.3.1 Oversikt

En annen, sentral side ved "safeguards"-kravet er kravet om at det eksisterer kontrollmekanismer rundt gjennomføringen av statlig overvåkning. Et godt utbygget regelverk vil kunne ha liten effekt dersom etterlevelsen av regelverket ikke blir kontrollert. Et viktig aspekt ved vurderingen av om det foreligger tilstrekkelige sikkerhetsmekanismer er derfor om det foreligger effektiv kontroll med myndighetenes handlinger.[109] Jeg vil i det videre redegjøre for innholdet av kravet til kontrollmekanismer, og fortløpende vurdere dataavlesingsreglene opp mot dette.

---

[107] Weber and Saravia v. Germany avsn. 137

[108] Se Weber and Saravia v. Germany avsn. 95-101. Se også Kennedy v. The United Kingdom til støtte for konklusjonen i dette avsnittet

[109] Kjølbro (2010) s. 667

Jeg vil se på prosessuelle mekanismer i forkant av iverksettelsen, og kontroll i etterkant. Spørsmålet er om disse er egnet til å sikre "adequate and effective guarantees against abuse." Et særlig spørsmål ved vurderingen av forhåndskontrollen ved domtolene, er om måten dataavlesingsreglene er utformet vanskeliggjør domstolskontrollen og etterlevelsen av kravet om "strict necessity" mellom middel og mål. Sammenhengen er relevant i den samlede vurderingen av om dataavlesingsreglene samsvarer med lovkravet i EMK artikkel 8.

4.3.2 Kravet til prosessuelle sikkerhetsmekanismer

Kravet til prosessuelle sikkerhetsmekanismer har inngått som en del av lovkravet helt tilbake til dommen Klass and Others v. Germany fra 1978, og innebærer i korte trekk at myndighetenes handlinger overfor individene, i den grad de utgjør inngrep i retten til privatliv, bør være underlagt en ytre kontroll, fortrinnsvis ved domstolene.[110] Kravet om uavhengig kontroll med myndighetenes handlinger er sentral i rettsstatsidealet, eller som Jeremy Waldron skriver: "The Rule of Law is not just about general rules; it is about their impartial administration."[111] Domsmyndighetenes kontroll skal bidra til å sikre at myndighetspersonene holder seg innenfor lovens rammer. Spørsmålet for dette avsnittet vil delvis være om systemet med forhåndskontroll formelt sett møter kravet i EMK, og også om domstolskontrollen innholdsmessig sett er tilfredsstillende, særlig opp mot kravet om "strict necessity."

Det følger av første setning i første ledd i strpl. § 216 o at tillatelse til å foreta dataavlesing gis av retten ved kjennelse. Rettens kjennelser er begrunnet, jf. strpl. § 52. Ved politiets begjæring av dataavlesing vil politiet fremlegge, og retten prøve, dokumentasjon og bevis i saken. Det kan gjøres unntak fra regelen om domstolenes forhåndstillatelse, jf. strpl. § 216 d, dersom det ved opphold er "stor fare" for at etterforskningen vil lide. Unntaksvis kan da ordre fra påtalemyndigheten tre i stedet for kjennelse av retten. Slik hastebeslutning må likevel forelegges for retten så raskt som mulig, og senest innen 24 timer etter at kontrollen er påbegynt. I et nær tilsvarende saksforhold i The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria fant EMD at en slik ordning var i samsvar med EMK.[112]

I henhold til straffeprosessloven er det altså uavhengig domsmyndighet som avgjør om politiet skal få tillatelse til å iverksette dataavlesing. Domsmyndighetene avgir begrunnede kjennelser, og vurderingene kan derfor også etterprøves. Dette tilfredsstiller ganske klart kravet til "independence, impartiality and a proper procedure" slik dette følger av EMD.[113] Så langt det

---

110 Klass and Others v. Germany, sitert i Rotaru v. Romania avsn. 59

111 Waldron (2008) s. 7

112 Se The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 84, jf. avsn. 82 og 16.

113 Rotaru v. Romania avsn. 59

gjelder de formelle kravene til prosessuelle mekanismer later det norske regelverket til å være i samsvar med kravet i EMK.

EMDs praksis viser at det ikke er tilstrekkelig at det eksisterer en uavhengig domsmyndighet som utøver en kontroll med myndighetene, det kreves at domsmyndighetene foretar en reell, effektiv prøving av om tiltaket er forholdsmessig. I Roman Zakharov v. Russia beskriver EMD de nærmere kravene til domstolskontrollen:

> "Turning now to the authorisation authority's scope of review, the Court reiterates that it must … ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means."[114]

Spørsmålet er hva som skal til for at domstolene kan ivareta dette formålet, i tråd med kravet i EMK. Prosessuelle sikkerhetsmekanismer hører til under vurderingen av om det foreligger "adequate and effective guarantees against abuse",[115] og det vil være av betydning om domstolskontrollen er tilfredsstillende med hensyn til å verne individene mot vilkårlige inngrep. Samtidig er andre aspekter av kontrollen av betydning som graden av sikkerhet mot "abuse", som myndighetenes avgjørelseskompetanse, graden av offentlighet, og muligheten for kontradiksjon. Jeg vil i det videre drøfte kvaliteten av domstolskontrollen.

Flere forhold kan tenkes å være av betydning for domstolenes prøving. Det ene er den generelle kvaliteten av domstolenes prøving. Det andre er, som påpekt tidligere, at også kvaliteten av rettsgrunnlaget domstolen prøver, vil ha betydning for kontrollen i den konkrete saken. Videre er det et poeng hvilken avgjørelseskompetanse som tilligger domstolene, om det er et spørsmål om enten-eller, eller om de har adgang til å vedta mellomløsninger.

Et eksempel på at domstolsprosedyrene i sin helhet ble ansett utilfredsstillende var dommen Roman Zakharov v. Russia. EMD kritiserer den russiske domstolskontrollen for å være "limited in scope," blant annet fordi domstolene var avskåret fra å få tilgang til dokumentasjon tilknyttet hemmelige politioperasjoner. Det var ikke påkrevet at domstolene vurderte inngrepets "proportionality", og lokale domstoler gav ofte tillatelser på svært tynt grunnlag.[116] Dette er ikke mangler som aktualiseres ved anvendelsen av straffeprosessloven. Svakheter ved den norske forhåndskontrollen er blant annet at avgjørelsene ikke er offentlige, og det skjer ingen

[114] Roman Zakharov v. Russia avsn. 270

[115] Szabó and Vissy v. Hungary avsn. 57

[116] Roman Zakharov v. Russia avsn. 261-263

kontradiksjon.[117] Slike svakheter er for så vidt iboende i et system for statlig, skjult overvåkning, men utgjør objektivt sett en svakhet ved kontrollsystemet i sin helhet. Prosedyrene for forhåndskontroll som sådan later likevel til å være i samsvar med EMK.[118]

Et annet forhold som kan påvirke kvaliteten av forhåndskontrollen er altså det underliggende rettsgrunnlaget. Etter mitt syn er strpl. § 216 o i stor grad utformet på en slik måte at domstolene er i stand føre effektiv kontroll med håndhevelsen av regelverket. Vilkårene om kvalifisert mistanke, henvisning til de konkrete lovovertredelsene som kan danne grunnlag for overvåkning, og den skjerpede terskelen (vesentlighetskravet) for å anvende dataavlesing som middel, bidrar til å gi domstolene grunnlag for å vurdere om inngrepet er "necessary" i henhold til EMK artikkel 8-2. At det underliggende rettsgrunnlaget på denne måten får betydning for kvaliteten av domstolsprøvingen illustrerer sammenhengen mellom de ulike komponentene i kravet til "safeguards" ved statlig overvåkning. Et klart, presist utformet rettsgrunnlag vil bedre danne grunnlag for en reell forhåndskontroll.

Et spørsmål som da dukker opp, er hva som eventuelt er betydningen av at strpl. § 216 o ikke regulerer selve utøvelsen av overvåkningen. At loven på dette området kan hende *burde* vært nærmere regulert, kan på den ene siden tenkes å avbøtes av en domstolskontroll, slik at domstolene kan holde etterforskningsmyndighetene i tøylene, så å si, for eksempel gjennom å sette som vilkår for tillatelsen at politiet må begrense hvilke informasjonsstrømmer de skal overvåke. På den andre siden kan det også tenkes å vanskeliggjøre domstolskontrollen, især sett opp mot kravet om "strict necessity" mellom inngrep og formål.

I et konkret tilfelle kan man se for seg dette: Politiet ønsker å overvåke en mistenkt i en sak om narkotikainnførsel. Politiet har forsøkt å avlytte kommunikasjonen til den mistenkte, men kommunikasjonen er kryptert og innholdet er utilgjengelig for politiet. Retten gir i kjennelse tillatelse til å foreta dataavlesing for å få tilgang til denne informasjonen, som politiet ellers er avskåret fra å innhente. Politiet installerer et software-program i mistenktes telefon[119], og har deretter tilgang til mistenktes meldinger, og kan avlytte innkomne telefonsamtaler mens de skjer. Politiet får samtidig tilgang til blant annet bildealbum, notater, e-post, andre kommunikasjonsprogrammer som Skype, Whatsapp, mistenktes Facebookkonto, og vedkommendes lokasjon hvis for eksempel GPS-funksjonen er aktivert. Denne tilleggsinformasjonen er fak-

---

[117] Jf. henholdsvis strpl. §§ 216 i og 216 e annet ledd. Det oppnevnes hemmelig forsvarer, jf. § 100 a, men dette kan likevel ikke anses likestilt med muligheten for den enkelte til selv å fremme sine synspunkter foran en dommer

[118] The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 84

[119] Prop. 68 L (2015-2016) s. 224. Dette kan gjøres for eksempel ved å sende programvaren som vedlegg eller skjult i et vedlegg i en e-post

tisk tilgjengelig for politiet, og det utvidede inngrepet i privatlivet et faktum, uavhengig av om politiet tar denne i bruk i etterforskningen.

Spørsmålet som oppstår er hvordan domstolene i forkant, når de ikke på forhånd kan ha oversikten over den fulle utstrekningen av overvåkningen, kan sikre at inngrepet de gir tillatelse til er "strictly necessary", slik konvensjonen krever. Rent konkret kan det tenkes å oppstå en risiko for at politiet i den enkelte sak har gått utenfor det som retten har ment var tilstrekkelig nødvendig og forholdsmessig. Det kan dermed tenkes at måten dataavlesingsreglene er utformet på bidrar til at domstolene vil komme noe til kort i å kontrollere i forkant at et inngrep er i samsvar med det strenge forholdsmessighetskravet mellom tiltaket og formålet.

Fra EMDs rettspraksis er det ikke avsagt noen avgjørelser som sier noe konkluderende om betydningen av dette. I Rotaru v. Romania forelå det ikke systemer for ekstern kontroll overhodet, så konsekvensen av at loven ikke anga rammer for utøvelsen av overvåkningen, ble ikke vurdert av EMD. Spørsmålet ble heller ikke problematisert i Liberty and Others.

Forhåndskontrollen fremstår ut over dette å være i samsvar med minstekravene i EMK.[120] Se til sammenligning The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria 14, hvor EMD anså at forhåndskontrollen var tilfredsstillende, på et faktagrunnlag med likhetstrekk med den norske straffeprosessloven. Dersom man legger til grunn at domstolene ikke nødvendigvis må gi politiet "blankofullmakt" eller avslå begjæringen i sin helhet, men har adgang til å begrense utstrekningen av overvåkningen, må dette anses å styrke domstolskontrollen, og i større grad kunne sikre nødvendighetskravet.

4.3.3 Etterhåndskontroll

EMD trekker frem at systemer for kontroll med gjennomføringen av overvåkningen også tilhører vurderingen av om det foreligger tilstrekkelige sikkerhetsmekanismer. I AEIHR and Ekimdzhiev v. Bulgaria påpekte EMD at systemet "Does not provide for any review of the implementation of secret surveillance measures by a body or official that is either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law."[121] Domstolen kritiserte altså at det ikke ble foretatt uavhengig evaluering av gjennomføringen av tiltaket. En slik evaluering vil ha en viktig funksjon når det kommer til å etterse at politiet har holdt seg innenfor rammene av gitte tillatelser.

---

[120] The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 84 jf. avsn. 14

[121] The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria avsn. 85

For politiets bruk av skjulte tvangsmidler følger det av strpl. § 216 h at det såkalte Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) fører kontroll med politiets og påtalemyndighetenes behandling av saker etter blant annet kapittel 16 d, dataavlesing.[122] I tillegg til dette kommer kommunikasjonskontrollforskriften, med hjemmel i strpl. § 216 k, til utfylling og gjennomføring av bestemmelsene i strpl. kapittel 16 a. Det følger både av forskriften og av strpl. § 216 o femte ledd at forskriften får anvendelse på reglene om dataavlesing. I § 7 er det listet opp en rekke opplysninger politiet er påkrevet å protokollføre i forbindelse med skjult overvåkning, blant annet grunnlaget for overvåkningen, og kjennelsen gitt av domstolene. I annet ledd er det for dataavlesing særskilt påkrevet at det føres logg over hvilke typer data som er avlest, for eksempel e-poster, tekstfiler, bilder, filmer, krypteringsløsninger og passord, og en nærmere beskrivelse av hvilken fremgangsmåte politiet har valgt ved gjennomføringen av avlesingen.

Disse opplysningene, sammen med politimesterens innberetning til riksadvokaten (jf. § 9), inngår i materialet som rapporteres til Kontrollutvalget. På bakgrunn av dette fører KK-utvalget kontroll med at politiets bruk av kommunikasjonskontroll, romavlytting og dataavlesing skjer innenfor rammen av lov, og at tvangsmiddelbruken begrenses mest mulig. Utvalget skal i tillegg særlig ha for øye den enkeltes rettssikkerhet (jf. § 14). Utvalget opererer som et uavhengig kontrollorgan, jf. § 18. Årlig utgir KK-utvalget en rapport med en oversikt over og gjennomgang av politiets bruk av kommunikasjonskontroll.

Denne ordningen later til å møte kravet i EMK, særlig hvis man ser på sammenlignbare ordninger som den som gjaldt i Kennedy v. The United Kingdom. Der anså EMD at en uavhengig "kommisær" som førte kontroll med og publiserte rapporter om overvåkningsorganenes operasjoner var av "particular value" og bidro til en "important control" med slike hemmelige tiltak.[123]

I tillegg til det eksisterende systemet for kontroll, skrev departementet følgende i lovforslaget:

> "Departementet legger til grunn at dataavlesing vil etterlate få ytre spor, og at det derfor er særlig viktig at politiets bruk av metoden dokumenteres på en måte som setter kontrollorganene i stand til å vurdere om det som er utført ligger innenfor de lovlige rammene, og så vidt mulig også til å konstatere at det ikke har blitt utført noe annet eller noe mer enn det som oppgis."[124]

---

[122] Strpl. § 216 o femte ledd hjemler anvendelsen av § 216 h for reglene om dataavlesing

[123] Kennedy v. The United Kingdom avsn. 166

[124] Prop. 68 L (2015-2016)

Det er i proposisjonen anerkjent at dataavlesing vil innebære utfordringer med hensyn til kontrollorganenes virksomhet. Utvalget består i dag av 4 faste medlemmer, som har KK-utvalget som biverv. For å kunne foreta en forsvarlig kontroll med bruken av dataavlesing vil det være behov for en mer fortløpende oppfølging. Det er foreslått å opprette et sekretariat med heltidsstillinger med dette til formål.[125]

I tillegg til KK-utvalget har vi et kontrollutvalg for etterretningstjenesten etter EOS-kontrolloven. Med hjemmel i § 1 er det opprettet et utvalg for å kontrollere etterretnings-, overvåknings- og sikkerhetstjenesten, det såkalte EOS-utvalget. Kontrollen har til formål blant annet å påse at det "ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene", jf. § 2 (1). Kontrollutvalget har til oppgave å føre regelmessig tilsyn med etterretnings-, overvåknings- og sikkerhetstjenesten, jf. § 3 første ledd.

Oppsummert eksisterer det prosedyrer for rapportering av overvåkningen som foretas av politi og etterretning. I samsvar med grunnleggende rettsstatsprinsipper er det oppnevnt et eksternt, uavhengig utvalg til å foreta kontroll med virksomheten, og min vurdering er at den informasjonen myndighetene er pålagt å opplyse om, danner grunnlag for at KK-utvalget kan foreta en reell vurdering av om myndighetene har holdt seg innenfor rammene av gitte tillatelser og menneskerettighetene.

4.3.4 Sammenfatning

Straffeprosessloven med forskrifter må anses å inneholde "adequate and effective guarantees against abuse" i samsvar med kravet i EMK og EMD. Kontrollen foretas av uavhengige organer, med dommere og medlemmer med juridisk kompetanse,[126] og grunnlagsmaterialet de fatter avgjørelser på er etter mitt syn slik at de i størst mulig grad er i samsvar med EMK og kravet om at inngrep ikke må gå ut over det som er "strictly necessary."

På ett punkt må det likevel tas forbehold. Så lenge rettsgrunnlaget i strpl. § 216 o ikke regulerer utøvelsen av overvåkning, vil domstolen ved forhåndskontrollen ha en vanskeligere jobb med å vurdere om inngrepet er i samsvar med kravet til "strict necessity". En lignende problemstilling har ikke vært oppe til avgjørelse i EMD, og det er derfor vanskelig å si med sikkerhet at kravet til prosessuelle sikkerhetsmekanismer av denne grunn ikke skulle være i samsvar med "safeguards"-kravet i EMK. På den ene siden eksisterer det et godt utbygget apparat for kontroll med at politiet har holdt seg innenfor rammen av overvåkningstillatelsene.

---

[125] Årsrapport 2015 fra utvalget for kommunikasjonskontroll, s. 13, og Prop. 68 L (2015-2016) s. 277

[126] Lederen for KK-utvalget må oppfylle de krav som stilles til høyesterettsdommere, se kommunikasjonskontrollforskriften § 13

På den andre siden har domstolene i forkant kanskje ikke et tilfredsstillende grunnlag for å si hvor disse rammene bør gå, og hvilket spillerom politiet har.

Et annet poeng er at domstolskontrollen kan bidra til å avhjelpe skjønnet ved anvendelsen av dataavlesing. Også for etterhåndskontrollen er dette et poeng: Kontrollorganene kan fange opp de tilfellene politiet eventuelt har gått ut over det som var strengt nødvendig. Dersom domstolen både har og tar i bruk en adgang til å sette vilkår for anvendelsen av dataavlesing, vil overvåkningen i større grad kunne rettes inn mot de informasjonsstrømmene som anses strengt nødvendig i en konkret sak, altså i aktuelle tilfeller begrense intensiteten av inngrepet.

4.4 Oppsummering

Gjennomgangen av den innholdsmessige reguleringen i straffeprosessloven og systemet med forhånds- og etterhåndskontroll av politiets utøvelse av regelverket, taler for at dataavlesingsreglene på de langt fleste områder er i samsvar med kravene til "safeguards.". De formelle vilkårene om vesentlig nødvendighet og kvalifisert mistankekrav, og de prosessuelle sikkerhetsmekanismene gjennom domstolenes prøving av dette, bidrar til å sikre at beslutning om overvåkning gjennom dataavlesing bare foretas etter en reell test av inngrepets "strict necessity", og derigjennom begrenser faren for vilkårlig inngripen fra myndighetene. KK-årsrapportene viser også at politiets bruk av kommunikasjonskontroll "gjennomgående er forsvarlig og godt begrunnet."[127]

En gjennomgang av rettskildematerialet kan likevel tyde på at strpl. § 216 o burde regulere nærmere selve utøvelsen av overvåkningen, og at dette utgjør et moment i helhetsvurderingen av lovkravet. Et av hensynene bak lovkravet for statlig overvåkning er å sikre at "The procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society.""[128] Når lovkravet er slik utformet at forhåndskontrollen ved domstolene ikke kan fungere helt tilfredsstillende, bør dette være et moment av en viss vekt. Dette særlig på bakgrunn av kravet om streng nødvendighet mellom inngrep og formål, slik dette kan utledes fra EMD og andre relevante rettskilder. Dersom man konkluderer med at også utøvelsen av overvåkningen er omfattet av det innholdsmessige kravet i lovkravet, og strpl. § 216 o ikke regulerer dette spørsmålet, må dette anses som en svakhet ved reguleringen av dataavlesing.

Vurderingen av om regelverket møter kravet til "adequate and effective guarantees against abuse" beror likevel på en konkret vurdering av en rekke ulike faktorer. Disse inkluderer, som

[127] Årsrapport 2015 s. 4

[128] Szabó and Vissy v. Hungary avsn. 57

referert tidligere, ”the nature, scope and duration of the possible measures”, hvilke vilkår som stilles for bruken, og om det i det hele tatt foreligger prosessuelle sikkerhetsmekanismer.[129] Den relative natur av denne vurderingen tilsier blant annet at dess mer inngripende tiltak, og dess større omfang, jo strengere krav stilles det til øvrige mekanismer i loven.[130]

Det er generelt høy terskel for å anvende dataavlesing, både på bakgrunn av kravet til strafferamme, og de øvrige vilkårene for inngrep, som redegjort for i denne oppgaven. Til dette kommer også kontrollen ved domstolene, som også vil prøve om vilkårene for inngrep foreligger. På den ene siden kan man se dette slik at lovgiver har tatt hensyn til dataavlesingens inngripende ”nature and scope” gjennom å sette strenge vilkår for dataavlesingen og kontrollen med denne, og dermed redusere faren for uforholdsmessige inngrep. I en helhetsvurdering vil disse komponentene i kravet kunne anses for å veie opp for de manglene som eventuelt foreligger ved innholdet i loven.

På den andre siden, tatt i betraktning lovkravets relative karakter, kunne en se for seg at lovreguleringen i større grad skulle reflektere det utvidede overvåknings- og inngrepspotensialet som ligger i dataavlesing sammenlignet med andre former for skjult overvåkning. Gjennom å sette en minste strafferamme på ti år for iverksettelse av dataavlesing, har Departementet lagt seg på samme terskel som ved kommunikasjonsavlytting og skjult ransaking.[131] Også for kommunikasjonskontroll og ransaking gjelder i tillegg vilkårene om at overvåkningen må være av vesentlig betydning, og at etterforskningen ellers i vesentlig grad blir vanskeliggjort.[132] Den generelle forholdsmessighetsregelen i strpl. § 170 a utgjør formelt sett den eneste skjerpende skranken for anvendelsen av dataavlesing.

Departementet trekker frem at dataavlesing åpner opp for mer *målrettet* overvåkning, i aktuelle tilfeller.[133] Dataavlesingens ”nature and scope” behøver derfor ikke alltid være av mer inngripende art enn andre tvangsmidler. Dette er en åpenbar fordel med dataavlesing som metode sammenlignet med for eksempel kommunikasjonsavlytting. Det som er av avgjørende i relasjon til “safeguards”-kravet må likevel være hvorvidt *rettsgrunnlaget* er slik utformet at det i størst mulig grad avverger faren for vilkårlige eller uforholdsmessige inngrep.

Hvis man ser gjennom smale brilleglass er det ikke åpenbart at regelutformingen ikke innebærer at systemet i en viss grad er ”prone to abuse”, slik EMD formulerer det i Szabó and Vissy.

---

[129] Szabó and Vissy v. Hungary avsn. 57

[130] Se også Prop. 68 L (2015-2016) s. 40

[131] Se henholdsvis strpl. §§ 216 a og 200 a

[132] Strpl. §§ 216 c og 200 a annet ledd

[133] Prop. 68 L (2015-2016) s. 265

I en helhetsvurdering fremstår likevel den øvrige regelgjennomføringen og de tilhørende kontrollmekanismene å være i samsvar med kravene i EMK. Særlig domstols- og etterhåndskontrollen synes egnet til å begrense rekkevidden av politiets skjønn ved utøvelsen av dataavlesing. Regelverket i sin helhet synes å møte de minstekrav til "adequate and effective guarantees against abuse" som EMD har oppstilt.

4.5 Avsluttende kommentarer til dataavlesingsreglene

Behovet for dataavlesing har vært utredet en rekke ganger, fra Politimetodeutvalgets NOU 2004: 6 Mellom effektivitet og personvern, av Metodekontrollutvalget i NOU 2009: 15, og sist i Prop. 68 L (2015-2016) som dannet grunnlag for lovvedtakelsen. Metodekontrollutvalget foreslo å ikke innføre dataavlesing som et selvstendig tvangsmiddel, men innføre "dataavlesing" som en metode under de andre, allerede eksisterende hjemlene for skjult overvåkning.[134] En begrunnelse for dette var at de ikke fant påvist et tilstrekkelig behov for en utvidelse utover denne.[135] I Prop. 68 L (2015-2016) ble det foreslått å innføre dataavlesing i den form den har i dag, som et selvstendig tvangsmiddel i straffeprosessloven. Reglene om dataavlesing er i gjeldende form foreslått videreført i den nye straffeprosessloven.[136]

På bakgrunn av konklusjonen under drøftelsen tidligere vil overvåkning gjennom dataavlesing ganske sannsynlig ikke innebære en krenkelse av retten til privatliv etter konvensjonen.[137] Det er etter mitt syn likevel grunnlag for å mene at rettsgrunnlaget kunne vært utformet på en måte som i større grad møter kravet til "strict necessity."

Det er flere måter man kan se for seg at en regelutforming i større grad kan speile nødvendighetskravet. For eksempel innebar Metodekontrollutvalgets forslag at dataavlesing ville bli anvendt mer "målrettet." Etter Metodekontrollutvalgets forslag ville dataavlesing kunne iverksettes med det formål å avlytte kommunikasjon, og på bakgrunn av systematikken i loven bare dersom tradisjonelle metoder for kommunikasjonskontroll kom til kort.[138] Et argument mot dette i proposisjonen var, blant annet, at det er behov for "Effektiv avlytting av kommunikasjon som foregår i former som straffeprosessloven § 216 a ikke gir egnet grunnlag for å kontrollere."[139] Departementet ønsket, og fant påvist et behov for, å utnytte det brede potensialet i dataavlesingsmetoden.[140] En kunne likevel se for seg en mellomløsning mellom

---

134 NOU 2009:15 s. 244

135 NOU 2009:15 s. 244

136 NOU 2016: 24 s. 56 og 341

137 Ref. sammenlignbare regelverk i Kennedy v. The United Kingdom og Weber and Saravia v. Germany

138 NOU 2009: 15 s. 245

139 Prop. 68 L (2015-2016) s. 264

140 Prop. 68 L (2015-2016) s. 261

det "alt eller intet" departementet landet på i Prop. 68 L (2015-2016). For eksempel kunne man følge Metodekontrollutvalgets forslag og lovfeste en anvendelse av dataavlesing for å muliggjøre kommunikasjonsavlytting, hemmelig ransaking og beslag,[141] men også hjemle en bruk av dataavlesing for tilfellene ut over dette. En kan tenke seg at man hermed kunne utnytte det fulle potensialet i dataavlesing, men bare der man fant dette godtgjort etter en vurdering av streng nødvendighet.

En annen løsning, som enklere kunne la seg gjennomføre under dagens regulering av dataavlesing, kunne være å lovfeste i strpl. § 216 o et pålegg for retten til å angi nærmere hvilke informasjonsstrømmer og former for data politiet i en konkret sak får tillatelse til å avlese. Dette vil kunne synliggjøre at dataavlesingen, i tråd med EMK artikkel 8-2, skal anvendes kun i den utstrekning det er strengt nødvendig. En lignende lovregulering finnes i engelsk lov, jamfør Kennedy v. The United Kingdom, hvor det følger av rettsgrunnlaget for anvendelsen av statlig overvåkning ("the Regulation of Investigatory Powers Act") at kjennelsen som tillater overvåkningstiltaket må inneholde en "Description of the communications to be intercepted …"[142] Til dette kommer at dersom domstolene allerede gjør bruk av en adgang til å begrense politiets overvåkning, kunne en lovfesting av dette sikre bedre etterrettelighet med anvendelsen av regelverket.

En alternativ lovregulering i tråd med et av disse forslagene vil kunne speile kravet om "strict necessity" i større grad enn under gjeldende regelverk.

En bemerkning til dataavlesingsreglene, som ikke vedgår lovkravet direkte, er at utformingen av rettsgrunnlaget også kan tenkes å redusere effektiviteten av dataavlesingsreglene. Hvis politiet først får adgang til å iverksette dataavlesing får de tilgang til en informasjonsstrøm av svært stort omfang, og av svært inngripende art. Terskelen for å gi en slik tillatelse må nødvendigvis ligge svært høyt. I omvendt fall kan man risikere at overvåkningstiltaket forløper i strid med det strenge kravet til nødvendighet, slik redegjørelsene i oppgaven kan tyde på. Kripos bekreftet også delvis dette, at dataavlesing vil kunne brukes i ytterst få og svært alvorlige tilfeller av kriminalitet. Gjennom en tilpasning i lovreguleringen kunne en se for seg at dataavlesingsreglene vil kunne få "økt effekt", ettersom terskelen for anvendelsen i aktuelle tilfeller kan tenkes å bli noe lavere.

Inntil videre kunne man se til Grl. § 92 som et mulig pålegg for domstolene til å sørge for at dataavlesingsreglene utøves innenfor rammene av EMK. Høyesterettsdommer Arnfinn Bård-

---

[141] NOU 2009: 15 s. 245-246

[142] Kennedy v. The United Kingdom avsn. 41. Det er her snakk om kommunikasjonsavlytting, ikke avlesing av data

sen skriver i en artikkel i Jussens Venner i januar i år at Grl. § 92 innebærer at "[menneskerettighetene i Grunnloven] normerer domstolenes egen virksomhet; den må naturligvis utøves i tråd med, og innenfor rammene av, Grunnlovens menneskerettsbestemmelser."[143] Etter avgjørelsen i HR-2016-2554-P er det slått fast at bestemmelsen innebærer at domstolene og andre myndigheter er pålagt å håndheve også menneskerettighetene på det nivå de er gjennomført i norsk rett.[144] Med bakgrunn i dette kan man argumentere for at domstolene ikke bare har en generell adgang til, men også er forpliktet til, å sette rammer for utøvelsen av dataavlesingen, i samsvar med retningslinjene fra EMD.

5 Konklusjon

Ser man reglene om dataavlesing opp mot lovkravet i sin helhet, møter disse de grunnleggende komponentene i kravet. Dataavlesing har grunnlag i nasjonal rett, og møter kravet til forutberegnelighet, i den utstrekning dette får anvendelse ved skjulte inngrep.

Hva gjelder de særlige kravene ved statlig overvåkning, vil jeg også her konkludere med at dataavlesingsreglene samlet sett fremstår tilfredsstillende i henhold til kravet i EMK.

Etter en drøftelse av problemstillingen i oppgaven kan man trekke noen slutninger. Man kan nok ikke slå strengt fast at EMD krever at regelverket regulerer nærmere utøvelsen av overvåkningen. Dette må likevel ganske klart utgjøre et moment i en helhetsvurdering av om lovverket er i samsvar med EMK. I lys av den øvrige reguleringen i straffeprosessloven, og kontrollmekanismene for etterlevelsen av denne, er det ikke av avgjørende betydning at strpl. § 216 o ikke gir retningslinjer for utøvelsen av overvåkningen. Flere momenter tilsier likevel at dataavlesingsreglene kunne regulert dette nærmere, for i større grad å sikre borgerne mot myndighetsmisbruk, i tråd med et av de grunnleggende hensynene bak lovkravet for statlig overvåkning.

[143] Bårdsen (2017)

[144] HR-2016-2554-P avsn. 70

Litteraturliste

Litteratur

Aall, Jørgen	*Rettsstat og menneskerettigheter*, 3. utg., 2015
Indreberg, Hilde	"Utfordringer for Høyesterett ved grunnlovfesting av flere menneskerettigheter", I: *Lov Sannhet Rett, Norges Høyesterett 200 år*, Tore Schei, Jens Edvin A. Skøghøy, Toril M. Øie (red.), 2015, s. 393-420
Kjølbro, Jon Fridrik	*Den Europæiske Menneskerettighedskonvention - for praktikere*, 3. udgave, 2010

Artikler

Bruce, Ingvild	"Datalagringsdirektivet og menneskerettighetene – replikk til Jon Wessel-Aas", *Lov og Rett 05/2010 (Volum 49)*, s. 296-298 (sitert fra Idunn.no)
Bårdsen, Arnfinn	"Grunnloven, straffeprosessen og strafferetten – noen linjer i høyesteretts praksis etter grunnlovsreformen 2014", *Jussens Venner 01/2017 (Volum 52)*, s. 1-44 (sitert fra Idunn.no)
Fause, Anett Beatrix Osnes	"Kravet til legalitet, nødvendighet og proporsjonalitet når det utøves polisiær eller påtalemessig myndighet som griper inn i vernet etter EMK art. 8 nr. 1", *Tidsskrift for norsk strafferett 01/2014 (Volum 14)*, s. 46-60 (sitert fra Idunn.no)
Waldron, Jeremy	"The Concept and The Rule of Law," *New York University School of law, Public law & legal theory research paper series, working paper no. 08-50* (november 2008) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1273005)

Lover

Grunnloven	Lov 17. mai 1814 Kongeriket Norges Grunnlov
EOS-kontrolloven	Lov 3. februar 1995 nr. 7 om om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste

EØS-loven	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde
Menneskerettsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
Politiloven	Lov 4. august 1995 nr. 53 om politiet
Politiregisterloven	Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten
Straffeloven	Lov 20. mai 2005 nr. 28 om straff
Straffeprosessloven	Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker

Forskrifter

Kommunikasjonskontrollforskriften	Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing

Forarbeider, proposisjoner og innstillinger

NOU 2004: 6	Mellom effektivitet og personvern
NOU 2009: 15	Skjult informasjon – åpen kontroll
NOU 2016: 24	Ny straffeprosesslov
St.prp. nr. 59 (2003-2004)	Om samtykke til godkjenning av EØS-komiteens beslutninger nr. 79/2003 og nr. 80/2003 av 20. juni 2003 og nr. 11/2004 av 6. februar 2004 om innlemmelse av direktiver på området for elektronisk kommunikasjon
Prop. 68 L (2015-2016)	Endringer i straffeprosessloven mv. (skjulte tvangsmidler)
Dokument 16 (2011–2012)	Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven

Rettsavgjørelser

Norges Høyesterett

Rt. 2000 s. 996

Rt. 2014 s. 1105

Den europeiske menneskerettighetsdomstolen

Amann w. Switzerland	The European Court of Human Rights, Strasbourg, 16. februar 2000 (Grand Chamber)
Gillan and Quinton v. The United Kingdom	The European Court of Human Rights, Strasbourg, 12. januar 2010
Kennedy v. The United Kingdom	The European Court of Human Rights, Strasbourg, 18. mai 2010
Klass and others v. Germany	The European Court of Human Rights, Strasbourg, 6. september 1978
Kruslin v. France	The European Court of Human Rights, Strasbourg, 24. april 1990
Kvasnica v. Slovakia	The European Court of Human Rights, Strasbourg, 9. juni 2009
Liberty and Others v. The United Kingdom	The European Court of Human Rights, Strasbourg, 1. juli 2008
Malone v. The United Kingdom	The European Court of Human Rights, Strasbourg, 26. april 1985
Munjaz v. The United Kingdom	The European Court of Human Rights, Strasbourg, 17. juli 2012
Roman Zakharov v. Russia	The European Court of Human Rights, Strasbourg, 4. desember 2015 (Grand Chamber)
Rotaru v. Romania	The European Court of Human Rights, Strasbourg, 4. mai 2000
Sunday Times v. The United Kingdom (No. 1)	The European Court of Human Rights, Strasbourg, 26. april 1979
Szabó and Vissy v. Hungary	The European Court of Human Rights, Strasbourg, 12. januar 2016
The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria	The European Court of Human Rights, Strasbourg, 28. juni 2009
Weber and Saravia v. Germany	The European Court of Human Rights, Strasbourg, 29. juni 2006

EU-domstolen

C-203/15 and C-698/15 Tele2 and Watson	Joined cases Tele2 Sverige AB (C-203/15) v. Post- och telestyrelsen and Secretary of State of the Home Department (C-698/15) v. Tom Watson, Peter Brice and Geoffrey Lewis, 21. December 2016

Andre internasjonale rettskilder

EMK	The European Convention on Human Rights, Roma 4. november 1950
EU-charteret	Charter of Fundamental Rights of the European Union, 7. desember 2000
EU-direktiv 2002/58	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
SP	International Covenant on Civil and Political Rights, 16. desember 1966
Wien-konvensjonen om traktatretten	Vienna Convention on the Law of Treaties, Wien 23. mai 1969

Rapporter

Kontrollutvalget for kommunikasjonskontroll	*Årsrapport 2015*, Oslo 13. juni 2016 (https://www.regjeringen.no/contentassets/0d8f3410e21f4783b77992a5baa61f1d/kkarsrapport2015pdf.pdf)

Andre kilder

Haugen, Finn	Utvalgsleder, Kontrollutvalget for kommunikasjonskontroll, e-post 9. mars 2017
Sætnan, Knut Jostein	Politiadvokat i Kripos, telefonsamtale 22. mars 2017